Jurnal E-Komtek
Vol. 8 No. 2 (2024) pp. 245-254
https://jurnal.politeknik-kebumen.ac.id/index.php/E-KOMTEK
p-ISSN : 2580-3719 e-ISSN : 2622-3066

Evaluation of Two-Factor Authentication (2FA) TOTP in Higher Education Using Vulnerability Assessment and CIA Triad

Heru Wijayanto Aripradono[1], Haeruddin[2], Kurnia Cantra[3]

[1-3]Department of Information Technology, Universitas Internasional Batam, Indonesia, 29426

2132014.kurnia@uib.edu

https://doi.org/10.37339/e-komtek.v8i2.2113

Published by Politeknik Piksi Ganesha Indonesia

Artikel Info
Submitted:
14-11-2024
Revised:
21-11-2024
Accepted:
22-11-2024
Online first :
26-11-2024

Abstract

Vulnerability exploitation in education websites often leads to data breaches, negatively impacting learning activities, notably higher education, which is highly susceptible to such attacks. This research evaluates the effectiveness of two-factor authentication in mitigating exploitability. To analyze issues further, vulnerability assessment tools, such as Burp Suite and ZAP, can explore website vulnerability and the CIA Triad framework (Confidentiality, Integrity, Availability). The analysis revealed three medium-level vulnerabilities and six low-level vulnerabilities; key topics such as CSRF (Cross-Site Request Forgery) and XSS (Cross-Site Scripting), compromise integrity, and MITM (Man-In-The-Middle) attacks threaten Confidentiality, these vulnerabilities indicate non-compliance with CIA Triad, mitigation strategy such are VPN (Virtual Private Network), and WAF (Web Application Firewall) were proposed. While two-factor authentication improves security, additional fixes and optimizations are required for its effective implementation in the education sector.

Keywords: *Two Factor Authentication, Vulnerability Assessment, CIA Triad, Man-In-The-Middle*

Abstrak

Eksploitasi kerentanan di situs web pendidikan sering kali mengarah pada pelanggaran data, yang berdampak negatif pada kegiatan pembelajaran, khususnya pendidikan tinggi, yang sangat rentan terhadap serangan semacam itu. Penelitian ini mengevaluasi efektivitas autentikasi dua faktor dalam memitigasi eksploitasi. Alat penilaian kerentanan, seperti Burp Suite dan ZAP, untuk mengeksplorasi kerentanan situs web, dan kerangka kerja CIA Triad (Kerahasiaan, Integritas, Ketersediaan), untuk menganalisis lebih lanjut. Analisis tersebut mengungkapkan 3 kerentanan tingkat menengah dan 6 kerentanan tingkat rendah yang ditemukan, masalah utama seperti CSRF (Pemalsuan Permintaan Lintas Situs) dan XSS (Skrip Lintas Situs), kompromi integritas, dan serangan MITM (Manusia di Tengah) mengancam kerahasiaan, kerentanan ini mengindikasikan ketidakpatuhan terhadap CIA Triad, strategi mitigasi seperti VPN (Jaringan Pribadi Virtual), dan WAF (Firewall Aplikasi Web) diusulkan. Meskipun autentikasi dua faktor meningkatkan keamanan, perbaikan dan pengoptimalan tambahan diperlukan untuk implementasi yang efektif di sektor pendidikan.

Kata-kata kunci: *Autentikasi Dua Faktor, Penilaian Kerentanan, CIA Triad, Manusia di Tengah*

1. Introduction

System access and information security were a crucial factor. Ease of system access can have a direct impact in the form of convenience for users [1]. With easy access to information, there is a need for information security, especially since the information stored is personal and sensitive. Data breach cases are increasingly rampant worldwide; based on the Identity Theft Resource Center report for the United States, there are 3,205, with 900 thousand victims of data breach cases in 2023 [2]. Based on Statista, in 2023, there were 1 million data breaches in Indonesia [3].

The education sector is vulnerable to data breaches since much of the information in higher education is personal and sensitive, such as identification numbers, addresses, phone numbers, research, and many more [4] [5]. There are significant vulnerabilities in the education sector, especially university websites, with a high level of vulnerability [6]. The level of attacks in the education sector was the highest in Check Point Research's 2023 report, stating there were 2,314 attacks every week against the education and research sector globally [7].

