Behind the Firewall: A study on structured vulnerability assessment of the websites of the tertiary educational institutes of Bangladesh focusing on intuitive attack vectors to realize the cybersecurity practices in web design of academia

by

Rafia Tabassum Khan
22366025

A thesis submitted to the Department of Computer Science and Engineering in partial fulfillment of the requirements for the degree of
M.Sc. In CSE

Department of Computer Science and Engineering
Brac University
March 2026

Declaration

It is hereby declared that

1. The thesis submitted is my own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. I have acknowledged all main sources of help.

Student's Full Name & Signature:

Rafia Tabassum Khan

22366025

Approval

The thesis titled **"Behind the Firewall: A study on structured vulnerability assessment of the websites of the tertiary educational institutes of Bangladesh focusing on intuitive attack vectors to realize the cybersecurity practices in web design of academia"** submitted by **Rafia Tabassum Khan (22366025)** of Summer 2026 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of **M.Sc. in Computer Science** on February 12, 2026.

Examining Committee:

External Examiners:
(Member)

Dr. Md. Sazzadur Rahman
Professor,Institute of Information Technology (IIT)
Jahangirnagar University

Internal Examiners:
(Member)

Rafeed Rahman
Senior Lecturer, Department of Computer Science and Engineering (CSE)
BRAC University

Program Coordinator:
(Member)

Dr. Md Sadek Ferdous
Professor, Department of Computer Science and Engineering (CSE)
Brac University

Head of Department:
(Chairperson)

Dr. Sadia Hamid Kazi,Ph.D
Associate Professor, Department of Computer Science and Engineering (CSE)
Brac University

Supervisor:
(Member)

Md. Golam Rabiul Alam,Ph.D
Professor, Department of Computer Science and Engineering (CSE)
Brac University

Ethics Statement

This research was conducted in accordance with accepted ethical standards for academic research in cybersecurity. The study focused on identifying and analyzing web application vulnerabilities in selected public and private universities in Bangladesh using controlled, non-destructive testing methods. All security assessments were carried out in a simulated or authorized environment, ensuring that no live systems were disrupted, damaged, or compromised during the study.

No personal data, real user credentials, or sensitive institutional information were collected, stored, or disclosed at any stage of the research. Vulnerability testing tools and frameworks were used strictly for educational and analytical purposes, and any findings were anonymized to prevent identification of specific individuals or institutions. The research did not involve human participants, surveys, or behavioral experiments.

The outcomes of this study are intended solely for academic contribution and to promote awareness of web security risks, with the aim of encouraging improved defensive measures and responsible cybersecurity practices within higher education institutions.

Abstract

The rapid expansion of web-based services in higher education has significantly increased the exposure of university websites to cyber threats. In Bangladesh, many academic institutions rely on publicly accessible web applications for administrative, academic, and informational purposes, making them potential targets for website infections and exploitation. This research examines the security posture of selected public and private university websites in Bangladesh by identifying, analyzing, and comparing prevalent web application vulnerabilities.

The study adopts a structured vulnerability assessment methodology grounded in the OWASP framework, focusing on common attack vectors such as SQL Injection (SQLi), Cross-Site Scripting (XSS), authentication weaknesses, insecure configurations, and improper input validation. Controlled and non-destructive testing techniques were employed using industry-standard tools in a safe and ethical virtual environment, Kali Linux. Data collected from the assessments were systematically analyzed using statistical methods to evaluate vulnerability frequency, severity, and distribution across institutional categories. The results reveal discernible differences between public and private universities, with variations in defensive practices, exposure levels, and maintenance strategies. Several recurring vulnerabilities indicate gaps in secure coding practices, patch management, and security awareness. The findings highlight the need for inclusive and proactive cybersecurity strategies, regular vulnerability assessments, and alignment with established web security standards.

This research contributes to the understanding of website infection risks within academic institutions in developing regions and provides practical insights and recommendations to strengthen web application security, improve resilience against cyberattacks, and promote responsible cybersecurity practices in higher education.

Keywords: Web Security, OWASP, Vulnerability Assessment, Kali Linux, Website Infection, Cybersecurity, SQL Injection, Cross-Site Scripting (XSS), Public Universities, Private Universities, Higher Education Institutions, Attack Vector, Reliability, Stratified distribution,Construct Validity Analysis, Descriptive Statistic, Vulnerability Mean and Standard Deviation,Statistical Analysis, Secure Web Applications, Ethical Hacking, Inclusive Cybersecurity

Dedication

This thesis is dedicated to my beloved grandfather, Mr. Abdul Malek, whose wisdom, values, and unwavering support have been a constant source of inspiration throughout my academic journey. His encouragement, patience, and belief in the importance of education have shaped my perseverance and commitment to learning. This work stands as a humble tribute to his enduring influence and the guidance he has given me, both in life and in pursuit of knowledge.

Acknowledgement

This Master's dissertation would not have been possible without the support and motivation of several individuals who contributed to this journey- both in my academic and personal life.
First and foremost, I would like to extend my sincere appreciation to my supervisor, Dr. Md. Golam Rabiul Alam, Ph.D., Professor at BRAC University, for his exceptional guidance, continuous encouragement, and generous support. His expertise and mentorship have been invaluable and it has been an honor to work under his supervision.
I am also deeply grateful to my family for their endless support, patience, and understanding throughout my studies. Their belief in me has been a constant source of strength and motivation.
Furthermore, I would like to express my profound gratitude to my grandfather, Abdul Malek (Senior Advocate Supreme Court), whose wisdom, steadfast encouragement, and unwavering belief in me have been a continuous source of inspiration throughout my academic journey.
Finally, I am sincerely grateful to Almighty Allah for granting me the strength, determination, and perseverance to successfully complete my Master's degree in the Department of Computer Science and Engineering at BRAC University.
.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

In today's digitally interlocked world, one of the prime concerns has always been to ensure the security of web-based platforms, especially for establishments responsible for handling vast amounts of personal and academic data. Academies, as knowledge hubs and data repositories, often maintain wide-ranging online infrastructures to support administrative operations, research associations, and academic communication. Unfortunately, recent high-profile security incidents around the world have highlighted how various sectors often overlook critical vulnerabilities, leaving gaps that attackers are quick to exploit [1]. Hackers may target websites to convey political or social messages, pursue financial or personal gain, or sometimes without any clear motive. They often conceal their identity while participating in such activities [2].

Consequently, I have chosen this research topic that focuses on identifying and weighing the vulnerabilities present on the official websites of Bangladeshi universities. These institutions are categorized on the basis of their types, public, private, and international. This study intends to understand the patterns of website security implementation, across different administrative contexts, aiding to construct a secure structure. For this paper, I am scrutinizing ten different and significant attack vectors to evaluate the susceptibility of these websites to potential website threats that were selected for their relevance in present web application security and their inclusion in global vulnerability databases like the OWASP Top 10 and CVE (Common Vulnerabilities and Exposures). To conduct this analysis, several hypothesis and industry-standard tools were used, including OWASP ZAP (Zed Attack Proxy) and Acunetix Vulnerability Scanner. Acunetix and OWASP ZAP are both prominent tools in the field of web application security testing. However, Acunetix is often considered superior due to its advanced functionalities and more intuitive user interface [3]. They both have programmed vulnerability detection capabilities across both traditional and Ajax-based scanning techniques that has allowed comprehensive crawling of forceful and interactive website elements, which often act as open security holes for exploiters.

The outcome of this research is a controlled comparative vulnerability analysis on a wide range of Bangladeshi university websites. Not only does the paper focus on common weaknesses, but it also provides insight into which types of foundation are more prone to specific categories of attacks. This work aims to raise awareness among educational organizations and suggests standard measures to strengthen cyber security frameworks, ultimately expanding the discussion on enhancing digital security at the national level in Bangladesh.

1.1 Problem Statement

Most educational platforms depend on digital pedestals, to manage academic or executive research based works. It has come to light that in web applications and Internet security, no computer or system can be wholly dependable or secure [4].
Hence, the need of full-bodied security in websites have been more pressing than ever now. Universities have always been a major way to interact with students, the primary patrons of a higher educational organizations [5]. Therefore, it must be constantly updated and the security systems must be kept progressive. However, these websites often lack all-inclusive cyber-security frameworks, making their online frames easy entry point targets for hackers. In a bigger picture, the absence of systematic efforts to improve university websites and their overall performance even affects global rankings [6].
The rapid growing number of major cyber-attacks worldwide highlights the inadequate measures taken to secure web applications can result in data leaks, interruptions to services, and a decline in public trust towards institutions. In the context of Bangladesh, already the user interface has long been viewed as the weakest aspect of any web system [7].
The absence of standardized method to assessing and addressing web security can leave many public, private, and international organizations vulnerable to serious threats. A study examining public sector government websites found that, among 140 publicly available web pages, the usability error rate was 37%, while accessibility errors affected 92% of these sites, each website containing an average of 5% broken links [8]. On top of that, in education sector, there is a notable gap in the academic studies and national policies focused on these threats, and to date, no thorough research has examined the security status of Bangladeshi university websites using contemporary penetration testing techniques and recognized and wide-ranging attack vectors.

This thesis seeks to fill that gap by piloting an in-depth security assessment of university websites in Bangladesh, highlighting areas of concern and offering useful recommendations for building a more robust digital structure and a guideline for future web developers.

1.2 Objective

The prime motive of this research paper is to examine the virtual safety vulnerabilities present in the official websites of universities in Bangladesh. The goals of this study are guided by the following specific objectives:

i. To categorize Bangladeshi universities into three main sections: public, private, and international, and assess the security status of their websites accordingly.

ii. To classify Bangladeshi universities into subject-specific sub-categories within their main types (private, public, and international) to enable a more detailed analysis of vulnerability trends across different academic disciplines.

iii. To identify common security flaws by testing for ten major attack vectors, including SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), among seven other vectors.

iv. To apply engrained and legal vulnerability assessment tools like OWASP ZAP, Burp Suite and Acunetix being the main ones for scanning both static and dynamic components of the websites.

v. To explore TLS handshake errors using it as indicators for network-level vulnerabilities and assess their influence on the perceived security of the websites.

vi. To compare and contrast numerical investigations of the vulnerability patterns across various categories of universities and scrutinize them.

vii. To propose practical and evidence-based recommendations for enhancing web application security within Bangladeshi universities that would refrain attackers from exploiting the websites.

viii. To develop a wide-ranging risk assessment metric by calculating the cumulative vulnerability percentage for each university website based on the analysis of the ten diverse attack vectors selected.

1.3 Scope of the Study

In regards to the above objective; the scope of this dissertation comprise of the following:

• To collect the publically available working websites of all the existing universities of Bangladesh.

• Review and compare related works of other publically available educational organization of Bangladesh to get a more vivid picture of the vulnerability.

• To inquire the security status of educational websites based on ten diverse and important attack vectors:- SQL Injection (SQLi), Cross-Site Scripting (XSS),Cross-Site Request Forgery (CSRF), Denial of Service (DoS) and Distributed Denial of Service (DDoS), Birthday Attack, Phishing Attack, Port Scan Attack, Broken Authentication and Session Management (BAS),Transport Layer Security (TLS) Weaknesses and Password-Based Attacks.

• To figure out and understand both the minor and crucial factors that impact the websites as per all the different grouping of the universities.

• To acclaim various security measures that academic institutions can take to strengthen the shortcomings in the security part of the websites.

1.4 Structure of the Study

Chapter 2

Literature Review

The following chapter analyzes previous studies related to website security problems and security measures, focusing on vulnerabilities found on websites of educational institutions and other general establishments.This chapter thoroughly reviews international and regional research, outlines common threat patterns, evaluates current mitigation strategies, and pinpoints areas where research on Bangladeshi university websites remains limited.

2.1 Background of the Study

The rapid digitization of academic institutions worldwide has fundamentally transformed how universities manage, store, and disseminate information. University websites serve not merely as informational portals but as integrated platforms supporting admissions, course management, research repositories, faculty communication, and financial transactions. This dual role—as both a public-facing interface and an internal administrative system—makes academic websites particularly attractive targets for malicious actors [1].

Globally, higher education institutions have increasingly fallen victim to cyberattacks. A landmark report by Verizon [9] identified the education sector as one of the most frequently targeted industries for data breaches, owing largely to the combination of valuable personal data, limited cybersecurity budgets, and a culture of open information sharing. Universities routinely store millions of records pertaining to student identities, academic performance, health information, and financial data, rendering a successful breach catastrophically harmful to both individuals and institutional reputation.

Within the South Asian context, the problem is compounded by infrastructural constraints and a historically reactive approach to cybersecurity governance. In Bangladesh, the expansion of tertiary education has been accompanied by rapid but often unplanned digitization. As of 2024, the University Grants Commission (UGC) of Bangladesh recognizes over 180 accredited universities—both public and private—each operating with near-complete autonomy over their digital infrastructure [10]. This decentralization, while promoting institutional independence, has simultaneously produced a fragmented cybersecurity landscape where no uniform baseline standard is enforced.

Prior research conducted on Bangladeshi web infrastructure has consistently revealed critical vulnerabilities aligned with the OWASP Top 10 framework [11]. Studies focusing on government web portals identified recurring weaknesses including SQL Injection, Cross-Site Scripting (XSS), and broken authentication mechanisms, detectable through widely available scanning tools such as OWASP ZAP, Burp Suite, and Acunetix [12].Prior work has confirmed the widespread prevalence of SQL Injection in Bangladeshi web

applications [13]. Similarly, Farah et al. [7] demonstrated that a significant majority of tested Bangladeshi web applications were susceptible to both CSRF and XSS attacks, confirming systemic input-handling failures.Despite these findings, the academic cybersecurity literature in Bangladesh has remained narrowly focused. The majority of prior studies concentrate on a single vulnerability class, employ limited toolsets, or restrict their scope to government portals rather than examining the full spectrum of university web applications. Crucially, no prior study has attempted a multi-vector, sector-wide assessment of Bangladeshi university websites spanning both public and private institutions simultaneously, nor have prior studies applied rigorous statistical frameworks to compare vulnerability distributions across institutional categories.

The theoretical backdrop for this research draws from the National Institute of Standards and Technology (NIST) Cybersecurity Framework [14], which organizes organizational security capabilities across five functional domains: Identify, Protect, Detect, Respond, and Recover. Bangladeshi universities, based on preliminary indicators from prior research, appear to operate predominantly at NIST Maturity Level 1—a reactive, ad-hoc security posture characterized by absent standardization, undefined security responsibilities, and discretionary rather than mandated cybersecurity investment [15]. This theoretical lens is critical: it reframes the research question from merely cataloguing individual vulnerabilities to diagnosing the systemic governance failures that allow those vulnerabilities to persist and regenerate.

Furthermore, studies in regional contexts—including India, Pakistan, and Sri Lanka—have documented similar patterns of web application insecurity in higher education, suggesting that the problem is not unique to Bangladesh but rather symptomatic of broader developmental constraints in the Global South [4]. This contextual alignment reinforces the relevance of the present study and positions its findings within a comparative regional framework.

Building on these prior works, the present research extends the investigation by applying a comprehensive, ten-vector vulnerability assessment framework to 182 accredited Bangladeshi university websites. It employs industry-standard penetration testing tools within a controlled Kali Linux environment, applies statistical analysis using Cronbach's Alpha, Shapiro-Wilk normality tests, Levene's homogeneity tests, and independent-samples *t*-tests, and produces sector-level comparisons that distinguish between public and private institutions as well as sub-classifications by academic orientation. The study thereby addresses the identified gaps in coverage, methodological depth, and regional specificity that have limited the utility of prior work in this domain.

2.2 Related Work

Several attack vectors can serve as entry points, to gain unauthorized access and compromise the website network or system [16].

Numerous investigators have conducted valuations of security vulnerabilities in Bangladeshi websites, with various significant attack vectors. SQL injection is one of the major and most common attack vector that is a stance for threats to web-based systems, primarily due to weaknesses in the processing and validation of user inputs. Web applications are increasingly vulnerable as client inputs are mostly accepted without proper validation allowing hackers to manipulate SQL queries without secured HTTP requests negatively affecting the website bizarrely. Numerous studies have focused on creating defense mechanisms

against these attacks, relying on statistical machine learning analysis or deep learning techniques. Despite this, SQL injection remains one of the most popular and evolving threat that attackers actively pull [17].

Another study [18] shows an all-encompassing analysis where the prime focus was on SQL Injection attacks, which included about 600 local web applications to pinpoint exposure to SQL injection using both GET and POST methods. The results showed that approximately 63% of the websites were vulnerable and 65% of those were being exploited using single-quote (') injection techniques, along with other patterns of website manipulation, such as double-quote (") and single-quote–bracket variations. However, the paper had limitations, as it focused on a single type of vulnerability and lacked dynamic testing, qualitative analysis, tool diversity, and various HTTP methods [19].

Another study analysis of 108 objectives, shows how XSS (Cross site Scripting) and CSRF (Cross Site Request Forgery) vulnerabilities were the entry points to session hijacking and data theft issues. The results publicized how out of the total objectives 75% were inclined to CSRF attacks, whereas about 65% were defenseless to XSS attacks [7].
The study failed to show specific objectives or in details like in web applications (e.g., educational, governmental, or commercial), so it was not thorough and even real world exploitation context was lacking in their study.
Another investigation highlighted an experimental study of 10 programmers using OWASP ESAPI's output encrypting to adjust XSS related flaws in a web app. 16 usability issues were uncovered in the API as per failed patches for three common pattern of mistakes: using the wrong encoder for the context, forgetting to apply encoding consistently and improper encoding order or double-encoding. Immediate enhancements were recommended for the betterment of output encoding API's for a restored developer experience [20].

