



Analysis of Higher Education SIAKAD Website Security Gaps Using the Vulnerability Assessment Method

Naufal Athif Syarifudin¹, Lila Setiyani^{2*}

STMIK Rosma, Indonesia | naufal.syarifudin@mhs.rosma.ac.id¹

STMIK Rosma, Indonesia | lila.setiyani@dosen.rosma.ac.id²

Received: 11-08-2023

Reviewed: 19-08-2023

Accepted: 21-08-2023

Abstract

SIAKAD is a website-based application designed to facilitate academic management and academic activities by universities. The SIAKAD system contains sensitive and important information from lecturers and students such as personal, academic, and financial information. Seeing the importance of information security, universities must be able to ensure that their SIAKAD is protected by a strong and reliable security system. To find out threats that can be exploited by hackers, it is necessary to analyze security holes in a system. The research procedure was carried out through (1) Terminal, Zenmap, Whois, Wappalyzer as tools for foot printing or data collection, (2) OWASP ZAP as a tool for conducting Vulnerability Scanning. The results of this study revealed that there were 11 vulnerabilities found, consisting of 5 medium vulnerability levels and 6 low level vulnerabilities. In addition, to deal with these vulnerabilities, this research also discusses solutions that can be alternatives for increasing information security in higher education SIAKAD.

Keywords: OWASP, Zenmap, Vulnerability, SIAKAD, Vulnerability Scanning

Introduction

SIAKAD is a website-based application designed to facilitate academic management and academic activities by universities. This system allows students and lecturers to access information about class schedules, announcements, exam results, grades, and other academic information online. The SIAKAD system contains sensitive and important information from lecturers and students such as personal, academic and financial information. Seeing the importance of information security, universities must be able to ensure that their SIAKAD is protected by a strong and reliable security system. A good security system at SIAKAD includes securing access, controlling access rights, data encryption, backup systems, periodic security testing, as well as monitoring and response actions in the event of a security breach. To find out threats that can be exploited by hackers, it is necessary to analyze security holes in a system.

Analysis of Higher Education SIAKAD Website Security Gaps Using the Vulnerability Assessment Method

Vulnerability Assessment is a method used to analyze security vulnerabilities in an application, using tools, one of which is OWASP ZAP. By ensuring the security of SIAKAD, universities can protect student and lecturer data and maintain the reputation of their institution. The system that researchers will carry out research on security gap analysis is the Academic Information System at XYZ college. XYZ has a SIAKAD website as a facility for students and lecturers to carry out their academic activities. This study aims to identify the vulnerability gaps in the SIAKAD system, and determine the level of danger for each threat. From the test results, it can be repaired immediately by XYZ to prevent system exploitation by hackers.

Some researchers reveal that to find out security holes in a website system, they can use the Vulnerability Assessment method. This is proven by research conducted by Riadi et.al that the Vulnerability Assessment Method can be used to analyze the security of the Open Journal System website(Riadi et al., 2020). Apart from that, research conducted by Orisa and Ardita also used the Vulnerability Assessment Method to improve the quality of website security(Orisa & Ardita, 2021). Research conducted by Sirait et.al also proved that Vulnerability can be used to determine vulnerabilities in network security systems(Sirait et.al. 2018). The Vulnerability Assessment method is also proven by research conducted by Maulana et al to analyze and find weaknesses in the PT Semen Tonasa website application(Maulana et al., 2017). Subsequent research conducted by Mulyanto et.al proved that the Vulnerability Assessment method can be used to determine security vulnerabilities on school websites (Mulyanto et al., 2021). In addition, Dewi et al also explained that the Vulnerability Assessment can be used to find out the vulnerability gaps on websites(Dewi et al., 2023). Research conducted by Indera et.al that the Vulnerability Assessment method is used to analyze security holes on the KPPM FRI website(Indera et al., 2023). Subsequent research conducted by Wibowo et al also proved that the Vulnerability Assessment method can be used to determine vulnerabilities and weaknesses on websites(Wibowo et al., 2019). The purpose of this study is to focus on obtaining information on security holes and vulnerabilities in the Academic Information System (SIAKAD) web application. The results of the tests that have been carried out can be used by IT staff and SIAKAD application developers in XYZ as evaluation material for repairs to systems that have known security holes.