The high rate of attacks increases data breaches; in the 2023 Verizon report, there were 238 data breaches [8], and the 2024 report stated as many as 1,537 data breaches [9] with the same attack pattern, such as vulnerability exploitation, there was an increase of 545.8% from the previous year, which is a significant increase. The increase in data breaches in the education sector is due to the rise in users and the digitisation of the education system [10], one of which is the academic portal [11]; with occurring information breach, mitigation is a solution that can be used to secure and reduce the impact of data breach [12].

A mitigation method in higher education web pages is using Two-Factor Authentication (2FA) [13]. 2FA is a security system that requires two ways to confirm a user's identity to avoid the risk of unauthorised access and identity theft [14]. The use of 2FA and authentication is proven in securing sectors other than education, such as the financial sector [15] [16] and the industrial sector [17].

The rarity of security research in higher education and the education sector needs to be more balanced with its importance and significance, especially in mitigating and reducing harm [18]. 2FA research and implementation in the academic system are not impossible; they are necessary, but the implementation of 2FA itself does not guarantee security [19]. 2FA itself also contains vulnerabilities that can and may be exploited. In several research studies regarding 2FA, one particular vulnerability was username exposure [20], unencrypted security key [21], and plain text backup key [22]. Vulnerability in 2FA [23] Data breaches render web pages insecure; due to these issues, it is necessary to understand how well 2FA can help and the preparation needed to mitigate cyber-attacks.

This research discusses the common issues on the web page and 2FA's efficiency in reducing issues; with the implementation of 2FA, 2FA can run without significant problems for the user [24].

2. Method

This research utilizes Vulnerability Assessment, which identifies, defines, and classifies vulnerabilities to seek preventive action and test efficiency [25]. Figure 1 illustrates the vulnerability assessment flowchart and the two-factor authentication method against the academic information system using the Penetration Testing tool and the CIA Triad.

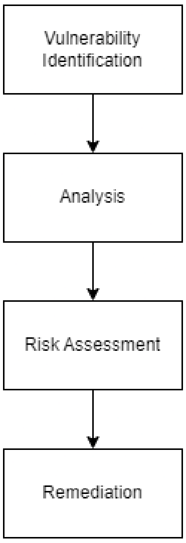


Figure 1. Vulnerability Assessment Flowchart

a. Vulnerability Identification

Vulnerability Identification is a vulnerability search phase using vulnerability identification tools such as Burp Suite, OWASP Zap, Nessus, and others; in this study using Burp Suite, as well as OWASP Zap, to search for vulnerability information on the higher education website that vulnerability information is needed to maximise the security system [26].

b. Analysis

Analysis is the vulnerability evaluation phase, namely, the vulnerability that exists in the system. In mitigating the TOTP Wordfence system on the higher education website using WPSchoolPress, such as the vulnerability of information integrity and TOTP information.

The vulnerabilities obtained can disrupt information security, which is the CIA Triad

(Confidentiality, Integrity, Availability), in mitigating and fixing problems that can cause material loss and material loss [27].

1. *Confidentiality*: security that focuses on Confidentiality and protection of information.
2. *Integrity*: security that focuses on the consistency and completeness of information.
3. *Availability*: security that focuses on the availability of information according to user requests.

Figure 2 presents the qualifications of the CIA Triad system, with each session fulfilled.

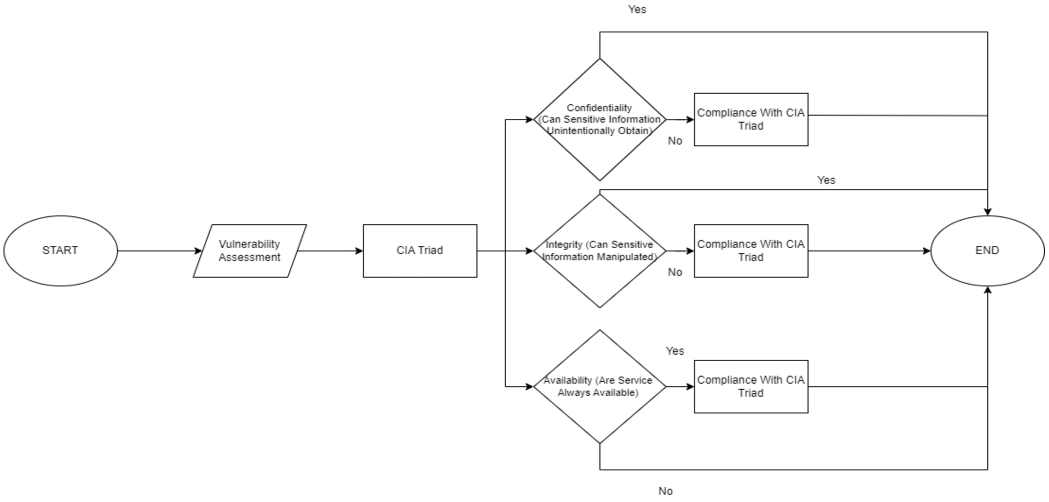

Yes
Confidentiality (Can Sensitive Information Unintentionally Obtain)
Compliance With CIA Triad
No
Yes
START
Vulnerability Assessment
CIA Triad
Integrity (Can Sensitive Information Manipulated)
Compliance With CIA Triad
No
END
Yes
Availability (Are Service Always Available)
Compliance With CIA Triad
No

