Cyber security threats and web vulnerability analysis of higher educational institutions in Bangladesh

Shadiqul Hasan Khan Janny[1], Md. Asadujjaman Noor[1], Mohammad Enan Al Harun Sahan[1], Sheikh Nafez Sadnan[1], Muhammad Towfiqur Rahman[1], Abu Saleh Md Bakibillah[2]
[1]Department of Computer Science and Engineering, School of Engineering, University of Asia Pacific, Dhaka, Bangladesh
[2]Department of Systems and Control Engineering, School of Engineering, Tokyo Institute of Technology, Tokyo, Japan

Article Info

Article history:

Received Sep 24, 2024
Revised Sep 29, 2025
Accepted Oct 14, 2025

Keywords:

Cyber security threats
Cyberattacks
Educational institutions
Information systems
Web vulnerabilities

ABSTRACT

This paper presents a comprehensive analysis of cyber security threats and web vulnerabilities in the context of higher educational institutions in Bangladesh, including twenty public and private universities. Educational institutions are highly vulnerable due to their negligence in maintaining a functional network, mainly owing to budgetary constraints. As a result, they have become a hacker playground for many ambitious adversaries to boast their technical skills, regardless of the harm they may inflict. Through the use of vulnerability assessment and penetration testing (VAPT), we conducted a methodical analysis of the institutions' web infrastructures, identify and categorize the prevalent security threats and vulnerabilities that may compromise the integrity, confidentiality, and availability of information systems. Our findings reveal significant disparities in the security strength of both public and private universities, with the latter demonstrating a higher degree of vulnerability due to varying factors, such as budget constraints, policy enforcement, and awareness levels. This study underscores the urgent need for robust cyber security frameworks tailored to the higher educational sector's unique requirements, advocating for proactive measures to mitigate potential cyber threats. The implications of this research extend beyond the academic domain, offering insights into national cyber security strategies and the safeguarding of critical information infrastructures.

Corresponding Author:

Muhammad Towfiqur Rahman
Department of Computer Science and Engineering, School of Engineering, University of Asia Pacific
Dhaka 1205, Bangladesh
Email: towfiq@uap-bd.edu

1. INTRODUCTION

Cyber security threats are the risks of experiencing cyberattacks that aim to harm or steal information, and money, or disrupt systems. There are many types of cyber security threats, such as malware, social engineering, software supply chain attacks, advanced persistent threats, distributed denial of service, man-in-the-middle, and password attacks. These threats are constantly evolving and becoming more complex to resolve. Some of the emerging threats and challenges in recent years include the use of artificial intelligence by attackers, the cybersecurity skills gap, vehicle hacking and internet of things (IoT) threats, threats facing mobile devices, cloud security threats, and state-sponsored attacks [1].

Web vulnerabilities can have various causes and effects, depending on the type and severity of the vulnerability. Some of the most common web vulnerabilities are broken access control, cryptographic failures, injection, and insecure design [2]. These vulnerabilities can allow attackers to gain unauthorized access, execute malicious code, steal sensitive data, or disrupt the service of the web application [2]. Cybercrime takes place whenever there is lax in cyber security. It is defined as the act of creating, distributing, altering, stealing, misusing, and destroying information through the computer manipulation of cyberspace; without the use of physical force and against the will or the interest of the victim [3]. Cybercrime can have detrimental effects on a person's finances, privacy, and even ability to access crucial services. One of the major ransomware outbreaks on record called WannaCry that targeted both private citizens and major corporations, resulting in monetary damage and the interruption of vital services. It knocked U.K. National Health Service hospitals offline and shut down a Honda Motor company in Japan [4]. According to a Forgenix survey [5], [6], 75% of e-commerce websites are at risk of some cyberattacks. Figure 1 illustrates different cyber security incidents that took place in recent years. These incidents highlight the massive amount of loss that occurred due to lax cyber security [7]-[11].

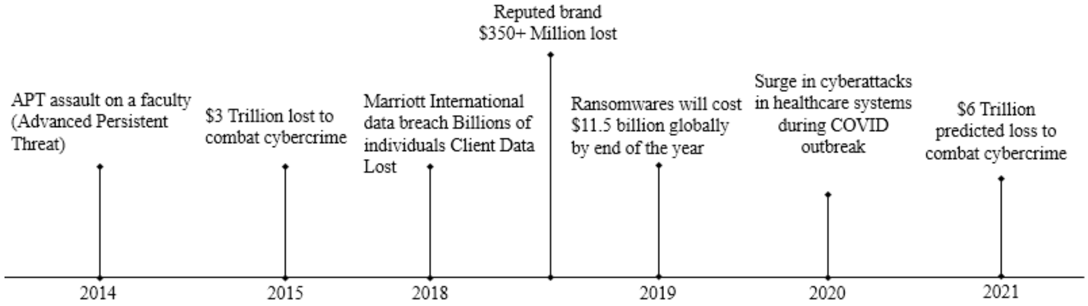
Reputed brand
$350+ Million lost
APT assault on a faculty (Advanced Persistent Threat)
$3 Trillion lost to combat cybercrime
Marriott International data breach Billions of individuals Client Data Lost
Ransomwares will cost $11.5 billion globally by end of the year
Surge in cyberattacks in healthcare systems during COVID outbreak
$6 Trillion predicted loss to combat cybercrime
2014
2015
2018
2019
2020
2021

Figure 1. Different cyber security incidents occurred in recent years globally

According to the McAfee mobile threat report, there is a significant increase in backdoors, fake applications and banking Trojans for mobile devices [12]. Besides, the malware attacks related to social media, the healthcare industry, cloud computing, IoT, and cryptocurrencies are also on the rise. The impact of cybersecurity to prevent these incidents from occurring is profound. The phishing method usually begins with an impersonated email, prompting individuals to log in to their accounts by utilizing the spoofed email. The emails continually look like valid emails because the phishers disseminate identical emblems and visual images as the actual website [13].

Cyber security is all about finding out vulnerabilities in a system and taking actions to resolve the issue or prevent it from reoccurring. The term vulnerability assessment and penetration testing (VAPT) was coined to represent these actions, where VA stands for vulnerability assessment and PT stands for penetration testing. The vulnerability management lifecycle can be separated into four steps, e.g., asset discovery and vulnerability assessment, vulnerability prioritization, vulnerability remediation, and verification [2]. Penetration testing is used by ethical hackers to conduct the testing of fully integrated and operational system infrastructure or networks. There are various methods used for vulnerability assessments. These methods can be separated into two types: automated and manual. Both methods are required to analyze, detect, and eliminate false positive vulnerabilities. Automated tools are mostly used to reduce the labor-intensive work that is required to conduct a testing procedure. Some international standards of vulnerability have determined the checks needed to be performed for manual testing, such as OWASP TOP 10 (2021) [2], CWE/SANS TOP 25 [14], ISO 27001 [15], PCI DSS 3.2 [16], MASVS [17], and WASC [18].