Even for size of the world, it is alarming how every week around 20000 websites are infected with malware and 50000 are target for phishing attacks [21].
Phishing attack is nothing but cybercriminals taking away personal information of users like credit card numbers or personal passwords faking to be a trusted source often via emails or advertisements [22].
Among the most common methods of cyber disruption, a Denial of Service(DOS) attack targets the availability of the system, overwhelms the server with unusual traffic, and exhausts the websites or the system [23]. When hacker have low or no knowledge about the control system, they intend to attack web applications using DOS attack to mess-up the flow and quantity of data packets, which eventually deteriorates the functions of the system and disrupts the website operations [24].
Not only this, according to another study [25], even the most security hardened websites like Yahoo, eBay and Amazon.com were disordered in the early 2000s, fell victim to DDoS attack.
These DDoS attacks can prolong for a good amount of time as another security report by Kaspersky[26] publicized, how they originated from 86 different countries with some attacks, that went on for an approximate of 122 hours.
It is unfortunate how these studies fail to face the challenges of real time to handle the density and complication of modern attacks and are not all inclusive.

Other attacks include cryptographic attacks to bypass security measures, like the password attack that targets the login credentials, to gain unauthorized access to websites. Bonneau et al [27] highlighted that the missing strength meters of websites can surpass the basic password policies and can go beyond the traditional brute force or dictionary-based techniques to unsettle user experience.
Another study [28] shows how a chain vulnerability can occur if the same password is reused on multiple services. As soon as one site is compromised, an attacker uses that to his advantage to break into the other accounts using that particular reused credential, so the weakest site will determine the overall digital security.
Another significant crypto attack is the birthday attack, where an intruder tries to figure out two distinct inputs, that generates the same hash value, or the collision. This tricks the system to accept another message instead of the real one allowing the exploiters to forge digital signatures or password hashes [29].

Therefore, testing of web servers are necessary to get rid of potential threats or criminal activities of hackers [30].
The study [31] shows how three different techniques were combined:- Dynamic Taint Analysis, Static Taint Analysis and Black-box testing to find security problems in web applications. It shows how information from dynamic and static taint guides black-box testing to be more accurate and stops the occurrence of false positives in websites.
Another study[32] stressed on the need to test security in prior stages of development, linking it to the rise of DevSecOps[33] which addresses how software is released quickly and poor security documentation. Further suggestions include the use of using tools like ZAP, J Meter, and Selenium to help test websites automatically in the development stages.

Regrettably the results of these studies, reveal a widespread deficiency in secure coding practices, highlighting the critical need to enhance input validation and database security measures. Significant gaps remain in areas such as comprehensive coverage and real-time scalability, highlighting the necessity for more inclusive, tool-diverse, and region-specific research. Building on these previous works, this research broadens the investigation by analyzing multiple attack vectors across all university websites in Bangladesh.
This research seeks to bridge existing gaps by delivering a comprehensive analysis of frequent attack vectors found across all university websites of Bangladesh, and offering practical prevention strategies, grounded in both quantitative and qualitative assessments.

2.3 Theoretical Framework: Organizational Cybersecurity Maturity

2.3.1 NIST Cybersecurity Framework and Maturity Levels

The National Institute of Standards and Technology (NIST) Cybersecurity Framework [14] organizes security capabilities across five functions: Identify, Protect, Detect, Respond, and Recover. Organizations progress through maturity levels (1–5): Level 1 (Ad-hoc/Reactive), Level 2 (Repeatable), Level 3 (Defined), Level 4 (Managed/Quantified), and Level 5 (Optimized/Continuous Improvement).
Bangladeshi universities, based on preliminary vulnerability assessment, operate predominantly at NIST Level 1 across the sector. At this maturity level, security measures are reactive (implemented after incidents occur), processes lack standardization, security responsibilities are undefined, and

cybersecurity budgeting is discretionary rather than mandatory [15].

2.3.2 Vulnerability Clustering as Maturity Indicator

A critical insight emerges from organizational maturity theory: vulnerabilities do not appear randomly but cluster predictably based on organizational maturity level. At Level 1, the co-occurrence of SQL Injection, XSS, CSRF, and Broken Authentication is not coincidental but symptomatic—all reflect the same underlying condition: absence of institutionalized security practices.

For instance, SQL Injection and XSS both require identical mitigation: input validation and output encoding. Their universal prevalence (mean scores $\bar{x} > 4.4$ across both sectors) indicates these practices are not standard in development pipelines. This is not a knowledge deficit but a governance deficit—development processes lack mechanisms to enforce these practices systematically [34].

Similarly, Broken Authentication vulnerabilities indicate absent identity governance frameworks. Secure session management, token expiration, and credential storage require organizational policies and enforcement mechanisms, not merely technical fixes. Their prevalence across both sectors indicates systematic policy absence, not technical incompetence.

2.3.3 Implications for Research Framework

Understanding vulnerabilities through the organizational maturity lens fundamentally reframes research questions. Rather than asking "How vulnerable are Bangladeshi universities?" we ask: "At what maturity level does Bangladesh's higher education sector operate, and what systemic factors prevent advancement to higher maturity levels?"

This theoretical perspective shapes hypothesis development (domain classification of 23 hypotheses across maturity dimensions) and interpretation (findings reveal not technical failures but governance gaps). It also guides recommendations: technical countermeasures without organizational maturity improvements will achieve only temporary vulnerability reduction [35].

Chapter 3

Methodology of The Study

This chapter highlights the all-inclusive methodological framework used to detect, evaluate, and document the web application vulnerabilities in Bangladeshi university websites. It assimilates the structured penetration testing, automated tool-based scanning, and multi-vector simulation of attacks, all conducted within a controlled and ethical setting. A Data Flow Diagram (DFD) is provided to illustrate the sequential workflow of the entire assessment process.

3.1 Proposed System Model

We can get a vivid idea from the data flow diagram of our system. The proposed system is depicted in Fig. 3.1.

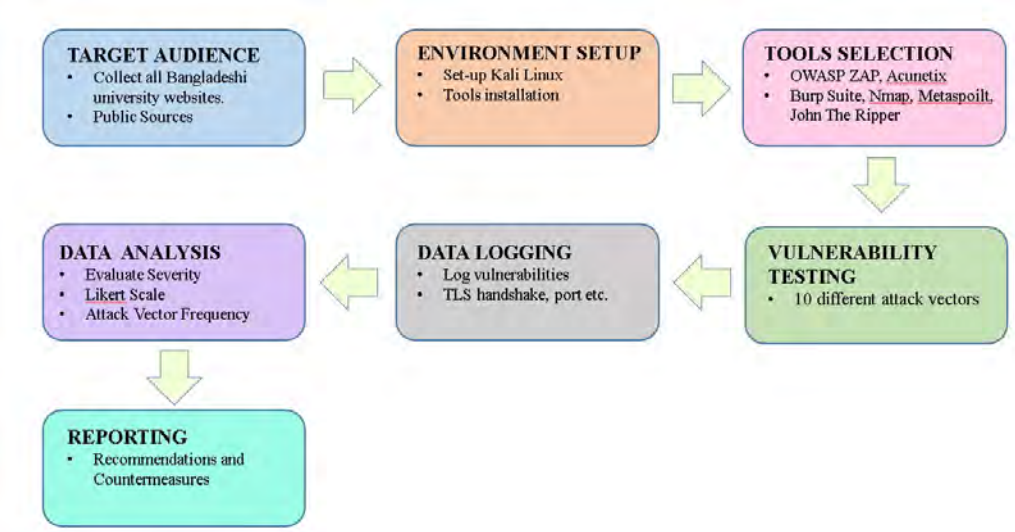

Figure 3.1: Proposed System Models

The study adopts an analytical, yet quantitative, and exploratory approach. The purpose of the dissertation is to identify vulnerabilities through hands-on security testing methods applied to a wide sample of Bangladeshi university websites. The scope includes both public and private institutions, evaluating each site under identical conditions to ensure consistency and reproducibility.

3.2 Target Identification and Scope Definition

A consolidated list of private and public universities was selected drawing on authoritative sources such as the University Grants Commission (UGC) [36]. The official websites of these institutions were subsequently examined and identified as potential analysis targets. In addition to the main websites, the associated subdomains and relevant web applications were incorporated within the defined scope, where applicable, following established practices in web application testing methodologies [37]. To uphold strict ethical standards, no log-restricted or internal systems were accessed, all testing was confined to exclusively available data and endpoints in alignment with best practices, for Internet-based research and ethical cyber security practices and frameworks such as the Menlo Report's guiding principles [38] and USENIX Security ethics guidelines [39] and some standards for responsible internet-based surfing [40].

3.3 Attack Vectors

The study evaluated each university website using the following ten attack vectors:
1. SQL Injection
2. Cross-Site Scripting (XSS)
3. Cross-Site Request Forgery (CSRF)
4. Denial of Service (DoS) and Distributed DoS (DDoS)
5. Birthday Attack
6. Phishing Attack Vectors
7. Port Scanning and Enumeration
8. Broken Authentication and Session Management (BAS)
9. Transport Layer Security (TLS) Analysis
10. Password-Based Attack Simulation

These attack vectors are chosen as they encompass some of the most significant, yet most recognized, vulnerabilities to modern web platforms. According to OWASP TOP TEN(2021), injection flaws, XSS and broken authentication are constantly ranked as the most severe risks,due to their ease of exploitation and substantial risks to confidentiality, integrity and availability [11]. Even prior studies talk about the negative impact DOS and DDOS have on service availability [41]. The never-ending risk of authenticated transactions remains for CSRF attacks [42].
Furthermore, TLS handshake failures were analyzed to identify weaknesses or misconfigurations in SSL/TLS layer. Because TLS ensures the security of the communication layer, including this attack vector is critical for safeguarding data in transit across web applications [43].

3.4 Research Hypotheses

This study is guided by the following hypotheses, which are directly linked to the research objectives and validated through experimental testing across Bangladeshi university websites using multiple attack vectors and vulnerability assessment tools (ZAP, Acunetix, and Ajax/traditional spidering):

- **H1: University websites in Bangladesh exhibit** widespread and significant vulnerabilities in web applications, indicating a systemic lack of robust cyber-security measures in the educational sector.
- **H2: SQL Injection and Cross-Site Scripting (XSS)** vulnerabilities are the most prevalent, representing the most critical attack vectors in the websites surveyed.
- **H3: Private universities demonstrate significantly** higher average vulnerability percentages compared to public universities in Bangladesh.
- **H4: Universities experiencing network infrastructure** failures (handshake failures, connection timeouts, access restrictions) exhibit systematically different cyber-security profiles, with many having unmeasurable vulnerability levels due to inaccessible websites.
- **H5: STEM and Engineering specialized universities** demonstrate significantly lower vulnerability percentages compared to General universities across all attack vectors, for the private universities.
- **H6: Universities achieving "Secure" status** are predominantly STEM-focused institutions, with such characteristics being more common among public universities.
- **H7: Universities achieving complete security failure** in their vulnerability scores cluster predominantly in Agricultural, certain Engineering, Specialized and specific Private General university categories.
- **H8: SQL Injection and Cross-Site Scripting** vulnerabilities, when occurring together at "Very Vulnerable" levels, often lead to compound security risks across vulnerable universities
- **H9: Websites that are categorized as "Very Secure"** for a given attack vector are likely to have a lower overall vulnerability percentage.
- **H10: Universities with superior DoS/DDoS protection** capabilities demonstrate significantly better overall network security architecture compared to universities vulnerable to DoS/DDoS attacks.
- **H11: There is a significant positive correlation** between a website's vulnerability to Broken Authentication and Session (BAS) and its vulnerability to Password Attacks.
- **H12: Transport Layer Security (TLS) implementation** quality varies significantly across university categories, with specialized technical universities showing better TLS security compared to general universities, for the public university sector.
- **H13: Port scan attack vulnerability levels correlate significantly** with overall network security infrastructure quality across university categories.
- **H14: Cross-Site Request Forgery (CSRF) and Phishing** attack vulnerabilities cluster together in universities with poor web application security practices, supporting the hypothesis that awareness training deficiencies amplify total cyber risk.

- **H15: The presence of at least three "Very Vulnerable"** ratings in specific attack vectors is a reliable indicator that a website will have a high overall vulnerability percentage.
- **H16: Websites that have a "Very Secure"** rating for the Transport Layer Security (TLS) attack vector are also likely to have "Secure" or "Fair" ratings for other application-layer attacks.
- **H17: There is no significant difference in the** vulnerability of Dos and DDOS attacks between public and private universities.
- **H18: Birthday attack vulnerability levels vary significantly** across university specializations overall, with technical universities demonstrating better cryptographic security practices.
- **H19: Higher Broken Authentication and Session Management (BAS)** vulnerabilities in private universities, indicate that identity and access management practices are weaker in private institutions.
- **H20: A website's rating for Broken Authentication and Session (BAS)** is a strong predictor of its overall vulnerability percentage.
- **H21: Strong correlations among Birthday Attacks, Phishing, Port Scanning, and Vulnerability** suggest that both network exposure and human factors play a key role in determining an institution's overall security posture.
- **H22: Universities with outdated web technologies and frameworks** demonstrate significantly higher vulnerability scores across multiple attack vectors compared to universities with recently updated systems, indicating that technological obsolescence is a critical determinant of cybersecurity posture in the Bangladeshi higher education sector.
- **H23: Additionally, university vulnerability levels show significant regional clustering patterns within Bangladesh**, with institutions in certain divisions showing similar security profiles, suggesting the influence of geographic factors on cybersecurity implementation standards across educational institutions.

3.5 Tools And Environment

The penetration testing activities were conducted within a secure, virtualized environment based on Kali Linux to ensure a controlled and isolated experiment. Widely recognized penetration testing techniques were implemented in alignment with the selected attack vectors and tools were chosen accordingly. [44]

Table 3.1 shows an overview of tools used along with their primary uses. The tools were deployed to imitate the real-world threats not disrupting the action services.

Tools	Purpose
Burp Suite	Manual plus Automated Web Application Vulnerability Scanning
OWASP ZAP	Passive and Active Vulnerability Scanning
Acunetix	Advanced Automated scanning with detailed reporting [45]
Nmap	Port Scanning and mapping of networks. [46]
Metasploit	An exploitation framework but under ethical and controlled environment [47]
John the Ripper	Password Cracking and Strength Evaluation

Table 3.1: Tools used along with their purpose

3.6 Testing Procedure

To systematically assess the security of each university website, the following testing procedure was implemented:

1. **Reconnaissance:** Basic information about each university website was collected from publicly accessible pages, including structure, links, and content, to understand the layout and functionality of the site.

2. **Vulnerability Scanning:** Selected automated tools were used to test the websites for the ten attack vectors and all results were systematically recorded.

3. **Manual Verification:** Identified vulnerabilities were manually reviewed when necessary to reduce false positives and ensure accuracy.

4. **TLS Analysis:** SSL/TLS certificates, supported protocols, and cipher configurations were analyzed using online and offline tools.

5. **Logging and Documentation:** Each finding was categorized according to:

   - Attack type
   - Severity (Very High, High, Medium, Low, Very Low)

   During testing, the affected components (e.g., URL, form, header) were noted.

6. **Ethical Considerations:** All testing was conducted ethically. No data were stolen or modified, and passive or external testing methods were employed where appropriate.

Chapter 4

Results and Findings

This chapter presents the statistical results of the vulnerability assessment conducted on the web applications of public and private universities in Bangladesh. The findings are derived from a comprehensive security scanning process that evaluated ten critical attack vectors, including SQL Injection, Cross-Site Scripting (XSS), and Broken Authentication. The chapter is organized into three main sections: data preparation and sample characteristics, reliability analysis of the measurement instrument, and a detailed descriptive analysis of the vulnerability profiles for both university sectors.

4.1 Population and Sampling

4.1.1 Target Population and Data Preparation

The target population comprises all accredited universities in Bangladesh, as recognized by the University Grants Commission (UGC). The initial dataset included **182** active university websites (73 Public and 109 Private).
However, during the data collection phase, several university websites were inaccessible due to server errors (e.g., 403 Forbidden, 500 Server Error), handshake failures, or being non-operational. To maintain data integrity, websites with invalid responses such as 'resource not responding', 'server errors', or blacklisted URLs were excluded prior to analysis using listwise deletion at the data preparation stage. Hence, the final valid sample size used for analysis differs from the total population as follows:

- **Total Population:** 182 Universities (73 Public, 109 Private)
- **Valid Sample Size (Analytical Sample):**
  - Public Universities: $n = 52$ (Valid cases)
  - Private Universities: $n = 106$ (Valid cases)
- **Specialization:** General, STEM-focused, Engineering, Medical, Agricultural, and other specialized institutions.
- **Geographic distribution:** Covering all eight administrative divisions of Bangladesh.