Figure 2. CIA Triad Implementation Flowchart

c. Risk Assessment

Risk Assessment evaluates vulnerability based on its level, including low to high levels, its impact, and the risk to the likelihood of vulnerability occurring to more clearly resolve and understand the vulnerability.

d. Remediation

Remediation is the end of the vulnerability assessment. It resolves the vulnerabilities obtained after the analysis phase and risk assessment to reduce the overall impact of losses.

3. Results and Discussion

a. Vulnerability Identification

Vulnerability Identification tests the security of the 2FA method in WordPress, using WPSchoolPress as an LMS (Learning Management System) shown in **Figure 3**, the 2FA TOTP method from Wordfence Login Security, Google Authenticator as a TOTP provider, and vulnerability search tools, namely Burpsuite, Foxy Proxy, and OWASP (Open Web Application Security Project) ZAP.

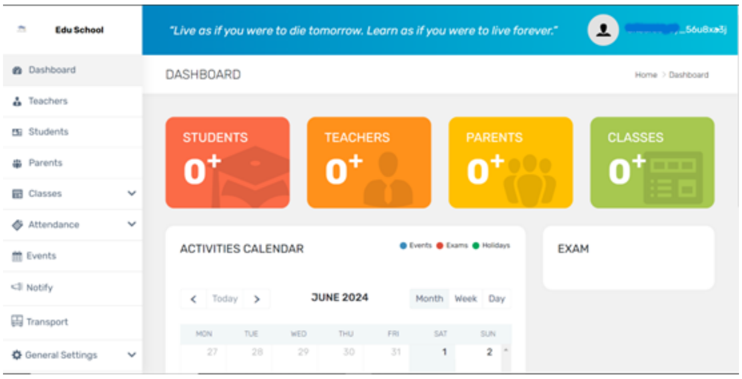


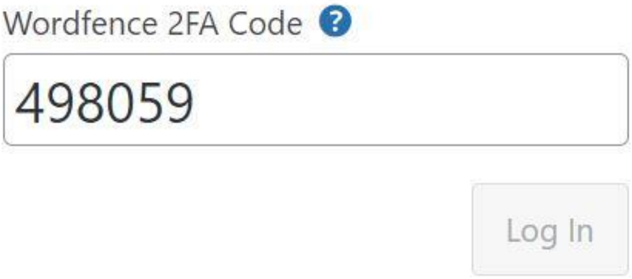
Figure 3. WPSchoolPress Interface

b. Analysis

This study's analysis uses two penetration testing tools, Burp Suite and OWASP Zap. The vulnerabilities are shown in **Figures 4**, **Figure 5**, and **Figure 6**.

1. Burp Suite

The use of Burpsuite and Foxy Proxy as supporting tools in finding vulnerabilities on the testing.authentication.my.id/wp-login.php/ website, with the HTTPS (Hypertext Transfer Protocol Secure) protocol, and using the intercept feature in Burpsuite in finding login page encryption vulnerabilities. The information contained in the server and user communication can be known; through this, the information contained, such as the user name and user password, will be known, not to mention the TOTP, known as "498059", which is listed in **Figure 4**, as well as **Figure 5** with the user name, password, and TOTP on the token.


