Analysis of Password Security Factors Among E-commerce Websites, News Portals, and Government Websites

by

Adhara Labannya
24141277
Dipannita Baidya
23341069
Nahian Hoque Dipto
20101260
Sahadat Hossain
20101421
Shantanu Das
23341068

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

Department of Computer Science and Engineering
Brac University
January 2024

Declaration

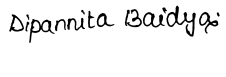
It is hereby declared that

1. The thesis submitted is our 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. We have acknowledged all main sources of help.

Student's Full Name & Signature:

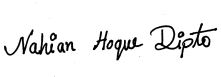
Adhara Labannya

24141277



Dipannita Baidya

23341069



Nahian Hoque Dipto

20101260

Sahadat Hossain

20101421

Shantanu Das

23341068

Approval

The thesis/project titled "Analysis of Password Security Factors Among E-commerce Websites, News Portals and Government Websites of Bangladesh" submitted by

1. Adhara Labannya (24141277)
2. Dipannita Baidya (23341069)
3. Nahian Hoque Dipto (20101260)
4. Sahadat Hossain (20101421)
5. Shantanu Das (23341068)

Of Summer, 2024 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on October 17, 2024.

Examining Committee:

Supervisor:
(Member)

Dr. S M Taiabul Haque
Associate Professor
Department of Computer Science and Engineering
BRAC University

Thesis Coordinator:
(Chair)

Md. Golam Rabiul Alam, PhD
Professor
Department of Computer Science and Engineering
BRAC University

Head of Department:
(Chair)

Sadia Hamid Kazi, PhD
Chairperson & Associate Professor
Department of Computer Science and Engineering
BRAC University

Abstract

This study aims to evaluate password security practices among the top e-commerce, news portal, and different government websites in Bangladesh along with the e-commerce websites in India. Drawing from the established heuristics as presented in the existing literature, we systematically assess the adherence of 72 websites to the essential security guidelines. We also find the relationship between password security and other external economic factors. The study sheds light on the prevalent inadequacies in password security practices among the prominent websites of different categories in Bangladesh as well as India. The implications of these findings underscore the urgency for solid security measures to fortify the user authentication systems and mitigate the risks posed by the potential cyber threats.

Keywords: Cybersecurity; Password; Authentication

Table of Contents

List of Figures

Nomenclature

The next list describes several symbols & abbreviation that will be later used within the body of the document

AES Advanced Encryption Standard

$CAPTCHA$ Completely Automated Public Turing test to tell Computers and Humans Apart

$CSRF$ Cross-Site Request Forgery

$HTTPS$ Hypertext Transfer Protocol Secure

$ICCIT$ International Conference on Computer and Information Technology

IdP Identity Provider

NID National Identification

OTP One-time password

$QUIC$ Quick UDP Internet Connection

SMS Short Message Service

SP Service Provider

TLS Transport Layer Security

XSS Cross-Site Scripting

Chapter 1

Introduction

1.1 Background

In the modern digital era, ensuring the safety of online accounts is of utmost importance. Passwords are an essential part of internet security because they serve as the first line of protection against unwanted access to private and sensitive information. A compromised password can have serious repercussions, such as identity theft and financial loss, since people engage in a variety of online activities, from social interactions to commercial transactions. Moreover, the interconnected nature of digital platforms underscores the importance of strong and unique passwords across different accounts to prevent unauthorized access cascading from one compromised account to another. Without strong password security protocols, people and companies alike are vulnerable to the ever-increasing risks posed by the cybercriminals looking to take advantage of weaknesses and obtain unauthorized access to sensitive data.

In the context of Bangladesh, two research works have been done previously, on password security factors among Bangladeshi government websites [11]; and password construction and management strategies [4]. This existing research on password security has demonstrated that users are not properly aware of the use of passwords and security systems. The most basic mistake done by the users is that when they see a website not providing any password instructions they use a very easy password for their own betterment of remembering the passwords later. Convenience-driven behavior and the need for simplicity may make users choose easy-to-remember passwords over more complicated but safer ones, undermining the significance of establishing strong password practices. In addition to that, prioritizing the enforcement of extra security information on websites would improve user protection against possible attacks. Websites can add another line of defense, lessening the impact of hacked passwords and strengthening overall security measures, by implementing multi-factor authentication and encouraging users to submit additional security details.

Nonetheless, the website administrators must feel obligated to safeguard users privacy and personal information. The password security not only protects users from potential security flaws but also attracts visitors and improves the online business's reputation. By giving security consideration top priority, website managers may

demonstrate their commitment to making their sites safe. This could raise end users' trust and engagement levels, which could contribute to the platform's long-term sustainability.

Thus, inspired by a famous paper called "The Password Thicket: Technical and Market Failures in Human Authentication on the Web [4]," this thesis focuses on checking how secure passwords are on about 72 different websites in Bangladesh and India. These websites include news and e-commerce sites, as well as the government websites in Bangladesh.

"The Password Thicket" paper shaped the conversation on online security by offering a fundamental knowledge of the technological and commercial shortcomings in the authentication process. The study highlighted the intricacies of password systems and the necessity of a comprehensive strategy to mitigate vulnerabilities. Using the knowledge gained from this important paper "The Password Thicket", keeping it as a foundation, this thesis research carefully examines password security procedures in the context of more or less 60 different websites in Bangladesh and 12 Indian websites.

Mostly, the work here is mainly to understand what security measures these websites use to protect these passwords. Finding out what is good and what may be improved is the aim that is needed to be accomplished. This concept originated after the study of existing relevant research in the context of Bangladesh, considering the fact that how Bangladeshis use the internet has major lack of understanding and thus implementation of security measures. In our research we mainly dive into how the websites of Bangladesh are not designed securely enough which enables users to keep up with their habit of not using safe internet protocols. The research aims to examine these websites in detail, with a particular focus on how the security and passwords are managed. Considering factors such as the ease of use and security of these websites in addition to their technical aspects. Improving the online experience requires an understanding of security from both a technological and human perspective.

The main reason for choosing these websites is because they represent the different types of online services that people in Bangladesh use on a daily basis. The main goal for this paper is to identify the strengths and weaknesses of the websites and also the paper might be useful to the people of Bangladesh who are using the websites.

Moreover, the vision of the research is examining the unique difficulties faced by Bangladeshi websites while proceeding forward. The thesis discusses topics including popular types of technology (TLS), heuristics of different websites, and how people use it. The aim is to ensure that the research is not only filled with complicated terms but also understandable to anyone.

At the start of exploring the websites of Bangladesh, the main aim is not just to find problems but to give real solutions. By the end of the research, the aim is to help not only each website individually but also make online spaces safer for everyone in

Bangladesh.

1.2 Problem Statement

Conducting a comprehensive analysis of password security practices across various website categories in Bangladesh, with a focus on identifying potential correlations between security strength and external factors. The previous works related to the password field clearly lack detailed analysis of factors in the password security field. In Bangladeshi context password security analysis has been done in specifically one paper that has highlighted six heuristics [11]. This paper represents the analysis in a broader spectrum with more number of heuristics and multiple categories of websites. Additionally, this work analyzes the password security factors among a few Indian websites to offer a comparison between the two countries. To protect financial, personal, and business data, password security is vital. For protecting the sensitive information and addressing emerging threats, an extensive analysis in password security is necessary.

1.3 Research Objectives

We have four main research objectives:

1. We conducted a comprehensive evaluation of password security among 60 e-commerce, news portal, and different government websites in Bangladesh.
2. We evaluated 12 Indian e-commerce websites in order to assess similarities and dissimilarities with Bangladeshi e-commerce websites.
3. We provided a comparison of the password security factors among websites of different categories.
4. We analyzed the relationship between password security and other external economic factors.

Chapter 2

Related Work

In this section, we offer a brief literature review of the existing works on password security. First, we highlight the related works that have been conducted in Bangladesh. Next, we discuss a few related studies in the context of other countries. Finally, we highlight the paper that served as a motivation for this thesis.

2.1 Password Studies in the context of Bangladesh

There have been a few studies analyzing the security of different kinds of websites in Bangladesh. In one of those works [12], the main goal was to evaluate the security posture of Bangladeshi government and financial websites by doing a vulnerability assessment. Four kinds of risk alerts were scanned and analyzed by the research using Acunetix and ZAP tools: High, Medium, Low, and Informational. The study provides mitigation strategies for the vulnerabilities found in addition to illustrating the security state of Bangladesh's official websites. Security issues that are less frequently highlighted in the nation are addressed by these mitigating techniques. The paper highlights how important it is to use safe coding practices while developing online applications in a variety of fields, such as finance, education, government, and non-government. According to the report, the growing number of websites has increased the security risk posed by poor coding. If these security flaws are not fixed, attackers may be able to take advantage of them and carry out activities like data breaches, the introduction of spam material, the spread of malware, malicious redirects, Denial-of-Service attacks, or even vandalism of websites. Furthermore, the selected main vulnerabilities—CJ, MC, CSRF, ID, and XSS—are found to be the most common individual vulnerability categories found on certain websites. With an emphasis on these particular weaknesses, the paper describes the security state of official websites in Bangladesh. The publication also provides mitigation solutions for these particular vulnerabilities, addressing security threats that haven't been thoroughly examined in the country.

In another work [11], the research paper examines the level of password security of several government websites in Bangladesh. The researchers conducted a thorough analysis of thirty-six government websites. They assessed these websites using six carefully chosen password security heuristics: Password Construction Guidelines, Password Recovery , CAPTCHA, Security Question, HTTPS Channel, Password Strength Meter. These are the most fundamental and basic metrics used to assess a

password's level of security. Based on all of the previously mentioned study findings and as described in the current article, it is feasible to conclude that none of the websites under investigation has demonstrated appropriate and functional security padding mechanisms. The fact that many of the websites lack instructions on how to construct passwords was one of the flaws that the researchers noticed, among other things. Since they assist users in creating secure passwords, these suggestions that are included in the study, as will be seen—are essential. Users are likely to add weak passwords to their accounts, leaving them open to hacking, if the aforementioned advice is not followed. Other issues, such as the fact that certain websites permitted the use of weak passwords while others had no established guideline on how passwords should be constructed, have also been emphasised in the aforementioned paper. It was noted, nonetheless, that several of these websites did not adopt secure HTTP platforms for online data transfers.

A separate study examined how Bangladeshi internet users create and maintain passwords and compared their practices to the users in the developed nations[13]. Using a survey, the authors gathered information from 75 undergraduate Computer Science students from two different universities in Bangladesh and contrasted it with the responses from the users in developed nations. According to the report, a large number of websites in Bangladesh lack appropriate password security mechanisms. The participants from Bangladesh showed a propensity to use fewer passwords than users from more developed nations. Remarkably, they tended to jot down passwords more often and disclose them less frequently. Furthermore, a discernible trend of infrequent password changes was seen among these individuals. Participants from Bangladesh tended to choose passwords with a lower proportion of personally significant phrases and numbers than those who participated from the first world. A considerable percentage of the users refrained from creating passwords with common Bengali or English terms. This study highlights the weaknesses in these experienced internet users' password management strategies.

2.2 Password Studies in Other Countries

The echoes of local concerns do not fully encompass the broader cybersecurity landscape. One famous work [1] mainly addresses the challenges and proposes solutions for the evolving vulnerabilities in Unix password security. It proposes a solution of a publicly available proactive password checker, aiming to empower users to choose safer passwords based on customize able security criteria. The ultimate goal is to enhance security by automating the process of educating users about password safety. The authors suggest that solid passwords act like strong fences, crucial for keeping potential threats away. The proactive checker proposed in the paper is a significant way to strengthen these digital defenses before any security breaches happen. The paper provides valuable insights, which focuses on evaluating password security practices among e-commerce and news portal websites.

Researchers also look into how users behave in reaction to various policies and how strong the passwords that are created as a result of such policies [6].The study offers a thorough examination of user attitude, behavior, and password strength across five

password-composition policies. After statistically analyzing password predictability, the authors discover that a number of widely accepted notions regarding password strength and composition are not true. In order to generate a number of recommendations for password composition regulations that produce strong passwords without unreasonably burdening users, they additionally connect their findings with user behavior and attitude. The study found that password-composition policies are not as effective as they are believed to be. The authors found that users tend to choose predictable passwords even when they are forced to comply with password policies. The study also found that users tend to use the same password across multiple accounts. The authors suggest that password restrictions should be created to motivate users to select unusual and one-of-a-kind passwords. They recommend that password regulations should be modified to incentive users to utilize passphrases rather than passwords. Passphrases are easier to remember and tougher to guess than passwords. Additionally, the authors advise creating password regulations that motivate users to utilize password managers.

Studying how passwords work is important to make the online world safer. An important research paper looks closely at what makes passwords strong or weak, doing practical tests to see how well they can resist attacks [10]. Moreover, the paper critically evaluates existing password composition rules enforced by popular websites. Emphasizing the collaborative efforts needed from both websites and users, the research not only identifies potential risks but also presents proactive measures to fortify digital data. The things we learn from these works will be a guide for us, helping us figure out the best ways to make passwords more secure on different websites.