In this paper, we investigate cybersecurity threats and web vulnerabilities in the websites of twenty universities in Bangladesh, comprising ten public (government-endorsed) and ten private (non-government) institutions. Our goal is to identify critical security threats and vulnerabilities specific to both public and private universities, emphasizing the importance of VAPT. Our study explores the societal implications of neglecting cybersecurity and reviews relevant sources to gain a comprehensive understanding of vulnerability analysis in this context. Despite an extensive literature review, we found no prior research directly addressing the cybersecurity challenges of higher education institutions in Bangladesh. This highlights the novelty of our work, which specifically targets the educational sector—a domain increasingly susceptible to cyberattacks as it undergoes rapid digital transformation. The potential consequences of such attacks can significantly disrupt academic operations and the broader education system. To enhance clarity, we have included two diagrams to illustrate our methodology and data collection procedure. The findings of our analysis are presented in detail in the Results section, offering valuable insights into the cybersecurity landscape of higher educational institutions in Bangladesh.

The paper is structured as follows. Section 1 describes the introduction, highlighting the global impact of cybersecurity weakness. Section 2 describes the literature review that analyzes different papers and their approaches and proposals regarding cyber security. Since we employed the VAPT protocol to expose the weak implementation of cyber security in Bangladesh, a spotlight on occurrences and articles concerning cyber breaches in Bangladesh were discussed. Section 3 discussed the methodology regarding the implementation of VAPT. Section 4 presents the results and discussion. Finally, section 5 gives a conclusion by discussing the impact of our findings, the shortcomings, and future works.

2. LITERATURE REVIEW

Strengthening cybersecurity defenses is essential as society becomes more dependent on digital infrastructure to maintain prosperity and collective security in the face of changing threats. Shah and Mehtre [14] presented an overview of an offensive method to safeguard cyber assets, which includes VAPT testing. Ravindran and Potukuchi [15] discussed the importance of VAPT in discovering security problems in online applications by addressing typical web vulnerabilities and security assessments. They attempt to give an understanding of various online application vulnerabilities and the exploitation approaches applied by attackers. Khera *et al.* [18] addressed the impact of VAPT assessment by addressing the impact of fast advancement. Goel and Mehtre [19] described various techniques used in VAPT, including static analysis, fuzz testing, black box testing, and automated testing. Prajapati and Upadhyay [20] suggested a hybrid strategy that incorporates numerous open-source VAPT technologies. Joshi [16] highlighted the necessity for a coordinated strategy to enhance the outcomes. Bangladesh, as a developing country, has witnessed significant growth in its digital infrastructure, making it susceptible to cyberattacks. This background study and literature review aim to provide insights into the current situation of cybersecurity in Bangladesh, focusing on key challenges, initiatives, regulations, and future prospects. In 2015, Bangladesh e-government computer incident response team (BGD e-GOV CIRT) was formed [17]. The government approved Digital Security act in 2018 to protect digital security and reduce crimes perpetrated on digital platforms [21]. Numerous cyberattacks and threats against Bangladeshi companies and government institutions have occurred in recent years.

2.1. Impact of cyberattacks on government institutions

Recently, cyberattacks' effects on government institutions of Bangladesh have drawn a lot of attention. On August 15, 2023, a cyberattack alert was issued, highlighting the susceptibility of crucial government systems [22]. There have been reports of data breaches exposing the private information of people [23], and around 240 government entities have been the target of cyberattacks, suggesting a general vulnerability [24]. Ongoing vulnerabilities are shown by past occurrences including the rapid action battalion (RAB) website attack in 2008 and the Bangladesh Police website hack in 2011 [25]. Moreover, hackers were able to get their hands on a server connected to the Bangladesh road transport authority (BRTA), which allowed for fraud and exposed vulnerabilities in the system [26]. Cyber-attacks have also affected critical businesses including aviation, as demonstrated by attempts to extort Biman Bangladesh Airlines [27] and the hacking of Chattogram customs' website [28]. In order to maintain stability and security in the face of growing cyber threats, Bangladesh must strengthen government systems and data security as it moves on with its digitization plans.

2.2. Impact of cyberattacks on business

A series of serious cyberattacks have severely affected the business environment in Bangladesh. Three individuals were apprehended when a shop's digital system was breached, which was a significant incident [29]. These incidents bring to light the dangers that businesses must take to protect their digital assets and customer data. Cyberattacks that target a variety of businesses highlight how pervasive cyber threats are, resulting in monetary losses and eroding consumer confidence. To strengthen the entire robustness of the business environment, businesses need to take proactive steps like robust cybersecurity, staff training, and teamwork. This is especially important in light of the widespread cyberattacks that have affected financial hubs, affecting both the institutions and their clients.

2.3. Impact of cyberattacks on financial sectors

Cyberattacks have severely impacted financial sectors in Bangladesh, with over 200 organizations, including banks, falling victim to cybercrimes [30]. Another attack targeted at least 147 Bangladeshi entities, including banks, highlighting the increasing frequency of such incidents [24]. The Bangladesh Bank cyber heist in 2016 underscored the magnitude of these risks [31]. In an incident involving a leading bank in Bangladesh, hackers stole $250,000, demonstrating the ongoing threat to banking institutions and their customers [32]. The Dutch-Bangla Bank was targeted by the Silence hacking group in an attempt to steal $3 million, revealing cybercriminals' adaptability in attacking financial resources [33]. These events emphasize the urgent need for Bangladeshi banks to strengthen their cybersecurity and risk mitigation strategies to protect assets and customer data.

2.4. Impact of cyberattacks on educational institutes

As seen by multiple events published in various sources, higher educational institutes or universities in Bangladesh have not been immune to the influence of cyber-attacks. The National University of Bangladesh was the victim of a cyber assault that exposed student information, exposing flaws in the education sector's cybersecurity architecture [34]. Similarly, renowned institutions, such as Dhaka University [35], Shahjalal University of Science and Technology [36], Chittagong University [37], had their websites hacked, demonstrating the pervasiveness of cyber threats affecting the higher education landscape. Moreover, email hacking in BRAC University [38] and North South University [39].

It has been raised concerning the security measures put in place by universities to protect their digital assets and sensitive information. Such instances highlight the urgent need for universities in Bangladesh to prioritize cybersecurity measures, invest in robust defensive systems, and raise staff and student knowledge to maintain the safe running of academic institutions in an increasingly digital world. To maintain the safeguarding of student information, academic integrity, and sensitive data, cybersecurity is critical in the educational industry. Because they store so much personal and academic data, educational institutions are often the focus of cyberattacks. Data theft, monetary loss, and reputational harm are all possible outcomes of breaches. Institutions may protect themselves from attacks and provide a secure learning environment for staff and students by putting strong cybersecurity measures in place, such as firewalls, encryption, and frequent security audits.

3. METHODS

3.1. Process flow of vulnerability analysis

For vulnerability analysis, firstly, the collection of all the source code of the web applications is required. For attackers to discover vulnerability and exploitation opportunities, the analysis of the source code is an important process. As attackers, we first sent requests to the victim machine. The request contained appropriate attack vectors or payloads. Once affected, the victim machines then sent back the scanned packets as a response. We then submitted the packets to a scanner or VA model to ascertain vulnerabilities. Depending on the signatures of vulnerabilities, the model validated our response. Before including these validated in the generated report, they were first accounted for and defined into three different categories. Figure 2 depicts the working process of vulnerability analysis.