Literature Review

1. SIAKAD

SIAKAD is an academic management information system that facilitates the management of students, grades, lecturers, scheduling, lecture records, and other information related to academic activities in tertiary institutions (Nuari, n.d.). This system is capable of supporting decision-making processes in universities (Siregar & Situmeang, 2022). Most college applications are built on a website platform, because of the ease of access (Suryandani et al., 2017). This information system aims to support higher education activities so that the stakeholders involved can feel satisfied with academic services (Suryawan & Prihandoko, 2018). Therefore, many tertiary institutions adopt this technology in order to improve academic services which specifically involve lecturers, students, academic administration and parents of students (Purwati et al., 2018).

2. Vulnerability Assessment

The vulnerabilities that exist in IT infrastructure can be identified by using the Vulnerability Assessment approach (Aziz, 2021). This approach is one of the preventive actions that is part of a series of technological controls (Moret, 2014). This approach technically conducts a thorough and in-depth security analysis of information security, by carrying out this approach, scanning networks, system configurations, how to manage the system and awareness of the system users involved are known for their potential vulnerabilities (Zattu Maharani et al., n.d.). This approach can be a guide as well as a strategy for managing information systems so that solutions can emerge before the system is exposed to information security risks (Cunong et al., 2020). In addition, by knowing the vulnerabilities or gaps in an information system, repairs are made for these gaps, which have an impact on increasing the performance of a system (Tania et al., 2018)

3. Open Web Application Security Project Zed Attack Proxy (OWASP ZAP)

OWASP ZAP is a vulnerability scanner tool that is open source, so that anyone can develop these tools to meet their needs (Elanda & Lintang Buana, 2021). These tools are managed by non-profit organizations, so they can support the success of these tools in the future (Hidayatulloh & Saptadiaji, 2021). OWASP was developed with the aim of providing a data source so that application developers can learn about website security systems and improve their security (Priyawati et al., 2022). In addition, the developer of these tools also opens opportunities for everyone in the field of information security to improve information system security by developing the OWASP application (Kuncoro & Rahma, 2021). These tools are capable of scanning vulnerabilities that can be used as a standard for testing, so that vulnerability information can be generated (Riandhanu, 2022).

Research Method

This study adopts the steps in the Vulnerability Assessment activity, which includes 4 steps (Akmal et al., 2017), as shown in Figure 1 below:



Figure 1. Vulnerability Assessment Stages

Foot printing

This stage is carried out by collecting data or information related to the target web, some of the applications used to carry out this stage include the terminal, Zenmap, Whois, and Wappalyzer (Akmal et al., 2017).

Analysis of Higher Education SIAKAD Website Security Gaps Using the Vulnerability Assessment Method

Vulnerability Scanning

At this stage, the vulnerability scanning tool, OWASP ZAP, is used. These tools are used for network scanning. This stage aims to obtain information from network vulnerabilities, which can be seen from the list of ports with open status, bugs in the application and others (Alwi et al., 2020).

Vulnerability Analysis

This stage involves analysis by the researcher of the vulnerability information found after scanning the target using OWASP ZAP. In addition, researchers will provide recommendations on how to fix or overcome the vulnerabilities that have been identified (Fauzan & Syukhri, 2021).

Result

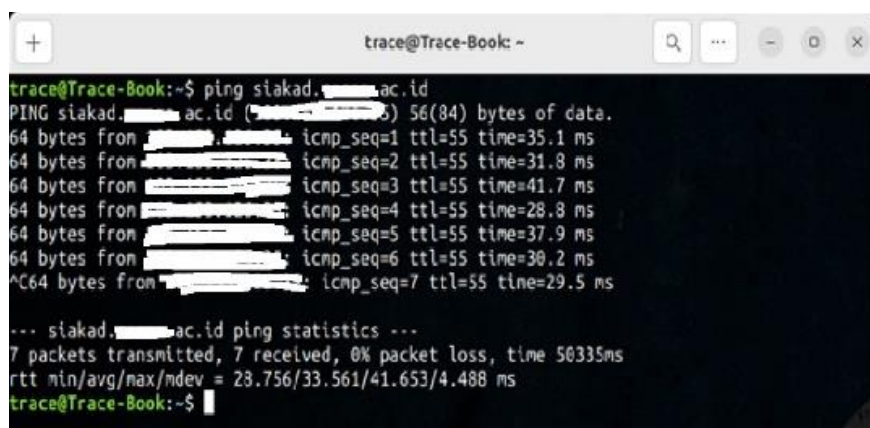
At this point, the research results will be explained based on the vulnerability assessment stages.

