E-ISSN : 2549 9459

JURNAL PERTAHANAN

Identity - Nationalism - Integrity

Indonesia Defense University

JURNAL PERTAHANAN
MEDIA INFORMASI TENTANG KAJIAN DAN STRATEGI PERTAHANAN YANG MENGEDEPANKAN IDENTITAS, NASIONALISME & INTEGRITAS
E-ISSN

Indonesia Defense University

E-ISSN: 2549-9459

Vol 8, No 3 (2022)

DOI: http://dx.doi.org/10.33172/jp.v8i3

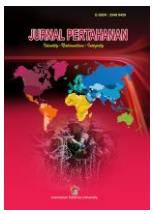
Table of Contents

Articles

INDEXED BY:

Jurnal Pertahanan

Media Informasi tentang Kajian dan Strategi Pertahanan
yang Mengedepankan *Identity*, *Nationalism* dan *Integrity*
e-ISSN: 2549-9459
http://jurnal.idu.ac.id/index.php/DefenseJournal



SECURITY ANALYSIS ON WEBSITES USING THE INFORMATION SYSTEM ASSESSMENT FRAMEWORK (ISSAF) AND OPEN WEB APPLICATION SECURITY VERSION 4 (OWASPv4) USING THE PENETRATION TESTING METHOD

Ditya Putri Anggraeni
Institut Teknologi Telkom Purwokerto
D.I Panjaitan Street No.128, Purwokerto, Central Java, Indonesia 53147
18102047@ittelkom-pwt.ac.id

Bita Parga Zen
Institut Teknologi Telkom Purwokerto
D.I Panjaitan Street No.128, Purwokerto, Central Java, Indonesia 53147
Corresponding Email: bita@ittelkom-pwt.ac.id

Mega Pranata
Institut Teknologi Telkom Purwokerto
D.I Panjaitan Street No.128, Purwokerto, Central Java, Indonesia 53147
mega@ittelkom-pwt.ac.id

Article Info

Article history:
Received : September 13, 2022
Revised : October 19, 2022
Accepted : December 21, 2022

Keywords:
Penetration Testing
ISSAF
OWASPv4
Cyber Security
Website

DOI:
http://dx.doi.org/10.33172/jp.v8i3.1777

Abstract

At this time in the rapid development of technology, there must be advantages and disadvantages of a system or technology that was created. Within the scope of the website, there are also many security holes that irresponsible parties can enter. The state of the website at the Telkom Purwokerto Institute of Technology, both University and Faculty websites, already uses Hypertext Transfers Protocol Secure (HTTPS). This study used the Information System Security Assessment Framework (ISSAF) and Open Web Application Project (OWASP) frameworks with the Penetration Testing method. This study aims to determine vulnerabilities on the website s1if.ittelkom-pwt.ac.id. The result of performing vulnerabilities is several vulnerabilities to the Institut Teknologi Telkom Purwokerto (ITTP) Informatics Study Program website, including not updating jquery on the ITTP website. Ten tests have been carried out, five tests using ISSAF and five tests using OWSP version 4. When performing vulnerabilities in the ISSAF framework, found robots files.txt on the S1 Informatics website which is quite crucial for s1if.ittelkom-pwt.ac.id website which contains an exploitable sitemap.

INTRODUCTION

In the modern era, technological developments experience very rapid changes. This can be seen by the number of users and website developers with different interests, such as education, organizations, agencies, and personal needs (Ghafir et al., 2018). Website is one of the information services that is widely accessed by users in the world of information technology that is connected to the internet (Sari & Putra, 2015).

A website is required to be able to meet the demands of many users with good results. In building a website, it is common for security holes to be breached by irresponsible users. In the world of information technology, security is an essential requirement in maintaining and ensuring the confidentiality, integrity, and availability of data or information (Mulyanto, Haryanti, & Jumirah, 2021).