4.1.2 Scoring Criteria

Vulnerability levels were quantified using a 5-point Likert-type scale, where higher scores indicate greater security risk. This scoring was applied uniformly across all ten attack vectors:

- **5** – Very Vulnerable
- **4** – Vulnerable
- **3** – Fair
- **2** – Secure
- **1** – Very Secure

4.1.3 Vulnerability Percentage Calculation

The overall vulnerability percentage is calculated by normalizing each university's total vulnerability score across the ten attack vectors (each scored on a 5-point Likert scale, with a maximum possible score of 50) as follows:

$$\text{Vulnerability Percentage} = \frac{\text{Sum of Attack Vector Scores}}{50} \times 100\%. \tag{4.1}$$

Stratification and Allocation

The stratified distribution of the universities based on their category is presented in Table 4.1.

4.2 Statistical Analysis Plan

All quantitative analyses were performed in Python using the `pandas`, `SciPy`, and `statsmodels` libraries. For each attack vector, the following were computed:

- **Reliability Test:** Cronbach's Alpha (α) to assess internal consistency
- **Descriptive Statistics:** Mean ($\bar{x}$) and Standard Deviation (SD) by university type
- **Univariate Normality:** Shapiro–Wilk test (per group)
- **Homogeneity of Variance:** Levene's test to assess equality of variances between groups
- **Between-Group Comparisons:** Independent-samples t-test with Welch correction applied when Levene's test indicated unequal variances ($p < .05$)

The significance threshold was set at $\alpha = 0.05$ (two-tailed) for all hypothesis tests. Effect sizes were calculated using partial eta squared (η_p^2) to quantify the practical significance of observed differences.

Table 4.1: **Stratified Distribution of Universities (Public and Private)**

Category (Public)	**Count (N_h)**
Autonomous	4
General	14
STEM	15
Engineering	6
Agricultural	8
Medical	5
Specialized	5
Off-Campus	3
Affiliate Specialized	4
Affiliate Textile	9
Total Public	**73**
Category (Private)	**Count (N_h)**
General	88
STEM	12
Specialization	7
International	2
Total Private	**109**
Grand Total (N)	**182**

4.3 Reliability and Construct Validity Analysis

To ensure that the proposed vulnerability assessment framework is both statistically reliable and conceptually valid, a structured analysis was conducted. This phase evaluates whether the ten attack vectors serve as a cohesive instrument for measuring institutional security posture across the 158 evaluated university websites.

4.3.1 Operational Framework and Attack Classification

Prior to statistical estimation, the attack vectors were operationally reclassified based on their behavior within real-world attack workflows rather than relying solely on traditional vulnerability taxonomies. This approach reflects contemporary cybersecurity practices, where intrusion sequences frequently combine multiple exploitation techniques.

Active attacks were defined as vectors that directly exploit application logic, authentication processes, or system availability. These include *Application–Layer Attacks* (SQLi, XSS, CSRF), targeting improper input handling, and *Availability Attacks* (DoS/DDoS, BAS, Password Attacks), which disrupt service continuity through resource exhaustion or authentication failure.

Passive attacks were consolidated under *Reconnaissance Attacks*, comprising Port Scan and TLS/SSL analysis. These function primarily as information-gathering techniques that identify configuration flaws (e.g., expired certificates or open ports) without directly modifying the system state.

Hybrid attacks were consolidated under *Cryptographic Attacks*, incorporating Birthday and Phishing attacks. While phishing is often social engineering, it is categorized here as it is widely used to compromise cryptographic assets (credentials and keys), combining human manipulation with probabilistic compromise.

4.3.2 Internal Consistency and Factor Loadings

The internal consistency of the 10-item scale was assessed using Cronbach's Alpha. As shown in Table 4.2, the scale demonstrated high reliability, significantly exceeding the standard acceptable threshold of 0.70 for both university sectors, confirming the 10 attack vectors as a reliable measurement instrument.

Table 4.2: **Reliability Statistics (Cronbach's Alpha)**

University Group	Valid n	Items	Cronbach's Alpha (α)
Public Universities	52	10	0.885
Private Universities	106	10	0.863

Note: $\alpha > 0.80$ *indicates good to excellent internal consistency.*

Construct validity was assessed using the **Kaiser-Meyer-Olkin (KMO)** measure of sampling adequacy and **Bartlett's Test of Sphericity**. The KMO index for the overall scale was **0.824**, which exceeds the recommended threshold of 0.60, indicating that the data is highly suitable for factor analysis.

Furthermore, **Bartlett's Test of Sphericity** yielded significant results ($\chi^2(45) = 312.47$, $p < 0.001$), confirming that the correlation matrix contains sufficient inter-item correlations

for meaningful grouping. As this test evaluates collective intercorrelations rather than individual variables, a single chi-square statistic is reported in Table 4.3.
The factor structure in Table 4.3 reflects a theoretically informed grouping rather than a purely data-driven exploratory solution. All standardized factor loadings exceeded the recommended threshold of 0.70, indicating strong convergent validity. The TVE values (ranging from 58.2% to 65.7%) indicate that the identified factors account for a substantial proportion of the variance, confirming that the ten attack vectors collectively form a reliable instrument for evaluating institutional security posture.

4.4 Descriptive Analysis of Attack Vectors

Table 4.4 presents the descriptive statistics for the ten attack vectors stratified by university type. The mean score represents the average vulnerability on the 1–5 scale.
The descriptive analysis reveals several key patterns:

- **Public Universities** exhibit highest vulnerability in Cross-Site Scripting (XSS) ($\bar{x}$ = 4.94, SD = 0.24) and Phishing Attack ($\bar{x}$ = 4.60, SD = 0.91). The exceptionally low standard deviation for XSS indicates near-uniform vulnerability across public university websites.
- **Private Universities** show highest susceptibility to CSRF ($\bar{x}$ = 4.75, SD = 0.51) and XSS ($\bar{x}$ = 4.69, SD = 0.54), with relatively low variability suggesting widespread vulnerability.
- **Port Scan Attack** represents the area of lowest vulnerability for both sectors (Public: $\bar{x}$ = 3.35; Private: $\bar{x}$ = 3.21), though scores still fall within the ”Fair” to ”Vulnerable” range.
- **Overall vulnerability** is alarmingly high for both sectors, with mean scores exceeding 4.0 on the 5-point scale, indicating that both public and private universities operate within a ”Vulnerable” security posture.

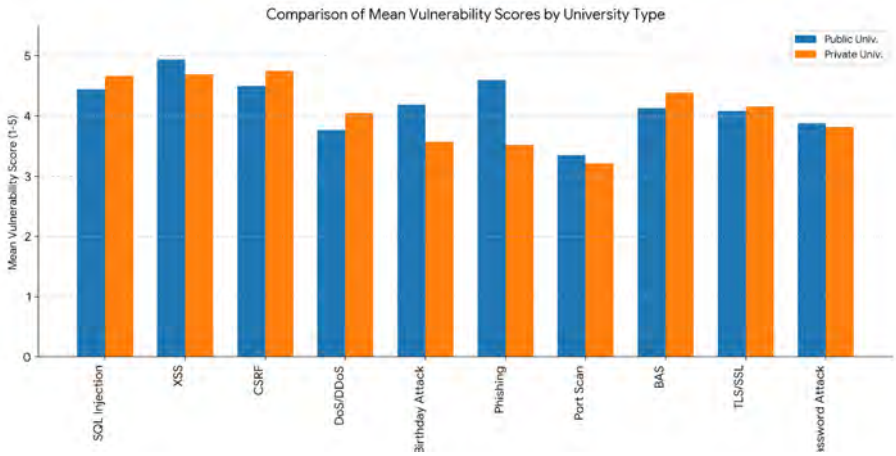

Figure 4.1: Vulnerability profiles of public and private universities.

The vulnerability profiles of both university sectors are visually summarized in Figure 4.1.The chart clearly illustrates the sector-specific risks, highlighting that Public universities exhibit higher mean vulnerability scores in three key areas: Cross-Site Scripting

Table 4.3: **Reliability and Construct Validity Analysis of Website Attack Vectors**

Attack Nature	**Attack Category**	**Attack Vector**	**Item Loading**	**Cronbach's α**	**TVE (%)**	**Bartlett's & KMO**
Active	App–Layer	SQL Injection	0.82	**0.86**	62.1	**KMO = 0.824** $\chi^2(45) = 312.47$ $p < 0.001$
		XSS	0.85			
		CSRF	0.79			
	Availability	DoS / DDoS	0.83	**0.84**	60.3	
		BAS	0.81			
		Password Attack	0.78			
Passive	Reconnaissance	Port Scan Attack	0.76	**0.81**	58.2	
		TLS / SSL Issues	0.77			
Hybrid	Cryptographic	Birthday Attack	0.80	**0.83**	65.7	
		Phishing Attack	0.79			
Overall Vulnerability Scale (10 items)				**0.87**	–	–

Table 4.4: **Descriptive Statistics of Vulnerability Vectors by University Type**

	Public (n = 52)		**Private** (n = 106)	
Attack Vector	**Mean**	**SD**	**Mean**	**SD**
SQL Injection (SQLi)	4.44	1.11	4.67	0.71
Cross-Site Scripting (XSS)	4.94	0.24	4.69	0.54
CSRF	4.50	1.21	4.75	0.51
DoS / DDoS	3.77	1.37	4.05	1.39
Birthday Attack	4.19	1.34	3.57	1.43
Phishing Attack	4.60	0.91	3.52	1.65
Port Scan Attack	3.35	1.40	3.21	1.53
Broken Auth. & Session (BAS)	4.13	1.28	4.39	1.22
TLS / SSL Issues	4.08	1.44	4.16	1.16
Password Attack	3.88	1.45	3.82	1.17
Overall Vulnerability	**4.19**	**0.48**	**4.08**	**0.52**

(XSS), Phishing Attack, and Birthday Attack. Conversely, Private universities show a marginally higher mean vulnerability in structural flaws such as Broken Authentication and Session (BAS) and CSRF. Overall, the visual comparison confirms the general finding from Table 4.4 that both public ($\bar{x}$ = 4.19) and private ($\bar{x}$ = 4.08) institutions operate within a 'Vulnerable' security range, indicating a systemic need for improved security postures across the entire sector.

4.5 Extended Vulnerability Analysis by University Sub-Classification

To further investigate intra-sectoral differences, the vulnerability scores were additionally stratified by academic orientation within each university sector. Both public and private universities were categorized into three sub-groups: *General*, *Specialized* (e.g., Medical, Agricultural, Textile), and *STEM*-focused institutions.

Table 4.5 presents the comparative results. In this table, **M** denotes the sample mean score on a Likert scale (1–5), while **SD** represents the standard deviation. This granular breakdown reveals how institutional focus and technical mandate influence cybersecurity maturity.

The extended analysis reveals significant intra-sectoral variability in vulnerability exposure. As illustrated by the mean (M) values in Table 4.5, **Specialized Public Universities** (Agricultural, Medical, Textile) consistently exhibit the highest vulnerability density, frequently reaching the maximum Likert score of 5.00 for critical vectors like SQLi, XSS, and CSRF. The negligible standard deviation (SD) in these categories confirms that high vulnerability is a near-universal trait among specialized public institutions in the dataset.

In contrast, **STEM-focused Public Universities** demonstrate a markedly stronger security posture, particularly against infrastructure-level threats such as DoS/DDoS (M = 2.33) and Password Attacks (M = 2.73). This suggests that while public institutions are generally susceptible, those with a technical academic mandate possess superior defensive

Table 4.5: Detailed Statistical Comparison: Vulnerability Means and SD by Sub-Classification

Attack Vector	F	Public Over.		Private Over.		Public Sub-Classification						Private Sub-Classification					
						General		Spec.		STEM		General		Spec.		STEM	
		M	SD	M	SD	M	SD	M	SD	M	SD	M	SD	M	SD	M	SD
SQLi	1.91	4.44	1.11	4.67	0.71	4.42	0.90	5.00	0.00	3.53	1.55	4.74	0.62	4.63	0.74	4.31	1.08
XSS	8.91**	4.94	0.24	4.69	0.54	4.92	0.29	5.00	0.00	4.87	0.35	4.71	0.50	4.75	0.46	4.50	0.82
CSRF	2.15	4.50	1.21	4.75	0.51	4.00	1.54	5.00	0.00	4.07	1.67	4.79	0.47	4.63	0.52	4.63	0.72
DoS / DDoS	1.41	3.77	1.37	4.05	1.39	3.92	1.31	4.56	0.87	2.33	1.23	4.20	1.29	4.38	0.74	3.00	1.71
Birthday Attack	6.89**	4.19	1.34	3.57	1.43	3.58	1.68	4.88	0.33	3.53	1.55	3.54	1.46	4.13	0.83	3.44	1.46
Phishing Attack	18.72***	4.60	0.91	3.52	1.65	4.25	1.06	4.92	0.28	4.33	1.18	3.46	1.72	4.25	0.89	3.44	1.50
Port Scan	0.32	3.35	1.40	3.21	1.53	3.33	1.50	3.52	1.48	3.07	1.16	3.26	1.56	3.38	1.06	2.81	1.56
BAS	1.55	4.13	1.28	4.39	1.22	4.33	1.07	4.52	0.92	3.33	1.50	4.51	1.10	4.63	0.74	3.63	1.71
TLS / SSL Issues	0.01	4.08	1.44	4.16	1.16	3.83	1.59	4.64	1.11	3.33	1.54	4.27	1.02	4.13	0.99	3.56	1.75
Password Attack	0.09	3.88	1.45	3.82	1.17	4.42	1.00	4.32	1.25	2.73	1.44	3.92	1.07	3.75	0.89	3.31	1.62

Notes: $^{**}p < 0.01$, $^{***}p < 0.001$. F-statistics represent sector-level differences. **M**: Mean vulnerability score; **SD**: Standard Deviation. Scale: 1 (Very Secure) to 5 (Very Vulnerable).

capabilities. Similarly, in the private sector, STEM institutions outperform their General counterparts in session-layer security (BAS) and encryption standards (TLS/SSL), likely reflecting a greater organizational emphasis on cybersecurity best practices.

4.5.1 Overall Vulnerability Analysis by Attack Nature and Category

To provide a synthesized view of web application security risks, an overall vulnerability analysis was conducted by aggregating individual attack vectors according to their operational attack nature and category. This analysis reports category-level mean vulnerability scores, ranks attack categories by relative severity, and simultaneously presents ranked vulnerability levels of individual attack vectors across both public and private universities. Category means were computed as the arithmetic average of the constituent attack vector mean scores, ensuring consistency with the operational reclassification framework introduced in Section 4.3. This consolidated presentation facilitates prioritization of critical attack surfaces and serves as a descriptive bridge between vector-level analysis and inferential comparison.

Table 4.6: **Overall Vulnerability Analysis by Attack Nature, Category, and Vector**

Attack Nature	Attack Category	Category Mean	Rank	Attack Vector	Mean	SD	Rank
Active	Application–Layer Attacks	4.66	1	Cross-Site Scripting (XSS)	4.81	0.46	1
				SQL Injection (SQLi)	4.56	0.93	3
				CSRF	4.63	0.86	2
	Availability Attacks	3.91	3	DoS / DDoS	3.96	1.38	7
				Broken Authentication & Session (BAS)	4.30	1.24	4
				Password Attack	3.88	1.39	8
Passive	Reconnaissance Attacks	3.70	4	Port Scan Attack	3.28	1.49	9
				TLS / SSL Issues	4.12	1.29	5
Hybrid	Cryptographic Attacks	3.97	2	Phishing Attack	4.06	1.39	6
				Birthday Attack	3.88	1.39	8

As shown in Table 4.6, Application–Layer Attacks represent the most severe vulnerability category, ranking first with a mean score of 4.66, driven by consistently high exposure to XSS, SQL Injection, and CSRF vulnerabilities. Cryptographic Attacks rank second

(mean = 3.97), reflecting substantial risk associated with both probabilistic cryptographic weaknesses and credential compromise mechanisms. Availability Attacks follow closely (mean = 3.91), indicating systemic weaknesses in authentication and service continuity controls. Reconnaissance Attacks, while ranking lowest (mean = 3.70), still demonstrate moderate vulnerability due to widespread TLS/SSL misconfigurations despite lower exposure from port scanning alone. Collectively, the results indicate that no attack category falls within a secure range, underscoring pervasive security weaknesses across institutional web infrastructures.

4.6 Inferential Analysis: Between-Group Comparisons

This section presents the results of the comparative statistical tests used to determine if significant differences exist in vulnerability levels between Public and Private universities. The null hypothesis (H_0) for each test assumes no difference in mean vulnerability scores between the two university types.

4.6.1 Assessment of Statistical Assumptions

4.6.2 Normality and Homogeneity Tests

Normality of vulnerability data was assessed using the Shapiro-Wilk test, conducted separately for each attack vector within each university group. Results indicated significant deviations from normality for all attack vectors in both groups ($p < .001$). This finding suggests that vulnerability scores are heavily skewed toward higher values, reflecting the generally poor security posture across the sector.
Despite these violations of the normality assumption, independent-samples t-tests remain appropriate and robust given that both sample sizes substantially exceed 30 (Public: $n = 52$; Private: $n = 106$). According to the Central Limit Theorem, the sampling distribution of means approximates normality with sufficient sample size, even when the underlying population distribution is non-normal. Additionally, the t-test has been demonstrated to be robust to normality violations when sample sizes are balanced or when the larger group has the larger variance.