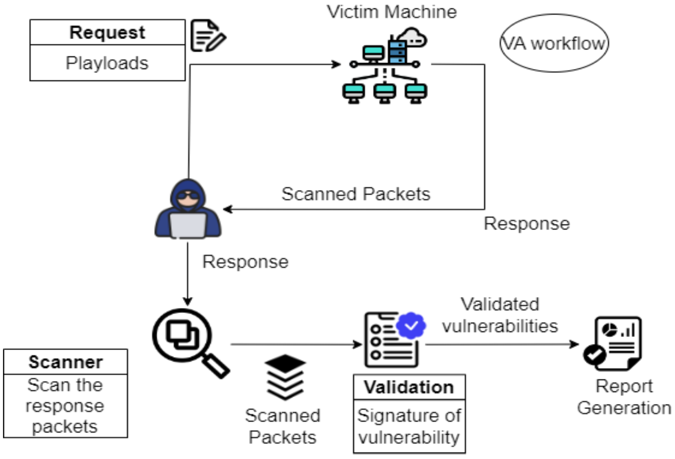

Figure 2. Process flow of vulnerability analysis

3.2. Data collection process

The data collection process for vulnerability analysis on multiple universities' data structures is illustrated in Figure 3. The first box is labeled "diffhttp-university.edu.txt", which suggests that the attack is initiated by looking for differences between the one university website and other universities' websites. Proper tools have been used to compare two files or sets of files.

a. Subdomain: in this stage we, as attackers, looked for subdomains of the university's website. Subdomains are websites that are part of a larger website, such as mail.university.edu or www.university.edu. Finding subdomains can help an attacker to identify additional targets for his attack.
b. Probing: our next step was to probe the university's network for vulnerabilities. This was done using a network scanner tool that can identify open ports, operating systems, and other devices on a network.
c. Fingerprints: after probing had been successful, our next goal was fingerprinting the university's web server. Fingerprinting is a technique used to identify the software and hardware being used by a web server. This information can help the attacker to identify potential vulnerabilities.
d. Portscan: using a VA analysis tool, we scanned the university's network for open ports. Open ports are ports that are listening for incoming connections. Attackers can use open ports to gain access to a network.
e. Ipspace: once a scan has been conducted, our next target is to discern the university's IP address space. The IP address space is the range of IP addresses that are assigned to the university. This information was of help for us to identify all of the devices that are on the university's network.
f. Banner grabbing: we used banner grabbing to gather information about a target system by analyzing the response, or "banner" it sent back when a connection was made. This helped us to identify software versions and potential vulnerabilities for exploitation.
g. Link finding: link finding is an essential step where we looked for links between the university's website and other websites. Finding links could help us to identify other websites that could be compromised if the university's website is compromised.

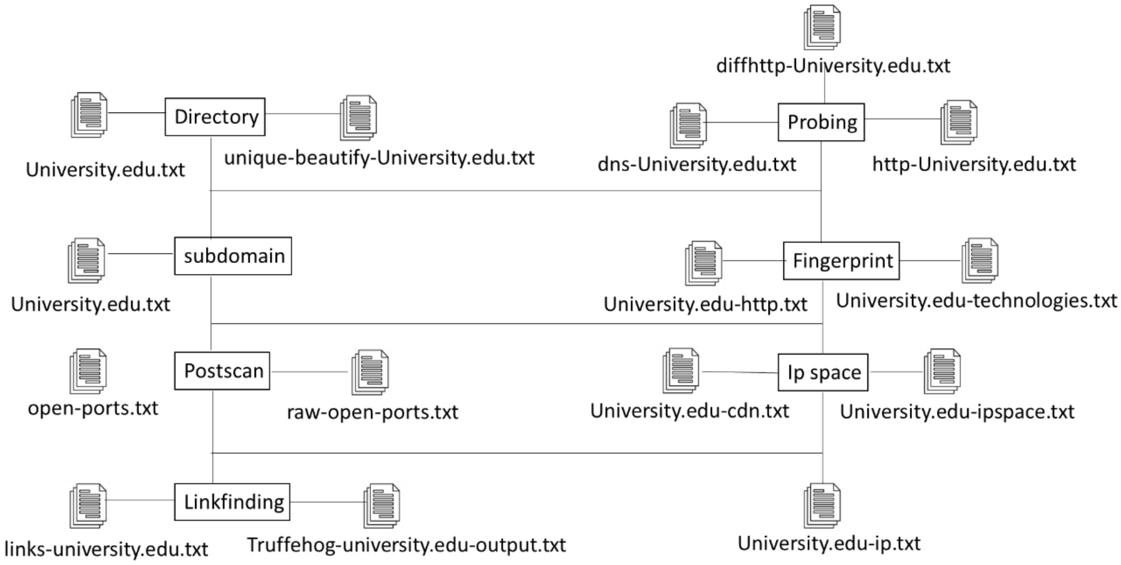

Figure 3. Data collection process for vulnerability analysis

3.3. Scan and validation of vulnerabilities

The scan and validation of vulnerabilities algorithm automate discovery and confirmation of security weaknesses by iterating over target assets, probing their accessibility, and exercising all reachable input endpoints with crafted payloads. For each accessible asset it crawls to enumerate parameterized URLs and input-accepting routes (including POST endpoints), then injects test payloads and inspects responses for signatures that indicate an exploitable condition. When response changes match the validator’s signatures the algorithm flags the endpoint as vulnerable; for issues that manifest outside the normal response channel (for example server-side request forgery (SSRF) or blind remote code execution (RCE)) it leverages out-of-band (OOB) monitoring services to confirm exploitation. Designed to be repeatable and extensible, this approach separates discovery, injection and validation phases to reduce false positives and support automated triage.

a. Initially, we verified asset accessibility through appropriate means (e.g., network connection, API availability). We also checked if the domain/IP is accessible through http protocol.
b. If the domain or IP was accessible, we then employed crawling techniques to systematically identify all input endpoints within the asset. The endpoint could have been parameterized URLs or any URL that accepted the POST method and allowed the input request to be made.

c. In the third step, we made a request to each parameterized URL or URLs, which were accepting input data with a crafted payload, and then waited for the response. If the crafted payload makes any changes in the response and matches with our validator signature, it will be vulnerable.
d. For vulnerabilities, such as SSRF or RCE, we used the "Out of bound" service.

Algorithm 1. Vulnerability analysis

```
while asset is not end:
        check if asset is accessible:
                crawl find all input endpoints
                inject payload
                receive response and validate if vulnerable or not.
```

4. RESULTS AND DISCUSSION

Our study investigates cybersecurity vulnerabilities across higher educational institutions in Bangladesh, emphasizing a comparative analysis between government and non-government institutions. By conducting VAPT, we highlight the distinct challenges faced by each institution type at various vulnerability levels. These findings provide valuable insights into the current cybersecurity landscape within the academic sector, underscoring areas where institutions need tailored security interventions to mitigate risk effectively.

High-severity vulnerability: a high-severity vulnerability is a security weakness in a software application or system that could allow an attacker to gain unauthorized access to sensitive data, disrupt operations, or take control of the system. The common vulnerability scoring system (CVSS) is a widely used standard for scoring the severity of vulnerabilities. CVSS scores range from 0 to 10, with higher scores indicating more severe vulnerabilities. Vulnerabilities with CVSS scores between 7.0 and 10.0 are considered to be high severity. These vulnerabilities are considered to be the most dangerous, as they can be easily exploited by attackers, even those with limited skills or resources. Server security misconfiguration, server-side injection, broken authentication and session management, sensitive data exposure, insecure os/firmware, broken cryptography, and automotive security misconfiguration. Table 1 gives high-severity vulnerabilities in public and private universities in Bangladesh.