To enhance our online security, it's crucial to understand how passwords can be at risk. In a separate work, the researchers [7] aim to highlight the pros and cons of various secure authentication methods, raising awareness about password attacks and the suitability of authentication methods for specific situations. The paper discusses password attacks, classifies password methods from different contributors, and provides a comparative analysis of various authentication methods. This survey advises users to understand password attacks and choose appropriate authentication methods based on their scenario and also suggests combining different password schemes, such as conventional passwords with keystroke dynamics or bio-metrics, for enhanced security. this study contributes valuable insights to our understanding of password vulnerabilities and potential solutions.

A lot of research has been conducted on Computer and Information Security (CIS) in the past years. From a business viewpoint, CIS plays a significant role so it is mainly concerned with protecting confidentiality, integrity, and accessible information when using computer systems. One study examines the password behavior of end-users by using a large questionnaire survey among end-users [3]. The study finds that the human factor is a major vulnerability in computer and information security, particularly in the context of password usage where past researches have given less importance. Users often differ from recommended password practices while making well-protected systems vulnerable. The study comes up with potential solutions such as using mnemonic techniques or graphical passwords, and emphasizes the need for

a balanced approach between human limitations and the quest for profound security. Insights from this study can guide our work by highlighting the importance of balancing human limitations and security measures influencing the implementation of more effective authentication methods, such as multi-factor authentication, with a focus on usability.

Understanding how people use passwords across different websites is crucial for enhancing online security. A study investigates the common practice of password reuse across multiple online platforms. By analyzing leaked passwords from different sites, the research finds that a significant number of users, approximately 43-51%, practice password reuse [9]. Addressing the difficulties associated with this practice, the study introduces a new password-guessing algorithm, surpassing traditional methods. It emphasizes the significance of improving cross-site password security. This research provides valuable perspectives on how people change passwords on various sites, which is important to support overall online security.

After a significant data breach in 2011, a research looked at how people in China create and use passwords [8]. The purpose of this study was to learn how culture influences the choice of passwords. The results indicate that, in comparison to users in the Western countries, many users in China are less concerned with security. Culture has an impact on how people create passwords. Password reuse is a popular practice in China, where users often use the same password across various websites. The study offers insightful information about password usage patterns and user behavior, which focuses our analysis towards possible cultural influences on Bangladesh's digital environment.

In summary, these worldwide research studies provide an overview of several facets of password security. They highlight the importance of proactive measures, cultural influences, and user behavior in fortifying digital defenses. Knowing these things will help us in our study regarding password security procedures on Bangladesh's most popular news portal,e-commerce, and other websites.

2.3 The Password Thicket

Despite years of study exposing its weaknesses, passwords continue to be the primary means of authentication. The solution extends beyond mere users. There is more to the scenario than just people reusing easy-to-guess passwords across devices and surrendering to memory loss. Websites are important, and they are frequently motivated by different goals. A complex web is produced by the need to gather information and promote exclusivity through password registration (even in situations where security isn't the top priority).

Passwords, although responsible for protecting user accounts on the internet, are susceptible to weaknesses arising from both industrial and technological causes. The systems that these precise protections are designed to safeguard, are compromised. This is the exact hindrance covered in the groundbreaking study of Joseph Bonneau and Sören Preibusch. [4].

Through an innovative study involving 150 unique websites, Bonneau and Preibusch reveal the complex intricacies of password usage practices on the internet. Their research presents a startling picture: whereas some websites place a high priority on security, others continue to use outdated methods that provide room for shortcomings. It is important to note that certain websites favor ease of use over security, even using passwords as a means of building psychological trust. This potentially hinders the adoption of more secure alternatives.

The researchers meticulously and precisely examined password-related practices on a range of websites to identify patterns and differences across several categories. Identity, E-commerce, and Content Sites are the three primary categories into which they divided the websites. The researchers were able to capture a broad range of online platforms with unique goals and functions, thanks to their categorization.

The approach of gathering data involved a comprehensive analysis of several password management-related factors. To obtain detailed information, researchers employed a combination of automated techniques and manual inspection. They examined areas such as how to register for a password, what advice to offer during registration, what passwords are required, how to log in, how to support federated identities, how to update passwords, how to recover passwords, how to implement security measures against password guessing, and user probing.

The study also explored the deployment of encryption, specifically Transport Layer Security (TLS), for securing password transmission. The researchers investigated whether websites used TLS consistently in a range of password-related interactions. Critical and in-depth examination of password sharing procedures was also conducted, with an emphasis on whether websites had implemented safeguards to prevent users from disclosing their credentials publicly to platforms such as BugMeNot.

Additionally, the researchers examined password usage practices on a broad range of websites using methodological and comprehensive approach. They used both automated and manual techniques, but statistical analysis gave the observed patterns a quantitative foundation. The study clarifies the complexities of password management in various online settings and provides insightful information for improving security and user experience.

Key observations from this multi-pronged analysis include:

- Inconsistent user experience: Basic password mechanisms were consistent, but security advice and requirements varied widely.
- Security weaknesses: Many sites neglected best practices like TLS deployment, password protection, and protection against guessing attacks.
- Internal inconsistencies: Security policies were often inconsistent within sites, suggesting a lack of intentional design.
- Absence of shared code: Little evidence suggested widespread code sharing for password authentication.

- Varied policies and motivations: Security policies varied more than security requirements, and motivations appeared to differ across industry segments.
- Market factors and security: Market position, growth, technical competence, and type of business influenced password security practices.
- Content sites' focus on data collection: Content sites prioritized email collection and validation over actual password security, suggesting data collection as a primary driver.

This study serves as a guideline for us to conduct the security analysis of different websites in Bangladesh. We examine more websites and use more heuristics than the prior works described in Section 2.1. Additionally, we try to find the relationship between password security and other external factors, mainly related to the economy.

Chapter 3

Heuristics Details

3.1 Evaluation Heuristic Details

We evaluated the 72 websites on the basis of 10 standard heuristics [4]. The following list of 10 essential heuristics provides guidance for evaluating various password security factors for any online service, including the websites in Bangladesh and India.

- H1: Password Construction Guidelines [11]
- H2: Enrollment requirements [4]
- H3: Password Registration [4]
- H4: Login [4]
- H5: Password Update [4]
- H6: Password Recovery [4]
- H7: Federated Identity [4]
- H8: Rate Limiting for Password [4]
- H9: Prevention of User Probing [4]
- H10: Encryption [4]

A brief description on these heuristics are given below-

3.1.1 H1: Password Construction Guidelines

Strong password creation is critical for user account security. Password guidelines, typically presented during registration, outline recommendations and requirements to enhance password strength[2]. These guidelines often address password length and composition. For example, a guideline might specify minimum password length and character type requirements (lowercase, uppercase, numbers, special characters).

Password security is measured by entropy, which reflects the difficulty of cracking a password through various attack methods like guessing, brute-force, and dictionary attacks [5]. Common password composition guidelines include:

- Basic8: Minimum length of 8 characters, no composition requirements (entropy: 18 bits).[6]
- Basic16: Minimum length of 16 characters, no composition requirements (entropy: 30 bits).[6]
- Dictionary8: Minimum length of 8 characters, no dictionary words allowed (entropy: 24 bits).
- Comprehensive8: Minimum length of 8 characters, no dictionary words allowed, composed of uppercase, lowercase, digits, and special characters (entropy: 30 bits) [6]

Displaying password construction guidelines during registration assists users in creating strong passwords and demonstrates the service provider's commitment to security. We have also accessed if there is a password strength meter in order to show whether a password is strong or not. The instruction is presented as a combination of text and image, with the password strength divided into three categories: weak, medium, and strong.

3.1.2 H2: Enrollment requirements

Websites usually ask for some information from the users before they enroll and after the users have submitted the required information, the websites go ahead to validate the information. Some of the information that is usually collected include personal information like name, email address and phone number. Some websites may also ask for the address of the user including the permanent and temporary address, NID, profile picture, and country of residence. After the submission of these data, websites perform validation processes to verify the accuracy of the contact information provided. This verification process usually involves sending a confirmation link to the registered email address or a one-time password (OTP). Or websites may choose to send an account registration notification through email. There are instances where websites use the provided phone number for verification through an OTP or a notification.

3.1.3 H3: Password Registration

Encouraging users to set strong and secure passwords is essential for safeguarding their accounts against potential threats. Websites can significantly enhance security by providing password advice and making it mandatory for users to adhere to these guidelines. The level of restriction imposed by the advice directly correlates with the strength of the password. At a minimum, websites may initiate a length restriction, requiring passwords to be at least 8 characters long. However, to ensure security further, more comprehensive guidelines can be enforced. This includes incorporating a

mixture of lowercase letters, uppercase letters, numbers, and special characters into the password. By mandating such complex criteria, websites can significantly decrease the probability of passwords being compromised through brute force methods.

3.1.4 H4: Login

During the login process the basic credentials required to login includes email or phone number or username along with password. Even though most of the websites usually include the criteria of both email and phone number as personal information, both are not used as identification mode often. Some websites tend to use email as identification and some use phone number as identification mode. Fewer websites also allow users to login both email and phone numbers and also send notification in both. The process of submitting a password involves the user entering the password in order to verify their identity. One of the most basic prerequisites for enabling digital access to systems and services is password submission. To ensure convenience and safety, the method incorporates multiple elements. The user inputs their password in the password area at the beginning of the process. In order to prevent shoulder surfing, this is typically some sort of masked field that displays dots or asterisks in place of the input. The password is entered by the user, and once client-side processing is finished, the data is sent to the server. Security is crucial to preventing hackers from decrypting data. Usually, this is accomplished using: TLS Encryption: It assists in encrypting the password when it is transferred over the Internet between hosts.

3.1.5 H5: Password Update

Password update requires a password update interface. After logging in, whether a website allows its user to update the password in the interface or not is discussed here. In case of updating password, previous credentials are required such as- reentering previous password. Again, there might be websites such as those who sent notifications regarding updating the password. The downside of the password update feature is that an attacker can use a session hijacking technique or even attempt to log in with a browser whose owner is out and change the user's password permanently to a known password. Such a behavior should be of concern, given that some of the sites surveyed allowed users to store cookies on their devices.

3.1.6 H6: Password Recovery

Users may forget passwords due to the sheer number of online accounts they manage. Password recovery mechanisms are essential to address this issue. Common recovery methods involve sending a reset link to a registered email address or phone number. These options are crucial for user convenience and maintaining service accessibility.

3.1.7 H7: Federated identity

Federated identity systems which are also called single sign-on (SSO), are very efficient in providing users with a single identity they can use in different websites. Federated identity is a process where a user authenticates his/her website or an application by using an identity from a third-party service provider like Google, Facebook or Microsoft among others. This minimizes the need for users to remember many passwords and can provide improved security by leveraging quality, secure, authentication services.

The idea of federal identity is based on the trust between the identity providers (IdPs) and the service providers (SPs). At any time when the user wishes to access the service, the SP will forward the user to the IdP for an authentication process. After a successful authentication, the IdP sends an assertion to the consumer SP to show that specific user is valid. It also makes login easier for the users and also shifts the authentication stresses from the SP to IdP which mostly has robust security measures.

Federated identity systems are advantageous for several reasons:

- **Improved User Experience:** Users can enjoy convenient login without having to memorize several usernames and passwords.
- **Enhanced Security:** Working with established IdPs can help enhance security through features like MFA, as well as monitoring for possible frauds and scams.
- **Simplified Management:** It gives service providers the ability to offload the authentication management task to IdP, and also minimize the occurrence of password breach attacks that arise due to compromised password storage databases.

However, federated identity also presents challenges:

- **Privacy Concerns:** This is so because users may be apprehensive about the transfer of their authentication details from one service to another.
- **Dependency on IdPs:** Service providers rely on the availability and security measures implemented by the IdPs.

In specific, federated identity systems present a notable trends towards more user friendly and secure authentication methods, although this novel approach for identity management should be considered and implemented very cautiously due to the risks related to privacy and dependence.

3.1.8 H8: Rate Limiting for Password Guessing

Rate limiting is essential to prevent password guessing from compromising the overall security of the accounts because it can make it unthinkable for an attacker to use a brute force attack by reducing the number of attempts they make to a negligible

amount. Additionally, it prevents credential stuffing by preventing repeated login attempts from users who enter false information and by creating a strong barrier against hackers. Moreover, it aids in defending against "dictionary attacks," which often filter passwords containing common terms. It assists in safeguarding user account login attempts and can sound the alert by bringing about further internal security, such as requesting for an extra password or momentarily locking the account. Furthermore, Rate limitation gives security officers more time to react to possible threats and stop any harm before an attacker gains access. It also makes it easier to notice and respond to suspicious activities.