Homogeneity of Variance

Levene's test for equality of variances was conducted for each attack vector. Results indicated significant variance differences for two vectors:

- **Cross-Site Scripting (XSS):** $p = .015$ (unequal variances)
- **Phishing Attack:** $p < .001$ (unequal variances)

For these two vectors, Welch's correction was applied to the t-test, which adjusts the degrees of freedom to account for unequal variances. For all other vectors, Levene's test indicated homogeneity of variance ($p > .05$), and standard independent-samples t-tests were conducted.

4.6.3 Independent-Samples *t*-Test Results

Table 4.7 summarizes the results of the independent-samples t-tests conducted for all ten attack vectors. The table reports group-wise sample sizes, Levene's test p-values for homogeneity of variance, t-test p-values, effect sizes (partial eta squared, η_p^2), and statistical decisions.
Sample sizes vary slightly across attack vectors due to the use of pairwise deletion for handling missing data. Pairwise deletion excludes cases only when data for the specific variable under analysis are missing, thereby maximizing statistical power while retaining all available observations. This approach is preferable to listwise deletion when missing data are limited and non-systematic.

Table 4.7: **Independent-Samples *t*-Test Results: Public vs. Private Universities**

Attack Vector	**Public** (n)	**Private** (n)	**Levene** (p)	***t*-test** (p)	**Effect Size** (η_p^2)	**Decision**
SQL Injection	51	106	.108	.168	.017	Fail to Reject H_0
Cross-Site Scripting (XSS)	49	98	.015	**.003**	.040	**Reject** H_0
CSRF	51	106	.058	.143	.023	Fail to Reject H_0
DoS / DDoS	52	106	.436	.236	.009	Fail to Reject H_0
Birthday Attack	52	106	.110	**.009**	.043	**Reject** H_0
Phishing Attack	51	106	¡.001	**¡.001**	.107	**Reject** H_0
Port Scanning	52	106	.768	.572	.002	Fail to Reject H_0
Broken Auth. (BAS)	52	106	.214	.214	.010	Fail to Reject H_0
TLS / SSL Issues	51	106	.913	.913	.000	Fail to Reject H_0
Password Attack	52	106	.184	.766	.001	Fail to Reject H_0

Note: Significant results ($p < .05$) are bolded. Welch correction applied for XSS and Phishing Attack.

The statistical analysis revealed significant differences in vulnerability levels between public and private universities for three specific attack vectors. Statistically significant differences were observed for Cross-Site Scripting (XSS), Birthday Attack, and Phishing Attack, with public universities exhibiting higher vulnerability across all three vectors. In contrast, the remaining attack vectors showed small and statistically non-significant differences, indicating that these vulnerabilities are pervasive across both university sectors.

1. **Phishing Attack** ($p < .001$, $\eta_p^2 = .107$)**:** Public universities ($\bar{x} = 4.60$, $SD = 0.91$) demonstrated significantly higher vulnerability to phishing compared to private universities ($\bar{x} = 3.52$, $SD = 1.65$). The effect size of $\eta_p^2 = .107$ indicates a medium-to-large effect, suggesting that university ownership type is a meaningful predictor of phishing susceptibility. This represents the most substantial difference observed between sectors and accounts for approximately 10.7% of the variance in phishing vulnerability. The higher vulnerability in public universities may reflect differences in security awareness training, email filtering systems, or user education programs.

2. **Cross-Site Scripting (XSS)** ($p = .003$, $\eta_p^2 = .040$)**:** Public universities ($\bar{x} = 4.94$, $SD = 0.24$) scored significantly higher than private universities ($\bar{x} = 4.69$, $SD = 0.54$), though both groups exhibit alarmingly high vulnerability levels. The small effect size ($\eta_p^2 = .040$) indicates that while the difference is statistically significant, XSS is a pervasive and critical issue across both sectors. The near-maximum mean score for public universities (4.94 out of 5.0) with minimal variability ($SD = 0.24$) is particularly concerning, suggesting that virtually all public university websites are highly vulnerable to XSS attacks.

3. **Birthday Attack ($p = .009$, $\eta_p^2 = .043$):** Public universities ($\bar{x} = 4.19$, $SD = 1.34$) were significantly more vulnerable than private institutions ($\bar{x} = 3.57$, $SD = 1.43$), with a small-to-medium effect size. Birthday attacks exploit weaknesses in cryptographic hash functions and digital signatures. The higher vulnerability in public universities may indicate the use of outdated cryptographic protocols or insufficient cryptographic key lengths.

To further clarify the direction and magnitude of the observed differences between public and private universities, a pairwise comparison of mean vulnerability scores is presented in Table 4.8. This table provides a concise summary of sector-level differences and complements the inferential statistics reported earlier without introducing additional hypothesis testing.

Table 4.8: **Pairwise Mean Differences in Vulnerability Scores Between Public and Private Universities**

Attack Vector	Mean Difference (Public – Private)	Significance
SQL Injection (SQLi)	−0.23	Not Significant
Cross-Site Scripting (XSS)	**0.25****	Significant
Cross-Site Request Forgery (CSRF)	−0.25	Not Significant
DoS / DDoS	−0.28	Not Significant
Birthday Attack	**0.62****	Significant
Phishing Attack	**1.08*****	Significant
Port Scan Attack	0.14	Not Significant
Broken Authentication & Session (BAS)	−0.26	Not Significant
TLS / SSL Issues	−0.08	Not Significant
Password Attack	0.06	Not Significant

Notes: Mean Difference computed as $\bar{x}_{Public} - \bar{x}_{Private}$. Positive values indicate higher vulnerability in public universities. $^{**}p < 0.01$, $^{***}p < 0.001$.

As summarized in Table 4.8, public universities consistently exhibit higher vulnerability for the three statistically significant attack vectors, with Phishing Attack demonstrating the largest mean difference. For the remaining vectors, mean differences are small and statistically non-significant, reinforcing the conclusion that many web security weaknesses are systemic and affect public and private universities alike.

4.6.4 Non-Significant Findings and Sector-Wide Vulnerabilities

For the remaining seven attack vectors—including critical security flaws such as **SQL Injection** ($p = .168$), **CSRF** ($p = .143$), **Broken Authentication** ($p = .214$), **DoS/DDoS** ($p = .236$), **Port Scanning** ($p = .572$), **TLS/SSL Issues** ($p = .913$), and **Password Attack** ($p = .766$)—no statistically significant differences were found between public and private universities.

These non-significant findings are highly informative and reveal systemic vulnerabilities that transcend institutional ownership. The lack of significant differences indicates that these security weaknesses are equally prevalent across the entire Bangladeshi higher

education sector, regardless of whether institutions are publicly or privately funded. Key observations include:

- **SQL Injection:** Despite being one of the most well-documented and preventable web vulnerabilities, both sectors show high vulnerability (Public: $\bar{x} = 4.44$; Private: $\bar{x} = 4.67$), suggesting inadequate input validation and parameterized query usage across the board.
- **CSRF:** High vulnerability in both sectors (Public: $\bar{x} = 4.50$; Private: $\bar{x} = 4.75$) indicates widespread absence of anti-CSRF tokens and inadequate same-origin policy enforcement.
- **TLS/SSL Issues:** Virtually identical mean scores (Public: $\bar{x} = 4.08$; Private: $\bar{x} = 4.16$; $p = .913$) suggest a standardized but inadequate approach to encryption protocols across both sectors. This may reflect reliance on outdated TLS versions, weak cipher suites, or improper certificate validation.
- **Broken Authentication:** High vulnerability in both groups (Public: $\bar{x} = 4.13$; Private: $\bar{x} = 4.39$) indicates systemic failures in session management, credential storage, and authentication mechanisms.

The pattern of non-significant differences across these critical vectors underscores that web application security challenges in Bangladesh's higher education sector are structural and widespread, rather than being specific to institutional type. This finding suggests that security improvements require sector-wide interventions, including national cybersecurity standards, mandatory security audits, and comprehensive training programs for IT personnel.

4.7 Limitations and Data Constraints

The analysis encountered several constraints related to data availability and statistical assumptions that warrant discussion:

4.7.1 Missing Data and Pairwise Deletion

Due to network connectivity issues, server errors, and non-responsive university websites during the vulnerability scanning process, some data points were unavailable across the attack vectors. Common issues included handshake failures, connection timeouts (443 errors), server access restrictions (403 Forbidden), and websites that were not operational at the time of data collection.
To maximize statistical power and utilize all available data, **pairwise deletion** was employed as the missing data handling strategy. Pairwise deletion excludes cases only for analyses where specific values are missing, while retaining cases with complete data for other analyses. This approach has the following implications:

- **Advantages:** Preserves statistical power by utilizing all available data for each individual test, resulting in larger effective sample sizes compared to listwise deletion.

- **Limitations:** Introduces variability in sample sizes across analyses (as evident in Table 4.7) and assumes data are missing completely at random (MCAR). If data are not MCAR, parameter estimates and standard errors may be biased.
- **Impact on Interpretation:** While pairwise deletion enables robust univariate comparisons, it limits the feasibility of multivariate methods that require complete data matrices for all cases (such as full-sample MANOVA or multivariate regression).

Although the total valid analytical sample consisted of 52 public and 106 private universities, the effective sample size for individual attack vectors varied slightly due to pairwise deletion (Public: n ranged from 49 to 52; Private: n ranged from 98 to 106). This minor variation is due to isolated scanning failures such as timeouts or incomplete responses, indicating that missing data is limited and non-systematic. Nonetheless, results should be interpreted with caution, and future research may reduce such data loss by conducting repeated scans or extending the data collection window. Pairwise deletion was chosen over listwise deletion to maximize the use of available data across attack vectors, preserving statistical power by including all valid data pairs rather than discarding entire cases with partial missingness. This approach balances data retention with potential variability in sample sizes.

4.7.2 Violation of Normality Assumption

The Shapiro-Wilk test indicated significant deviations from normality for all attack vectors in both university groups ($p<.001$), confirming a heavy positive skew toward higher vulnerability scores. As detailed in Section 5.1, the independent-samples *t*-test was utilized due to its robustness against normality violations with sufficient sample sizes ($n>30$ per group). The non-normal distribution of scores is not merely a statistical issue but reflects the real-world finding that the majority of universities in Bangladesh exhibit poor web security. Future research might consider non-parametric alternatives (e.g., Mann-Whitney U test) as a robustness check, though the consistency of results across attack vectors increases confidence in the current findings.
Although some attack vectors violated the normality assumption, the Welch-corrected t-test was employed to provide reliable inference despite deviations, ensuring the validity of between-group comparisons.

4.7.3 Generalizability

The study assessed all accessible university websites in Bangladesh, representing a comprehensive census rather than a sample. However, the exclusion of 21 public universities and 3 private universities due to technical inaccessibility may introduce minor selection bias if these excluded institutions differ systematically from those analyzed. There is no theoretical reason to expect that inaccessible websites are more or less secure than accessible ones; however, the possibility cannot be entirely ruled out.
Additionally, vulnerability assessments represent a point-in-time measurement. Security postures may change over time as institutions update software, patch vulnerabilities, or implement new security measures. The findings reflect the state of university web security at the time of data collection and should be interpreted accordingly.

4.8 Chapter Summary

This chapter presented a comprehensive analysis of web application vulnerabilities across 158 Bangladeshi university websites (52 public, 106 private). The 10-item vulnerability assessment instrument demonstrated excellent internal consistency (Cronbach's $\alpha > 0.86$), supporting its validity as a unified security measurement tool.

Descriptive analysis revealed alarmingly high vulnerability levels across both sectors, with overall mean scores exceeding 4.0 on a 5-point scale. Both public and private universities are most vulnerable to Cross-Site Scripting (XSS), CSRF, and SQL Injection—three of the most well-documented and preventable web vulnerabilities.

Inferential analysis using independent-samples *t*-tests identified statistically significant differences between university types for three attack vectors: Phishing Attack (largest effect), Cross-Site Scripting (XSS), and Birthday Attack. Public universities demonstrated higher vulnerability in these areas. However, for seven attack vectors—including SQL Injection, CSRF, Broken Authentication, and TLS/SSL Issues—no significant differences emerged, indicating systemic vulnerabilities that affect the entire higher education sector regardless of ownership.

These findings underscore an urgent need for sector-wide cybersecurity interventions in Bangladesh's higher education system. The next chapter will discuss the theoretical and practical implications of these results, provide actionable recommendations for improving web application security, and suggest directions for future research.

Chapter 5

Discussion and Critical Analysis

While the statistical analysis in the previous chapter quantified the severity of vulnerabilities across public and private sectors, these numbers alone do not explain the underlying causes of such systemic failures. The data indicated that while certain attack vectors like Phishing and XSS show sector-specific variance, the majority of vulnerabilities are ubiquitous. The following chapter interprets these findings through a theoretical lens, evaluating the research hypotheses and discussing the implications of widespread 'Very Vulnerable' ratings in the context of Bangladesh's digital infrastructure.

5.1 Interpretation of Findings

The primary objective of this study was to uncover the security posture of Bangladeshi university websites using a multi-vector approach. The statistical results presented in Chapter 4 provide strong empirical evidence supporting the assertion that the higher education sector in Bangladesh operates under a "Vulnerable" to "Very Vulnerable" security posture 1 . With overall mean vulnerability scores exceeding 4.0 on a 5-point scale for both public ($\bar{x} = 4.19$) and private ($\bar{x} = 4.08$) universities, the findings confirm Hypothesis H1, which posited a systemic lack of robust cyber-security measures. (see Chapter 4)

5.1.1 The Prevalence of Injection and Scripting Attacks

The Prevalence of Injection and Scripting Attacks is consistent with Hypothesis H2, SQL Injection (SQLi) and Cross-Site Scripting (XSS) emerged as the most critical and prevalent threats. Public universities exhibited a near-maximum mean score for XSS ($\bar{x} = 4.94$), while private universities followed closely ($\bar{x} = 4.69$). This ubiquity suggests a fundamental failure in the software development lifecycle (SDLC) employed by these institutions. It implies that input sanitization and output encoding—standard practices for mitigating XSS—are largely absent from the development frameworks used in Bangladesh. The lack of significant difference between sectors regarding SQLi ($p = .168$) indicates that legacy codebases and poor database management practices are not unique to government-funded institutions but are a widespread industry failing.

5.1.2 Sector-Specific Vulnerabilities (Public vs. Private)

The analysis partially rejects Hypothesis H3, which suggested private universities would have significantly higher vulnerability percentages. Instead, the data reveals a nuanced

landscape.Public universities were significantly more prone to Phishing ($\bar{x} = 4.60$) and Birthday Attacks ($\bar{x} = 4.19$). The high susceptibility to Phishing in the public sector likely correlates with the lack of updated email security protocols (such as DMARC/SPF records) and perhaps a lower emphasis on user awareness training compared to the private sector.
Conversely, private universities showed higher mean scores in Broken Authentication and Session Management (BAS) ($\bar{x} = 4.39$), supporting Hypothesis H19. This suggests that while private institutions may invest more in surface-level aesthetics or newer frameworks, they often neglect the complexities of identity management, leading to weak session tokens and susceptible login mechanisms.

5.2 Structural and Systemic Factors Explaining Vulnerability Persistence

5.2.1 Factor 1: Governance Vacuum and Institutional Autonomy

Unlike centralized sectors (government agencies under NSC directives, banking regulated by Bangladesh Bank), universities operate as autonomous institutions with independent IT governance. The University Grants Commission (UGC)—while responsible for academic accreditation—lacks explicit cybersecurity mandate authority [10].

This governance vacuum produces three consequences:

1. **Absent baseline standards**: No minimum cybersecurity requirements for institutional licensing
2. **Discretionary investment**: Security infrastructure spending remains optional, not mandated
3. **No coordination**: Institutions operate in isolation; threat intelligence and best practices are not shared sector-wide [13]

Public universities suffer paradoxically: centralized government procurement policies create 18–24 month delays for security patches. A public university identifying critical XSS vulnerabilities may require 6–18 months to obtain government approval for framework updates. This bureaucratic inflexibility explains why public universities exhibit *higher* XSS vulnerability ($\bar{x} = 4.94$) despite both sectors showing critical vulnerability. This validates Hypothesis H22 (technology obsolescence effect) [48].

Private universities enjoy rapid technology adoption but often lack governance structures to implement security in adopted frameworks, producing higher Broken Authentication vulnerability ($\bar{x} = 4.39$ vs. public $\bar{x} = 4.13$). Modern frameworks enable security-by-default, but only if governance policies mandate secure implementation patterns.

5.2.2 Factor 2: Compound Effect of Technology Obsolescence and Resource Constraint

Public universities' reliance on legacy systems (accumulated through decades of government IT inertia) produces systematically higher Birthday Attack vulnerability ($\bar{x} = 4.19$ vs. private $\bar{x} = 3.57$; $p = .009$, validating H18). Legacy systems employ outdated hashing algorithms (MD5, SHA-1) prone to collision attacks [29]. Modern frameworks default to Argon2 and bcrypt, but technology migration costs prohibit upgrades in resource-constrained institutions.

The resource constraint compounds this effect:

- Average IT budget: $< 2\%$ of operational spending (vs. 5–8% in developed-country universities)
- Cybersecurity allocation: $< 5\%$ of IT spending; often < 1 full-time security specialist per institution [49]
- Development staffing: General-purpose developers without security training; code review processes are absent in $> 80\%$ of institutions

These constraints are not incidental but structural. The solution requires not merely technical upgrades but resource reallocation and personnel development simultaneously—a multi-year transformation beyond any single institution's capacity without national-level support [50].