Table 1. High-severity vulnerabilities in public and private universities

Government institutions	Vulnerabilities found	Non-government institutions	Vulnerabilities found
Gov A	5	Non gov A	115
Gov B	0	Non gov B	76
Gov C	4	Non gov C	197
Gov D	33	Non gov D	46
Gov E	0	Non gov E	63
Gov F	33	Non gov F	0
Gov G	12	Non gov G	19
Gov H	2	Non gov H	67
Gov I	80	Non gov I	0
Gov J	55	Non gov J	0

A noticeable disparity exists in high-severity vulnerabilities between government and non-government institutions. Consistent with trends observed in studies on cybersecurity within educational sectors of other developing nations [40], our data reveal that non-government institutions report significantly higher counts of high-severity vulnerabilities compared to government ones. For instance, "Non gov C" and "Non gov A" showed the highest counts in this category, with 197 and 115 vulnerabilities respectively, while three government institutions (gov B, gov E, and gov J) reported none. This divergence may reflect how resource allocation, access to robust cybersecurity frameworks, and centralized governance structures impact vulnerability management. Government institutions might have benefitted from a centralized support structure that provides consistent cybersecurity funding and policy enforcement.

Medium-severity vulnerabilities: medium-severity vulnerabilities are security weaknesses that can be exploited by attackers to gain some level of access to a system or data. The CVSS is a widely used standard for scoring the severity of vulnerabilities. CVSS scores range from 0 to 10, with higher scores indicating more severe vulnerabilities. Vulnerabilities with CVSS scores between 4.0 and 6.9 are considered to be of medium severity. They are less severe than critical or high-severity vulnerabilities, but they can still pose a significant risk to organizations. Types of medium-severity vulnerabilities can include server security misconfiguration, sensitive data exposure, cross-site scripting (XSS) [41], broken access control (BAC), cross-site request forgery (CSRF) [42], application-level denial-of-service (DoS), insecure OS/Firmware, automotive security misconfiguration. Table 2 gives the medium-severity vulnerabilities in public and private universities.

Medium-severity vulnerabilities are prevalent across both government and non-government institutions, though non-government institutions generally report higher numbers. This finding aligns with studies indicating that institutions with limited budgets and less formalized security practices often exhibit a greater presence of medium-severity vulnerabilities, such as those arising from outdated software and inadequate configuration [42]. In our data, "Non gov C" recorded 352 medium-severity vulnerabilities, underscoring how non-government institutions face continuous challenges in addressing these vulnerabilities. These medium-level risks, commonly found in educational institutions worldwide, can be addressed through more structured maintenance practices and security policies tailored to resource-constrained environments. Regular security audits and updates could significantly reduce the prevalence of these vulnerabilities.

Table 2. Medium-severity vulnerabilities in public and private universities

Government institutions	Vulnerabilities found	Non-government institutions	Vulnerabilities found
Gov A	141	Non gov A	326
Gov B	57	Non gov B	65
Gov C	40	Non gov C	352
Gov D	264	Non gov D	90
Gov E	5	Non gov E	151
Gov F	79	Non gov F	8
Gov G	192	Non gov G	107
Gov H	9	Non gov H	69
Gov I	128	Non gov I	120
Gov J	78	Non gov J	169

Low-severity vulnerabilities: low-severity vulnerabilities are the ones that do not pose a significant threat to the security of an application but may still need to be fixed or mitigated. Some examples of low-severity vulnerabilities are information disclosure, insufficient session expiration, missing security headers, and weak password policy. Table 3 shows the low-severity vulnerabilities in public and private universities in Bangladesh.

Table 3. Low-severity vulnerabilities in public and private universities

Government institutions	Vulnerabilities found	Non-government institutions	Vulnerabilities found
Gov A	227	Non gov A	357
Gov B	57	Non gov B	79
Gov C	104	Non gov C	343
Gov D	274	Non gov D	164
Gov E	11	Non gov E	161
Gov F	116	Non gov F	5
Gov G	259	Non gov G	125
Gov H	11	Non gov H	173
Gov I	273	Non gov I	151
Gov J	95	Non gov J	167

Low-severity vulnerabilities also follow a similar pattern, with non-government institutions exhibiting generally higher counts. For instance, "Non gov A" recorded the highest at 357, while "Gov I" had the highest among government institutions at 273. Although low-severity vulnerabilities are often less critical individually, their accumulation can present multiple potential attack vectors if left unchecked. Addressing these low-severity vulnerabilities could elevate the baseline security weakness across both government and non-government institutions.

These findings are consistent with broader research that links institutional structure and resource access to variations in cybersecurity vulnerability levels. Non-government institutions, particularly in developing countries, often face more significant cybersecurity challenges due to limited funding and support for security frameworks compared to government-run institutions. In Bangladesh, this vulnerability disparity may reflect similar structural issues, where government institutions benefit from centralized policies and support mechanisms that enable more consistent risk management. Addressing this imbalance is essential for promoting cybersecurity resilience across the academic sector. Figures 4 and 5 respectively show the vulnerabilities in government and non-government institutions in Bangladesh.

However, our study is limited by the sample size, which includes only 20 institutions, potentially restricting the generalizability of the results. A larger sample encompassing more institutions across varied regions and including different types of academic institutions, such as technical and vocational colleges, could yield a more comprehensive understanding of the cybersecurity landscape in Bangladesh’s education sector. Additionally, our focus on vulnerability presence without analysing the likelihood of exploitation or breach incidence limits the contextual insight into the real-world impact of these vulnerabilities. Further research could address these areas, as well as investigate other factors influencing vulnerability management, such as administrative oversight and policy compliance, to provide a more nuanced understanding of cybersecurity in educational institutions.

By utilizing our vulnerability scanner, we have found several bugs and their frequency in different university websites. Here is a detailed view of the number of vulnerabilities in both institution categories. The vulnerability list and count in government and non-government universities in Bangladesh are given in Tables 4 and 5, respectively.