Wordfence 2FA Code

498059

Log In

Figure 4. TOTP Wordfence

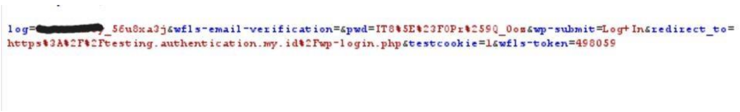
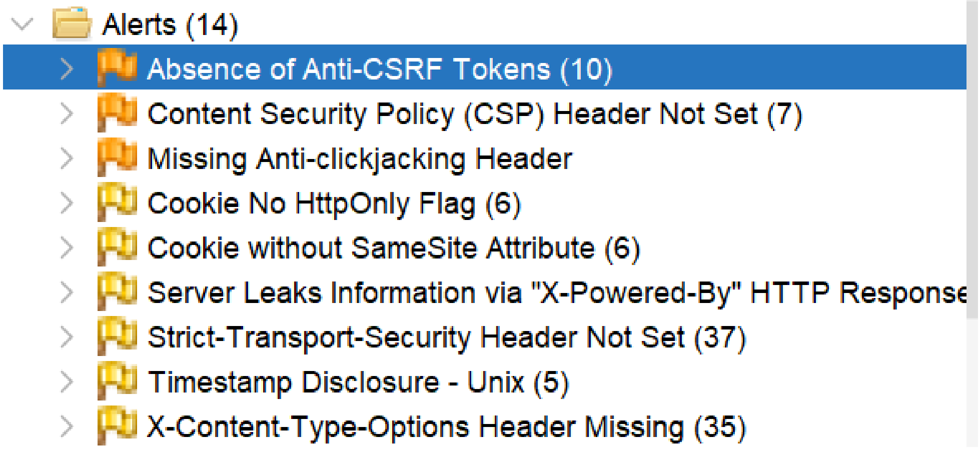

```
log=[redacted]_56u8xa3j&wfls-email-verification=&pwd=IT8%5E%23F0Pr%259Q_0os&wp-submit=Log+In&redirect_to=
https%3A%2F%2Ftesting.authentication.my.id%2Fwp-login.php&testcookie=1&wfls-token=498059
```

Figure 5. Burpsuite Outcome

2. OWASP ZAP

OWASP ZAP (Zed Attack Proxy) is an application used in the search for page vulnerabilities, using Manual Explore, searching for login system vulnerabilities; several vulnerabilities can be found on the college website, with three medium-level vulnerabilities and six low-level vulnerabilities, which are shown in **Figure 6**.



Alerts (14)
- Absence of Anti-CSRF Tokens (10)
- Content Security Policy (CSP) Header Not Set (7)
- Missing Anti-clickjacking Header
- Cookie No HttpOnly Flag (6)
- Cookie without SameSite Attribute (6)
- Server Leaks Information via "X-Powered-By" HTTP Response
- Strict-Transport-Security Header Not Set (37)
- Timestamp Disclosure - Unix (5)
- X-Content-Type-Options Header Missing (35)

Figure 6. Web Page Vulnerability Using OWASP ZAP

3. CIA Triad

The CIA Triad, Confidentiality, Integrity, and Availability, is the basis of information security; with the vulnerabilities contained, the web page does not meet the security standards stated in Figure 2. The CIA Triad analysis is explained below.

- Confidentiality

One vulnerability in the Confidentiality of the web page is the transportation of sensitive information, such as TOTP, that can be known, so it does not meet the confidentiality requirements. With this information, an MITM (Man-In-The-Middle) Attack can occur.

- Integrity

Several information integrity vulnerabilities unrelated to TOTP, such as CSRF (Cross-Site Request Forgery) and XSS (Cross-Site Scripting), can attack user identity forgery.

- Availability

In Figure 6, there is no information or vulnerabilities related to TOTP, nor information on vulnerabilities outside of TOTP.

c. Risk Assessment

Vulnerabilities in the web page in Figure 6, there are a total of 9 vulnerabilities, of which there are three medium-level vulnerabilities and six low-level vulnerabilities; the vulnerabilities will be explained in **Table 1**.

Table 1. Vulnerability Table

Vulnerability	Explanation	Risk
Absence of Anti-CSRF Tokens	CSRF (Cross-Site Request Forgery) is a security attack that involves forging a user's identity to manipulate and record the user's personal information.	Medium
Content Security Policy (CSP) Header Not Set	A layer of detection and mitigation of XSS (cross-site scripting) attacks and Data Injection attacks.	Medium
Missing Anti-clickjacking Header	Defence system against clickjacking attacks.	Medium
Cookie No HttpOnly Flag	HttpOnly cookies can be accessed in JavaScript, which leads to session hijacking.	Low
Cookie without SameSite Attribute	Cookies may be sent due to "Cross Site Scripting" requests.	Low
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Server Leaks Information via “X-Powered-By” HTTP Response Header Field(s) is the current server information.	Low
Strict-Transport-Security Header Not Set	There is no HSTS (HTTP Strict Transport Security) on the webpage that forces users to use HTTPS.	Low
Timestamp Disclosure - UNIX	Timestamp Disclosure - UNIX is the timestamp information and technology used.	Low
X-Content-Type-Options Header Missing	X-Content-Type-Options Header Missing is a MIME-Sniffing (Multipurpose Internet Mail Extension) prevention for Cross-Site Scripting attacks.	Low

d. Remediation

Fixing vulnerabilities, namely from MITM, using VPN (Virtual Private Network), DNSSEC (Domain Name System Security Extensions) [28], and HSTS can improve web page security.