3.1.9 H9: Prevention of user Probing

Preventing "user probing," which is the act of an attacker making arbitrary assumptions or seeking to confirm whether an account or other piece of information exists on the system, is one of the main obstacles to system security from malevolent attackers. In case of login, enrollment and reset user probing can take place. After providing an incorrect credential in any phase, the error text or explicitly mentioning the particular credential that is incorrect plays a vital role here.
The preventive steps limit the total amount of requests made within a given time frame externally. This holds true, for instance, for account registration, login attempts, and password recovery procedures. Also implement temporary and permanent lock outs. Following a preset number of unsuccessful attempts to log in: Temporarily deny the user's account till they log in. Initially, in order for this method to work, each unsuccessful attempt must result in an extension of the lockout duration. In order to stop automated scripts from accessing the login, registration, and password recovery pages, CAPTCHA should be added to all of these pages.

3.1.10 H10: Encryption

Data privacy is mostly protected by encryption, which is the process of transforming data into a coded format that cannot be read without the right decryption key. It is essential to password security because it protects passwords during transmission across networks using protocols like TLS and hashes them to ensure that they are kept securely. On the other hand, authentication is the process of confirming the identity of users or devices using multi-factor authentication, biometric techniques, and passwords to see if they are authentic and valid. As they give people reassurance and protection against data breaches and unwanted access to their systems, encryption and the usage of authentication discussed above come into play as crucial components in enhancing password security and data security in general.

3.2 Evaluation Process

We assessed the different aspects of the 72 websites to analyze their effectiveness and security measures. Our primary objective was to assess the efficiency and reliability

of key website functions such as enrollment, login/logout, password update, password reset, and password probing across different platforms. We used a combination of evaluation methods to offer insights into the strengths and weaknesses of these critical aspects of website security. The following sections present detailed descriptions of our evaluation process which we implemented in order to have a thorough understanding of the security landscape of these websites [4].

3.2.1 Enrolment-

All user data such as pseudonyms, email IDs, and passwords was generated using identical fake user data. The recipients were all signed with their unique postal addresses at each location, ensuring that any subsequent emails would be tracked to the correct location. All password advice provided to the user prior to registration, as well as any information required to create the account, would be kept on record [4].

3.2.2 Login/Logout-

Once the email address is verified (if necessary), the email is signed up and then the account is logged in and logged out. In regular login, the TLS record and details were shown if present, along with the data submitted to the server; and the persistent login cookie saved in the browser was shown. After the login the pages were checked out for the details that the particular account was enabled to access [4].

3.2.3 Password Update-

After signing in again, it is noticed that passwords can be changed through a separate "Change Password" interface. This is when the testers checked for password requirements by putting figures to the passwords that would be accepted. Level one is where one tries to register with a short password that is three digits in length. A one-character password 'P' rejected resulted in 'P^n' form to be concatenated for each specific case n until the established minimum length was assumed. The upper bound test is not done but the upper bound is recorded only if it is mentioned explicitly in the site.After testing length boundaries, attempts were made with the passwords "1234... n" and "password." In the vast majority of cases, if they were considered appropriate, it was presumed that the site was imposing no limitations except from those related to length. Attempts were made to surpass these filters by using passwords of a different complexity, and then rules were implemented including alphabets, numbers, non-dictionary elements and so on. Lastly, a tried password that was previously used was set for the password history test performance. An email account was looked at in the post update to see whether a message was sent regarding a password change [4].

3.2.4 Password Reset-

After the password was changed, the account was logged off once again. Initially, it was tested if the feedback was provided to differentiate a valid username and invalid password or invalid username. Afterwards, the password reset procedure was started. Generally, this was done by sending an email with either the original

password, a new temporary password or a reset link; or by OTP in phone number or email. These were then used to log in one last time to the account to see if a password update was forced after completion of the protocol [4].

3.2.5 Password Probing-

After the password was changed, the account was logged off once again. Initially, it was tested if the feedback was provided to differentiate a valid username and invalid password or invalid username. Afterwards, the password reset procedure was started. Generally, this was done by sending an email with either the original password, a new temporary password or a reset link; or by OTP in phone number or email. These were then used to log in one last time to the account to see if a password update was forced after completion of the protocol [4].

BD Ecommerce	**BD Government**	**BD Content**	**IND Ecommerce**
Aarong	Bangladesh Scout	Prothom Alo	MobileGo
Banglashoppers	Police Clearance	Daily Star	Himalaya
Startech	NBR E-learning	RTV	Click on Care
Robishop	BD Computer Council	NTV Online	My Indian Brand
Agora	NWPGCL	Amader Shomoy	Industry Buying
Trade Bangla	MyGov.bd	Bonikbarta	Joy by Nature
Daraz	Digital Service Portal	Daily Nayadiganta	Indiamart
Unimart	Muktopath	Somoy News	Make My Trip
Shopno	Career Portal Service	BanglaNews24	Firstcry
Bikroy	National E-Procurement	BDNews24	Desi Hangover
Othoba	VAT Online	Bangla Tribune	Dablr Shoes
Foodpanda	RAJUK	Dhaka Post	BlinkStore
Ryans Computer	E-recruitment	Daily Inqilab	
Ajker Deal	OSSPID	Samakal	
Smartdoko	Teletalk	KalerKantho	
Chaldal	NID	Jugantor	
Rokomari	Import and Exports	Bangladesh Pratidin	
ClickBD	Teachers Govt	The Daily Ittefaq	
Pickaboo	Bangladesh Railway	JagoNews24	
Techland	LIMA	The Business Standard	

These are the websites that has been analyzed, and they are categorized into distinct columns. These columns represent e-commerce, content, government, and Indian websites, respectively.

Chapter 4

Findings

In our evaluation of the different website functionalities, we collected data and conducted analyses on them to find out trends and results of the operational mechanisms and security protocols of the websites but there was an issue: among the 72 websites(Bangladeshi e-commerce, Bangladeshi content, Bangladeshi government and Indian e-commerce sites) studied, we observed that while all 20 e-commerce websites allowed user registration, only 2 out of the 20 content websites offered this feature. The main sign up method in the content websites was to use federated identity. This is a clear indication that there are differences in the strategies that various website categories employ in terms of user interaction and account sign up. The e-commerce websites are selected on the basis of highest traffic the websites ha sin that month. The website SimilarWeb[14] is used to determine the traffic and highest ranks. The government website list was taken from the paper "A Study of Password Security Factors among Bangladeshi Government Websites"[11]. According to the ranks the websites that allowed to create accounts are evaluated. The evaluation time frame was from October,2023-June,2024. In case of Indian websites after inspecting more than 110 websites only 12 websites could be selected because evaluation could be done of those websites which allowed us signing up using email address. Due to limitations regarding access of Indian phone numbers most of the renowned websites could not be evaluated.
The subsequent sections provide a comprehensive description of the data collection process and the results obtained in case of Bangladeshi e-commerce, Bangladeshi content, Bangladeshi government and Indian e-commerce sites.

4.1 H1- Password Construction Guidelines

Password complexity guidelines are rules defining the minimum strength requirements for passwords enforced by websites to mitigate hacking risks. In the analysis of 72 websites examined, we observed a diverse range of approaches to password complexity. We established a classification system (PG-1 to PG-6) to categorize password complexity requirements [11] as follows:

- PS: No specific guidelines were provided, potentially leaving user accounts vulnerable.
- PG-1: Minimum of 4 characters (relatively weak).

- PG-2: Minimum of 6 characters.
- PG-3: Minimum of 6 characters with mixed complexity (including uppercase and lowercase letters, numbers, and symbols).
- PG-4: Minimum of 8 characters.
- PG-5: Minimum of 8 characters with mixed complexity.
- PG-6: Minimum of 8 characters with high complexity (including letters, numbers, and special characters).

4.1.1 E-commerce Websites

A much smaller number of websites (only 2, representing 5% of the total websites) did not have any password complexity requirements (PS), potentially leaving user accounts vulnerable. In some cases, only 1 website (or 2.5% of the total) opted for alternative methods of account verification, such as sending one-time passwords (OTPs) or creating system-generated passwords for users. Interestingly, a significant portion of websites (18 out of 40, or 45%) did not offer user account creation at all. These websites were all from the newspaper category. E-commerce websites demonstrated a stronger focus on password security. Among the 20 e-commerce websites examined, the majority (17 out of 20, or 85%) enforced password complexity guidelines during user enrollment. These guidelines mandated a minimum password length, with 3 websites (15%) requiring a minimum of 8 characters with mixed complexity (PG4-6), similar to Bangla Shoppers, which enforces a strong password policy of PG6 requiring at least 8 characters with a minimum of two-character classes (lowercase letters, uppercase letters, digits, or special characters) as shown in Figure 4.1. A larger portion (9 websites, or 45%) allowed for slightly weaker passwords with a minimum length of 6 characters (PG2), some of which also required mixed complexity (PG3). The remaining 5 websites (25%) allowed for the weakest passwords of 4 or 5 characters (PG1) with varying complexity requirements.

4.1.2 Bangladeshi Government Websites

The analysis of password construction guidelines across 20 government websites reveals significant variations in security practices. Out of the 20 websites, 8 websites (40%) enforce a minimum password length of 8 characters. Among these, 5 websites (25%) require high complexity passwords, including uppercase letters, lowercase letters, digits, and special characters (PG6). These websites include Bangladesh Computer Council, Bangladesh Scout, MyGov.bd, Police Clearance, and National E-Government Procurement. The remaining 3 websites mandate mixed complexity, requiring combinations of letters and numbers (PG5), such as Rajuk, E-Recruitment, and VAT Online. Meanwhile, 9 other websites follow a slightly lower standard, requiring a minimum length of 6 characters with mixed complexity (PG3). These websites include the Career Service Portal, DPDC Career Portal, and North-West Power Generation Company Limited (NWPGCL). Notably, 1 website, NBR E-Learning, lacks both a length restriction and password complexity guidelines (PS), potentially leaving user accounts vulnerable. Across all the examined websites, there is

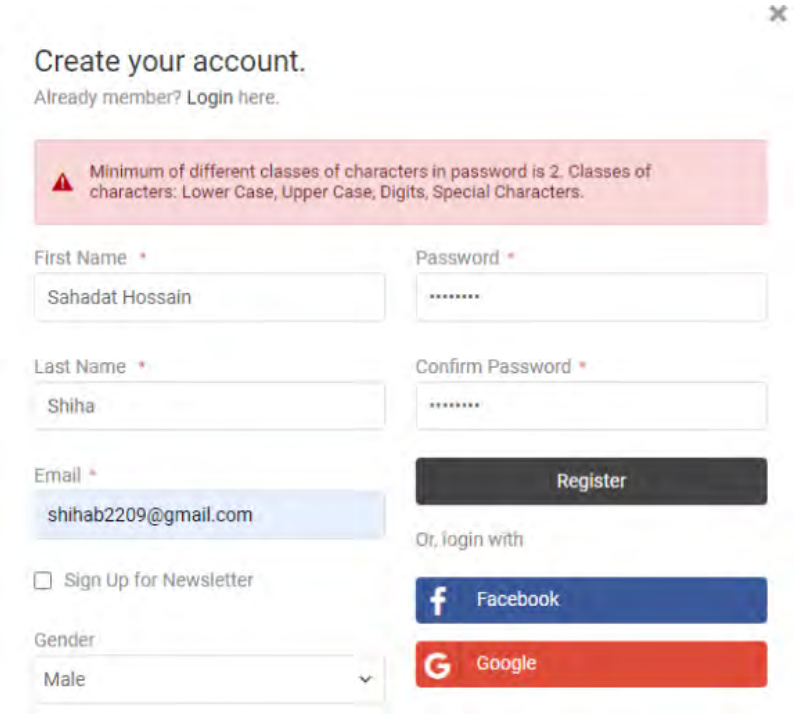


Figure 4.1: Example of Password Policy at Bangla Shoppers

no restriction on the use of dictionary words, indicating room for improvement in strengthening password security policies.

4.1.3 Indian E-commerce Websites

The analysis of 20 Indian e-commerce websites shows a notable divergence in password security practices. The most commonly enforced password length across the websites is 5 characters, which aligns with (PG1-2) in our classification system. Only 2 websites, My Indian Brand and Make My Trip, require a minimum password length of 8 characters with high complexity (PG6), including uppercase letters, lowercase letters, numbers, and special characters. Additionally, Blinkstore and FirstCry do not provide an option for password setup, while Indiamart has a password setup interface but does not mandate any length restriction or password guidelines (PS). While most websites fail to impose strict password requirements, none of the analyzed sites restrict the use of dictionary words, further highlighting the need for enhanced password policies to safeguard user accounts from potential attacks.

4.1.4 Newspaper Websites

Newspaper websites stood out for their lenient password security practices. Only a very small proportion (2 out of 20, or 10%) enforced any password complexity guidelines during user enrollment. This is concerning as it weakens account security and leaves user accounts vulnerable to hacking attempts.