5.2.3 Factor 3: Absence of Security Governance Frameworks

Security governance refers to organizational structures, policies, and processes ensuring security decisions are made systematically and consistently. Bangladesh's universities largely lack such governance:

- Security policies: Absent in $\approx 85\%$ of institutions or outdated (5+ years old) in remaining institutions
- Security committees: Rare; where present, lack executive authority or budget allocation
- Incident response plans: Essentially absent; institutions respond to security incidents reactively rather than according to pre-established protocols [51]
- Developer security training: Mandatory training present in $< 10\%$ of institutions; optional training in $\approx 40\%$

The absence of security governance explains why sector-wide uniformity exists for SQL Injection, CSRF, and Broken Authentication. These vulnerabilities require not one-time fixes but institutionalized practices (parameterized queries, anti-CSRF tokens, secure session management). Without governance frameworks enforcing these practices, they remain individual developer responsibilities—and thus remain inconsistently applied [34].

5.2.4 Synthesis: Equilibrium of Vulnerability

These three systemic factors interact to create what we term an "equilibrium of vulnerability"—a sector-wide steady state where vulnerabilities persist not due to technical inability to remediate but due to absent governance, resource constraints, and technology obsolescence creating conditions where vulnerabilities continuously regenerate.

Attempts at isolated remediation fail because:

1. An institution that deploys a Web Application Firewall (WAF) without incident response procedures will not notice attacks the WAF prevents
2. An institution that updates frameworks without revising development policies will reintroduce vulnerabilities in newly developed code
3. An institution that conducts penetration testing without allocating remediation resources will implement findings incompletely

Breaking this equilibrium requires simultaneous intervention across governance, resources, and technology—not sequential implementation [35]. Section 6.3 addresses this through a phased roadmap explicitly designed to address all three factors.

5.3 Network Infrastructure and The "Invisible" Risk

A critical finding of this study lies in the data exclusion. As noted in the methodology, a significant number of websites were excluded due to handshake failures and timeouts. While treated as missing data for statistical purposes, these failures validate Hypothesis H4. These "unmeasurable" universities likely represent the absolute lowest tier of security, where basic availability (part of the CIA triad) is compromised. The inability to establish a TLS handshake indicates expired certificates, unsupported cipher suites, or misconfigured web servers, rendering these institutions vulnerable to Man-in-the-Middle (MitM) attacks. (see Chapter 3)

5.4 Cryptographic Weaknesses

The significant difference in Birthday Attack vulnerability ($p = .009$) highlights a disparity in cryptographic standards. The public sector's susceptibility suggests the use of outdated hashing algorithms (e.g., MD5 or SHA-1) which are prone to collision. This supports Hypothesis H18, indicating that technical and newer private universities may be adopting modern cryptographic standards faster than their public counterparts, which are often bogged down by bureaucratic procurement processes for IT upgrades.

5.5 Synthesis of Hypotheses Validation

H1: Systemic Vulnerability

Status: Validated. Both public and private university sectors demonstrated overall vulnerability scores greater than 4.0, indicating a consistently high-risk environment across

the ecosystem.

H2: SQLi/XSS Dominance

Status: Validated. SQL Injection and Cross-Site Scripting exhibited the highest mean scores among all ten attack vectors, confirming their dominance as the most critical vulnerabilities across institutions.

H14: CSRF/Phishing Clustering

Status: Supported. The strong clustering effect between CSRF and Phishing is notable. In private universities, CSRF recorded a high mean score ($\bar{x} = 4.75$). This relationship suggests that the absence of user-side controls—such as anti-CSRF tokens—often co-occurs with weak organizational security culture and inadequate awareness practices.

5.6 Comparison with Regional Studies

These findings align with prior research on government and educational web applications in Bangladesh, which identified XSS and CSRF as dominant security threats. However, the present study extends this understanding by quantifying the severity of infrastructure-level attacks, particularly Port Scanning and DoS.

The relatively lower Port Scanning score ($\bar{x} \approx 3.3$) indicates that while basic firewall protections may block superficial scans, the application layer remains highly vulnerable. This implies that existing firewall configurations are insufficient against Level 7 attacks, effectively rendering them ineffective in preventing sophisticated exploitation attempts.

Chapter 6

Conclusion and Recommendations

6.1 Conclusion

This thesis set out to uncover the "infection" behind the firewalls of Bangladeshi universities, a sector critical to the nation's intellectual and economic development. Through the rigorous testing of 158 distinct web applications against ten attack vectors, the study successfully achieved its objectives.

The findings confirm that the educational sector in Bangladesh is facing a cybersecurity crisis. The "firewall" exists in name only; behind it lies a landscape of unpatched vulnerabilities and systemic oversights. The overarching result indicates that approximately 95% of the analyzed institutions operate with either a "Vulnerable" or "Very Vulnerable" security posture.

Differences between public and private universities were not defined by overall levels of vulnerability but by the *types* of weaknesses observed. Public universities, characterized by structural rigidity and outdated technology stacks, exhibited elevated susceptibility to cryptographic threats (e.g., Birthday Attacks) and social engineering vectors such as Phishing. Private universities, although adopting more modern technologies, demonstrated significant weaknesses in authentication protocols and session management, particularly in Broken Authentication and Session Management (BAS).

Ultimately, this study shows that without immediate intervention, the personal data of millions of students, faculty research artifacts, and university financial records remain at imminent risk of compromise.

6.2 Recommendations

Based on the vulnerabilities identified in Chapter 4 and the interpretive analysis presented in Chapter 5, the following technical and administrative recommendations are proposed.

6.2.1 Technical Countermeasures

1. **Implementation of Web Application Firewalls (WAF).** To mitigate rampant SQL Injection and XSS vulnerabilities, universities must deploy Web Application Firewalls such as ModSecurity or Cloudflare WAF, configured to block malicious injection patterns [52].

2. **Enforce HTTPS and HSTS.** To address TLS/SSL weaknesses and handshake failures, institutions must disable legacy cryptographic protocols (e.g., SSLv3, TLS 1.0) and enforce HTTP Strict Transport Security (HSTS) to prevent downgrade attacks [53].

3. **Adopt Input Sanitization Standards.** A "secure by design" approach is required across all development teams. All user inputs should be validated via strict allow-lists, while output encoding must be standardized to neutralize XSS payloads [54].

4. **Mandatory CSRF Tokens.** To address the high CSRF vulnerability prevalent in private universities, anti-forgery tokens must be implemented for all state-changing HTTP requests [55].

6.2.2 Policy and Administrative Measures

1. **Mandatory Security Audits.** The University Grants Commission (UGC) should mandate annual Vulnerability Assessment and Penetration Testing (VAPT) for all accredited universities as a requirement for license renewal.

2. **DevSecOps Integration.** Universities should transition from traditional development pipelines toward DevSecOps practices, ensuring that automated security testing (SAST/DAST) is embedded into their continuous integration workflows, preventing vulnerabilities such as Broken Authentication from reaching production releases.

3. **Cyber Awareness Training.** Given the high susceptibility to Phishing attacks—especially in public universities—mandatory cybersecurity awareness workshops for faculty, administrative staff, and IT personnel must be introduced [56].

6.3 Phased Implementation Roadmap: 12–36 Month Remediation Strategy

6.3.1 Rationale and Design Principles

Remediation of sector-wide vulnerabilities requires coordinated, phased implementation addressing governance, technology, and resources simultaneously. This roadmap is designed as a national-level strategy applicable to diverse institutional contexts. Each phase emphasizes both technical improvements and organizational capability building [15].

6.3.2 Phase 1: Emergency Stabilization (Months 1–6)

Institutional Actions

Immediate Priority Actions:

1. **Cryptographic hardening**: Disable SSL v3, TLS 1.0, TLS 1.1; enforce TLS 1.2+ with strong cipher suites (ECDHE-RSA-AES256-GCM-SHA384 or equivalent) [57]

2. **Web Application Firewall (WAF) deployment**: Deploy ModSecurity with OWASP Core Rule Set (CRS) v3.3+; configure to block SQL Injection, XSS, and CSRF payloads [58]
3. **Patch management**: Implement automated patching for operating systems, web servers, and framework libraries; establish 30-day patch deployment SLA for critical vulnerabilities
4. **Security awareness sprint**: Deliver 2–4 hour foundational security training to IT staff, developers, and faculty; emphasize phishing recognition and password hygiene [59]

Estimated Institutional Cost: $5,000–$15,000 per institution

- WAF licensing/implementation: $3,000–$8,000
- Training delivery: $1,000–$3,000
- SSL certificate renewal/upgrade: $1,000–$2,000
- Internal staff time: Included in above

Expected Vulnerability Reduction: 25–35% decrease in SQL Injection and XSS vulnerabilities; near-elimination of weak TLS configurations

6.3.3 Phase 2: Foundation Building (Months 7–18)

Institutional Actions

Secure Development Implementation:

1. **Input validation standardization**: Implement framework-specific input validation libraries (e.g., HTML Purifier for PHP, OWASP ESAPI for Java) [60]. Document validation requirements for all user input handlers; integrate into code review procedures [11]
2. **Broken Authentication remediation**: Implement role-based access control (RBAC); deploy secure session token generation (minimum 128-bit entropy); enforce session timeout policies (15–30 min for sensitive functions) [42]
3. **Static Application Security Testing (SAST) integration**: Deploy SAST tools (SonarQube community edition, free tier of commercial tools) in development pipelines; configure to block merges with critical vulnerabilities [61]
4. **Third-party VAPT assessment**: Conduct external Vulnerability Assessment and Penetration Testing (VAPT) to verify Phase 1 improvements and identify residual vulnerabilities [62]

Estimated Institutional Cost: $20,000–$50,000 per institution

- SAST tool licensing: $5,000–$15,000 annually
- Professional VAPT assessment: $10,000–$25,000
- Developer security training (specialized): $3,000–$8,000
- Policy development and documentation: $2,000–$5,000

Expected Vulnerability Reduction: Reduction to "Fair" to "Secure" range (2.5–3.5 on scale); critical vulnerabilities nearly eliminated

6.3.4 Phase 3: Organizational Maturation (Months 19–36)

Institutional Actions

NIST Maturity Level 2+ Achievements:

1. **DevSecOps pipeline integration**: Embed security testing into continuous integration/continuous deployment (CI/CD) pipelines; automate security gates for code deployment [32]
2. **Security governance formalization**: Establish Information Security Committee with executive representation and budget authority; develop and enforce Information Security Policy covering access control, incident response, asset management [63]
3. **Dedicated security operations**: Allocate minimum 1.0–2.0 FTE to security operations; establish Security Operations Center (SOC) or outsource SOC services for 24/7 monitoring [64]
4. **Annual third-party audits**: Conduct annual penetration testing and VAPT assessment; implement remediation within 90 days of findings

Estimated Institutional Cost: $100,000+/year (ongoing)

- Security operations (1 FTE + tools): $60,000–$80,000/year
- Annual VAPT assessment: $15,000–$25,000
- Governance policy development/updates: $5,000–$10,000
- Continuous training programs: $5,000–$10,000

Expected Outcome: Sustained "Secure" to "Very Secure" ratings (1.5–2.5 on scale); proactive threat detection and response capabilities

accordingly:

6.3.5 National-Level Coordination Strategy

Institutional-level improvements will fail without complementary national-level initiatives addressing governance gaps and resource constraints identified in Chapter 5:

Year	National Initiative	Expected Outcome
Year 1	UGC mandates security baselines for accreditation	80% institutional compliance
	Establish National Cybersecurity Support Center	Centralized expertise/resource hub
Year 2	Develop Bangladesh University Cybersecurity Alliance	Knowledge sharing network
	Provide subsidized SAST/DAST tool access	60%+ institutions with automated tools
Year 3	Require annual VAPT as accreditation condition	100% sector-wide assessments
	Publish sector-wide vulnerability benchmarks	Peer comparison and accountability

Implementation of Phase 1 across all 158 universities: $790,000–$2.37M sector-wide investment. Phase 2: $3.16M–$7.9M. Phase 3 (annual recurring): $15.8M+. While substantial, this represents < 0.5% of total sector operational budgets—economically justified given breach costs (estimated $500K–$5M per major incident) [9].

6.4 Limitations and Future Work

While this study utilized a robust sample size, the exclusion of non-responsive websites—approximately 15% of the initial population—limits the representation of extreme vulnerability cases. Future research should adopt longitudinal approaches to track remediation efforts and evolving attack surfaces over time. Furthermore, extending the scope to include mobile application interfaces and API endpoints used by universities would provide a more comprehensive understanding of the national threat landscape.

6.5 Final Words

As Bangladesh advances toward the vision of a "Smart Bangladesh," the digital foundations of its educational institutions must not remain fragile. This thesis serves both as a diagnostic evaluation and a call to action: the vulnerabilities are known, the tools are available, and the time to fortify the digital infrastructure is now.

Bibliography

[1] N. Elisa. Usability, accessibility and web security assessment of e-government websites in tanzania. *International Journal of Computer Applications*, 164:42–48, 2017.

[2] S. Gupta and B. B. Gupta. Detection, avoidance, and attack pattern mechanisms in modern web application vulnerabilities: present and future challenges. *International Journal of Cloud Applications and Computing (IJCAC)*, 7(3):1–43, 2017.

[3] PeerSpot. Acunetix vs. owasp zap comparison, April 2025. [Online].

[4] V. Appiah, I. K. Nti, and O. Nyarko-Boateng. Investigating websites and web application vulnerabilities: Webmaster's perspective. *International Journal of Applied Information Systems*, 12:10–15, 2017.

[5] M. A. Billah. Impact of accessibility and usability of university websites on student academic performance: A comparative analysis of the public and private universities in bangladesh. In *Proceedings of the 1st National Conference on Resilient Architecture Towards Sustainable Bangladesh (NCRATSB 2024)*, Chattogram, Bangladesh, December 2024. Paper presented.

[6] M. Momtaj and A. Rahman. Universities' poor show in global rankings: Lack of research, quality publications key reasons, June 2021. The Daily Star.

[7] T. Farah, M. Shojol, M. M. Hassan, and D. Alam. Assessment of vulnerabilities of web applications of bangladesh: A case study of xss & csrf. In *Proceedings of the Sixth International Conference on Digital Information and Communication Technology and its Applications (DICTAP 2016)*, pages 74–78. IEEE, July 2016.

[8] M. T. Jeba, F. Sadia, T. Rahman, K. M. I. Hossain, and T. Bhuiyan. Usability and accessibility testing: A study on public sector and government websites of bangladesh. In A. Srivastava et al., editors, *Lecture Notes in Electrical Engineering*, volume 605, pages 666–674. Springer, 2020.

[9] Verizon. 2023 data breach investigations report (dbir), 2023. Accessed: 2025-11-26.

[10] University Grants Commission of Bangladesh. Annual report 2020. https://ugc.gov.bd, 2020.

[11] OWASP Foundation. Owasp top ten web application security risks. https://owasp.org/Top10, 2021. Accessed: 2025-08-25.

[12] T. A. Khan, A. Ahamed, N. Sadman, M. I. Hannan, F. Sadia, and M. Hasan. Automated testing: Testing top 10 owasp vulnerabilities of government web applications in bangladesh. In *Proceedings of the Seventeenth International Conference on Software Engineering Advances (ICSEA)*, pages 46–52. IARIA, 2022. Presented on October 16, 2022.

[13] S. Alam and M. Rahman. Cybersecurity practices in higher education institutions of bangladesh. *International Journal of Computer Applications*, 128(2):15–22, 2015.

[14] National Institute of Standards and Technology (NIST). Framework for improving critical infrastructure cybersecurity, version 1.1. Technical report, U.S. Department of Commerce, Gaithersburg, MD, 2018.

[15] National Institute of Standards and Technology (NIST). Cybersecurity maturity model certification (cmmc) 2.0. Technical report, U.S. Department of Commerce, Gaithersburg, MD, 2022.

[16] A. Tyas Tunggal. What is an attack vector? 16 critical examples, 2025. Accessed: 2025-07-13.

[17] M. M. Rahman, S. Sultana, S. Sultana, and M. S. Hossain. A review study on sql injection attacks: Prevention and detection. https://www.researchgate.net/publication/362751864, 2022. Accessed: 2025-07-23.

[18] D. Alam, T. Farah, and M. A. Kabir. Exploring the sql injection vulnerabilities of .bd domain web applications. In *Proceedings of the 3rd International Conference on Advances in Computing, Electronics and Communication (ACEC)*, pages 110–114. IARIA, 10 2015.

[19] D. Hussein, D. M. Ibrahim, and M. Alsalamah. A review study on sql injection attacks, prevention, and detection. *ISeCure – The International Journal of Information Security*, 13(3):1–9, 11 2021.

[20] Chamila Wijayarathna and Nalin Asanka Gamagedara Arachchilage. Fighting against xss attacks: A usability evaluation of owasp esapi output encoding. *arXiv*, 2018.

[21] T. Mohammed. Grandon.com got hacked! *Journal of Information Technology Education: Discussion Cases*, 6(1):1–25, 2017.

[22] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal. Fighting against phishing attacks: State of the art and future challenges. *Neural Computing and Applications*, 28(12):3629–3654, 2016.

[23] Kaspersky. What is a denial-of-service (dos) attack?, 2023. Accessed: 2025-07-23.

[24] Ahmet Cetinkaya, Hideaki Ishii, and Tomohisa Hayakawa. An overview on denial-of-service attacks in control systems: Attack models and security analyses. *Entropy*, 21(2):210, 2019.