1. Foot printing

At this stage the targets to be analyzed will be presented by displaying Terminal, Zenmap, Whois, and Wappalyzer.

2. Terminal

The first tool used is the Terminal. The terminal is a tool available on the Linux operating system, its function is the same as the command prompt (CMD) on the Windows operating system. In the first foot printing activity, the terminal is used to ping the domain (siakad.xyz.ac.id) which is intended to identify the server IP of the SIAKAD website.



```
trace@Trace-Book: ~  
trace@Trace-Book:~$ ping siakad.103.153.100.ac.id  
PING siakad.103.153.100.ac.id (103.153.100.5) 56(84) bytes of data.  
64 bytes from 103.153.100.5: icmp_seq=1 ttl=55 time=35.1 ms  
64 bytes from 103.153.100.5: icmp_seq=2 ttl=55 time=31.8 ms  
64 bytes from 103.153.100.5: icmp_seq=3 ttl=55 time=41.7 ms  
64 bytes from 103.153.100.5: icmp_seq=4 ttl=55 time=28.8 ms  
64 bytes from 103.153.100.5: icmp_seq=5 ttl=55 time=37.9 ms  
64 bytes from 103.153.100.5: icmp_seq=6 ttl=55 time=30.2 ms  
64 bytes from 103.153.100.5: icmp_seq=7 ttl=55 time=29.5 ms  
--- siakad.103.153.100.ac.id ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 50335ms  
rtt min/avg/max/mdev = 28.756/33.561/41.653/4.488 ms  
trace@Trace-Book:~$
```

Figure 2. Ping Test

The results of the ping test, which was carried out as shown above, yielded information that the server IP of siakad.xyz.ac.id was [103.153.xxx.xx].

3. Zenmap

Foot printing activities are then carried out using Zenmap tools. The purpose of using this tool is to perform network scanning, network mapping, and port scanning on the SIAKAD website. The target entered is (103.153.xxx.xx), the scan profile used by default is Intense Scan. The scan results are presented in Figure 3 below:

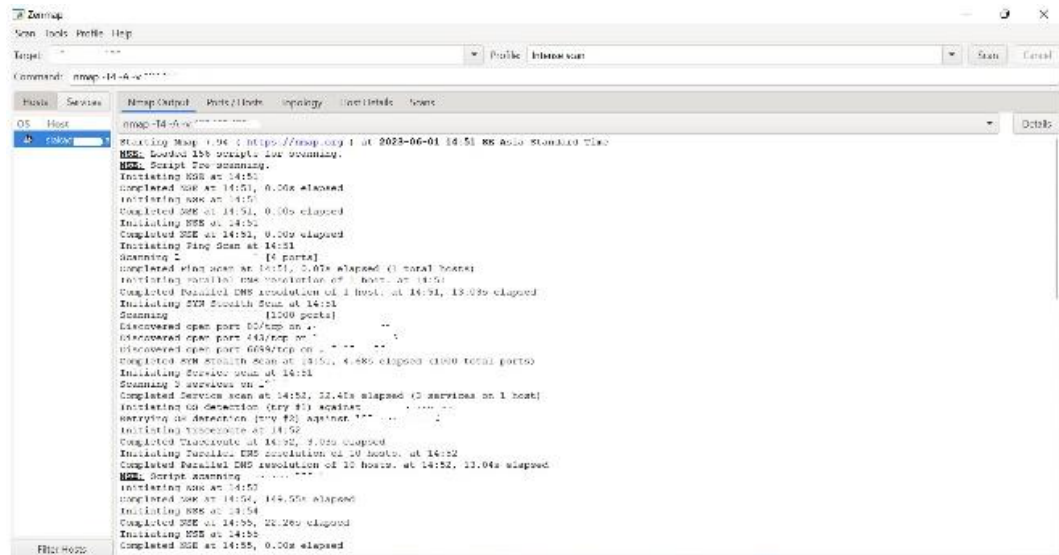


Figure 3. Nmap Output (Zenmap scan)