Although the usage of passwords as a security feature is critical, only one site (Foodpanda) of the research had a password meter inside the registration process. Only two websites show the password strength meter during password update operation but it does not show the meter during registration phase. However, no content websites practice the use of password strength meters.

Website Category	OTP	PS	PG-1	PG-2	PG-3	PG-4	PG-5	PG-6
E-commerce	1	3	4	5	4	2	0	1
News Portal	0	0	0	0	0	1	1	0
Government	1	1	0	0	10	0	3	5
Indian E-commerce	0	0	7	0	1	0	0	2

Table 4.1: Password Guidelines

4.2 H2: Enrollment Requirements

4.2.1 Personal Data Collected

All of the E-commerce websites collected personal data of their users. The most common of which were name, phone number and email address, collected by 6 websites (30%). More detailed information included Date of Birth, gender, address, profile picture. Among content websites, only 2 (10%) of them stored personal details of their users in which both collected mail, number and phone number. Any notification from these websites are usually sent in users' mail.

The analysis of enrollment requirements across 20 government websites reveals that all of them collect personal data. The most commonly gathered information includes name, email, date of birth, mobile number, and address. For instance, the Bangladesh Scout and Police Clearance websites collect essential data such as first name, last name, email, and phone number. In contrast, the North-West Power Generation Company Limited and NBR Learning gather more detailed personal identifiers, including NID numbers and additional demographic information like gender and religion.

In the analysis of enrollment requirements across 12 websites, it was found that the majority collect personal data during the registration process. Specifically, 10 out of 12 websites collect personal data, resulting in a percentage of approximately 83.33%. The most commonly collected personal information includes first name, last name, and email address, which are gathered by nearly all the websites. However, Dablrshoes stands out by collecting more detailed information, including birthday, gender, marital status, address, and postal code.

4.2.2 Email Verification

After the completion of the enrollment process, most sites immediately sent an email to the specified account. Among these, 12 (60%) sites sent an account sign up notification or a link to verify the account. Some of these sites also send an OTP instead of a verification link. It is interesting to note that the distribution of sites mandating email verification is as follows: 12 e-commerce sites, and 2 content sites. Among the content websites, Prothom Alo used mail verification whereas Daily Star used phone number verification after enrollment. It is important to note that websites of Bangladesh are heavily reliant on phone numbers for verification, besides email. A few websites used phone numbers to send notifications or OTP but verification links were only sent in email. All the websites do not exhibit the trend of email addresses taking the place of usernames. Even the display of username in websites is not frequently seen. 7 of the websites displayed the username in the account.

Regarding email verification, all 20 websites send a verification link, notification, or OTP after account registration, ensuring that users confirm their identities. However, five websites, including MyGov.bd, DPDC, and VAT Online, utilize phone numbers for verification instead of email. This approach enhances security by requiring users to verify their accounts through a method that is often more immediate and accessible. Notably, websites like Bangladesh Computer Council and National e-Government Procurement send notifications through both email and mobile, providing a dual-layer verification process that further secures user accounts. 11 websites have a tendency of using username in their website. Interestingly, some websites have also used NID or gmail instead of using user names.

Regarding email verification, 9 websites send a verification link or notification after account registration. These websites include Himalaya, Dablrshoes, Industry Buying, and MakeMyTrip, among others. Among them, 2 websites utilize phone numbers for verification instead of email, specifically BLINKSTORE and MakeMyTrip. Additionally, MakeMyTrip is notable for sending notifications via both email and phone number, ensuring a dual verification process for enhanced security. This analysis highlights the differing practices in personal data collection and email verification across the websites, underscoring the importance of secure enrollment processes. Almost 50% of the Indian websites have displayed username in their websites which is higher compared to Bangladeshi e-commerce and government websites.

4.3 H3: Password Registration

4.3.1 Advice Given

It is known that users are more likely to and bound to create stronger passwords when password construction advice is provided. Even then, only 4 out of 20 e-commerce websites (20%) provided advice, while this number for content websites is even less. Only one website, which is the Prothom Alo, suggested password advice for its users. The advice given in content websites offered more variations such as uppercase letter, lowercase letter, special character along with the more common

advice - mixture of numbers and letters. For a content website, the advice is very generic- to only use letter + number. For government websites, the advice given is seen more as almost half of websites(12 out of 20) have different password advice including using uppercase letters, lowercase letters, numbers and special characters. For Indian websites, the number of websites which have given advice for password formation is 16%(2 out of 12) which is comparatively lower than the other mentioned categories.

4.3.2 Password Requirements

None of the E-commerce websites and Content websites prohibited the use of dictionary words. The websites accept predictable dictionary words such as “password”, “strong”, “123456”. Apart from length restriction, other more complex requirements were relatively rare, only 4 sites implemented the necessary use of both letters and numbers. Among these, only 2 mandated using uppercase, lowercase letters and digit while only one website: Bangla Shoppers enforced using at least one special character, and merely 2 sites necessitating the presence of non-alphanumeric symbol characters.
In government websites as 12 of them have given password construction guidelines, Among them 8 websites have mentioned the use of uppercase letters or lowercase letters or both of them. Again 6 websites have mandatory special character usage in case of forming passwords. The common advice- mixture of numbers and letters is also seen here. The variation of password requirements is seen more in government sites than e-commerce websites. All the websites have allowed the usage of predictable dictionary words like “password”, “strong”, “123456”.

In the Indian website category, among 12 websites only 2 websites have explicitly mentioned the use of number, letter and special character. Other 10 websites did not provide any instruction.2 websites(Blinkstore and FirstCry) did not have any password system; they are accessed through one time OTP which is sent to the email address or phone number. Every website permits the use of common vocabulary terms such as ”strong,” ”password,” and ”123456.”

4.4 H4: Login

4.4.1 Identification

Contrary to expecting users to use a username specific to the site, the majority of the e-commerce sites (100%) allowed users to identify themselves while signing in with the use of Email address. While passwords are still being collected, it seems that sites are accepting the fact that users have too many accounts that require unique usernames for each one and this is evidenced by the shift to the use of email addresses for username. However, as we can see passwords continue to be gathered at the same time websites seem to understand that users have too many identities to remember unique handles for each site, as evidenced by use of e-mail as handles instead of unique usernames. The common pattern noticed in this case is that all

the websites did not allow login using username.

In the government website category, similar pattern is notice where all the government websites allowed users to login with their email. But in this area the dependency of phone number is more. Websites like VAT ONLINE allowed users to login to the site using phone number. Even the notification sent in phone number is more in this case.

In the case of Indian websites, the majority of websites(91%) have used email addresses as their mode of identification. Only one website(FirstCry) has the option of sending OTP to either email Address or phone number .

The pattern of username being used instead of phone number and email address is not common in Bangladesh as well as India.

4.4.2 Password Submission

The majority of the websites tested collected passwords during routine login using an HTML input=text form element. At any point, four websites allowed password submission into an unstarred input=password element. Some of the websites displayed input=hidden in those cases the inform form cannot be known. Again, there was mixed success with TLS deployment to secure password submission. Majority of websites using TLS have TLS deployment to secure password submission of the users. POST action in login form is present in almost all the websites except for 3. Among them two are content websites that do not allow password update.

In the government website category, 11 websites have allowed password submission using HTML input=text form element. The percentage of HTML input=text form element and unstarred input=password element is almost 50-50 in this category. A few websites have given input=hidden which is not a high number. The rate of TLS deployment is very high in ethos category. 18 out of 20 websites have TLS deployment in their websites for secure password transmission. Bangladesh Scout has no encryption for password transmission. Only one website(NBR eLearning) has used QUIC for secure authentication.

In the Indian website category, Only three websites—testing, collecting, and employing an HTML input=text form element—collected passwords during ordinary login. On a significant number of websites, the input form was hidden. The number of TLS deployment in case of securing password submission is less in Indian websites. Almost 58% of websites have used QUIC for secure password submission of the users.

4.5 H5: Password Update

The majority of the e-commerce sites incorporated an interface for resetting the password which can be changed to a new log-in value. Among them only 2 websites included password strength meters in their update interface. Still it had is-

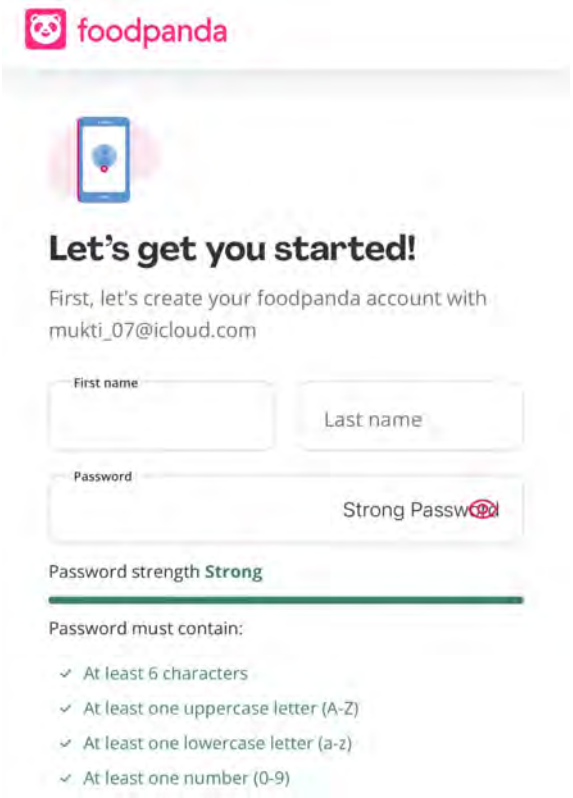


Figure 4.2: Foodpanda Password Strength Meter

sues such as- considering passwords like: password: carboncarbon → very strong, password:carbon123456→ strong, password: carbon123412→ very strong) . Interestingly, this changes the behavior of the sites: only 3 sites did not allow password updating in the update interface, instead using the password recovery mode to allow users to update their own passwords. Among the 3, 2 of them were content websites. The 2 content websites that allow us to login do not have any password update interface.

Majority (17, 89%) of the e-commerce sites demand entry of an existing password before that can be changed as a defense mechanism against this, and it is several times more likely that newspaper sites would require it but they did not use it. Only 1 website sent OTP to the phone number of the account holder in order to update the password. A total of 4 e-commerce sites attempted to notify the account owner of a change in passwords thereby sending an email to the account holder. Retail sites that ran online as a part of their business were found to be increasingly preferable to this specific strategy. Bangla Shoppers sent a message in the email after password update: "Your Bangla Shoppers password has been changed". Most of the websites only had a popup after updating the password.

In the case of government websites, most websites provide a password reset page that allows users to modify their log-in credentials. It's worthy to note how this alters the behavior of the websites: only 10%(2 websites) prevented users from changing their passwords via the update interface, allowing them to do so via the password recovery option. Only 3 websites altogether made an attempt to send the account holder an

email informing them of a password change. Most websites send the notification if the account is created using a phone number. In a website named Police clearance it did not maintain the password requirement criteria and allowed passwords with any length. My Gov.bd sends OTP through a phone number which is different from the other websites.

In Indian websites the rate of websites allowing password update is less. Out 0f 12, 8 websites did not allow users to update their password as they did not have an interface. The rate is 66% which is higher compared to other categories.Only one website(My Indian brand) has informed the account user after password update Interestingly, IndiaMart does not have a signup interface. Rather after logging in with a one time OTP it allows the user to create an account using password which can be named as an update interface.

4.6 H6: Password Recovery

Other than four sites the remaining pages have methods of password recovery in case a person forgets the password. Aarong and BanglaShoppers are the websites when previously checked had the option for password recovery but in recent times while checking it again a problem was found that for password recovery the reset link was never sent to the email address. The same problem occurred with the website Techland where they did not send any recovery link in the email. Secondly, a website named Unimart had an issue with password recovery too, so whenever a forgotten password was clicked it showed "500 Something went wrong. Looks like the server failed to load your request". Thus, this site also has no password recovery mechanism. The password recovery mechanisms that our websites follow are mostly email based recovery, out of 20 e-commerce websites 8 sites have the email based recovery, 3 of them have both email and phone no. based recovery and 5 websites have only the phone number based recovery. So, total 16 of the e-commerce sites have a recovery mechanism and as mentioned above 4 of the websites have none. Again, in terms of content websites only 2 were evaluated as the other 18 had no account creating system. Those 2 sites also had the email based recovery method only. So, in total out of 22 websites evaluated "e-commerce and content" together, 15 websites follow the email based recovery method.

In government websites, the password recovery feature is available on 17 websites. In the Police clearance website it sends randomly generated passwords(numerical code) for recovering passwords through phone number or email address.

In the case of Indian websites, The rate of websites not allowing recovery is higher that is 83%. Two websites(Blinkstore and FirstCry) does not support any password system so recovering phase does not work in these websites.