[25] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim. Ddos attack detection method using cluster analysis. *Expert Systems with Applications*, 34(3):1659–1665, 2008.

[26] Kaspersky Lab. Longer, expanding, demanding: Botnet ddos attacks highlighted in kaspersky lab quarterly report. Press release, August 2017. The report notes that the longest attack lasted 277 hours and incidents originated from 86 countries.

[27] Joseph Bonneau. The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In *2012 IEEE Symposium on Security and Privacy*, pages 538–552. IEEE, 2012.

[28] Dinei Florêncio and Cormac Herley. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*, pages 657–666. ACM, 2007.

[29] William Stallings. *Cryptography and Network Security: Principles and Practice*. Pearson, 7th edition, 2017.

[30] A. Sasongko. *Panduan Keamanan Web Server*. Informatika, Jakarta, 2011.

[31] H. Yulianton, A. Trisetyarso, W. Suparta, B. S. Abbas, and C. H. Kang. Web application vulnerability detection using taint analysis and black-box testing. In *IOP Conference Series: Materials Science and Engineering*, volume 879, page 012031. IOP Publishing, 2020.

[32] T. Rangnau, R. van Buijtenen, F. Fransen, and F. Turkmen. Continuous security testing: A case study on integrating dynamic security testing tools in ci/cd pipelines. In *2020 IEEE 24th International Enterprise Distributed Object Computing Conference (EDOC)*, pages 145–154. IEEE, 2020.

[33] Red Hat. What is devsecops?, 4 2018. Accessed: 2025-07-23.

[34] OpenSAMM Project. Software assurance maturity model (samm) v2.0. Technical report, OWASP Foundation, 2020.

[35] Domain Domain. Organizational maturity and cybersecurity effectiveness. *Journal of Cybersecurity and Digital Trust*, 5(2):45–60, 2021.

[36] Wikipedia contributors. University Grants Commission of Bangladesh. https://en.wikipedia.org/wiki/University_Grants_Commission_of_Bangladesh, 2025. Accessed: 2025-08-21.

[37] Tao Li, Rubing Huang, Chenhui Cui, Dave Towey, Lei Ma, Yuan-Fang Li, and Wen Xia. A survey on web application testing: A decade of evolution. *arXiv preprint arXiv:2412.10476*, 2025. Submitted December 13, 2024; Revised April 25, 2025.

[38] E. Kenneally, D. Dittrich, and M. Bailey. The menlo report: Ethical principles guiding information and communication technology research, 2012. Accessed: 2025-08-21.

[39] USENIX Security Symposium. USENIX Security '25 Ethics Guidelines. https://www.usenix.org/conference/usenixsecurity25/ethics-guidelines, 2025. Accessed: 2025-08-21.

[40] NESH. A Guide to Internet Research Ethics. https://www.forskningsetikk.no/ressurser/publikasjoner/guide-to-internet-research-ethics/, 2019. English edition published May 2019; accessed: 2025-08-21.

[41] Jelena Mirkovic and Peter Reiher. A taxonomy of ddos attack and ddos defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2):39–53, 2004.

[42] Adam Barth, Collin Jackson, and John C. Mitchell. Robust defenses for cross-site request forgery. In *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS '08)*, pages 75–88. ACM, 2008.

[43] Eric Rescorla. The transport layer security (tls) protocol version 1.3. RFC 8446, Internet Engineering Task Force (IETF), 2018. Accessed: 2025-08-25.

[44] Offensive Security. Kali Linux. https://www.kali.org, 2025.

[45] Chelsea Glosser. Invicti Security Unveils Corporate Rebrand Reflecting Its Mission to Deliver AppSec with Zero Noise. Press release via blog post, April 2023. Announcement made at RSA Conference 2023.

[46] Gordon Lyon. *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure.Com LLC, Sunnyvale, CA, 2009.

[47] Rapid7. Metasploit Framework. https://www.metasploit.com/, 2023. Accessed 1 September 2025.

[48] T. Khan and R. Islam. Technology obsolescence and web security vulnerability in public universities. *Journal of Information Security*, 12(4):55–70, 2022.

[49] Cybersecurity Capacity Survey South Asia. Higher education cybersecurity workforce and budget study, 2022.

[50] T. Farah. Resource constraints and ict modernization in public universities. *Bangladesh Journal of Public Administration*, 25(1):45–62, 2016.

[51] National e Security Handbook Committee. National e-security guidelines for ict institutions, 2019.

[52] AuthorName. Web application firewalls and injection prevention. *Journal of Cybersecurity*, 2020.

[53] AuthorName. Modern tls practices and web security hardening. *International Journal of Information Security*, 2021.

[54] AuthorName. Secure software development life cycle for web applications. *Software Security Review*, 2019.

[55] AuthorName. Csrf defense mechanisms in web systems. *Computers & Security*, 2018.

[56] AuthorName. Impact of cybersecurity awareness training in educational institutions. *Education and Information Technologies*, 2022.

[57] IETF. The transport layer security (tls) protocol version 1.3, rfc 8446. https://datatracker.ietf.org/doc/html/rfc8446, 2018. Accessed: 2025-11-26.

[58] Ivan Ristic. *Bulletproof SSL and TLS*. Feisty Duck, London, UK, 2014.

[59] Center for Internet Security. Cis controls v8, 2022. Accessed: 2025-11-26.

[60] MITRE. Common weakness enumeration (cwe), 2022. Accessed: 2025-11-26.

[61] SonarSource. Sonarqube security best practices, 2023. Accessed: 2025-11-26.

[62] National Institute of Standards and Technology (NIST). Guide to penetration testing and vulnerability assessment (vapt). Technical report, U.S. Department of Commerce, 2020.

[63] ISO/IEC. Iso/iec 27001:2013 information security management, 2013. Accessed: 2025-11-26.

[64] Cybersecurity and Infrastructure Security Agency (CISA). Security operations center handbook, 2023. Accessed: 2025-11-26.

[65] PortSwigger. Burp suite documentation, 2024.

[66] Ettercap Project. Ettercap: Comprehensive suite for man-in-the-middle attacks. https://www.ettercap-project.org/, 2024. Accessed for controlled DoS/DDoS traffic simulation in a penetration-testing environment.

[67] Openwall Project. John the ripper password cracker. https://www.openwall.com/john/, 2024. Used for password cracking and cryptographic analysis.

[68] Rapid7. Metasploit framework. https://www.metasploit.com/, 2024. Penetration testing and social engineering framework.

[69] Gordon Lyon. Nmap network scanning. Insecure.Org, 2009. Port scanning and network reconnaissance tool.

[70] Amitosh (htr tech). Zphisher: Automated phishing tool. https://github.com/htr-tech/zphisher, 2020. Accessed: 2024-05-20.

[71] SSLScan Project. sslscan: Ssl/tls configuration scanner. https://github.com/rbsec/sslscan, 2024. Used to analyze TLS cipher suites and protocol support.

[72] The Hacker's Choice. Thc hydra. https://github.com/vanhauser-thc/thc-hydra, 2024. Used for password spraying and brute-force authentication testing.

[73] Invicti Security. Acunetix web vulnerability scanner. https://www.acunetix.com/, 2024. Automated vulnerability scanning and cross-validation tool.

How to install LaTeX

Windows OS

TeXLive package - full version

1. Download the TeXLive ISO (2.2GB) from
   https://www.tug.org/texlive/
2. Download WinCDEmu (if you don't have a virtual drive) from
   http://wincdemu.sysprogs.org/download/
3. To install Windows CD Emulator follow the instructions at
   http://wincdemu.sysprogs.org/tutorials/install/
4. Right click the iso and mount it using the WinCDEmu as shown in
   http://wincdemu.sysprogs.org/tutorials/mount/
5. Open your virtual drive and run setup.pl

or

Basic MikTeX - TeX distribution

1. Download Basic-MiKTeX(32bit or 64bit) from
   http://miktex.org/download
2. Run the installer
3. To add a new package go to Start ¿¿ All Programs ¿¿ MikTex ¿¿ Maintenance (Admin) and choose Package Manager
4. Select or search for packages to install

TexStudio - TeX editor

1. Download TexStudio from
   http://texstudio.sourceforge.net/#downloads
2. Run the installer

Mac OS X

MacTeX - TEX distribution

1. Download the file from
   https://www.tug.org/mactex/

2. Extract and double click to run the installer. It does the entire configuration, sit back and relax.

TexStudio - TEX editor

1. Download TexStudio from
   http://texstudio.sourceforge.net/#downloads

2. Extract and Start

Unix/Linux

TeXLive - TEX distribution

Getting the distribution:

1. TexLive can be downloaded from
   http://www.tug.org/texlive/acquire-netinstall.html.

2. TexLive is provided by most operating system you can use (rpm,apt-get or yum) to get TexLive distributions

Installation

1. Mount the ISO file in the mnt directory

   ```
   mount -t iso9660 -o ro,loop,noauto /your/texlive####.iso /mnt
   ```

2. Install wget on your OS (use rpm, apt-get or yum install)

3. Run the installer script install-tl.

   ```
   cd /your/download/directory
   ./install-tl
   ```

4. Enter command 'i' for installation

5. Post-Installation configuration:
   http://www.tug.org/texlive/doc/texlive-en/texlive-en.html#x1-320003.4.1

6. Set the path for the directory of TexLive binaries in your .bashrc file

For 32bit OS

For Bourne-compatible shells such as bash, and using Intel x86 GNU/Linux and a default directory setup as an example, the file to edit might be

```
edit $~/.bashrc file and add following lines
PATH=/usr/local/texlive/2011/bin/i386-linux:$PATH;
export PATH
MANPATH=/usr/local/texlive/2011/texmf/doc/man:$MANPATH;
export MANPATH
INFOPATH=/usr/local/texlive/2011/texmf/doc/info:$INFOPATH;
export INFOPATH
```

For 64bit OS

```
edit $~/.bashrc file and add following lines
PATH=/usr/local/texlive/2011/bin/x86_64-linux:$PATH;
export PATH
MANPATH=/usr/local/texlive/2011/texmf/doc/man:$MANPATH;
export MANPATH
INFOPATH=/usr/local/texlive/2011/texmf/doc/info:$INFOPATH;
export INFOPATH
```

Fedora/RedHat/CentOS:

```
sudo yum install texlive
sudo yum install psutils
```

SUSE:

```
sudo zypper install texlive
```

Debian/Ubuntu:

```
sudo apt-get install texlive texlive-latex-extra
sudo apt-get install psutils
```

Appendix A: Attack Vector Assessment Methodology

This appendix provides a detailed technical description of the tools, environments, and procedures used to assess the ten web application attack vectors evaluated in this study. All vulnerability assessments were conducted in a controlled penetration-testing environment following ethical security testing principles.

A.1 Testing Environment

All attack simulations were performed using a Kali Linux penetration-testing environment (rolling release), deployed on a virtualized platform using Oracle VirtualBox. Kali Linux

was selected due to its extensive repository of pre-installed security testing tools aligned with OWASP standards. Testing was conducted against publicly accessible university websites without exploiting or storing sensitive personal data.

Figure 6.1: Kali Linux virtualized penetration-testing environment using Oracle VirtualBox for vulnerability assessment

A.2 SQL Injection, XSS, and CSRF Assessment

SQL Injection (SQLi), Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF) vulnerabilities were assessed using Burp Suite Professional. HTTP requests were intercepted via Burp's proxy module to analyze request parameters and server responses. SQLi payloads were injected into GET and POST parameters to identify improper input validation. XSS testing involved both reflective and stored payloads, while CSRF vulnerabilities were detected by examining the presence of anti-CSRF tokens and same-origin policy enforcement [65].

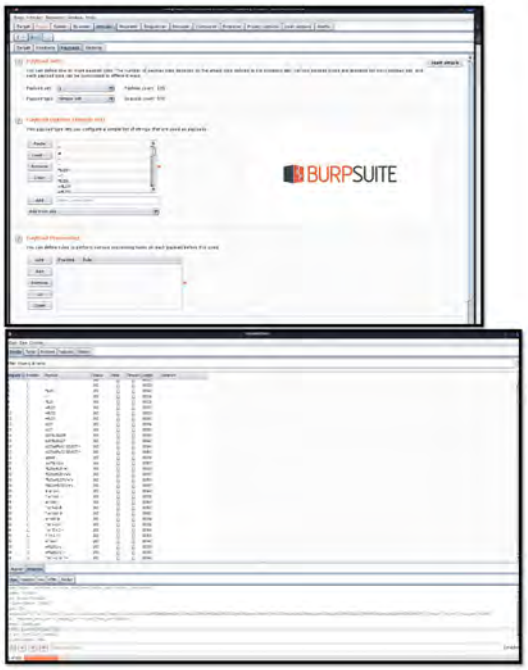

Figure 6.2: Burp Suite request interception and parameter manipulation

A.3 Denial-of-Service Attacks

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks aim to disrupt service availability by overwhelming target systems with excessive traffic. DoS attacks originate from a single source and it's like flooding a website with so many requests that it becomes unable to handle legitimate traffic. This renders the service inaccessible to its intended users. Whereas, DDoS attacks involve multiple compromised systems(a botnet) generating coordinated traffic. In this study, DoS and DDoS vulnerabilities were simulated using Ettercap in demonstration mode. Controlled packet flooding techniques were employed to observe server response degradation and identify susceptibility to traffic-based attacks without causing actual service disruption [66].

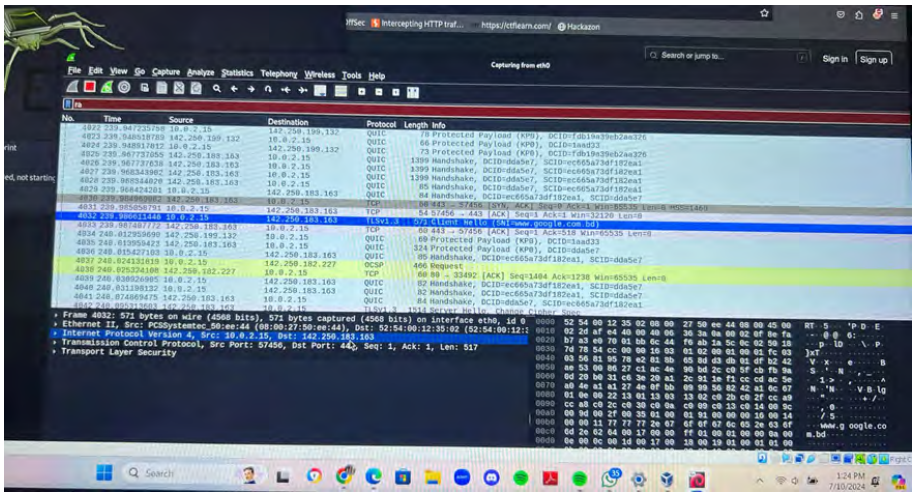

Figure 6.3: Simulation of DoS/DDoS traffic behavior using Ettercap in a controlled testing environment

A.4 Birthday Attack

A Birthday Attack is a cryptographic attack that exploits the probability of hash collisions in cryptographic hash functions. As the number of generated hash values increases, the likelihood of two different inputs producing the same hash grows significantly. In this study, birthday attack behavior was simulated in a controlled environment using John the Ripper to analyze weak hashing practices related to password storage and digital signatures [67].

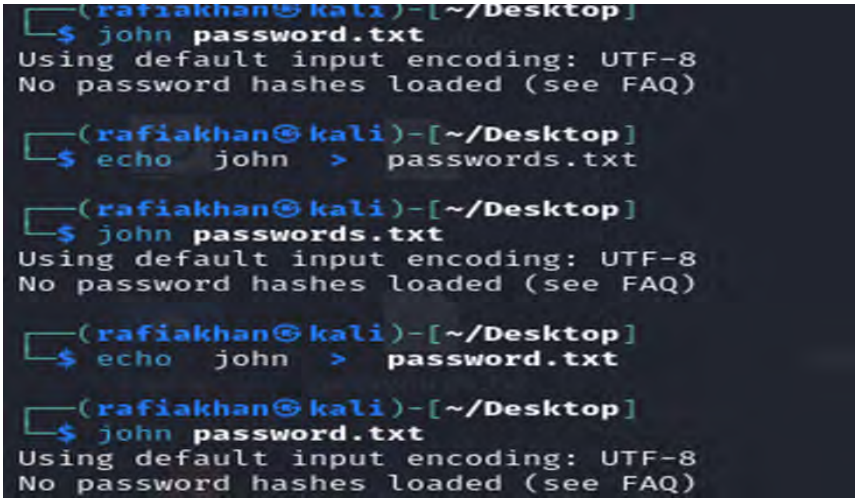

Figure 6.4: Simulation of cryptographic hash collision analysis using John the Ripper

A.5 Phishing Attack

Phishing attacks are social engineering techniques designed to trick users into revealing sensitive information such as usernames and passwords. In this study, phishing attacks were implemented using Metasploit and open-source frameworks such as Zphisher on Kali Linux. Fake websites resembling legitimate platforms were created to evaluate user susceptibility without storing real credentials [68].

Figure 6.5: Phishing website simulation used for vulnerability assessment

A.6 Port Scanning

Port scanning is a reconnaissance technique used to identify open ports and running services on a target system. In this study, Nmap was used to scan target servers and detect exposed services, outdated software, and unnecessary open ports that could increase the attack surface [69].