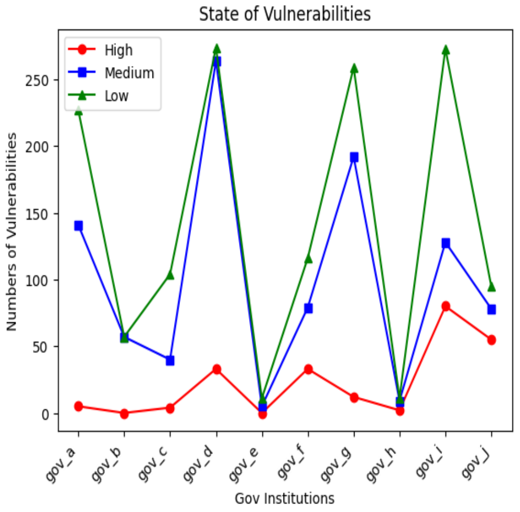

Figure 4. Vulnerabilities in government institutions

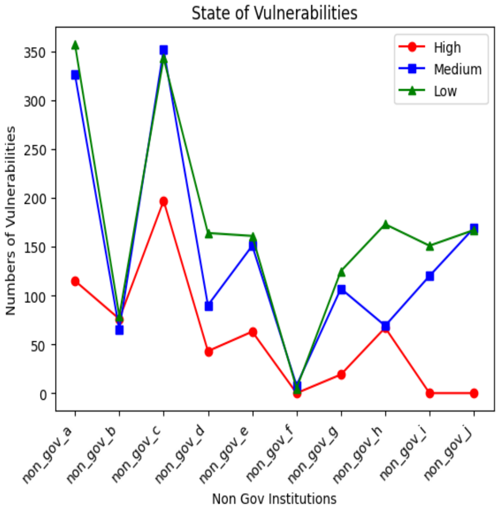

Figure 5. Vulnerabilities in non-government institutions

Table 4. Vulnerability list and count in government universities in Bangladesh

Targets	Gov A	Gov B	Gov C	Gov D	Gov E	Gov F	Gov G	Gov H	Gov I	Gov J
XSS (H)	0	0	0	4	0	1	0	0	21	25
SQL injection (H)	0	0	2	1	0	0	0	0	39	20
Server directory traversal (H)	3	0	0	2	0	2	5	0	0	0
Backup database and file folder (H)	0	0	2	2	0	4	1	0	8	0
TLS/SSL problem (H)	3	38	17	128	5	30	119	7	47	23
dotenv .env file disclosure	0	0	0	2	0	6	2	0	0	0
SSRF (H)	0	0	0	1	0	1	0	0	0	2
Vulnerable package dependencies	0	0	0	5	0	8	3	0	2	0
WordPress multiple vulnerabilities	0	1	2	3	0	1	0	0	0	0
Development configuration files	36	0	1	16	0	8	6	0	2	2
Debug mode enabled	0	0	0	3	0	6	10	0	3	3
Log file publicly accessible	38	0	0	5	0	0	1	0	0	0
Git repository found (H)	0	0	0	0	0	7	1	0	0	3
Vulnerable JavaScript libraries	63	2	8	0	2	16	0	1	51	35
Code execution attacks (H)	0	0	0	0	0	0	0	0	0	2
Malware and Trojan shell script (H)	0	0	0	0	0	0	0	0	0	2
Microsoft IIS tilde directory	0	0	0	0	0	0	0	0	0	0
Source code discloser (H)	0	0	0	0	0	0	0	0	0	0
CSRF	0	0	0	0	0	0	0	0	0	0

Table 5. Vulnerability list and count in non-government universities in Bangladesh

Targets	Non gov A	Non gov B	Non gov C	Non gov D	Non gov E	Non gov F	Non gov G	Non gov H	Non gov I	Non gov J
XSS(H)	3	4	103	15	6	0	2	0	0	0
SQL injection (H)	2	41	17	1	13	0	0	0	0	0
Server directory traversal(H)	2	0	0	1	1	0	0	63	0	0
Backup database and file folder(H)	2	0	0	3	1	0	3	4	0	0
TLS/SSL problem(H)	302	29	89	47	59	5	11	29	5	6
dotenv .env file disclosure	0	1	0	0	0	0	1	0	0	0
SSRF(H)	2		5	1	4	0	1	0	0	0
Vulnerable package dependencies	5	0	20	2	7	0	2	0	6	9
WordPress Multiple Vulnerabilities	32	20	71	2	15	0	7	0	0	0
Development configuration files	7	5	42	18	5	0	2	6	0	0
Debug mode enabled	1	0	0	0	2	0	9	1	0	0
Log file publicly accessible	3	0	0	0	0	0	0	0	0	0
Git repository found (H)	1	1	0	0	0	0	0	0	0	0
Vulnerable JavaScript libraries	53	19	279	30	38	0	35	20	40	37
Code execution attacks (H)	0	0	0	0	0	0	0	0	0	0
Malware and Trojan shell script (H)	4	0	3	1	0	0	0	0	0	0
Microsoft IIS tilde directory	3	0	0	0	1	0	0	0	0	0
Source code discloser (H)	1	1	4	4	0	0	1	0	0	0
CSRF	1	4	4	15	0	0	0	0	0	0

As the name suggests, the higher the severity of the vulnerability the more damages it can cause. Medium severity vulnerabilities can spiral into a major issue and be responsible for massive losses. These listed vulnerabilities can be exploited in various ways and can have significant impact on the cyber sector. Cross-Site Scripting: this vulnerability enables attackers to inject malicious scripts into web pages intended for users to view. This can lead to unauthorized access to user sessions, modification, and defacement of websites, in addition to distribution of malware. Students and faculty members' information may be compromised, resulting in possible damage to the institution's reputation.

a. SQL injection: malicious SQL code could be included in input fields, allowing adversaries to access, modify, or delete database contents. This facilitates unlawful access to student records, financial data, and other protected information. A study in 2016 showed the prevalence of SQL injection vulnerabilities in Bangladeshi web apps, underlining the need for robust security precautions [43].
b. Server directory traversal: this would allow an attacker to access restricted directories and retrieve sensitive files from the server. It could expose configuration files, passwords, and personal data of students and staffs.
c. Backup database and file folder exposure: vulnerability of this type can lead to similar consequences to server directory traversal. As backup mostly protects the same data in the event of any mishap to the server.
d. Dotenv (.env) file disclosure: .env files are mostly used to store sensitive database credentials and API keys. Disclosure of this file leads to the exposure of this valuable information. This grants attackers unrestricted and unauthorized access and increases the potential of future cyber-attacks.
e. Server-side request forgery: in SSRF, attackers can manipulate the server to make unauthorized requests to internal or external systems, potentially accessing internal services, bypassing firewalls, and leading to data exposure. SSRF vulnerabilities are recognized as significant security risks [44].
f. Vulnerable package dependencies: usage of outdated and insecure packages can cause many known vulnerabilities, in turn, making the system susceptible to exploits and compromising overall security. Frequent updates and patch management are necessary to reduce these potential risks [45].
g. WordPress multiple vulnerabilities: unattended WordPress sites can be exploited to obtain unauthorized access, inject malicious content, or disrupt website functionality. Given the widespread use of WordPress in educational institutions, we've found that such vulnerabilities can have serious consequences. Recent reports have highlighted critical vulnerabilities in WordPress learning management system (LMS) plugins, affecting numerous educational platforms [46].
h. Development configuration files exposure: development configuration files can reveal sensitive data if exposed. This data includes information about the application's structure, database connections, and other critical settings, aiding attackers in crafting targeted exploits [47].

i. Debug mode enabled: applications running in debug mode can expose detailed error messages and system information, which can also provide attackers with insights into potential vulnerabilities and system architecture. It's recommended to disable debug mode in production environments to prevent such information leakage.
j. Log file publicly accessible: log files are used to track status of a server or system. They aren’t meant for users to see rather for the administrators and developers to check on the performance of the system. Public access to log files can disclose user activities, system errors, and other sensitive information, aiding attackers in understanding system behaviour and identifying weaknesses.
k. Git repository found: git repositories should be private as they are used for production. Exposed repository can assist attackers with sensitive information.
l. Vulnerable JavaScript libraries: outdated JavaScript libraries with known vulnerabilities should not be utilized as they can allow attackers to exploit client-side scripts, leading to XSS attacks, data manipulation, and other client-side exploits [48].
m. Code execution attacks: this type of vulnerability allows attackers to execute arbitrary code on the server, potentially leading to full system compromise, unauthorized access, and deployment of malware.
n. Malware and Trojan shell scripts: malicious scripts act as Trojan and can provide attackers with backdoor access, enabling persistent threats, data exfiltration, and further network infiltration.
o. Microsoft IIS tilde directory vulnerability: exploitation of this vulnerability can allow attackers to itemize short file and directory names, potentially revealing sensitive files not intended for public access [49].
p. Source code disclosure: unless the project is an open source and meant for public use, source codes are supposed to stay private. Attackers can detect and abuse vulnerability of the system easily by analysing the source code.
q. Cross-site request forgery: tricking users into performing unintended actions on authenticated sessions, leading to unauthorized transactions, changes in user settings, or data manipulation are types of CSRF attacks. These attacks undermine user trust and can lead to severe consequences [50].