Password Recovery	Content	Ecommerce	Government	Indian
Reset	2	16	17	10
Email Only	2	8	7	10
Phone number	0	5	7	0
Email & Phone number both	0	3	3	0
None Available	18	4	3	2

Table 4.2: Password Recovery Identification

4.6.1 Email Based Recovery

As it is mentioned above that most of the websites follow email based recovery mechanisms. 8 websites out 20 e-commerce which is 40% of the e-commerce websites only follow email based recovery method. Basically, the email-based recovery contains recovery mechanisms like Cleartext, Random Passwords, OTP(One Time Password) and reset link. Here, 6 of the websites provide reset links for password recovery which is 35% out of the 20 e-commerce sites. 2 of the websites provide OTP in the email which is 10% out of 20 ecommerce sites. Furthermore, a website named startech gives a random generated password and Agora provides cleartext through email. Moreover, the 2 content sites that have been evaluated give a reset link to the email.

For government websites, Only emails are used as a recovery technique on 40%(8 websites) of government websites. OTP (One Time Password), reset links, random passwords, cleartext, and other recovery procedures are essentially included in the email-based recovery. Out of the 20 government websites, 4 of them offer reset links for password recovery. This represents 20% of the total. 5% out of 20 government websites, or 1 of them, provide an OTP by email.

In Indian websites the number of Email based recovery is the highest. 10 websites use email based recovery method that means they sent the reset link in the email address.

4.6.2 Phone Number Based Recovery

Phone number based recovery mainly takes place by giving OTP that was given to the provided number to reset the password. Out of 20 e-commerce sites there are only 5 sites that use the Number based recovery method which is 25% of the 20 e-commerce websites. Again, none of the content sites uses the number based recovery.

For government websites 8 websites have allowed phone number based recovery system which makes 40% of the total number.

In Indian websites, Not even a single website of the total of 12 e-commerce websites,

employs the number-based recovery strategy.

4.6.3 Email and Phone number Based Recovery

3 of the e-commerce sites have both Email and Phone number based recovery methods that is 15% of the 20 e-commerce sites. Two of them provide OTP to both email and phone number and the other gives a randomly generated password.

Similarly only 3 government websites have used both email and phone number as a recovery system that makes up 15% of the government websites. All three of them has sent OTP in the phone number and reset link to the email address.

In Indian websites, Of the 12 Indian e-commerce sites, no websites opted for recovery options based on both phone number and email.

4.7 H7: Federated Identity

4.7.1 Analysis of Federated Identity Adoption Across Bangladeshi Websites

Federated identity systems, also known as single sign-on (SSO), offer users the convenience of accessing multiple platforms using credentials from a trusted third-party provider, such as Google or Facebook. This analysis evaluates the adoption of federated identity among 60 websites in Bangladesh, including e-commerce platforms, news portals, and government websites.

4.7.2 Limited Federated Identity Support

Overall, support for federated identity remains scarce across Bangladeshi websites. Out of the 60 websites analyzed, only 21 (35%) provide users with the option to register or log in using a federated identity provider. Popular platforms like BIKROY.COM (Figure 4.3) offer federated login options through Google and Facebook, enabling users to bypass the traditional account creation process.

4.7.3 E-Commerce Leads the Way

Federated identity adoption is most prevalent within the e-commerce sector, where 85% (17 out of 20) of the surveyed websites support login through platforms such as Facebook, Google, and Instagram. This demonstrates the sector's focus on streamlining the user registration process to enhance user experience and boost engagement.

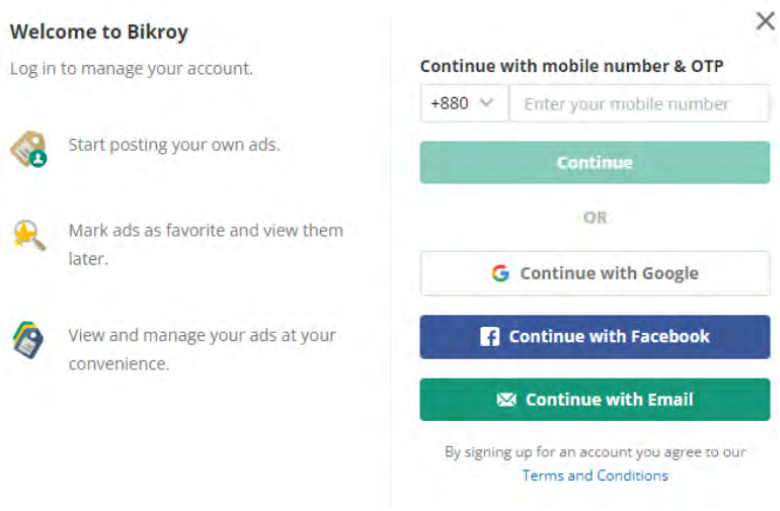


Figure 4.3: Example of Federated Identity Login Option on BIKROY.COM

4.7.4 News Portals Lag Behind

In stark contrast, only 10% (2 out of 20) of news portals provide federated identity options. Notably, many news portals do not offer any account creation mechanism at all. This lack of user authentication suggests that news portals are lagging behind in both adopting user-friendly features and securing user data through federated identity.

4.7.5 Federated Identity Adoption in Government Websites

Our evaluation of 20 government websites reveals even lower adoption rates. Only two websites, including Muktopaath and OSSPID, support federated identity through third-party providers like Google, Facebook, and LinkedIn. However, the remaining 90% of government websites rely solely on traditional login methods. This reluctance to adopt federated identity may be attributed to concerns over data privacy, security, or dependence on legacy systems.

4.7.6 SSO Adoption in Indian Websites

In the evaluation of Indian websites, SSO adoption is equally limited. Only 2 websites out of the 20 analyzed support SSO, showing a similar hesitation towards adopting third-party login methods.

4.8 H8: Rate Limiting for Password Guessing

4.8.1 Rate Limiting Practices Across Bangladeshi Websites

Rate limiting is a key security measure designed to protect against brute-force attacks by limiting the number of incorrect password attempts allowed within a specific

period. This section examines the adoption of rate limiting mechanisms across e-commerce, news, and government websites in Bangladesh.

4.8.2 E-Commerce and News Portal Analysis

Among Bangladeshi e-commerce websites, 55% (11 out of 20) do not implement any form of rate limiting. Websites such as Daraz and Ajkerdeal allow unlimited password guessing attempts, leaving them vulnerable to brute-force attacks. Conversely, 45% of e-commerce websites, such as Chaldal, enforce rate limits, locking accounts after multiple incorrect attempts. For example, Prothom Alo enforces rate limits, while The Daily Star does not implement this security measure.

4.8.3 Rate Limiting in Government Websites

Rate limiting adoption within government websites presents a mixed picture. While 55% of the government sites we analyzed do not enforce any limits on password guessing, certain websites, such as the Police Clearance portal, lock accounts after five incorrect attempts, gradually increasing the lockout duration with each failure. Websites like Bangladesh Railway implement stricter policies, blocking access entirely after four incorrect attempts.

This inconsistency in security practices reveals that many Bangladeshi government websites fail to fully implement rate-limiting protections, potentially exposing sensitive information to attacks.

4.8.4 Rate Limiting in Indian E-Commerce Platforms

Indian e-commerce websites display a more widespread adoption of CAPTCHA as a mechanism for limiting password guessing attempts. However, a significant portion, 75%, do not enforce proper rate limiting, leaving them vulnerable to attacks. High-traffic platforms like MakeMyTrip implement more stringent policies, locking accounts after five failed attempts and requiring a password reset, similar to the more secure Bangladeshi e-commerce sites.

While rate limiting practices are increasingly common among high-profile websites in both Bangladesh and India, the inconsistent enforcement across various sectors—particularly in government and content websites—poses a significant security risk. The e-commerce sector, both in Bangladesh and India, shows similar trends, though the implementation of CAPTCHA and stricter enforcement on major platforms in India provides a slightly better defense against brute-force attacks.

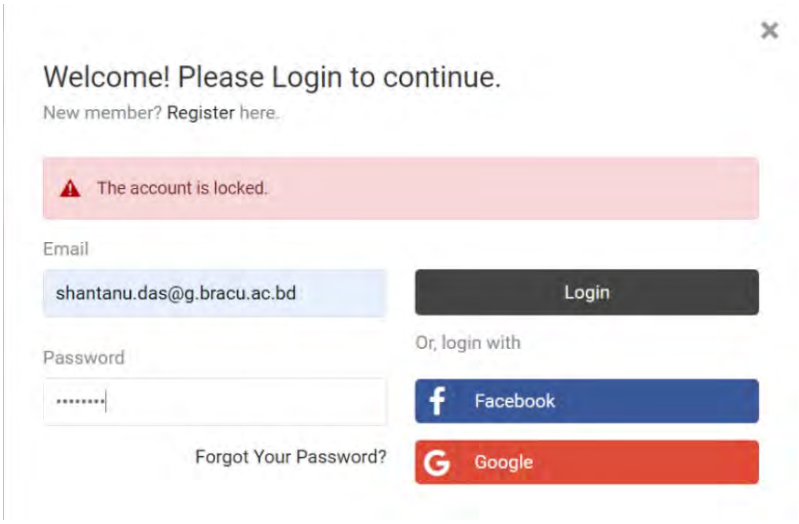


Figure 4.4: Rate Limit for Password Guessing

4.9 H9: Prevention of user probing

There has to be a mechanism which ensures that attackers do not know or understand the registered email address or phone number of users because it is not wise to allow users to have ease while registering themselves to use such sites. This method reduces the user probing attack where a hacker uses a lookup file to enter various passwords into any website. However, users, also reuse their email addresses and/or telephone numbers on many platforms making the situation more serious if these credentials are leaked in the login process of one service. For example, if someone wants to penetrate Bob's account on platform A, they search for the site where he has access on B, C, and D. That gives the attacker the ability to employ the same credentials for multiple accounts if Bob reuses passwords. This implies that websites have to isolate mechanisms that can easily be exploited by hackers to start attacking the accounts by email or phone identification. We have examined several interfaces that can be exploited for such probing: login/register, authentication and password retrieval.

4.9.1 Login

Bangladeshi E-commerce and Content Websites: If there is no correlation between the provided data and an inaccurate identity or an invalid password, user probing can happen via the login screen. After entering a particular email address, 3 websites assure us if the email address provided is valid or not. Majority(17) of websites displayed a general error message either for incorrect email address or incorrect password. It appears that most sites either consider this kind of probing to be a serious threat or believe that the easiest way to implement it is to use a general error answer, based on the general opposition to it. Noticeably one website(Food panda) implemented CAPTCHA in their login interface. After providing incorrect credentials it demands to solve the CAPTCHA.

Indian E-commerce Websites: In the analysis of CAPTCHA implementation

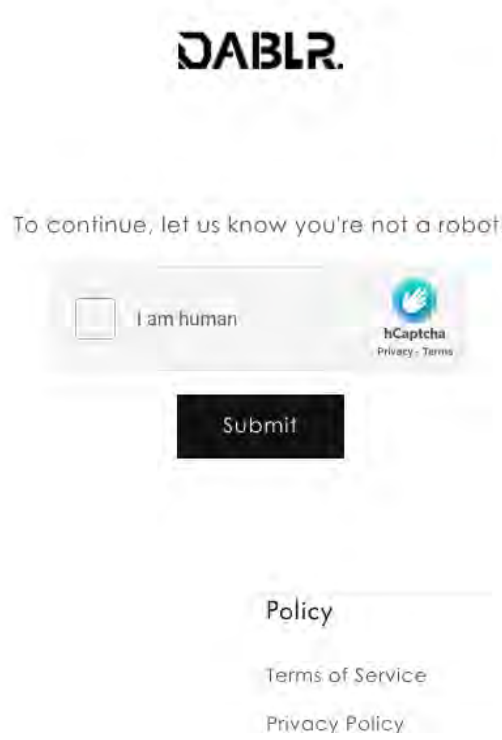


Figure 4.5: Dablrshoes locking the website after 5 unsuccessful tries

among Indian websites, it was found that most of the websites do not utilize as a security measure. Only FirstCry, DesiHangover, Dablrshoes uses the CAPTCHA system in the login and registration phase.. This means that about 33% of the websites employ CAPTCHA during the login phase and registration, indicating a moderate level of security in this critical area where user credentials are entered. Additionally, effective prevention of password probing is crucial here as continuous password probing can lead to a CAPTCHA detection system. If an attacker can determine valid email addresses or usernames, they may engage in attempts to guess passwords of all other websites.

Bangladeshi Government Websites: The analysis of CAPTCHA implementation in the login phase reveals that 5 out of the 20 government websites (25%) utilize this security feature. The websites that incorporate CAPTCHA during login include Bangladesh Computer Council, NBR Learning, MyGov.bd, VAT Online, OSSPID. However, a significant majority, 15 websites, do not employ CAPTCHA in this phase, which raises concerns about their vulnerability to brute force attacks but some of the websites do have a mechanism for brute force attacks as they block the login page after multiple login attempts. The absence of CAPTCHA in the login phase for many websites indicates a potential risk for unauthorized access to user accounts.