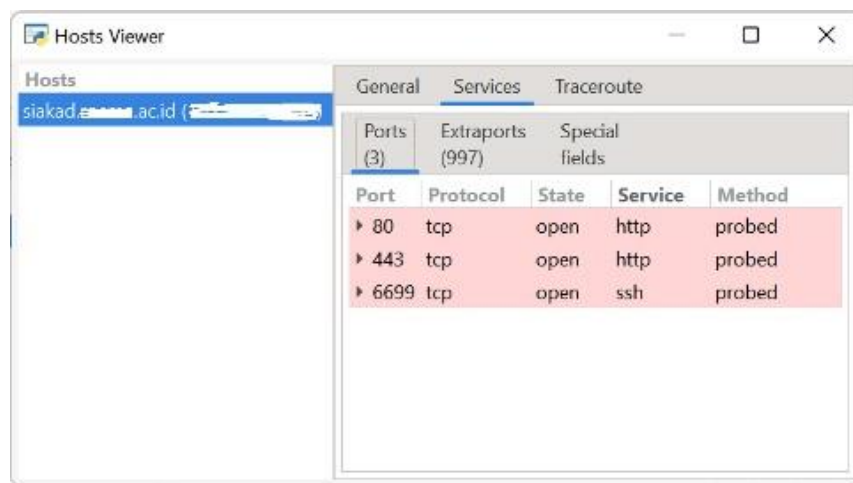


Figure 4. Open port (Zenmap scan)

Analysis of Higher Education SIAKAD Website Security Gaps Using the Vulnerability Assessment Method

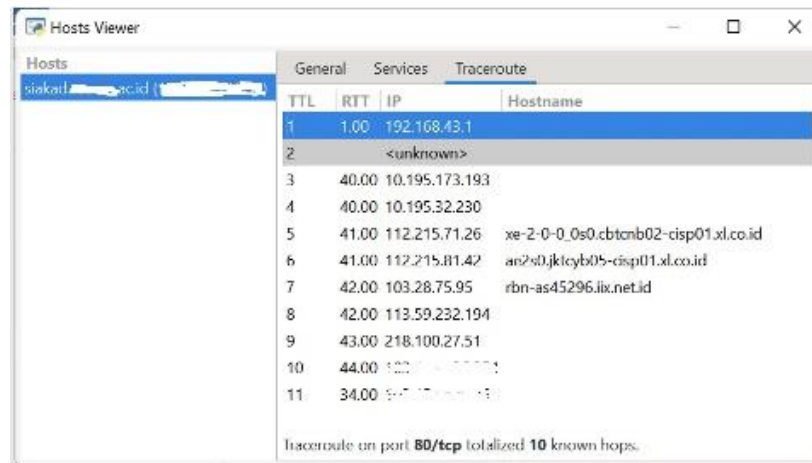


Figure. 5 Test route (Zenmap scan)

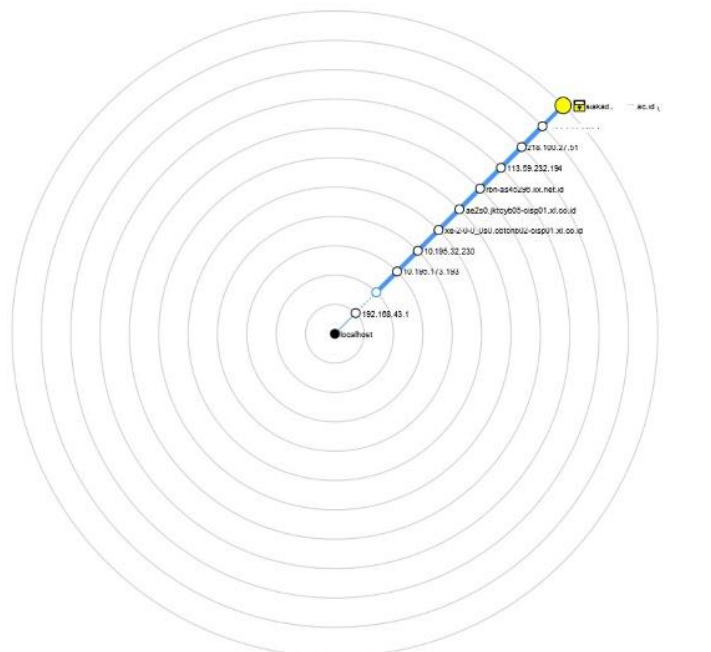
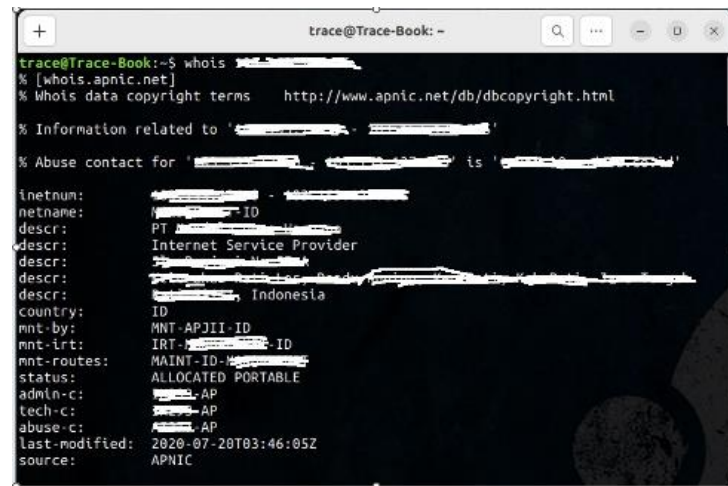