Many web page vulnerabilities, such as CSRF and XSS, can be mitigated using WAF (Web Application Firewall) [29]. Vulnerabilities such as Timestamp Disclosure—Unix can be mitigated by ensuring that the information contained does not contain any sensitive information.

The solution in this research is not absolute; it is only a preventive measure. The research aims to determine the effectiveness of 2FA and its vulnerability.

e. Discussion

In the Burp Suite analysis, MITM vulnerabilities can be exploited, so it can be stated that using TOTP is unsafe because it is vulnerable to MITM attacks. However, with the MITM attack prevention system, TOTP can still be used; a time-based security system can minimize brute force attacks. The use of ZAP provides essential information on the vulnerabilities that exist in the system. However, the use of TOTP can help the system's security. Vulnerabilities can still be exploited, and preventive actions and repairs can be done quickly to mitigate attacks and exploits.

Grouping the vulnerability levels in ZAP provides an understanding of the importance of system improvements and preliminary improvements; they can be used with the addition of mandatory vulnerability improvements. With enhancements, TOTP can be used to its full potential and thus become helpful.

4. Conclusion

TOTP Authentication can help maintain information security, primarily if the user's username and password are known or breached; TOTP implementation can help web pages from data breaches caused by vulnerability exploitation. If page security is good, implementing TOTP only sometimes provides security to higher education web pages. Improvements to the website must still be made to ensure security is maintained, and the website must continue to improve. The CIA Triad method only explores some of the problems that arise, so further research is needed, using a different framework that can examine far more vulnerabilities, using this research as a guide.

References

[1] F. A. Aridinta and G. Widijoko, "Analisis pengaruh kenyamanan layanan online terhadap kepuasan konsumen mobile commerce di Indonesia," *J. Ilm. Mhs. FEB*, vol. 7, no. 2, pp. 1–23, 2019.

[2] "2023 Data Breach Report," 2024. [Online]. Available: https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf.

[3] "Global accounts breached by market 2023 | Statista." Accessed: Aug. 28, 2024. [Online]. Available: https://www.statista.com/statistics/1307524/number-of-accounts-exposed-worldwide-by-country/.

[4] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," *Futur. Internet*, vol. 13, no. 2, pp. 1–40, 2021, doi: 10.3390/fi13020039.

[5] A. Arista and K. N. M. Ngafidin, "An Information System Risk Management of a Higher Education Computing Environment," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 12, no. 2, pp. 557–564, 2022, doi: 10.18517/ijaseit.12.2.13953.

[6] P. Jarupunphol, S. Seatun, and W. Buathong, "Measuring vulnerability assessment tools performance on the university web application," *Pertanika J. Sci. Technol.*, vol. 31, no. 6, pp. 2973–2993, 2023, doi: 10.47836/pjst.31.6.19.

[7] Check Point, "Check Point Cyber Security Report 2023," *Check Point Res.*, 2023, [Online]. Available: https://resources.checkpoint.com/cyber-security-resources/2022-cyber-security-report.

[8] Verizon, "DBIR: Data Breach Investigations Report 2023," 2023, [Online]. Available: https://www.verizon.com/business/resources/T717/reports/2023-data-breach-investigations-report-dbir.pdf.

[9] "DBIR: Data Breach Investigations Report 2024," 2024, [Online]. Available: https://www.verizon.com/business/resources/Tad3/reports/2024-dbir-data-breach-investigations-report.pdf.

[10] L. A. Alexei and A. Alexei, "Cyber security threat analysis in higher education institutions as a result of distance learning," *Int. J. Sci. Technol. Res.*, no. 3, pp. 128–133, 2021.

[11] A. S. Sikder, "Cybersecurity framework for ensuring confidentiality, integrity, and availability of university management systems in university management systems in Bangladesh," no. 1, pp. 17–39, 2023.

[12] J. E. W. Prakasa, "Peningkatan keamanan sistem informasi melalui klasifikasi serangan terhadap sistem informasi," *J. Ilm. Teknol. Inf. Asia*, vol. 14, no. 2, p. 75, 2020, doi: 10.32815/jitika.v14i2.452.