To improve efficiency and reliability, a significant investment has been made by industry and government to build a smarter and more automated/connected power system. With the support of information and communications technology (ICT), power system operators can perform operation and control tasks based on data acquired from remote facilities, for example the advanced automation system isolates a faulted segment by opening switching devices (e.g., circuit breakers and automated reclosers) and sends the fault information back to the control center (Sun, Hahn, & Liu, 2018). Since power grids span a wide geographic area, public and private networks (e.g., fiber optics, RF/microwave, cellular) can provide a communication path between remote sites and a control center. These capabilities also open doors for attackers to access a power grid and cause disruptions to the normal operation of the grid. Cyber attackers also can access power system communication networks and connect to remote access points at a power system infrastructure. This can lead to serious and harmful consequences. As a result, the cyber security of smart grids has been recognized as a critical issue (Sanjaya, Sasmita, & Arsa, 2020).

Within the website, there are many security holes that can be entered by other parties or hackers. They hack websites by being exposed (disseminated) and not exposed (not disseminated). One of the recent problems is that the security system of Bank Indonesia was hacked by Ransomware. Ransomware is malware and malware has a habit to stop processes on the design and retain data by using an encryption system that can harm the data (Bolanio, Paredes, Yoldan, & Acapulco II, 2021; Darmawan, 2019). The data was taken from one employee's data on laptop loans and event proposals (CNN Indonesia, 2022).

The state of the website at the Telkom Purwokerto Institute of Technology, both University and Faculty websites, already uses Hypertext Transfers Protocol Secure (HTTPS). That way, perform a pre-emptive vulnerability to the website of the Faculty of Informatics (Haeruddin & Kurniadi, 2021). There are several recommended frameworks for conducting penetration testing, including ISSAF (Information System Security Assessment Framework), a structured penetration testing framework that categorizes information system security in various domains and details evaluation criteria or specific tests for each part. Then there is the Open Web Application Security Project (OWASP) which is an organization that focuses on improving software security (Pratama & Wiradarma, 2019).

A previous study entitled Security Assessment Analysis Using the Penetration Testing Method in Maintaining the Security Capability of National Defense Information Technology tries to improve computer system security from illegal data theft with security breaches on computer networks in testing the security enhancement of the firewall defense system (Alfidzar & Zen, 2022). When conducting a penetration test at the security

assessment stage by using the standard OWASP and CVSS (Common Vulnerability Scoring System) vulnerability stages, the most basic things a network needs are routers and servers. In the results of this study, several gaps can be exploited by irresponsible parties (Zen, Gultom, & Reksoprodjo, 2020). The next research is entitled Website Security Analysis With Information System Security Assessment Framework (ISSAF) and Open Web Application Security Project (OWASP) in 2021 by Agus Rochman, Rizal Rohian Salam, and Sandi Agus Maulana. Computer security systems are increasingly needed to avoid cyber crimes by irresponsible parties. The test results can be a solution to overcome problems on the information system web server, where there are several gaps that irresponsible parties can exploit. One of the gaps that can be accessed is the target website activates a public HTML page. This allows direct access to the phpMyAdmin database page without logging into Cpanel (Rochman, Salam, & Maulana, 2021). The purpose of this study is to find out the security gaps on the s1if.ittelkom-pwt.ac.id website, and find out the effect of penetration testing on the website s1if.ittelkom-pwt.ac.id.

METHODS

In the flow of this research, this study describes the stages of work to be carried out with the object of research, namely the website s1if.ittelkom-pwt.ac.id. In the ISSAF method, there are three stages, namely:

1. Planning and Preparation. This phase contains steps to exchange information, plan, and prepare for tests.
2. Assessment. This phase is the phase of conducting penetration tests. In the assessment phase, a multilevel approach is carried out. Each tier will provide broader access to the desired information assets.
3. Clean-up and Destroy Artefacts. All information created or stored on the tested system must be deleted.

Then in the OWASP version 4 method, there are several stages as follows:

1. Authentication Testing. Authentication is the act of constructing and confirming something that the claim made is true. Authorization Testing.
2. Authorization is a concept that allows access to resources for those who are allowed to use them.
3. Session Management Testing is defined as the set of all controls that set full state interaction between users and web-based applications.

This research flow will be used as a guideline during the research so that the results of the research carried out do not deviate from the objectives in the background. In this study using the penetration testing method (Prasad, Abraham, Suhas, & Kumar, 2011), before penetration testing the authors conducted vulnerability testing first.