Figure 6. Network Topology (Zenmap Scan)

The information obtained after scanning using Nmap includes open ports, traceroute, and network topology.

4. Whois

Whois is a tool that can be used to find out the identity of a website.



```
trace@Trace-Book: ~  
trace@Trace-Book:~$ whois [redacted]  
% [whois.apnic.net]  
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html  
  
% Information related to '[redacted]'  
% Abuse contact for '[redacted]' is '[redacted]'  
  
inetnum:      [redacted]  
netname:      [redacted] ID  
descr:        PT [redacted]  
descr:        Internet Service Provider  
descr:        [redacted]  
descr:        [redacted] Indonesia  
country:      ID  
mnt-by:       MNT-APJII-ID  
mnt-irt:       IRT-[redacted]-ID  
mnt-routes:    MAINT-ID-[redacted]  
status:        ALLOCATED PORTABLE  
admin-c:       [redacted]-AP  
tech-c:        [redacted]-AP  
abuse-c:        [redacted]-AP  
last-modified: 2020-07-20T03:46:05Z  
source:        APNIC
```

Figure 7. Whois result

The information obtained from the results of the above analysis includes, IP address, server location, and email address.

5. Wappalyzer

Wappalyzer is a tool available in a web browser (add-on), its function is to find out the information technology used on a website.

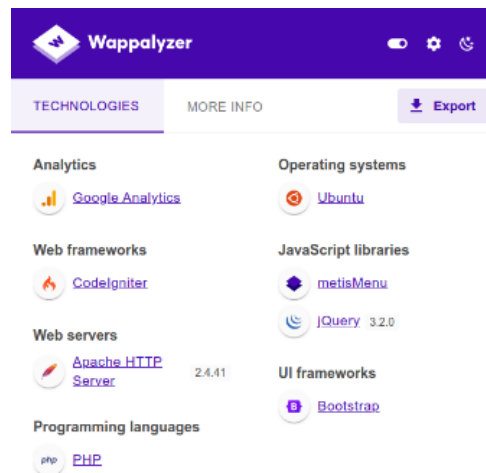


Figure 8. Technology analysis used to use Wappalyzer tools

From the results of checking carried out by the Wappalyzer tool, it is known that the technology information used on the website (siakad.xyz.ac.id) includes information on web servers, operating systems, web frameworks, CSS frameworks, and programming languages used.

6. Vulnerability Scanning

The second stage is scanning the SIAKAD website using the OWASP ZAP tool. Scan results using OWASP ZAP can be seen in the image below:

Analysis of Higher Education SIAKAD Website Security Gaps Using the Vulnerability Assessment Method

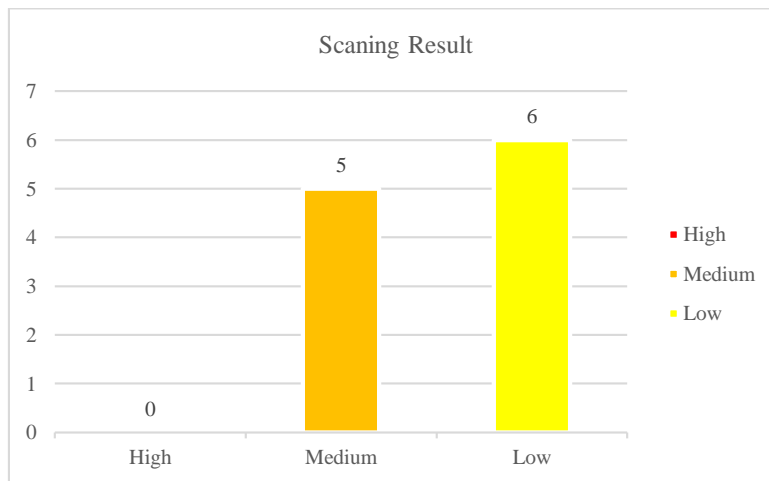


Figure 9. Scanning result

Based on Figure 9, OWASP ZAP shows 3 categories of vulnerability levels found on the SIAKAD website, from the highest to the lowest level (High, Medium, Low). The following is a table that presents a list of vulnerabilities in SIAKAD:

Table 1 List Vulnerability in SIAKAD

No	Vulnerabilities Name	Level
1	Absence of Anti-CSRF Tokens	Medium
2	Content Security Policy (CSP) Header Not Set	Medium
3	Hidden File Found	Medium
4	Missing Anti-clickjacking Header	Medium
5	Vulnerable JS Library	Medium
6	Cookie Without Secure Flag	Low
7	Cookie without SameSite Attribute	Low
8	Cross-Domain JavaScript Source File Inclusion	Low
9	Server Leaks Version Information via "Server" HTTP Response Header Field	Low
10	Strict-Transport-Security Header Not Set	Low
11	X-Content-Type-Options Header Missing	Low

From the results of the Vulnerability Scanning test on the target (siakad.xyz.ac.id) using the OWASP ZAP tool a total of 11 vulnerabilities were found. Of the 11 vulnerabilities found, 0 are high level vulnerabilities, 5 are medium level vulnerabilities, and 6 are low level vulnerabilities.

Discussion

Vulnerability Analysis

From the scanning results, it was found that the level of vulnerability on the SIAKAD website was high, medium, and low. Each of these vulnerabilities can have an impact on website security. Next, we present the vulnerabilities found and we also present alternative solutions to prevent the risks, as shown in table 3 below:

Table 2. Impact and Solution

No	Vulnerability Name	Impact	Alternative Solution
1	Absence of Anti-CSRF Tokens	An attacker can effectively perform any operation as a victim. If the victim is an administrator or privileged user, the consequences can include gaining complete control over the web application - deleting or stealing data or using it to launch other attacks against all users of that website. Because the attacker has the identity of the victim, the scope of CSRF is limited only by the privileges of the victim.	Websites must implement a strong Anti-CSRF Tokens mechanism. The CSRF token must be securely stored on the server side and associated with the appropriate user session. This can be done using good session management and secure token storage techniques, such as storing them in encrypted cookies
2	Content Security Policy (CSP) Header Not Set	The SIAKAD website is vulnerable to Cross-Site Scripting (XSS) attacks. This attack allows attackers to insert malicious scripts into web pages and execute them in the user's browser, which can result in data theft to fake sites or distribution of malware.	Ensure that the website server is configured to set the Content-Security-Policy header.
3	Hidden File Found	Can leak administrative, configuration, or credential information that could be exploited by attackers to attack systems.	Consider whether the component is really needed or not, otherwise disable it. If required, ensure access to it requires appropriate authentication and authorization.
4	Missing Anti-clickjacking Header	The SIAKAD website is vulnerable to clickjacking attacks. This attack involves deceiving users by manipulating the appearance of web pages.	Setting the X-Frame-Options Header and Using the Content Security Policy (CSP).
5	Vulnerable JS Library	The SIAKAD website is vulnerable to Cross Site Request Forgery (CSRF), Cross Site	Upgrade jQuery to the latest version.

Analysis of Higher Education SIAKAD Website Security Gaps Using the Vulnerability Assessment Method