[13] P. Kautwima, T. Haiduwa, K. Sai, V. Hashiyana, and N. Suresh, "System end-user actions as a threat to information system security," *Int. J. Netw. Secure. Its Appl.*, vol. 13, no. 6, pp. 71–83, 2021, doi: 10.5121/ijnsa.2021.13606.

[14] J. Dutson, D. Allen, D. Eggett, and K. Seamons, "Don't punish all of us: measuring user attitudes about two-factor authentication," *Proc. - 4th IEEE Eur. Symp. Secure. Priv. Work. EUROS PW 2019*, pp. 119–128, 2019, doi: 10.1109/EuroSPW.2019.00020.

[15] H. U. Khan, M. Sohail, S. Nazir, T. Hussain, B. Shah, and F. Ali, "Role of authentication factors in fin-tech mobile transaction security," *J. Big Data*, vol. 10, no. 1, 2023, doi: 10.1186/s40537-023-00807-3.

[16] K. M. Fitria, "Analisis serangan malware dalam perbankan dan perencanaan solusi keamanan," *J. Inform. dan Tek. Elektro Terap.*, vol. 11, no. 3, 2023, doi: 10.23960/jitet.v11i3.3312.

[17] I. Alsmadi, Z. Dwekat, R. Cantu, and B. Al-Ahmad, "Vulnerability assessment of industrial systems using Shodan," *Cluster Comput.*, vol. 25, no. 3, pp. 1563–1573, 2022, doi: 10.1007/s10586-021-03330-3.

[18] N. S. Fouad, "Securing higher education against cyber threats: from an institutional risk to a national policy challenge," *J. Cyber Policy*, vol. 6, no. 2, pp. 137–154, 2021, doi: 10.1080/23738871.2021.1973526.

[19] A. R. Pratama and F. M. Firmansyah, "Until you have something to lose! Loss aversion and two-factor authentication adoption," *Appl. Comput. Informatics*, 2021, doi 10.1108/aci-12-2020-0156.

[20] J. Berrios, E. Mosher, S. Benzo, C. Grajeda, and I. Baggili, "Factorizing 2FA: forensic analysis of two-factor authentication applications," *Forensic Sci. Int. Digit. Investig.*, vol. 45, p. 301569, 2023, doi: 10.1016/j.fsidi.2023.301569.

[21] C. Ozkan and K. Bicakci, "Security analysis of mobile authenticator applications," *2020 Int. Conf. Inf. Secur. Cryptology, ISCTURKEY 2020 - Proc.*, pp. 18–30, 2020, doi: 10.1109/ISCTURKEY51113.2020.9308020.

[22] C. Gilsenan, F. Shakir, N. Alomar, and S. Egelman, "Security and privacy failures in

popular 2FA apps," *32nd USENIX Security. Symp. USENIX Security. 2023*, vol. 3, pp. 2079–2096, 2023, doi: https://dl.acm.org/doi/10.5555/3620237.3620354.

[23] R. Grimes, "The many ways to hack 2FA," *Netw. Secur.*, vol. 2019, no. 9, pp. 8–13, 2019, doi: 10.1016/S1353-4858(19)30107-2.

[24] G. F. Nama. Moreover, K. Muludi., "Implementation of two Factor authentication (2FA) to enhance the security of academic information system," *J. Eng. Appl. Sci.*, no. 112, 2018.

[25] I. G. N. Mantra, M. S. Hartawan, H. Saragih, and A. A. Rahman, "Web vulnerability assessment and maturity model analysis on Indonesia higher education," *Procedia Comput. Sci.*, vol. 161, pp. 1165–1172, 2019, doi: 10.1016/j.procs.2019.11.229.

[26] M. Rajab and A. Eydgahi, "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education," *Comput. Secur.*, vol. 80, pp. 211–223, 2019, doi: 10.1016/j.cose.2018.09.016.

[27] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electron.*, vol. 12, no. 6, 2023, doi: 10.3390/electronics12061333.

[28] E. Ylli and J. Fejzaj, "Man in the middle: Attack and protection," *CEUR Workshop Proc.*, vol. 2872, no. May, pp. 198–204, 2021.

[29] M. Srokosz, D. Rusinek, and B. Ksiezopolski, "A new WAF-based architecture for protecting web applications against CSRF attacks in the malicious environment," *Proc. 2018 Fed. Conf. Comput. Sci. Inf. Syst. FedCSIS 2018*, vol. 15, pp. 391–395, 2018, doi: 10.15439/2018F208.