The implications of our findings suggest a need for further research into the specific types of vulnerabilities identified and the potential risk posed to institutional operations. Studies on similar educational contexts have recommended targeted approaches for improving cybersecurity in resource-constrained institutions, such as implementing standardized security protocols and focusing on cost-effective mitigation strategies. Furthermore, government institutions in Bangladesh might serve as case studies to illustrate how centralized policies and consistent funding can effectively support cybersecurity initiatives [51]. Future research could benefit from examining these initiatives in detail to develop models that non-government institutions can adapt to strengthen their own cybersecurity frameworks.

Our study highlights significant cybersecurity challenges within higher education in Bangladesh, with a particular emphasis on the greater vulnerability burden among non-government institutions. These findings underscore the importance of targeted, evidence-based measures to reduce the susceptibility of these institutions to high-severity risks. Expanding upon these insights through further research could aid in developing effective cybersecurity frameworks tailored to the needs of the academic sector, ultimately promoting a safer and more secure environment for higher education institutions in Bangladesh.

5. CONCLUSION

The findings from this study shed light on critical cybersecurity vulnerabilities within higher educational institutions in Bangladesh, underscoring the challenges faced by both government and non-government institutions. By analyzing high, medium, and low-severity vulnerabilities across these institutions, we reveal a concerning disparity: non-government institutions exhibit notably higher vulnerability counts, particularly for high-severity risks, compared to their government counterparts. This difference likely reflects disparities in cybersecurity resources, governance structures, and policy implementations between the two groups. The prevalence of medium and low-severity vulnerabilities across both types of institutions further indicates a need for systemic improvements in routine security practices.

These results hold important implications for the academic community in Bangladesh and beyond. For researchers, our findings underscore the need to investigate the unique cybersecurity challenges faced by non-government institutions, particularly in contexts where resources are limited. Practically, these insights emphasize the importance of targeted interventions, such as developing cost-effective security frameworks and implementing standardized policies to mitigate risk across the sector. By addressing vulnerabilities in a structured and resource-conscious manner, non-government institutions, in particular, can better protect their assets, data, and users.

Moreover, our study suggests pathways for future research that could enhance cybersecurity resilience in educational institutions. Expanding on this work by exploring the impact of specific cybersecurity policies, resource allocation models, and institutional practices could yield valuable insights. Similarly, longitudinal studies that examine the effectiveness of various security interventions over time would help identify sustainable strategies for reducing vulnerabilities across both government and non-government institutions.

Our study highlights significant cybersecurity challenges in Bangladesh's higher educational sector, underscoring the need for policy-driven, resource-efficient approaches to vulnerability management. Addressing these gaps will not only protect institutional networks and data but also contribute to a safer academic environment for students and staff. By continuing to study and improve cybersecurity in higher education, we can foster a resilient digital infrastructure that supports the educational and research missions of these institutions, ultimately benefiting the broader community and strengthening national cybersecurity resilience.

FUNDING INFORMATION

Authors would like to express their gratitude to the Institute for Research, Innovation, and Development (IRID), University of Asia Pacific Bangladesh for their funding. Email: sultan_mahmud@uap-bd.edu and Telephone: +8802-58157091, Ext-521

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Shadiqul Hasan Khan Janny	✓									✓				
Md. Asadujjaman Noor		✓				✓			✓					
Mohammad Enan Al Harun Sahan		✓							✓					
Sheikh Nafez Sadnan	✓					✓			✓					
Muhammad Towfiqur Rahman	✓				✓					✓				
Abu Saleh Md Bakibillah	✓				✓					✓				

C	: **C**onceptualization	I	: **I**nvestigation	Vi	: **Vi**sualization
M	: **M**ethodology	R	: **R**esources	Su	: **Su**pervision
So	: **So**ftware	D	: **D**ata Curation	P	: **P**roject administration
Va	: **Va**lidation	O	: Writing - **O**riginal Draft	Fu	: **Fu**nding acquisition
Fo	: **Fo**rmal analysis	E	: Writing - Review & **E**diting		

CONFLICT OF INTEREST STATEMENT

The authors declare that there are no conflicts of interest related to this study.

DATA AVAILABILITY

Data availability is not applicable to this paper as no datasets were generated or analyzed during the current study.

REFERENCES

[1] S. Zaman *et al*., "Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey," *IEEE Access*, vol. 9, pp. 94668-94690, 2021, doi: 10.1109/ACCESS.2021.3089681.

[2] M. Idris, I. Syarif, and I. Winarno, "Web application security education platform based on OWASP API security project," *EMITTER International Journal of Engineering Technology*, vol. 10, no. 2, pp. 246-261, 2022, doi : 10.24003/emitter.v10i2.705

[3] N. K. Rai, "Cyber crime and society: An analysis," *International Journal of Creative Research Thoughts*, vol. 9, no. 8, pp. a112-a117, 2021.

[4] Q. Chen and R. A. Bridges, "Automated behavioral analysis of malware: A case study of WannaCry ransomware," in *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Cancun, Mexico, Dec. 2017, pp. 454–460, doi: 10.1109/ICMLA.2017.0-119.

[5] M. Kashif, M. K. Javed, and D. Pandey, "A surge in cyber-crime during COVID-19," *Indonesian Journal of Social and Environmental Issues (IJSEI)*, vol. 1, no. 2, pp. 48–52, 2020.

[6] A. F. A. Naim and A. M. Ghouri, "Exploring the role of cyber security measures (encryption, firewalls, and authentication protocols) in preventing cyber-attacks on e-commerce platforms," *International Journal of eBusiness and eGovernment Studies*, vol. 15, no. 1, pp. 444-469, 2023.

[7] S. O. Manjare, *E-security evolution: Navigating the E-commerce cybersecurity landscape*, Artificial Intelligence for Cyber Security and Industry 4.0, CRC Press, pp. 292-318, 2025.

[8] O. Aslan and R. Samet, "A Comprehensive Review on Malware Detection Approaches," *IEEE Access*, vol. 8, pp. 6249–6271, 2020, doi: 10.1109/ACCESS.2019.2963724.

[9] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber security threats and vulnerabilities: a systematic mapping study," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 3171–3189, 2020, doi: 10.1007/s13369-019-04319-2.

[10] A. C. Cinar and T. B. Kara, "The current state and future of mobile security in the light of the recent mobile security threat reports," *Multimedia Tools and Applications*, vol. 82, no. 13, pp. 20269-20281, 2023.