No	Vulnerability Name	Impact	Alternative Solution
		Scripting (XSS), and SQL Injection attacks	
6	Cookie Without Secure Flag	Cookies on the SIAKAD website can be accessed via an unencrypted connection.	Make sure the secure flag is set for cookies that contain such sensitive information.
7	Cookie without SameSite Attribute	The SIAKAD website is vulnerable to Cross Site Request Forgery (CSRF), Cross Site Script Inclusion (XSSI) attacks, and Timing Attacks.	Ensure Same Site Attribute is set to 'loose' or ideally 'strict' for all cookies.
8	Cross-Domain JavaScript Source File Inclusion	Websites that run one or more JavaScript files from third-party domains. If a third party intentionally or unintentionally stores harmful content, that content can be added and executed in the victim's web application. This possibility occurs when the external JavaScript is not validated. This can lead to user data leaks.	Make sure the number JavaScript files are created only from trusted sources, and the sources cannot be controlled by end-users.
9	Server Leaks Version Information via "Server" HTTP Response Header Field	The website server leaks version information through the "Server" HTTP response header. Access to this information can facilitate attackers to identify other vulnerabilities that are targeted by the website server.	Make sure that the website server is configured to hide the "Server" header or provide general details.
10	Strict-Transport-Security Header Not Set	The SIAKAD website is vulnerable to Man-In-The-Middle attacks such as protocol downgrades and cookie piracy.	Ensure that the website server is configured to implement HTTP Strict-Transport-Security (HSTS).
11	X-Content-Type-Options Header Missing	Vulnerable to MIME Sniffing, Cross Site Scripting (XSS), Data Leakage.	Ensure that the application/website server sets the Content-Type header correctly and sets the X-Content-Type-Options

No	Vulnerability Name	Impact	Alternative Solution
			header to 'no sniff' for all web pages.

Conclusion

From the results of the analysis of security gaps on the SIAKAD website, it can be concluded that the target website has found vulnerabilities that can be exploited by irresponsible hackers. There were 11 vulnerabilities found, consisting of 5 medium level vulnerabilities and 6 low level vulnerabilities. By finding security holes or vulnerabilities on the SIAKAD website, researchers provide recommendations for solutions for website developers and IT staff to immediately evaluate and repair security holes in the system.

Declaration of conflicting interest

The authors declare that there is no conflict of interest in this work.

References

- Akmal, A. M., Heryana, N., & Solehudin, A. (2017). Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment. *Al-Irsyad*, 105(2), 79.
- Alwi, E. I., Herdianti, H., & Umar, F. (2020). Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning. *INFORMAL: Informatics Journal*, 5(2), 43. <https://doi.org/10.19184/isj.v5i2.18941>
- Aziz, M. (2021). Vulnerability Assesment Untuk Mencari Celah Keamanan Web Aplikasi E-Learning Pada Universitas Xyz. *Jecsit*, 1(1), 101–109.
- Cunong, D. N., Saputra, M., & Puspitasari, W. (2020). *ANALYSIS OF OROS MODELER DATA REPORTING PROCESS TO SAP HANA IN ACTIVITY BASED COSTING FOR INDONESIA TELECOMMUNICATION INDUSTRY*. 7(1).
- Dewi, M., Budiono, A., & Hediyanto, U. Y. K. S. (2023). *Vulnerability Assessment pada Website Rekrutasi Asisten (IRIS) Fakultas Rekayasa Industri menggunakan Nikto dan Nessus*. 10(2), 1631–1636.
- Elanda, A., & Lintang Buana, R. (2021). *ANALISIS KUALITAS KEAMANAN SISTEM INFORMASI E-OFFICE BERBASIS WEBSITE PADA STMIK ROSMA DENGAN MENGGUNAKAN OWASP TOP 10* (Vol. 6, Issue 2).
- Fauzan, F. Y., & Syukhri, S. (2021). Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang. *Voteteknika (Vocational Teknik Elektronika Dan Informatika)*, 9(2), 105. <https://doi.org/10.24036/voteteknika.v9i2.111778>

Analysis of Higher Education SIAKAD Website Security Gaps Using the Vulnerability Assessment Method