4.9.2 Enrolment

Bangladeshi E-commerce and Content Websites: This is essentially a basic issue because websites that provide free accounts have to verify with users whether

their accounts were effectively activated.By completing a CAPTCHA before confirming whether an identifier is available for a new account, this probing point can be reduced. Likewise, the very structure of webmail services exposes a user probing facility by default. Instead, the majority of websites offered immediate notification of the IDs' availability. 3 websites do not use any kind of identifiers even though one of them uses CAPTCHA. Most of the websites(17) use Identifiers but among them the use of CAPTCHA is very less. Among 22 websites including e-commerce and content sites, only 2 websites implemented CAPTCHA in their restriction phase. One is an e-commerce site and another one is a content website.

Indian Ecommerce Websites: During the enrollment phase, only two sites, DesiHangover and Dablrshoes, provide CAPTCHA protection. This accounts for approximately 17% of the websites having CAPTCHA during the enrollment process. The limited use of CAPTCHA in this phase raises concerns, as it is essential to secure user registration against automated attacks that could compromise personal data. By confirming account identifiers without sufficient protection, these sites remain vulnerable to password probing, where attackers can test multiple passwords against valid usernames.

Bangladeshi Government Websites: In the enrollment phase, 7 websites (35%) implement CAPTCHA to enhance security against automated registrations. These websites are Bangladesh Computer Council, NBR Learning, MyGov.bd, DPDC, VAT Online, National e-Government Procurement, and LIMA. While this demonstrates a proactive approach to safeguarding the registration process, 13 websites still lack CAPTCHA in this phase, which could allow for the possibility of automated bots creating accounts. The implementation of CAPTCHA during enrollment is crucial for ensuring that only legitimate users can register.

4.9.3 Reset

Bangladeshi E-commerce and Content Websites: Resetting the password for a target identifier is another way for attackers to test the password reset interface. In order to prevent password probing, none of the websites use CAPTCHA in the reset interface. Around 14 websites explicitly provide information on whether the email address provided is valid or not. Only 4 websites do not provide any information regarding this. The other 2 websites provide an error text. Protected login and enrollment is seen in few of the websites. Not even a single website implemented a protected reset.

Indian E-commerce Websites: In the password reset phase, only Dablrshoes implements CAPTCHA, representing about 8% of the total analyzed websites. The absence of CAPTCHA in the password reset phase is particularly concerning, as it is a vulnerable point where users may be targeted for unauthorized access. Many sites explicitly indicate whether the email address provided is valid, which can further facilitate password probing. Overall, Dablrshoes is the only site that provides CAPTCHA across all three phases (login, enrollment, and password reset), while several other sites do not implement CAPTCHA in any phase. This highlights a

significant gap in security measures that could expose user data to potential threats.

Bangladeshi Government Websites: The password reset phase shows that 5 websites (25%) utilize CAPTCHA to secure this critical process. The websites that incorporate CAPTCHA in the password reset phase include NBR Learning, My-Gov.bd, DPDC, VAT Online, and Bangladesh Scout. Despite this, 15 websites do not employ CAPTCHA during password resets, which could expose users to risks of unauthorized password changes. The lack of CAPTCHA in this phase is particularly concerning, as it is essential for preventing malicious actors from easily resetting passwords and gaining access to user accounts. Overall, the inconsistent use of CAPTCHA across these phases highlights the need for improved security measures to protect user information effectively.

4.10 H10: Encryption

TLS is a vital tool for building secure communication channels over the internet through encrypting information between the user's browser and the server. The study examines the use of TLS across various password entry forms: registration, logging in, password change, and changing password after reset.

4.10.1 Bangladeshi E-commerce and Content Websites:

The research on TLS implementation across different password entry forms (enrolment, login, password update, and password retrieval) and there were found to be considerable gaps among how the websites safeguard customer data. Of 20 e-commerce store websites assessed, 65%(13 websites) had implemented TLS to absolutely cover all authentication forms, whereas 35%(7 websites) of them did not offer this service at all, which might result in high security risks. TLS certificate take up was higher in e-commerce sites than content sites; given that these sites need to provide secure mechanisms for online payments. Among these 13 websites, only 4 of them are using an older version (TLS 1.2) and the other websites are up to date. For content websites, only DailyStar is using TLS version 1.2.

4.10.2 Indian E-commerce websites:

The analysis of encryption practices across Indian websites evaluated various protocols and encryption standards to determine the level of security implemented for user data protection. A total of 5 websites utilize TLS for secure communication. Some websites implement TLS 1.3, while others use TLS 1.2. Notably, a few websites do not implement any TLS encryption at all. This results in approximately 41% of the websites employing TLS, indicating a significant commitment to secure data transmission.

In terms of the QUIC protocol, known for its low-latency performance and enhanced security features, four websites utilize this technology. This accounts for about 50%

of the websites using QUIC, showcasing a growing trend towards adopting modern protocols that improve both security and user experience.

4.10.3 Bangladeshi Government Websites:

The analysis of encryption practices across government websites reveals varying implementations of TLS (Transport Layer Security) and other encryption protocols. A significant majority of these websites, specifically 15 out of 20, utilize TLS, indicating a strong commitment to secure communications. Among these, several websites employ TLS 1.2. In contrast, a more secure version, TLS 1.3, is used by a few sites. However, five websites do not specify the use of TLS, raising concerns about their encryption practices and the potential risks associated with unsecured communications.

Chapter 5

Discussion

We have divided our Bangladeshi website analysis into three different categories. First one is e-commerce where we have evaluated 20 different websites on the basis of 10 heuristics. Second category was content websites which basically included the newspaper websites where we could fully evaluate 2 websites only and other 18 websites had preliminary evaluation as they did not have any password system. Finally the third category is Government websites of Bangladesh, we have evaluate 20 of these websites on the basis of the same heuristics. For further comparison, we have evaluated 12 Indian websites in order to find similarity in patterns, security and accessibility.

5.1 Evaluation Scoring Mechanism

H1 Password construction guideline (score = 1pt)
Minimum Password Length:
Contains Symbols:
Use special characters:

H2 Enrolment email contents (score = 1pt)
Email Verification:
Cleartext-password:

H3 Password Registration (score = 1pt)
Non-dictionary:
Not Previously used:
Not a common word:
Graphical strength indicator:

H4 Login (score = 1pt)
Identification:
Username:

H5 Password update (score = 1pt)
Password re-entry required:
Notification sent:

Required after recovery:

H6 Password Recovery Mechanism (score = 1pt)
Personal knowledge :
Reset-link:

H7 Federated login support (score = 1pt)
OpenId provided:
OpenId accepted:
Facebook Connect accepted:

H8 Rate Limiting (score = 1pt)
Brute force Restrictions: None (CAPTCHA, reset)

H9 User Probing Restriction: (CAPTCHA only) (score = 1pt)
Enrollment (CAPTCHA):
Login:
Reset (CAPTCHA) :

H10 Encryption (score = 1pt)
TLS deployment:

Each heuristic is assigned 1 point, which is divided equally among its subsections. For example, if a heuristic has three subsections, each one is worth 0.333 points. A website earns points based on how well it meets the requirements of each subsection. If it meets all the requirements under a heuristic, the website receives the full 1 point for that category. The overall score shows how well the website follows important security and usability guidelines.

5.2 Comparing between Bangladeshi e-commerce vs Bangladeshi contents websites

This comparative analysis examines 20 Bangladeshi e-commerce websites and 20 content websites, evaluating their approaches to password security based on some key factors like: TLS implementation, use of QUIC, encryption standards, guessing attack prevention, and HTTPS adoption. These factors are crucial for ensuring the security and privacy of user data, particularly passwords, which are central to user authentication processes. The objective is to highlight the differences between the two categories of websites and assess which sector demonstrates better practices in safeguarding user credentials.

5.2.1 TLS Implementation

For TLS Implementation, 13 out of the 20 e-commerce websites have adopted TLS. On the content side, 7 out of the 20 websites have implemented TLS accounting for

35%. E-commerce websites show a higher adoption of TLS than content websites, with 65% of e-commerce platforms securing their communications through TLS compared to 35% of content websites. This difference suggests that e-commerce sites prioritize secure transactions and data protection due to the nature of the data they handle, which includes sensitive financial and personal information. On the other hand, content websites, while adopting TLS to some extent, may not face the same level of urgency regarding data protection, resulting in a slower adoption rate.

5.2.2 Use of QUIC

In terms of QUIC Implementation, 7 out of the 20 e-commerce websites have adopted QUIC representing 35% of e-commerce websites. For content websites, 13 out of 20 have implemented QUIC representing 65% of content websites. Content websites are leading in the adoption of QUIC, with 65% implementing the protocol, compared to 35% of e-commerce websites. This suggests that content websites are focusing on improving connection speed and reducing latency, which can be critical for delivering media content or news updates efficiently. E-commerce websites, while also using QUIC, are more likely to focus on balancing speed with other security measures like TLS. The lower adoption rate in e-commerce sites could be attributed to the greater complexity involved in handling financial transactions securely, which may require more time for widespread adoption of QUIC.

5.2.3 Guessing Attack Prevention

Guessing attacks represent a considerable security threat, as attackers systematically attempt to gain access to user accounts by testing numerous password combinations. In this evaluation, a substantial number of e-commerce websites have implemented robust rate-limiting measures to thwart such attacks. These measures often include locking accounts after a predetermined number of failed login attempts, significantly reducing the likelihood of unauthorized access. E-commerce platforms, which typically manage highly sensitive user data, such as financial and personal information, have a strong incentive to adopt these protective measures. The heightened security requirements in the e-commerce sector are indicative of the increased risks associated with handling sensitive transactions. In contrast, while a portion of content websites has also adopted similar protections, their lower overall implementation of guessing attack prevention measures suggests a comparatively diminished perception of risk. This discrepancy leaves content websites more susceptible to potential vulnerabilities, as they may not be as proactive in reinforcing account security against such threats.
In Fig. 5.1 in case of e-commerce websites, FoodPanda holds the highest position with the score 6 and incase of content websites Prothom Alo holds the highest position with the score 5.65. The overall mean evaluation score of E-commerce VS Content Websites is 3.74.

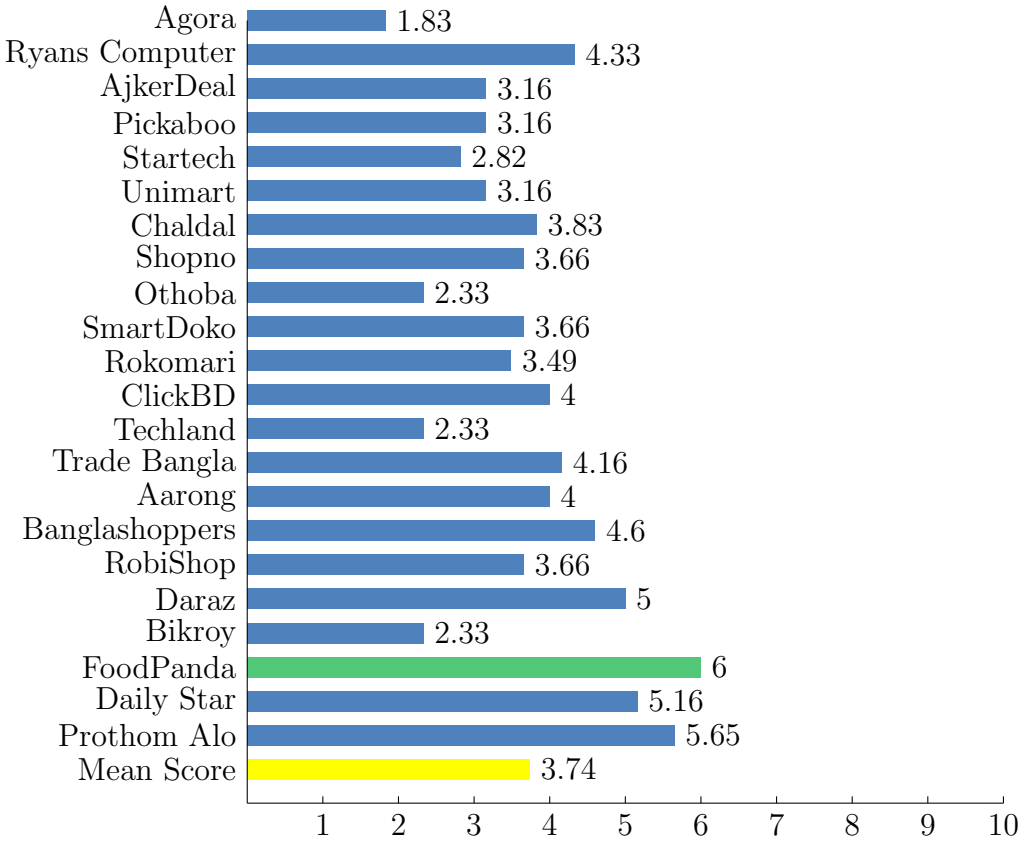


Figure 5.1: E-commerce & Content Websites Evaluation Score

5.3 Comparing between Bangladeshi private (20 e-commerce and 2 contents) vs Bangladeshi government

An examination of password management practices across 20 e-commerce websites as well as 2 content websites and 20 government websites in Bangladesh reveals significant variances and areas requiring improvement. E-commerce platforms generally demonstrate inconsistencies in their password policies. These websites typically mandate a minimum password length of between 6 and 8 characters but exhibit considerable variation in the enforcement of complexity requirements. A prevalent issue is the absence of password strength meters, which are essential for guiding users in creating robust passwords. Furthermore, the implementation of CAPTCHA mechanisms is notably infrequent, potentially exposing these platforms to increased risks from automated attacks. The process for updating passwords is inconsistent; while some platforms require users to re-enter their current passwords, others do not, further highlighting variability in security practices. The password reset process often suffers from issues such as link expiration and inadequate confirmation notifications, which can hinder effective user recovery.