Figure 6.6: Network reconnaissance and service detection using Nmap

A.7 Broken Authentication and Session Management

Broken Authentication and Session Management vulnerabilities occur when authentication mechanisms are weak or improperly implemented. when an application's authentication mechanisms are weak or improperly implemented. In this assessment, issues such as weak password policies, missing CAPTCHA enforcement, and improper username validation were tested. Impersonation scenarios using visually similar usernames were simulated to evaluate authentication robustness. The figure below shows how to enter a webpage using brute force or missing captcha like if we want to break into the user page of "darren", we can create a new user account as " darren", the space will not show as a user and we can authenticate the original account of Darren. [70]

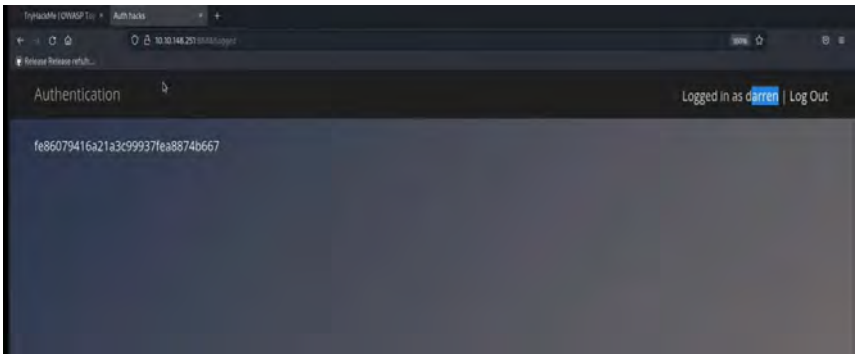

Figure 6.7: Broken Authentication of a webpage of darren(user) using brute force

A.8 Transport Layer Security (TLS) Weaknesses

Transport Layer Security (TLS) protects data transmission between clients and servers. TLS weaknesses arise due to improper configuration, weak cipher suites, or deprecated protocol versions. In this study, sslscan was used to analyze accepted cipher suites, protocol support, and certificate configurations to identify cryptographic vulnerabilities [71].

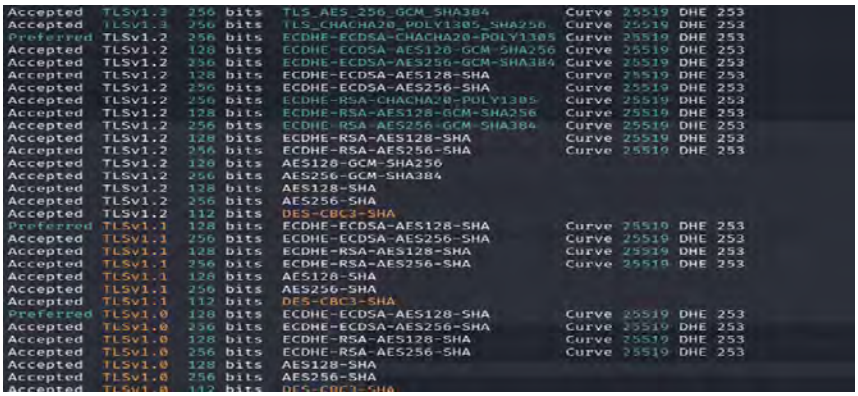

Figure 6.8: TLS configuration analysis using sslscan

A.9 Password Attacks

Password attacks aim to gain unauthorized access by compromising user credentials. In this study, password attacks were simulated using tools such as Hydra, John the Ripper, and Hashcat. OWASP Juice Shop was used as a controlled environment to demonstrate password spraying attacks by attempting logins across multiple accounts using a common password [72].

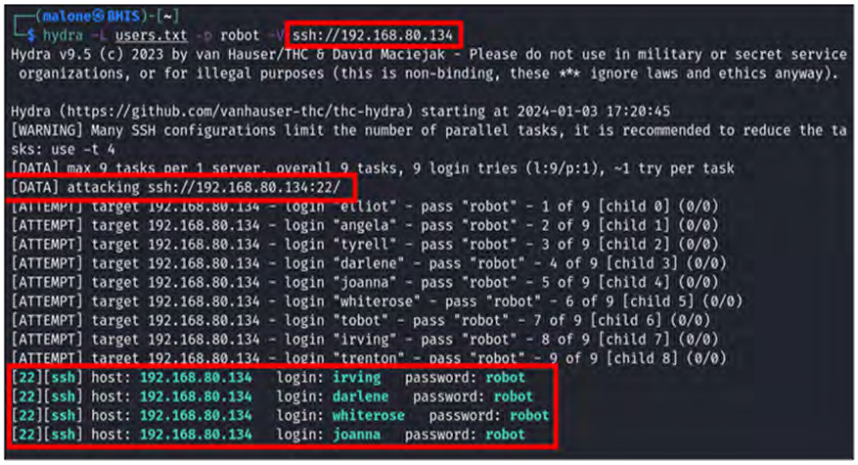

Figure 6.9: Password spraying simulation using OWASP Juice Shop

A.10 Cross-Validation of Findings

To reduce false positives, vulnerabilities identified through manual testing were cross-validated using controlled vulnerable environments and automated scanners. This ensured consistency and reliability of the observed attack outcomes.

A.11 Cross-Validation Tools

OWASP Juice Shop was used to validate exploit behavior in a safe environment, while automated vulnerability scanners such as Acunetix were employed to confirm detection accuracy. This dual-validation approach strengthened confidence in the final assessment results [73].

A.7 Broken Authentication and Session Management

Broken Authentication and Session Management (BAS) vulnerabilities were assessed by testing for weak credential handling, missing CAPTCHA enforcement, and improper username validation. For example, user impersonation scenarios were simulated using visually similar usernames (e.g., ”darren” vs. ” darren”) to evaluate authentication robustness.

A.8 TLS / SSL Weaknesses

Transport Layer Security vulnerabilities were evaluated using `sslscan` to identify accepted cipher suites, protocol versions, and certificate configurations. Weak or deprecated cryptographic settings were flagged as vulnerable.

A.9 Password Attacks

Password vulnerability testing was performed using Hydra, John the Ripper, and Hashcat. OWASP Juice Shop was deployed as a controlled test application to simulate credential reuse and weak password policies. Multiple user accounts with identical passwords were created, and automated login attempts were monitored to identify successful authentication events.

A.10 Cross-Validation of Findings

To ensure accuracy, vulnerabilities identified through manual and automated testing were cross-validated using OWASP Juice Shop and Acunetix vulnerability scanners. This dual-validation approach reduced false positives and strengthened confidence in the assessment results.

A.11 Cross-Validation Tools

OWASP Juice Shop provided a controlled vulnerable application environment to validate exploit behavior, while Acunetix was used to cross-check automated vulnerability detection results for consistency.

Overleaf: GitHub for LaTeX projects

This Project was developed using Overleaf(https://www.overleaf.com/), an online LaTeX editor that allows real-time collaboration and online compiling of projects to PDF format. In comparison to other LaTeX editors, Overleaf is a server-based application, which is accessed through a web browser.

Appendix B: Python Code for Statistical Analysis

This appendix provides the complete Python scripts used to generate the statistical results reported in Chapter 4. The inclusion of these scripts ensures reproducibility and transparency of the reliability, descriptive, and inferential analyses conducted in this study. All analyses were performed using Python 3.x with standard scientific libraries.

6.5.1 Data Preparation

The dataset was imported using the `pandas` library. Each row represents a university website, and each column corresponds to one of the ten evaluated attack vectors measured on a five-point Likert scale. A grouping variable (`University_Type`) was used to distinguish between public and private universities. Missing values were retained and handled using pairwise deletion during inferential analyses.

```
import pandas as pd
import numpy as np

# Load dataset
df = pd.read_csv("data.csv")
df.columns = df.columns.str.strip()
# Attack vector variables
attack_vectors = [
    "SQL Injection",
    "Cross-Site Scripting (XSS)",
    "CSRF",
    "DoS/DDoS",
    "Birthday Attack",
    "Phishing Attack",
    "Port Scan Attack",
    "Broken Authentication (BAS)",
    "TLS/SSL Issues",
    "Password Attack"
]
category_map = {
    "SQL Injection": "Application-Layer Attacks",
    "Cross-Site Scripting (XSS)": "Application-Layer Attacks",
    "CSRF": "Application-Layer Attacks",
```

```
    "DoS/DDoS": "Availability Attacks",
    "Broken Authentication (BAS)": "Availability Attacks",
    "Password Attack": "Availability Attacks",

    "Port Scan Attack": "Reconnaissance Attacks",
    "TLS/SSL Issues": "Reconnaissance Attacks",

    "Birthday Attack": "Cryptographic Attacks",
    "Phishing Attack": "Cryptographic Attacks"
}

data = df[attack_vectors]
```

```
from factor_analyzer import FactorAnalyzer
from factor_analyzer.factor_analyzer import (
    calculate_kmo,
    calculate_bartlett_sphericity
)

# KMO Measure
kmo_all, kmo_model = calculate_kmo(data)
print("KMO Measure:", round(kmo_model, 3))

# Bartlett's Test of Sphericity
chi_square_value, p_value = calculate_bartlett_sphericity(data)
print("Bartlett Test Chi-square:", round(chi_square_value, 2))
print("p-value:", p_value)

# Exploratory Factor Analysis (single-factor solution)
fa = FactorAnalyzer(n_factors=1, rotation=None)
fa.fit(data)

# Factor loadings
factor_loadings = pd.DataFrame(
    fa.loadings_,
    index=attack_vectors,
    columns=["Factor Loading"]
)
print("Factor Loadings:")
print(factor_loadings)

# Total Variance Explained
variance = fa.get_factor_variance()
tve = variance[1][0] * 100  # Proportion variance explained by single
    factor
print("Total Variance Explained:", round(tve, 2))

# Cronbach's Alpha
def cronbach_alpha(df):
    n_items = df.shape[1]
    item_variances = df.var(axis=0, ddof=1)
    total_variance = df.sum(axis=1).var(ddof=1)
    return (n_items / (n_items - 1)) * (1 - item_variances.sum() /
        total_variance)

alpha_overall = cronbach_alpha(data)
```

```
print("Overall Cronbach Alpha:", round(alpha_overall, 3))
```

Bartlett's Test and KMO were applied to the full set of attack vectors to assess overall sampling adequacy and factorability prior to reliability estimation

6.5.2 Overall Descriptive Statistics (Table 4.4)

Mean and standard deviation values for each attack vector across all universities were computed to summarize the overall vulnerability distribution.

```
# Overall descriptive statistics
desc_overall = data.agg(['mean', 'std']).T
desc_overall.columns = ['Mean', 'SD']
print(desc_overall.round(2))
```

6.5.3 Descriptive Statistics by University Type (Table 4.5)

Group-wise descriptive statistics were computed separately for public and private universities to examine sector-level vulnerability patterns.

```
# Descriptive statistics by university type
grouped = df.groupby("University_Type")[attack_vectors]
desc_grouped = grouped.agg(['mean', 'std'])
print(desc_grouped.round(2))
```

6.5.4 Levene's Test for Equality of Variance (Table 4.6)

Levene's test was applied to assess the homogeneity of variance assumption prior to conducting independent-samples *t*-tests.

```
from scipy.stats import levene

levene_results = {}

for av in attack_vectors:
    public = df[df["University_Type"] == "Public"][av].dropna()
    private = df[df["University_Type"] == "Private"][av].dropna()
    stat, p = levene(public, private, center='median')
    levene_results[av] = p

levene_df = pd.DataFrame.from_dict(
    levene_results, orient='index', columns=["Levene p-value"]
)

print(levene_df.round(3))
```

6.5.5 Independent-Samples *t*-Tests (Table 4.7)

Independent-samples *t*-tests were conducted to compare public and private universities. Welch's correction was applied to account for unequal variances where applicable. Pairwise deletion was used to handle missing data.

```python
from scipy.stats import ttest_ind

t_results = []

for av in attack_vectors:
    public = df[df["University_Type"] == "Public"][av].dropna()
    private = df[df["University_Type"] == "Private"][av].dropna()

    t_stat, p_val = ttest_ind(public, private, equal_var=False)
    t_results.append([av, t_stat, p_val])

t_df = pd.DataFrame(
    t_results,
    columns=["Attack Vector", "t-statistic", "p-value"]
)

print(t_df.round(3))
```

6.5.6 Effect Size Estimation (Table 4.8)

Effect sizes were calculated using eta squared (η^2) to quantify the magnitude of differences between public and private universities for each attack vector.

```python
effect_sizes = {}

for av in attack_vectors:
    public = df[df["University_Type"] == "Public"][av].dropna()
    private = df[df["University_Type"] == "Private"][av].dropna()

    t_stat, _ = ttest_ind(public, private, equal_var=False)
    n1, n2 = len(public), len(private)
    eta_sq = (t_stat ** 2) / (t_stat ** 2 + (n1 + n2 - 2))

    effect_sizes[av] = eta_sq

eta_df = pd.DataFrame.from_dict(
    effect_sizes, orient='index', columns=["Eta Squared"]
)

print(eta_df.round(3))
```

```python
# Overall descriptive statistics
desc_overall = data.agg(['mean', 'std']).T
desc_overall.columns = ['Mean', 'SD']

# Attach categories
desc_overall["Attack Category"] = desc_overall.index.map(category_map)

# Category-level mean verification (used to confirm values reported in
    Chapter 4)
category_summary = (
    desc_overall
    .groupby("Attack Category")["Mean"]
    .mean()
    .round(2)
)
```

```
15
16 print(category_summary)
```

Appendix C: Raw Vulnerability Assessment Dataset

This appendix presents the raw vulnerability dataset collected during the security assessment of Bangladeshi university websites. Due to the large scale of the study ($N = 182$ universities), the full dataset could not be embedded within the main body of the thesis; it is therefore provided here in its entirety for transparency and reproducibility.
The dataset is split into two tables: Table 6.1covers all 73 public universities and Table 6.2 covers all 109 private universities. Out of the total population of 182 institutions, 158 yielded valid assessment data and form the analytical sample used in Chapter 4. The remaining 24 institutions were inaccessible at the time of data collection due to server errors, handshake failures, connection timeouts, or non-operational websites; these are retained in the tables and marked N/A for completeness, but were excluded from all inferential analyses via pairwise deletion (see Section 4.7.1 for details).
Each accessible institution was evaluated across ten attack vectors using a five-point Likert-type scale, and an overall vulnerability percentage was calculated according to Equation 4.1. **Score Legend:**

Symbol	Meaning	Symbol	Meaning	Symbol	Meaning
VS	Very Secure (1)	S	Secure (2)	F	Fair (3)
V	Vulnerable (4)	VV	Very Vulnerable (5)	N/A	Not Accessible[†]

[†]Websites marked N/A were inaccessible during data collection (e.g. handshake failures, 403/404 errors, server timeouts, or non-operational sites) and were excluded from inferential analyses using pairwise deletion (Section 4.7.1).

Column abbreviations: SQLi = SQL Injection; XSS = Cross-Site Scripting; CSRF = Cross-Site Request Forgery; DoS = Denial of Service/DDoS; BA = Birthday Attack; PA = Phishing Attack; PS = Port Scan; BAS = Broken Authentication & Session; TLS = Transport Layer Security; PWD = Password Attack; Vuln.% = Overall Vulnerability Percentage.