[11] M. C. Arcuri, L. Gai, F. Ielasi, and E. Ventisette, "Cyber attacks on hospitality sector: stock market reaction," *Journal of Hospitality and Tourism Technology*, vol. 11, no. 2, pp. 277–290, 2020, doi: 10.1108/JHTT-05-2019-0080.

[12] A. Reijonen, "The Evolution of Mobile Malware," M.S. thesis, JAMK Univ. of Applied Sciences, Jyväskylä, Finland, 2024.

[13] M. F. Ansari, P. K. Sharma, and B. Dash, "Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training," *International Journal of Smart Sensor and Adhoc Network.*, pp. 61–72, 2022, doi: 10.47893/ijssan.2022.1221.

[14] S. Shah and B. M. Mehtre, "An overview of vulnerability assessment and penetration testing techniques," *Journal of Computer Virology and Hacking Techniques*, vol. 11, no. 1, pp. 27–49, 2015, doi: 10.1007/s11416-014-0231-x.

[15] U. Ravindran and R. V. Potukuchi, "A Review on Web Application Vulnerability Assessment and Penetration Testing," *Review of Computer Engineering Studies*, vol. 9, no. 1, pp. 1–22, 2022, doi: 10.18280/rces.090101.

[16] P. K. Joshi, "Achieving PCI-DSS Compliance in Payment Gateways: A Comprehensive Approach," *Journal of Technology and Systems*, vol. 6, no. 7, pp. 13-31, 2024, doi: 10.47941/jts.2299.

[17] C. Team, "One year of BGD e-GOV CIRT establishment; BGD e-GOV CIRT | Bangladesh e-Government Computer Incident Response Team," BGD e-GOV CIRT, 2016. [Online]. Available: https://www.cirt.gov.bd/one-year-of-bgd-e-gov-cirt-establishment/. (Accessed 8 May 2024).

[18] Y. Khera, D. Kumar, S. Sujay, and N. Garg, "Analysis and Impact of Vulnerability Assessment and Penetration Testing," in *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, Faridabad, India, Feb. 2019, pp. 525–530, doi: 10.1109/COMITCon.2019.8862224.

[19] J. N. Goel and B. M. Mehtre, "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology," *Procedia Computer Science*, vol. 57, pp. 710–715, 2015, doi: 10.1016/j.procs.2015.07.458.

[20] D. V. Prajapati and D. Upadhyay, "Cyber Defence A Hybrid Approach for Information Gathering and Vulnerability Assessment of Web Application (Cyberdrone)," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 5, pp. 65–72, 2019, doi: 10.26438/ijcse/v7i5.6572.

[21] A. K. Khan and M. A. Islam, "Examining the impact of the digital security act 2018 on self-censorship practices among journalists in Bangladesh," in *7th International Conference Freedom of Expression In Asia*, 2022, pp. 25-42.

[22] H. Hossain, R. K. Shohag, N. C. Nath, and S. D. Dalia, "Cybercrime as a Threat to the Banking Sector: A Perspective from Commercial Banks in Bangladesh," *International Journal of Cybersecurity Intelligence & Cybercrime*, vol. 8, no. 1, 2025, doi: 10.52306/2578-3289.1189.

[23] M. T. Islam and B. U. Khan, "Impacts of data localization policies and lessons for Bangladesh," *International Data Privacy Law*, vol. 14, no. 2, pp. 150-168, 2024, doi: 10.1093/idpl/ipae002.

[24] S. Rahman, "240 govt entities, banks come under cyber-attacks," The Financial Express, Aug. 21, 2022. [Online]. Available: https://thefinancialexpress.com.bd/national/240-govt-entities-banks-come-under-cyber-attacks-1661080789.

[25] M. S. Rana, "A Critical Analysis of the Escalating Cybercrime and its Impact in Bangladesh," *CIFILE Journal of International Law*, vol. 5, no. 9, pp. 40-49, 2024, doi: 10.30489/cifj.2023.407899.1075.

[26] R. Reheean, G. S. Sami, S. I. Ahmed, and A. D. Nipa, "Understanding the economic impact of botnets in Bangladesh: insights and strategies from attacker & victim perspectives," M. S. Thesis, Department of Computer Science and Engineering, Brac University, Dhaka, Bangladesh, 2024.

[27] M. N. Hasan, "Unveiling the Shadows: Exploring Cyber Criminology and the Plight of Cyber Victimization in Bangladesh," *Jus Corpus Law Journal*, vol. 3, pp. 139-174, 2022.

[28] A. R. M. Shaikh, "Exploring online radicalization in bangladesh: strategies and evolving dynamics," M. S. Thesis, University of Dhaka, Dhaka, Bangladesh, 2024.

[29] T. Report, "3 held over hacking into Shwapno's digital system," *The Business Standard*, 2021. [Online]. Available: https://www.tbsnews.net/bangladesh/crime/3-held-over-hacking-shwapnos-digital-system-285250. (Accessed: 9 May 2024).

[30] M. S. A. Kabir, "Lessons Learned From the Bangladesh Bank Heist," *ISACA Journal*, vol. 6, pp. 1-4, 2023.

[31] S. Rahman, "Latest cyber-attack hit at least 147 Bangladeshi entities," *The Financial Express*, 2021, [Online]. Available: https://thefinancialexpress.com.bd/sci-tech/latest-cyber-attack-hit-at-least-147-bangladeshi-entities-1617416432. (Accessed: 9 May 2024).

[32] M. Kabir and M. M. Hosen, "A Study of Financial Crimes in the Banking Sector of Bangladesh," *International Journal of Law and Public Policy (IJLAPP)*, vol. 6, no. 2, pp. 49-57, 2024, doi: 10.36079/lamintang.ijlapp-0602.677.

[33] J. Tessitore and S. Woolfson, eds., *A Global Agenda: Issues Before the 55th General Assembly of the United Nations*, Lanham, MD: Rowman & Littlefield Publishers, p. 317, 2000.

[34] K.-E.-K. Babu,"Cyber Security and Its Reality In Bangladesh: An Analysis Of Existing Legal Frameworks*," Journal of Information System Security*, vol. 17, no. 3, pp. 145–162, 2021.

[35] M. R. Islam, M. R. I. Jishan, A. Tasnim, T. Rahman, M. M. Hossen, and M. J. Niene, "Social Responsibilities of Computer Engineers in Bangladesh Context," B.Sc. thesis, Dept. of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh, 2023.

[36] R. H. Dolon, M. Ridowan, and I. J. Mouri, "The Resilience of Digital Bangladesh: A Case Study on Web Vulnerabilities in the Private Sector of Bangladesh," in *Proceedings of the 3rd International Conference on Computing Advancements*, Oct. 2024, pp. 183-191, doi: 10.1145/3723178.3723203.

[37] T. H. Mohammad, "Cybersecurity in Bangladesh's banking industry: trends, challenges, and strategic interventions," *Global Journal of Allied Sciences and Engineering*, vol. 1, no. 1, pp. 1-11, 2025.

[38] M. A. Haque *et al.*, "Cybersecurity in universities: An evaluation model," *SN Computer Science*, vol. 4, no. 5, 2023, doi: 10.1007/s42979-023-01984-x.