In contrast, government websites in Bangladesh generally demonstrate a more robust approach to password security. These platforms frequently impose clearer password guidelines, which typically include requirements for a combination of uppercase and

lowercase letters, numbers, and special characters. CAPTCHA is more commonly integrated during both registration and login phases, providing additional protection against automated attacks. The password update process is generally more secure, requiring the entry of the current password alongside the new one, and often maintaining consistent guidelines throughout. Recovery options are also more comprehensive, with many systems offering both email and OTP-based verification, although there are still issues related to the consistency of verification processes and the effectiveness of reset interfaces.

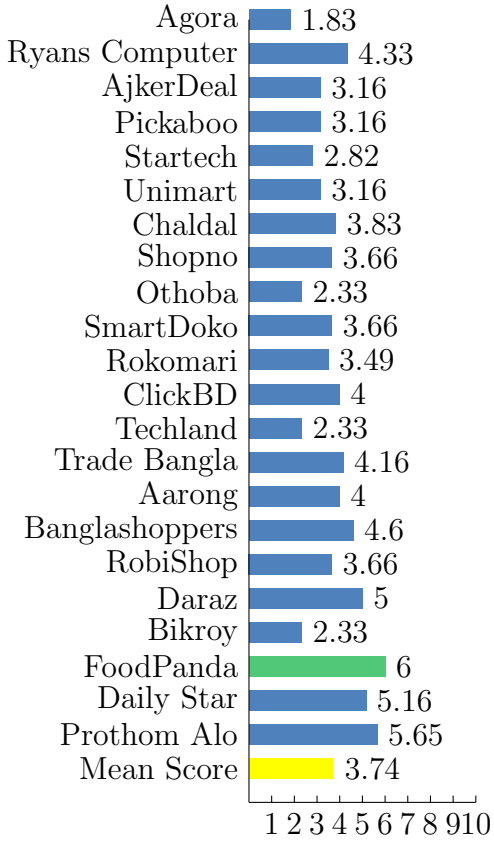


Figure 5.2: E-commerce & Content Websites Evaluation Score

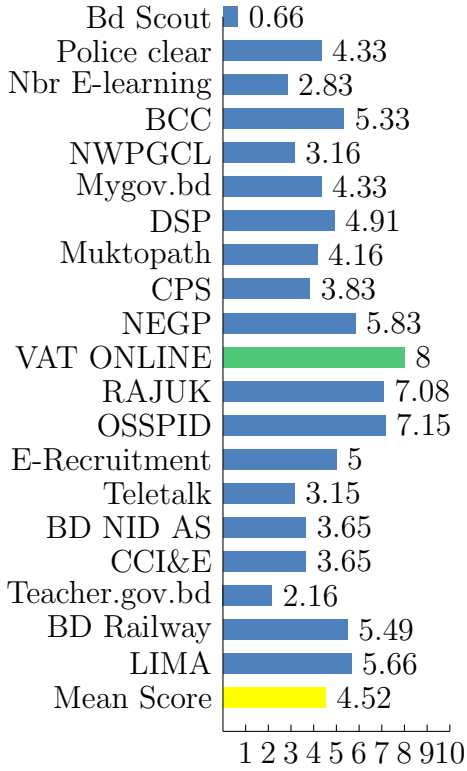


Figure 5.3: Bangladeshi Government Websites Evaluation Score

Overall, the comparative analysis underscores that government websites tend to implement more stringent security measures compared to their e-commerce counterparts. Addressing the identified gaps in password management practices within e-commerce platforms—such as the enhancement of password strength meters, the consistent application of complexity guidelines, and the adoption of effective CAPTCHA and rate limiting measures—would substantially improve security. For government websites, while existing practices are generally more robust, there remains room for improvement in ensuring uniformity in verification and recovery processes. Enhancing these practices across both sectors is essential for bolstering overall security and protecting user data.

The examination of authentication and encryption practices among government websites and e-commerce/content websites in Bangladesh reveals notable differences in

security implementation, particularly concerning the effectiveness of their authentication mechanisms and the use of advanced encryption protocols.

5.3.1 TLS Implementation

Both government and e-commerce websites demonstrate a commitment to securing data transmission through the implementation of TLS (Transport Layer Security). A significant number of government sites utilize TLS 1.3, the most current version known for its superior performance and security features, while many e-commerce websites also leverage this protocol, with instances of TLS 1.2 still in use. This alignment indicates a shared recognition of the importance of secure communications; however, the government websites show a more consistent application of the latest standards.
In Fig. 5.3 in case of Bangladeshi Government websites, VAT ONLINE holds the highest position with the score 8 and Bangladesh Scout holds the lowest position with the score 0.66. VAT ONLINE has the highest score in case of E- commerce, Government and content websites category. The overall mean evaluation score of Bangladeshi Government websites is 4.52.

5.3.2 Use of QUIC

In terms of performance optimization, e-commerce websites are more progressive, with several adopting QUIC (Quick UDP Internet Connections) to enhance both speed and security. The government websites, on the other hand, lack explicit mention of QUIC, potentially indicating a lag in the adoption of more advanced networking protocols. This difference suggests that e-commerce platforms may be better positioned to deliver faster and more reliable user experiences, a crucial factor in competitive online markets.

5.3.3 Guessing Attack Prevention

A significant security concern emerges in the area of guessing attack prevention. Government websites exhibit a troubling lack of effective rate limiting and user verification mechanisms, which increases vulnerability to password guessing attacks. Many government sites allow unlimited login attempts, exposing them to considerable risk. Conversely, while e-commerce websites also demonstrate similar deficiencies in guessing attack prevention measures, they appear to be more inclined towards adopting best practices such as implementing account lockouts and CAPTCHA mechanisms to thwart such attacks. This indicates a more proactive approach in the commercial sector, likely driven by the need to protect consumer data and maintain trust.

In conclusion, while both government and e-commerce websites in Bangladesh have made strides in employing essential security protocols like TLS , critical differences remain in their authentication practices and proactive security measures. Government websites display a greater reliance on older standards and lack effective

mechanisms to mitigate guessing attacks, potentially jeopardizing sensitive data. E-commerce and content websites, while still needing improvement in areas such as password policies and guessing attack prevention, demonstrate a more adaptive approach to contemporary security challenges by using the latest version of TLS. Enhancing security measures across both sectors is vital to protect user information and build trust in online services, particularly as cyber threats continue to evolve.

5.4 Comparing between Bangladeshi e-commerce vs Indian e-commerce

After reviewing 12 Indian e-commerce websites, we identified a number of significant patterns and procedures related to user registration and authentication. One common observation is that the majority of these websites demand email addresses or cell phone numbers to be entered upon registration. It's interesting to note that most login processes employ OTP (One-Time Password) verification, which differs from the conventional username-password approach yet streamlines the login process. Users are usually requested to reset their password for subsequent sign-ins after successfully logging in using OTP, indicating a focus on account security beyond the first OTP-based access. But none of the websites we looked at use CAPTCHA techniques while users are logging in or registering. This omission may make them more vulnerable to automated bot attacks, which are a serious risk in the current security environment. Another noteworthy observation is that many of these platforms share similar website layouts, indicating a possible reliance on common templates or design frameworks. This uniformity might suggest a lack of diversity in user experience and design innovation across the Indian e-commerce space. Furthermore, the difference between Indian personal brands and bigger e-commerce platforms is an important discovery. Numerous Indian websites, particularly those that are smaller or more personal, typically prioritize email or other kinds of communication above phone number registration. Nonetheless, bigger, more well-known e-commerce sites need the registration of a phone number in order to create an account, indicating a greater dependence on mobile connection for communication and verification.

As it's mentioned in the previous section that the E-commerce platforms have often shown inconsistencies in their password policies. While most require a minimum password length of 6 to 8 characters, there is significant variation in how complexity requirements are enforced. A common problem is the lack of password strength meters, which are crucial for helping users create strong passwords. Additionally, CAPTCHA mechanisms are rarely implemented, potentially increasing vulnerability to automated attacks. The process for updating passwords varies as well, with some sites requiring users to re-enter their current password, while others do not, further emphasizing differences in security practices. The password reset process is also problematic, with issues like link expiration and insufficient confirmation notifications, making it difficult for users to recover their accounts efficiently.

While the analysis of the Bangladeshi e-commerce websites and Indian e-commerce websites we see some similarities and some major differences which are as follow:

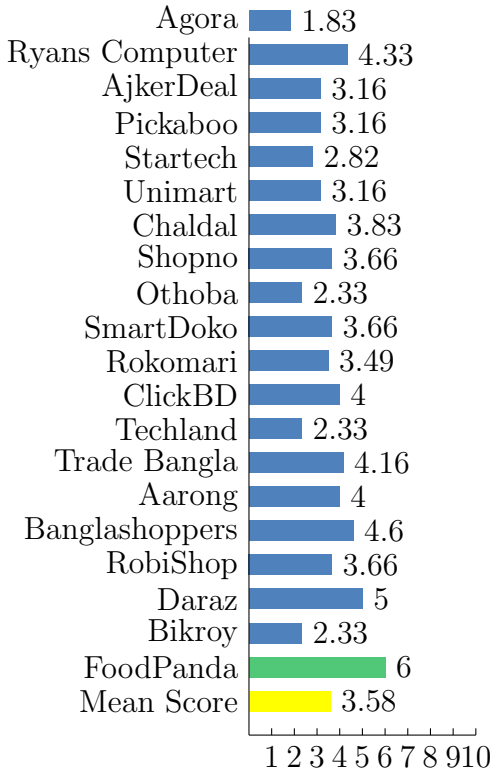


Figure 5.4: Bangladeshi E-commerce Websites Evaluation Score

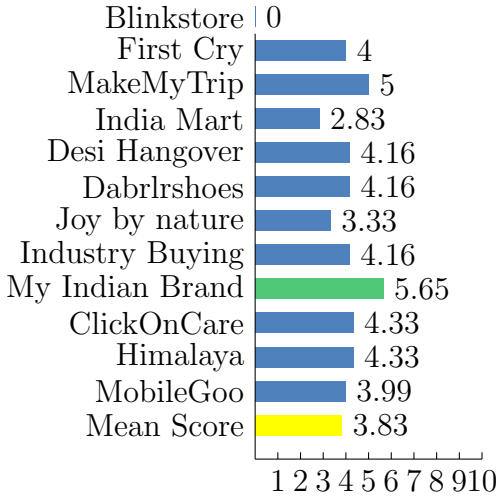


Figure 5.5: Evaluation Score of Indian Websites.

5.4.1 TLS implementation

A review of 20 Bangladeshi e-commerce websites revealed that 13 use TLS 1.2 or 1.3 encryption protocols, reflecting a strong commitment to security by adopting advanced standards that protect sensitive data. In comparison, out of 12 Indian e-commerce websites, only 5 have implemented these protocols, indicating a lower but still notable focus on secure communication. This alignment between both countries' platforms demonstrates a shared understanding of the importance of encryption, though Bangladeshi websites show a more consistent application of the latest standards. The disparity suggests that while progress has been made, Indian e-commerce platforms could benefit from broader adoption of TLS to ensure enhanced protection for users across the board.

In Figure 5.4, in case of Bangladeshi e-commerce websites, FoodPanda holds the highest position with evaluatuion score 6 and the overall mean evaluation score of Bangladeshi E-commerce Websites is 3.58. In Figure 5.5, in case of Indian websites, My Indian Brand holds the highest position with evaluation score 5.65 and the overall mean evaluation score of Indian e-commerce Websites is 3.83.