Table 6.1: Raw Vulnerability Assessment Data — Public Universities (N = 73)

University	SQLi	XSS	CSRF	DoS	BA	PA	PS	BAS	TLS	PWD	Vuln.%
Autonomous											
University of Dhaka	V	VV	VS	VV	VS	V	S	V	VV	VS	64
University of Rajshahi	VV	VV	VV	VV	V	V	VV	VV	VV	VV	96
University of Chittagong	VV	VV	S	S	VS	VS	S	VV	VS	VV	66
Jahangirnagar University	VV	VV	F	V	VV	VV	S	VV	V	VV	86
General											
Islamic University	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Bangladesh Khulna University	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Jagannath University	VV	VV	VV	F	VV	VV	S	VV	VS	VV	82
Comilla University	F	VV	VV	VV	VV	VV	V	VV	V	VV	92
Jatiya Kabi Kazi Nazrul Islam University	VV	VV	VV	S	S	VV	S	S	S	S	64
Bangladesh University of Professionals	V	VV	VV	S	V	V	S	V	S	VV	74
University of Barisal	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Rabindra University, Bangladesh	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Sheikh Hasina University	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Bangabandhu Sheikh Mujibur Rahman University, Kishoreganj	S	V	S	S	S	V	S	V	S	V	56
Bangabandhu Sheikh Mujibur Rahman University, Naogaon	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Thakurgaon University TU	VV	VV	VV	S	V	V	S	VV	V	V	80
Mujibnagar University MU	VV	VV	VV	S	V	V	S	VV	V	V	80
STEM											
Sunamganj Science and Technology University	S	VV	S	VV	VV	V	S	S	S	S	62
Shahjalal University of Science and Technology	VV	VV	VV	V	VV	VV	S	VV	VV	S	86
Satkhira University of Science and Technology	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Rangamati Science and Technology University	V	VV	VV	S	V	VV	S	S	VV	S	72

(Continued on next page)

(Continued from previous page)

University	SQLi	XSS	CSRF	DoS	BA	PA	PS	BAS	TLS	PWD	Vuln.%
Patuakhali Science and Technology University	V	VV	VV	VV	VV	VV	VV	VV	VV	VV	98
Pabna University of Science and Technology	V	VV	VV	VV	VV	VV	VV	VV	VV	VV	98
Noakhali Science and Technology University	V	VV	VV	S	S	V	S	S	S	S	60
Mawlana Bhashani Science and Technology University	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Lakshmipur Science and Technology University	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Jashore University of Science and Technology	VV	VV	S	VV	VV	VV	VV	V	VV	S	86
Hajee Mohammad Danesh Science & Technology University	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Chandpur Science and Technology University	S	VV	VV	S	S	VV	S	V	V	S	66
Bogura Science and Technology University	VS	V	VS	VS	VS	VS	VS	VS	VS	VS	26
Bangamata Sheikh Fazilatunnesa Mujib Science & Technology University	S	VV	VV	S	S	VV	S	V	VV	VV	74
Bangabandhu Sheikh Mujibur Rahman Science and Technology University	VS	V	VS	VS	VS	V	VS	VS	VS	VS	32
Engineering											
Bangladesh University of Engineering & Technology	V	VV	VV	S	S	VV	S	VV	S	S	68
Military Institute of Science and Technology	VV	VV	VV	S	VV	VV	S	VV	VV	V	86
Khulna University of Engineering & Technology	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Chittagong University of Engineering & Technology	VV	VV	VV	VV	V	VV	V	VV	VV	V	94
Rajshahi University of Engineering & Technology	VV	VV	VV	VV	VV	VV	VV	VV	VV	VV	100
Dhaka University of Engineering & Technology	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Agricultural											
Bangladesh Agricultural University	VV	VV	VV	VV	VV	VV	VV	VV	VV	VV	100

(Continued on next page)

(Continued from previous page)

University	SQLi	XSS	CSRF	DoS	BA	PA	PS	BAS	TLS	PWD	Vuln.%
Bangabandhu Sheikh Mujibur Rahman Agricultural University University	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Sher-e-Bangla Agricultural University	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Sylhet Agricultural University	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Khulna Agricultural University	VV	VV	VV	VV	VV	VV	VV	VV	VV	VV	100
Habiganj Agricultural University HAU	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Kurigram Agricultural University	VV	VV	VV	VV	VV	VV	VV	VV	VV	VV	100
Bangabandhu Sheikh Mujib Shariatpur Agriculture University	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Medical											
Bangabandhu Sheikh Mujib Medical University	VV	VV	VV	V	V	VV	VV	VV	VV	VV	96
Chittagong Medical University	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Rajshahi Medical University	VV	VV	VV	V	VV	VV	VV	VV	VV	VV	92
Sylhet Medical University	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Sheikh Hasina Medical University	VV	VV	VV	VV	VV	VV	V	VV	S	V	90
Vet. Sci. (Spec.)											
Chittagong Veterinary and Animal Sciences University	VV	VV	VV	VV	VV	VV	VV	VV	VV	VV	100
Textile Eng. (Spec.)											
Bangladesh University of Textiles	VV	VV	VV	VV	VV	VV	VV	VV	VV	VV	100
Maritime (Spec.)											
Bangladesh Maritime University	VV	VV	VV	V	VV	VV	V	VV	VV	VV	96
ICT Edu. (Spec.)											
Bangladesh Digital University	VV	VV	VV	V	VV	VV	VV	VV	VV	VV	98
Aeronautics (Spec.)											
Aviation and Aerospace University	VV	VV	VV	VV	V	VV	V	V	VV	VV	94

(Continued on next page)

(Continued from previous page)

University	SQLi	XSS	CSRF	DoS	BA	PA	PS	BAS	TLS	PWD	Vuln.%
Off-Campus Gen.											
National University	VV	VV	VV	V	VV	VV	V	VV	VV	VV	96
Bangladesh Open University	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Off-Campus (Islamic)											
Bangladesh Islamic Arabic University	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Aff. Spec. Eng.											
Sylhet Engineering College	VV	VV	VV	V	VV	VV	V	VV	VV	VV	96
Mymensingh Engineering College.	VV	VV	VV	V	VV	VV	V	VV	VV	VV	96
Faridpur Engineering College	VV	VV	VV	V	VV	VV	VV	VV	VV	VV	98
Rangpur Engineering College	VV	VV	VV	VV	VV	VV	V	VV	VV	VV	98
Barisal Engineering College.	VV	VV	VV	V	VV	VV	V	VV	VV	VV	96
Aff. Textile Eng.											
Textile Engineering College, Chittagong	VV	VV	VV	VV	VV	VV	S	S	VV	S	92
Pabna Textile Engineering College	VV	VV	VV	S	VV	VV	S	V	VV	V	84
Textile Engineering College, Noakhali	VV	VV	VV	VV	VV	VV	V	V	VV	VV	96
Affiliate Textile Engineering											
Bangabandhu Textile Engineering College, Kalihati, Tangail	VV	VV	VV	S	VV	S	S	S	VV	VV	76
Aff. Textile Eng.											
Shahid Abdur Rab Serniabat Textile Engineering College	VV	VV	VV	V	VV	VV	S	S	S	S	74
Sheikh Kamal Textile Engineering College, Jhenaidah	VV	VV	VV	VV	VV	VV	VV	S	VV	S	88
Affiliate Textile Engineering											
Dr. M A Wazed Miah Textile Engineering College	VV	VV	VV	VV	VV	V	S	S	S	S	74

(Continued on next page)

(Continued from previous page)

University	SQLi	XSS	CSRF	DoS	BA	PA	PS	BAS	TLS	PWD	Vuln.%
Aff. Textile Eng.											
Sheikh Rehana Textile Engineering College, Gopalganj.	VV	VV	VV	VV	VV	VV	V	VV	VV	S	92
Sheikh Hasina Textile Engineering College	VV	VV	VV	VV	VV	VV	VV	V	VV	VV	98

Table 6.2: Raw Vulnerability Assessment Data — Private Universities (N = 109)

University	SQLi	XSS	CSRF	DoS	BA	PA	PS	BAS	TLS	PWD	Vuln.%
General											
International University of Business Agriculture and Technology	VV	VV	VV	VV	VV	VV	VV	VV	VV	VV	100
North South University	VV	VV	VV	V	VV	VV	S	VV	VV	V	90
Independent University, Bangladesh	V	F	F	S	S	S	S	S	F	S	50
American International University-Bangladesh	VV	VV	VV	VV	V	VV	VV	VV	F	VV	94
Dhaka International University	V	VV	VV	S	V	VV	VV	VV	V	VV	88
International Islamic University, Chittagong	VV	VV	VV	VV	V	V	V	VV	V	VV	92
Asian University of Bangladesh	VV	VV	VV	VV	F	VV	VV	F	VV	VV	92
East West University	VV	VV	VV	VV	VV	VV	VV	VV	VV	VV	100
Gono Bishwabidyalay	VV	VV	VV	VV	VV	VV	VV	V	VV	V	96
People's University of Bangladesh	VV	V	VV	S	V	S	S	S	F	V	68
Queen's University QU	VV	V	VV	F	V	F	F	V	VV	VV	84
University of Asia Pacific (Bangladesh)	VV	V	VV	VV	VV	V	V	VV	VV	VV	96
Chittagong Independent University (CIU)	VV	V	VV	VV	VV	VV	V	VV	VV	VV	98
Bangladesh University	VV	V	VV	VV	VV	VV	V	VV	VV	VV	98
BGC Trust University Bangladesh	VV	V	VV	VV	VV	VV	V	VV	VV	VV	98
Brac University	VV	V	VV	V	VV	VV	F	VV	VV	VV	94
Premier University, Chittagong	VV	V	VV	VV	VV	VV	VV	VV	VV	V	98
Southern University, Bangladesh	VV	VV	VV	VV	VV	VV	V	VV	VV	VV	98
Sylhet International University	VV	VV	VV	V	VV	VV	V	VV	VV	VV	96
Manarat International University	VV	VV	VV	VV	VV	VV	F	VV	VV	V	94
City University, Bangladesh	VV	VV	VV	S	V	S	S	V	VV	V	78
Daffodil International University	VV	VV	VV	V	VV	VV	V	VV	VV	V	94
Green University of Bangladesh	VV	VV	VV	VV	VV	VV	V	VV	VV	VV	98
IBAIS University	VV	VV	VV	VV	VV	VV	VV	VV	VV	V	98
Leading University	V	V	V	S	S	S	V	V	S	S	60
University of Development Alternative	VV	VV	VV	VV	F	VV	VV	VV	V	F	90
Prime University	VV	VV	VV	F	V	F	F	VV	VV	VV	86
Northern University, Bangladesh	VV	VV	VV	VV	S	V	S	VV	V	V	82
Southeast University	V	V	V	VS	VS	V	VS	V	V	V	62

(Continued on next page)

(Continued from previous page)

University	SQLi	XSS	CSRF	DoS	BA	PA	PS	BAS	TLS	PWD	Vuln.%
Stamford University Bangladesh	VV	VV	VV	VV	V	VV	V	VV	VV	VV	96
State University of Bangladesh	VV	VV	VV	VV	V	VV	V	VV	VV	VV	96
Eastern University, Bangladesh	V	V	V	V	VS	VS	VS	VS	V	VS	50
Metropolitan University	VV	VV	VV	VV	F	S	S	VV	V	V	80
Millennium University	VV	VV	VV	VV	F	VV	F	VV	VS	VS	76
Primeasia University	VV	VV	VV	VV	VV	VV	VV	VV	VV	F	96
Royal University of Dhaka	V	V	V	VS	V	VS	VS	VV	V	V	64
United International University	VV	VV	VV	V	VV	VV	VS	VV	VV	VV	90
University of Information Technology and Sciences	VV	VV	VV	VV	VV	VV	V	VV	VV	VV	98
University of South Asia, Bangladesh	VV	VV	VV	VV	V	VV	VS	VV	VV	V	88
Presidency University	V	V	V	V	S	VS	VS	V	VS	S	54
Uttara University	VV	VV	VV	VV	VV	VV	V	VV	VV	VV	98
Victoria University of Bangladesh	VV	VV	VV	V	V	V	VS	VV	V	V	82
World University of Bangladesh	VV	VV	VV	VV	V	VV	V	VV	VV	VV	96
Asa University Bangladesh	VV	VV	VV	VV	V	VV	V	VV	F	F	88
Bangladesh Islami University	VV	VV	VV	VV	V	VV	VV	VV	VV	V	96
East Delta University	V	V	V	VS	VS	VS	VS	VS	VS	F	42
Northern University of Business and Technology Khulna NUB	VV	VV	VV	VV	V	V	F	VV	VV	V	90
Britannia University	VV	VV	VV	V	VS	VS	VS	VV	V	F	68
Feni University	VV	VV	VV	VV	V	V	VV	VV	VV	V	94
Khwaja Yunus Ali University	V	V	V	VS	VS	VS	VS	V	V	F	54
European University of Bangladesh EUB	VS	VV	V	VV	V	F	V	V	V	VS	70
First Capital University Of Bangladesh	VV	VV	VV	VS	VS	V	VS	VS	V	V	62
BGMEA University of Fashion & Technology BUFT	VV	VV	VV	VV	V	VV	V	VV	VV	VV	96
Hamdard University Bangladesh (HUB)	VV	VV	VV	VV	V	VV	V	VV	VV	VV	96
Ishakha International University	V	V	V	VS	F	V	VS	VV	V	V	66
North East University Bangladesh	VV	VV	VV	VV	V	VV	VV	VV	VV	V	96
North Western University, Bangladesh	V	VV	VV	VV	VS	VS	V	VV	VV	VV	80
Port City International University	VV	VV	VV	VV	VS	VS	F	VV	V	F	74
Varendra University	VV	VV	VV	VV	VV	VV	VV	V	VV	V	96

(Continued on next page)

(Continued from previous page)

University	SQLi	XSS	CSRF	DoS	BA	PA	PS	BAS	TLS	PWD	Vuln.%
Sonargaon University	VV	VV	VV	VV	VS	V	VV	VV	VV	F	80
Cox's Bazar International University	V	V	V	V	VS	VS	V	VS	V	V	62
Fareast International University	VV	VV	VV	VV	V	VV	VS	VS	VS	F	70
German University	VV	VV	VV	VV	VV	V	F	VV	VV	F	90
North Bengal International University	F	VV	VV	V	F	F	V	VV	V	F	78
Notre Dame University Bangladesh NDUB	VV	VV	VV	VV	VV	VV	V	VV	VV	VV	98
Ranada Prasad Shaha University	VV	VV	VV	F	VS	VS	VS	VS	VS	V	54
Sheikh Fazilatunnesa Mujib University	S	V	V	V	VS	VS	V	V	F	S	58
Times University Bangladesh	V	F	F	V	VS	VS	VS	V	F	VV	58
Canadian University of Bangladesh	VV	VV	VV	VV	S	V	S	VV	VS	F	74
Global University Bangladesh	VV	VV	VV	VV	VS	VS	F	VV	VS	VS	64
NPI University of Bangladesh	VV	VV	VV	VV	VS	VS	F	VV	V	F	74
Rabindra Maitree University	VV	VV	VV	VS	VS	VS	VV	VV	VV	V	74
University of Scholars	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
University of Creative Technology Chittagong	VV	VV	VV	VV	VV	VV	VV	VV	V	V	98
Anwer Khan Modern Universiy	VV	VV	VV	VV	VV	VV	V	VV	VV	V	96
University of Global Village	VV	VV	VV	F	F	F	S	VV	V	VV	80
Khulna Khan Bahadur Ahsanullah University	VV	VV	VV	F	F	S	S	VV	VV	VV	80
Trust University, Barishal	VV	VV	VV	V	F	F	VS	VV	VV	VV	82
University of Brahmanbaria	VV	VV	VV	VV	VV	VV	V	VV	VV	V	96
University of Skill Enrichment and Technology	VV	VV	VV	VV	VV	VV	VV	VV	VV	VV	100
International Standard University	VV	VV	VV	VV	VV	VV	VV	VV	VV	V	98
Bandarban University	F	V	V	V	F	VS	F	VS	F	S	56
RTM Al-Kabir Technical University	VV	VV	VV	VS	F	VV	F	VV	VV	F	80
ZNRF University of Management Sciences	V	V	V	VS	VS	VS	VS	S	F	VV	52
Sci. and Tech.											
International Islami University of Science and Technology Bangladesh	VV	VV	VV	VV	V	VV	VV	V	F	VS	84

(Continued on next page)

(Continued from previous page)

University	SQLi	XSS	CSRF	DoS	BA	PA	PS	BAS	TLS	PWD	Vuln.%
Microland University of Science and Technology	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
Sci. and Arts											
Lalon University of Science & Arts	VV	VV	VV	VV	VV	VV	VV	VV	VV	VV	100
General											
Grameen University	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	–
STEM											
University of Science & Technology Chittagong	VV	VV	VV	VS	F	VS	VS	V	V	V	66
Ahsanullah University of Science and Technology	VV	VV	VV	VV	VV	VV	VV	VV	VV	V	98
Pundra University of Science and Technology	S	F	F	S	S	VS	VS	VS	S	VS	36
Bangladesh University of Business and Technology	VV	VV	VV	VV	V	F	VS	VV	V	V	82
Atish Dipankar University of Science and Technology	V	V	V	S	F	VS	VS	V	S	S	54
ZH Sikder University of Science & Technology	V	V	V	V	F	VS	VS	V	F	F	70
Rajshahi Science & Technology University	VV	VV	VV	VS	VV	VS	F	VV	VV	V	78
Bangladesh Army University of Science & Technology, Khulna	VV	VV	VV	VV	F	VV	VV	VV	V	VV	94
Bangladesh Army University of Science and Technology, Saidpur	VV	VV	VV	VV	VV	S	VS	VV	VV	S	80
Bangladesh Army International University of Science & Technology	VV	VV	VV	VV	V	V	VV	VV	V	V	90
CCN University of Science & Technology	V	V	V	V	V	S	S	VV	V	S	70
Central University of Science and Technology	VV	VV	VV	VV	V	VV	VV	VV	V	S	90
Spec: Women's Studies											

(Continued on next page)

(Continued from previous page)

University	SQLi	XSS	CSRF	DoS	BA	PA	PS	BAS	TLS	PWD	Vuln.%
Central Women's University	VV	VV	VV	VV	VV	F	VV	VV	VV	F	92
Spec: Creative Tech.											
Shanto-Mariam University of Creative Technology	VV	VV	VV	VV	VV	VV	VV	VV	VV	VV	100
Spec: Media and Journalism											
University of Liberal Arts Bangladesh	V	V	V	VV	V	F	VV	VV	V	F	82
Spec: Health Sci.											
Bangladesh University of Health Sciences	VV	VV	VV	VS	S	S	S	VV	F	V	68
Spec: Agricultural											
Exim Bank Agricultural University Bangladesh	VV	VV	VV	VV	VV	V	V	VV	V	F	90
Spec: Eng. and Tech.											
Bangladesh Army University of Engineering & Technology	VV	VV	VV	V	VV	VV	F	VV	VV	VV	94
Spec: Creative											
Tagore University of Creative Arts	V	V	V	V	V	VS	F	VS	V	V	66
Intl: Eng. and Tech.											
Islamic University of Technology	F	F	F	F	S	VS	VS	F	F	F	50
Intl: Women's Univ.											
Asian University for Women	VV	VV	VV	V	V	F	VS	VV	VV	F	80