[39] S. Desk, "BracU registrar's email 'hacked' to send warning against BCL," *The Daily Star*, 2022. [Online]. Available: https://www.thedailystar.net/shout/news/bracu-registrars-email-hacked-send-warning-bcl-3116951. (Accessed 5 May 2024).
[40] R. J. Rony and N. Ahmed, "Teens online behavior and support interventions in Bangladesh," *ACM Journal on Computing and Sustainable Societies*, vol. 3, no. 1, pp. 1-22, 2025, doi: 10.1145/3704813.
[41] F. Kasami, "Analysis and Strategies for Security Improvement–Case Study of the Municipality of Brvenica," Ph.D. dissertation, South East European University, Tetovo, North Macedonia, 2025.
[42] K. Al-talak and O. Abbass, "Detecting server-side request forgery (SSRF) attack by using deep learning techniques," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 12, 2021, doi: 10.14569/IJACSA.2021.0121230.
[43] D. Alam, M. A. Kabir, T. Bhuiyan and T. Farah, "A Case Study of SQL Injection Vulnerabilities Assessment of .bd Domain Web Applications," in *2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec)*, Jakarta, Indonesia, 2015, pp. 73-77, doi: 10.1109/CyberSec.2015.23.
[44] J. Mukamisha, A. Iradukunda, E. Manzi and J. D. Ndibwile, "Mitigating Server-Side Request Forgery (SSRF) Attacks: An Empirical Analysis of Deep Learning-Based Approaches,"in *2025 9th International Conference on Cryptography, Security and Privacy (CSP)*, Okinawa, Japan, 2025, pp. 112-119, doi: 10.1109/CSP66295.2025.00027.
[45] M. Mthunzi and S. Maqolo, "Mobile, App, and Cloud Security: Threats, Vulnerabilities, and Defense Mechanisms," preprint, 2025, doi: 10.5281/zenodo.17371091.
[46] D. T. Murphy, M. F. Zibran and F. Z. Eishita, "Plugins to Detect Vulnerable Plugins: An Empirical Assessment of the Security Scanner Plugins for WordPress," in *2021 IEEE/ACIS 19th International Conference on Software Engineering Research, Management and Applications (SERA)*, Kanazawa, Japan, 2021, pp. 39-44, doi: 10.1109/SERA51205.2021.950927.
[47] T. Mataracioglu, "Comparison of PCI DSS and ISO/IEC 27001 Standards," *ISACA Journal*, vol. 1, 2016.
[48] Y. Sadqi and Y. Maleh. "A systematic review and taxonomy of web applications threats," *Information Security Journal: A Global Perspective*, vol. 31, no. 1, pp. 1-27, 2022, doi: 10.1080/19393555.2020.1853855.
[49] I. Tyshyk and H. Hulak, "Testing an organization's information system for unauthorized access," *Cybersecurity Providing in Information and Telecommunication Systems II 2024*, 2024, pp. 17-29.
[50] A. Sudhodanan, R. Carbone, L. Compagna, N. Dolgin, A. Armando, and U. Morelli, "Large-Scale Analysis & Detection of Authentication Cross-Site Request Forgeries," in *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, Paris, France, 2017, pp. 350-365, doi: 10.1109/EuroSP.2017.45.
[51] A. S. Sikder and M. R. Islam, "Enhancing Cyber-Resilience within Bangladesh's Legal Framework: Evaluating Preparedness and Mitigation Strategies against Technologically-Driven Threats.: Enhancing Cyber-Resilience within Bangladesh's Legal Framework." *International Journal of Imminent Science & Technology*, vol. 1, no. 1, pp. 40-57, 2023, doi: 10.70774/ijist.v1i1.6.

BIOGRAPHIES OF AUTHORS

Shadiqul Hasan Khan Janny is a Security Researcher with industry experience in computer and network security. He received a degree in Computer Science and Engineering, with a focus on Computer Engineering, from the University of Asia Pacific. His primary research interests lie in web application security, vulnerability analysis, and secure system design. He can be contacted at email: It.khanjanny@gmail.com.

Md. Asadujjaman Noor is a Cyber Security Engineer who specializes in digital forensics, penetration testing, and secure system design, focusing on advanced security solutions. He holds a B.Sc. in Computer Science and Engineering from the University of Asia Pacific and is currently pursuing his Master's in Computer Science at Jahangirnagar University, where his research explores Post-Quantum Cryptography and AI-powered Cyber Security Frameworks. He has served as a Judge and Keynote Speaker at several national cybersecurity events. Passionate about innovation, he is dedicated to strengthening AI-driven cyber resilience and promoting cyber awareness across communities. He can be contacted at email: asadujjaman1122@gmail.com.

Mohammad Enan Al Harun Sahan is a Computer Science enthusiast with strong interests in cybersecurity, artificial intelligence, blockchain technologies, and secure distributed systems. He earned his B.Sc. in Computer Science and Engineering from the University of Asia Pacific, where he explored concepts involving blockchain and federated learning. He is motivated to deepen his expertise at the intersection of security and intelligent systems, with the long-term goal of contributing to impactful, peer-reviewed research. He can be contacted at email: enanalharun@gmail.com.

Sheikh Nafez Sadnan is an IT engineer with professional experience in web development, computer networking, blockchain, and data science. He received his B.Sc. degree in Computer Science and Engineering from the University of Asia Pacific (UAP), Bangladesh. He has worked with several leading organizations in Bangladesh, including bKash Limited and National Energy Services Limited (NESL). He has participated in numerous cybersecurity events held in Bangladesh, as well as hackathons organized by NASA, and contributed to the 45th ICPC World Finals as part of the organizing team. His research interests include data-driven technologies, artificial intelligence, cybersecurity, and emerging innovations in information systems. He can be contacted at email: nafez.sadnan95@gmail.com.

Muhammad Towfiqur Rahman received his Ph.D. degree under Electrical and Computer Systems Engineering, Monash University in 2021. He also completed his M.Sc. in Communication Engineering from International Islamic University Malaysia and bachelor's Degree in Computer Science and Engineering and MBA degree from International Islamic University Chittagong. He is currently working as an Assistant Professor at University of Asia Pacific, Bangladesh. His research interests include high-speed optical visible light communication, 5G/6G communications, optical wireless communication, machine learning, robotics, AI driven drone technology, and cybersecurity. He can be contacted at email: towfiq@uap-bd.edu.

Abu Saleh Md Bakibillah received the M.Sc. degree in information technology from Stuttgart University, Stuttgart, Germany, in 2013, and the Ph.D. degree in mechatronics engineering from Monash University, Melbourne, VIC, Australia, in 2020. He was a Project Engineer at Bay Power Limited, Bangladesh, in 2008, and then joined the Department of Electrical and Electronic Engineering at the International Islamic University Chittagong (IIUC), Bangladesh, as a Lecturer in 2009 and was promoted to an Assistant Professor in 2014. From 2014 to 2016, He was an Assistant Professor in the Department of Electrical and Electronic Engineering at American International University Bangladesh (AIUB), Bangladesh. He worked as a Postdoctoral Research Fellow in the Department of Robotics and Mechatronics Engineering at Monash University, Malaysia Campus, from 2021 to 2022. Currently, he is a Specially Appointed Assistant Professor in the Department of Systems and Control Engineering, School of Engineering, at the Institute of Science Tokyo, Japan. He can be contacted at email: bakibillah.a.aa@m.titech.ac.jp.