5.4.2 Use of QUIC

QUIC (Quick UDP Internet Connections) is used to enhance speed and security of the websites. In the analysis of 20 Bangladeshi e-commerce websites, only 7 were found to use QUIC, while 6 out of 12 Indian e-commerce websites had implemented it. This suggests that Indian websites show a stronger focus on QUIC implementation, prioritizing the performance and security advantages it offers for enhancing user experience and secure data transmission.

5.4.3 Guessing Attack Prevention

Our research into Indian and Bangladeshi e-commerce websites revealed notable differences in their defenses against guessing attacks. Indian websites generally demonstrate stronger protection, with most implementing rate-limiting for password attempts, a key measure in mitigating such attacks. While many Bangladeshi websites also incorporate rate-limiting, a significant portion still lack this critical feature. Interestingly, some Bangladeshi websites employ CAPTCHA during the registration process, a security measure absent in Indian sites at this stage. However, Indian platforms commonly use CAPTCHA after multiple failed password attempts, enhancing their resistance to guessing attacks. These findings suggest that both Bangladeshi and Indian e-commerce websites are taking proactive steps to safeguard user data and maintain consumer trust, though there is room for improvement in their security practices.

Finally, the review of e-commerce websites from Bangladesh and India reveals places where security standards may be strengthened as well as areas where they are already strong.Nonetheless, websites from Bangladesh stand out for utilizing CAPTCHA while registering. The implementation of contemporary encryption methods such as TLS and QUIC is indicative of ongoing endeavors to guarantee safe data transfer. All things considered, platforms in Bangladesh and India are making significant progress in improving security; but, more work is still needed to completely safeguard customer data and preserve confidence.

5.5 Interesting patterns and insights

We evaluated 72 websites across four main categories: 20 Bangladeshi E-commerce websites, 20 Bangladeshi content/news websites, 20 Bangladeshi government websites, and 12 Indian e-commerce websites. By comparing these websites, we were able to extract interesting patterns and insights related to password security. Below is a detailed comparison of security factors across these categories and in comparison to Indian e-commerce websites.

5.5.1 Password Complexity Requirements

Across the different categories of Bangladeshi websites, we observed significant variation in password complexity requirements:

- **E-commerce websites** in Bangladesh generally displayed lenient requirements. Most sites only enforced a basic minimum length for passwords (5-8 characters), with many allowing dictionary words, and lacking requirements for including a mixture of letters, numbers, or special characters. This suggests a lower emphasis on robust password policies among e-commerce platforms.
- **Content/news websites** also showed similar trends, with weak enforcement of complex passwords. These websites often did not advise users to create strong passwords, and in some cases, they lacked even basic restrictions on dictionary words.
- **Government websites,** on the other hand, exhibited comparatively better password policies. Many government websites enforced a minimum of 8 characters and required a combination of letters, numbers, and special characters. However, there were still inconsistencies; while some sites, like the Police Clearance website, enforced strong password guidelines, others accepted passwords as short as one character.
- **Indian e-commerce websites** typically had higher password requirements, with many requiring at least one number, letter, and special character for a password to be valid. However, some Indian websites relied more on OTP-based verification, which led to relaxed password requirements.

5.5.2 One-Time Password (OTP) Usage

A striking difference emerged in the use of OTP:

- **Indian e-commerce websites** made extensive use of OTP during both the registration and login phases, as well as for password recovery. This reliance on OTP for user verification is a common security strategy in India, where it often serves as a substitute for stringent password requirements.
- **Bangladeshi websites** especially those in the e-commerce and content categories rarely used OTP. While some government websites did include OTP, it was usually limited to password recovery, rather than being an integral part of the login or registration process.

This difference reflects a more security-conscious approach in Indian websites, where OTP provides an additional layer of authentication beyond passwords. In Bangladesh, the lower prevalence of OTP means users are often reliant solely on the security of their passwords, which are not always robust.

5.5.3 CAPTCHA

In terms of the adoption of CAPTCHA, the results varied significantly:

- **Bangladeshi e-commerce and content websites** generally lacked effective protections. CAPTCHA was rarely used during the login or registration process, leaving these sites vulnerable to password guessing attacks.
- **Bangladeshi government websites** were slightly better in this regard, with a few sites incorporating CAPTCHA during password recovery or login attempts. For example, the Police Clearance website used CAPTCHA after several failed login attempts, but such protections were not uniformly applied across all government sites.
- **Indian e-commerce websites** showed more frequent use of CAPTCHA to prevent automated attacks. Many Indian platforms limited the number of incorrect password attempts before requiring CAPTCHA validation, thus adding a protective layer against hacking attempts.

5.5.4 Password Recovery Mechanisms

The mechanisms for password recovery also differed across categories:

- **Bangladeshi e-commerce and content websites** typically relied on email-based recovery systems. However, these systems were often poorly implemented. Many websites did not send confirmation emails or password reset links promptly, and some did not enforce re-entry of current passwords before updating them.
- **Government websites** had mixed results in terms of password recovery. Some, like the Bangladesh Computer Council website, offered robust email-based recovery with reset links sent directly to the user's inbox. Others, however, had broken recovery processes where users were not sent the necessary verification codes.
- **Indian e-commerce websites** provided more efficient recovery mechanisms, largely centered around OTP sent via email or SMS. This was consistent across most Indian websites, further reinforcing their reliance on OTP for account security.

5.5.5 Federated Login and Social Media Authentication

The use of federated login systems (e.g., Google or Facebook authentication) varied across the websites:

- **Bangladeshi e-commerce and content websites** largely did not offer federated login options. This lack of integration with social media or OpenID systems may limit user convenience but can also reduce exposure to vulnerabilities associated with third-party authentication.
- **Indian e-commerce websites** were more likely to offer federated login through platforms like Google or Facebook, which, while convenient, brings with it certain risks if not implemented securely.

Comparison between 20 Bangladeshi E-commerce and 50 E-commerce websites that was evaluated in "The Password Thicket" paper

According to "The Password thicket"[4] paper the mean evaluation score of 50 e-commerce websites that were evaluated stands at 4.74. On the other hand, in this evaluation the mean evaluation score of 20 Bangladeshi e-commerce websites stands at 3.58. Clearly the Bangladeshi websites are lagging in security practices in comparison with the foreign websites.

5.6 Implications and Recommendations

The preliminary analysis underscores the need for uniform security standards across all types of websites. While some e-commerce platforms set a high standard, there is a critical need for newspaper websites to elevate their security practices. Key recommendations include:

- **Enhancing Password Guidelines:** Implementing stricter password construction guidelines across all websites can significantly improve security.
- **Adopting CAPTCHA and Rate Limiting:** To prevent automated attacks, websites should incorporate CAPTCHA and rate limiting for password guessing.
- **Federated Identity Support:** Encouraging more websites to adopt federated identity options can streamline user authentication and reduce password fatigue.
- **Strengthening Encryption Practices:** Ensuring robust encryption and authentication mechanisms are in place to protect user data during transmission and storage.

The evaluation scores provide a snapshot of current security practices and highlight areas where websites can upgrade their defenses to protect user accounts better. By addressing these gaps, websites can enhance user trust and safeguard against unknown threats in the digital landscape.

Chapter 6

Conclusion

In this analysis, there are examinations of 72 total websites which are 20 Bangladeshi e-commerce, 20 Bangladeshi content, 20 Bangladeshi Government and 12 Indian e-commerce sites. This examination of websites is intended to enrich the knowledge of website design, its functionality, and their contents in every context. The main focus was comparing these websites with one another and identifying subtle trends. Furthermore, the identification is not only the distinctions but also the similarities of the information that is provided as example, user experience similarities between Bangladeshi e-commerce and Indian e-commerce websites, and equal access to all governmental and non-governmental online resources is provided. This broad analysis will provide useful information on the specific features and emerging patterns in website creation across different sectors and countries.

The thesis is based on password security practices across a spectrum of top e-commerce and news portals, and government websites in Bangladesh with 12 Indian e-commerce websites, emphasizing an urgent need for strengthening cybersecurity measures. Inspired by an influential research paper [4], this paper aims to systematically assess websites' adherence to established security guidelines. Leveraging a comprehensive analysis framework, the examination includes factors such as password complexity, uniqueness, hashing mechanisms, and adherence to established heuristics.

A comparative analysis between different Bangladeshi websites and Indian websites underscores distinct security concerns. Specifically, Bangladeshi and Indian e-commerce websites experience higher risks due to the nature of the provided services and products which involve processing of users' financial data, while news portal websites have the greatest number of weaknesses in the problem area, including missing or insufficient user identification and vulnerability to data leakage. Furthermore, there are issues in some of thr Bangladeshi Government websites. Due to lack of enough security, there are chances in data getting stolen as well.

However, the findings of this thesis will not only encourage security measures but will also undoubtedly provide important recommendations to users, regulators, and website administrators. This means that in addition to highlighting frequent security risks, it also offers potential solutions and guidance on how to enhance the security of different websites. As attempts to mitigate recently emerging cybersecu-

rity risks gain momentum globally, this research bolsters related studies discovered in the literature [12] – [11].

Ultimately, this evaluation and identification of security areas that may be vulnerable will lead to a more secure system and safer path in Bangladesh. The search for the optimal security measures, driven by this study, is successful in preserving user data and enhancing consumers' overall trust and sense of security while using online platforms, resulting in a more robust and efficient online environment for all users.

Bibliography

[1] D. V. Klein, "Foiling the cracker: A survey of, and improvements to, password security," *Programming and Computer Software*, vol. 17, no. 3, Mar. 1992. [Online]. Available: http://www.osti.gov/scitech/biblio/459485.

[2] S. Furnell, "An assessment of website password practices," *Computers security*, vol. 26, no. 7-8, pp. 445–451, Dec. 2007. DOI: 10.1016/j.cose.2007.09.001. [Online]. Available: https://doi.org/10.1016/j.cose.2007.09.001.

[3] P. Hoonakker, N. Bornoe, and P. Carayon, "Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 53, no. 6, pp. 459–463, Sep. 2009. DOI: 10.1518/107118109x12524441081983. [Online]. Available: https://doi.org/10.1518/107118109x12524441081983.

[4] J. Bonneau and S. Preibusch, "The Password Thicket: technical and market failures in human authentication on the web.," *WEIS*, Jan. 2010. [Online]. Available: http://preibusch.de/publications/Bonneau_Preibusch__password_thicket.pdf.

[5] W. Ma, J. Campbell, D. Tran, and D. Kleeman, "Password Entropy and Password Quality," *2010 Fourth International Conference on Network and System Security*, Sep. 2010. DOI: 10.1109/nss.2010.18. [Online]. Available: https://doi.org/10.1109/nss.2010.18.

[6] S. Komanduri, R. Shay, P. G. Kelley, *et al.*, "Of passwords and people: measuring the effect of password-composition policies," *Association for Computing Machinery*, May 2011. DOI: 10.1145/1978942.1979321. [Online]. Available: https://doi.org/10.1145/1978942.1979321.

[7] M. Raza, M. Iqbal, M. Sharif, and W. Haider, "A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication," *World Applied Sciences Journal*, pp. 439–444, Jan. 2012. DOI: 10.5829/idosi.wasj.2012.19.04.1837. [Online]. Available: http://idosi.org/wasj/wasj19(4)12/1.pdf.

[8] Y. Cheng, J.-L. Hung, and Z. Lin, "An analysis view on password patterns of Chinese internet users," *Nankai Business Review International*, vol. 4, no. 1, pp. 66–77, Mar. 2013. DOI: 10.1108/20408741311303887. [Online]. Available: https://doi.org/10.1108/20408741311303887.

[9] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The Tangled Web of Password Reuse," *Network and Distributed System Security Symposium*, 2014. DOI: 10.14722/ndss.2014.23357. [Online]. Available: https://doi.org/10.14722/ndss.2014.23357.

[10] K. Chanda, "Password Security: An analysis of password strengths and vulnerabilities," *International Journal of Computer Network and Information Security*, vol. 8, no. 7, pp. 23–30, Jul. 2016. DOI: 10.5815/ijcnis.2016.07.04. [Online]. Available: https://doi.org/10.5815/ijcnis.2016.07.04.

[11] A. A. Chowdhury, F. Chowdhury, and S. Ferdous, "A Study of Password Security Factors among Bangladeshi Government Websites," *arXiv (Cornell University)*, Dec. 2020. [Online]. Available: http://arxiv.org/pdf/2012.01765.pdf.

[12] M. A. Masum, M. R. I. Sachcha, and A. Nayem, "Security Analysis of Government amp; Financial Websites of Bangladesh," *International journal of education and management engineering*, vol. 12, no. 2, pp. 21–29, Apr. 2022. DOI: 10.5815/ijeme.2022.02.03. [Online]. Available: https://doi.org/10.5815/ijeme.2022.02.03.

[13] T. Alam, "Password construction and management strategies of the online users of bangladesh: A demographic comparison with the users of the first-world countries."

[14] *SimilarWeb Digital Intelligence: Unlock your Digital growth.* [Online]. Available: https://www.similarweb.com/.