- Hidayatulloh, S., & Saptadiaji, D. (2021). Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP). *Jurnal Algoritma*, 18(1), 77–86. <https://doi.org/10.33364/algoritma/v.18-1.827>
- Indera, R., Budiono, A., & Hediyanto, U. Y. K. S. (2023). *Vulnerability Assessment Pada Situs Web KPPM FRI Dengan Burp Suite dan Intruder*. 10(2), 1623–1630.
- Kuncoro, A. W., & Rahma, F. (2021). Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review. *Automata*, 3(1), 1–5.
- Maulana, R., Liwanto, I., & Lucman, C. (2017). Software Testing pada Aplikasi Website PT Semen Tonasa menggunakan Metode Assessment Vulnerability. *Jurnal Insypro (Information System and Processing)*, 2(2), 3–6. <https://doi.org/10.24252/insypro.v2i2.4069>
- Moret, W. (2014). Vulnerability Assessment Methodologies: A Review of the Literature. *United States Agency for International Development (USAID)*, 54(2), 1–89.
- Mulyanto, Y., Haryanti, E., & Jumirah, J. (2021). Analisis Keamanan Website Sman 1 Sumbawa Menggunakan Metode Vulnerability Asement. *Jurnal Informatika Teknologi Dan Sains*, 3(3), 394–400. <https://doi.org/10.51401/jinteks.v3i3.1260>
- Nuari, N. (n.d.). *PERANCANGAN APLIKASI LAYANAN MOBILE INFORMASI ADMINISTRASI AKADEMIK BERBASIS ANDROID MENGGUNAKAN WEBSERVICE (STUDI KASUS REG.B UNIVERSITAS TANJUNGPURA)*.
- Orisa, M., & Ardita, M. (2021). VULNERABILITY ASSESMENT UNTUK MENINGKATKAN KUALITAS KEMANAN WEB. In *Jurnal MNEMONIC* (Vol. 4, Issue 1).
- Priyawati, D., Rokhmah, S., & Utomo, I. C. (2022). Website Vulnerability Testing and Analysis of Internet Management Information System Using OWASP. *International Journal of Computer and Information System (IJCIS) Peer Reviewed-International Journal*, 03(03), 2745–9659.
- Purwati, A. A., Hamzah, M. L., Hamzah, & Rahman, S. (2018). PENGARUH KUALITAS SISTEM INFORMASI AKADEMIK TERHADAP KEPUASAN DAN LOYALITAS MAHASISWA PERGURUAN TINGGI THE. *Journal of Economic, Business and Accounting (COSTING)*, 2(1), 84–92.
- Riadi, I., Yudhana, A., & Korspondensi, P. (2020). ANALISIS KEAMANAN WEBSITE OPEN JOURNAL SYSTEM MENGGUNAKAN METODE VULNERABILITY ASSESSMENT. 7(4). <https://doi.org/10.25126/jtiik.202071928>
- Riandhanu, I. O. (2022). Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi. *Jurnal Informasi Dan Teknologi*, 4(3), 160–165. <https://doi.org/10.37034/jidt.v4i3.236>
- Sirait, F., Studi, P., Elektro, T., Teknik, F., Buana, U. M., Studi, P., Elektro, T., Teknik, F., & Buana, U. M. (2018). Implementasi Metode Vulnerability Dan Hardening Pada Sistem Keamanan Jaringan. *Jurnal Teknologi Elektro*, 9(1), 16–22.
- Siregar, B., & Situmeang, M. (2022). *Pemanfaatan SIAKAD dalam Menunjang Pelaksanaan Pendidikan serta Manfaatnya bagi Institusi dan Mahasiswa Utilization*. 2(1), 210–216.
- Suryandani, F., Basori, B., & Maryono, D. (2017). PENGEMBANGAN SISTEM

- INFORMASI AKADEMIK BERBASIS WEB SEBAGAI SISTEM PENGOLAHAN NILAI SISWA DI SMK NEGERI 1 KUDUS. *Jurnal Ilmiah Pendidikan Teknik Dan Kejuruan*, 10(1), 71. <https://doi.org/10.20961/jiptek.v10i1.14976>
- Suryawan, M. B., & Prihandoko, P. (2018). Evaluasi Penerapan SIAKAD Politeknik Negeri Madiun Menggunakan Pendekatan TAM dan EUCS. *Creative Information Technology Journal*, 4(3), 233. <https://doi.org/10.24076/citec.2017v4i3.113>
- Tania, A. M., Setiyadi, D., Khasanah, F. N., Kunci, K., Cvss, :, Linux, K., & Website, K. (2018). Copyright@2018. P2M STMIK BINA INSANI Keamanan Website Menggunakan Vulnerability Assessment. *INFORMATICS FOR EDUCATORS AND PROFESSIONALS*, 2(2), 171–180.
- Wibowo, F., Harjono, H., & Wicaksono, A. P. (2019). Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS. *Jurnal Informatika*, 6(2), 212–217. <https://doi.org/10.31311/ji.v6i2.5925>
- Zattu Maharani, M., Rossi Andrian, H. S., & Juli Irzal Ismail, S. S. (n.d.). *ANALISIS KEAMANAN WEBSITE MENGGUNAKAN METODE SCANNING DAN PERHITUNGAN SECURITY METRIKS ANALYSIS WEBSITE SECURITY USING SCANNING METHOD AND CALCULATION OF SECURITY METRICS*.