The first stage of the study is the analysis of the problem. Then a literature study is carried out. The next stage is to prepare the device. Next is the system configuration, namely installing and configuring the software that will be used in this study. The next stage is to attack or test the s1if.ittelkom-pwt.ac.id website. The next stage is data collection and analysis. Penetration testing is a method for evaluating the security of computer systems and networks. Evaluation is carried out by simulating an attack. The next stage is to conclude.

In this era of sophisticated and all-digital technology, there must be advantages or disadvantages of a system or technology that was created, especially in the scope of the website. The website also has security, one of which is the Open Web Application Security Project (OWASP). The security of this website has different encryption, and also has different security holes that hackers can enter. If the hacker has managed to enter the website's

system or database, then it will take data or illegally hijack the website (Rochman et al., 2021).

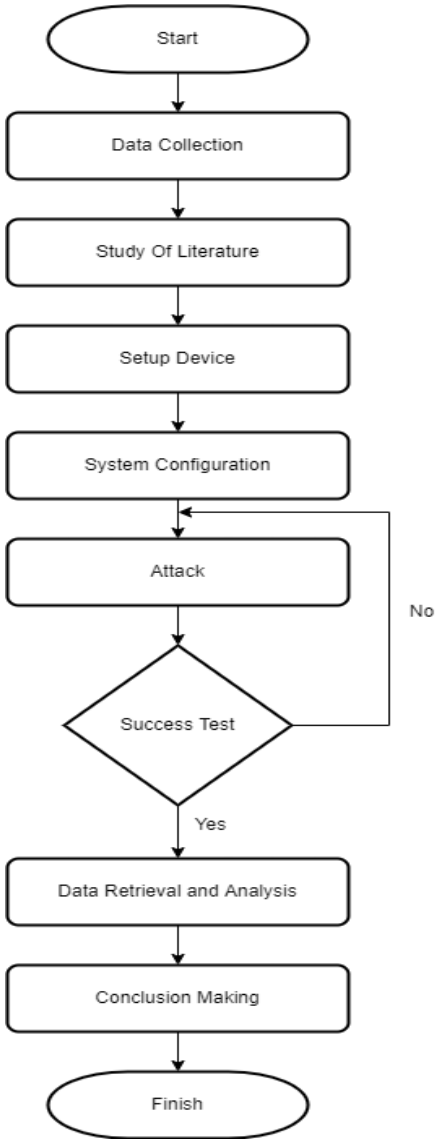


Figure 1. Research flowchart
Source: Processed by the Authors, 2022

Starting from the problem above, there is a method called penetration testing. Penetration testing is a method that can find open security loopholes or loopholes that will be entered by hackers (Haeruddin & Kurniadi, 2021), the attacks carried out in this study are Denial of Service (DoS), SQL Injection and Brute Force attacks. Penetration testing methods can be done using ISSAF and OWASP tools, Information System Security Assessment Framework (ISSAF) is a structured penetration testing framework that has the advantage of security control with stages of Planning and Preparation, Evaluation, Vulnerability Identification, and Penetration. Open Web Application Security Project (OWASP) aims to create software security from unauthorized parties with stages of Authentication Testing, Authorization Testing. This research uses the penetration testing (pentest) method to test the s1if.ittelkom-pwt.ac.id website, the pentest method is also widely used.

RESULT AND DISCUSSION

Types of preprocessing that in the results and discussion, the carried out 2 methods, namely testing the Information System Assessment Framework (ISSAF) approach and testing the Open Web Application Security Project (OWASP) method. What is explained in the ISSAF and OWASP methods are the stages of testing. In this case study, the implementation was carried out on the s1if.ittelkom-pwt.ac.id website which is known to still have vulnerabilities that can be exploited by irresponsible parties. This method can be done on other websites, to find out the security system of a website.

Testing the Information System Assessment Framework (ISSAF) Method

Planning and Preparation

Table 1. Case Study Information

No	Case	Information
1	The web used In this study	https://s1if.ittelkom-pwt.ac.id/
2	Web IP Address	IP 180.250.247.93
3	Date of Testing Web	stages from July 17, 2022, to July 31, 2022.
4	Permission	Have done permission on the agency (Lawful Penetration)

Source: Website S1IF IT Telkom, 2022

Assessment

1. Information Gathering
   a. Domain Info
      During the stage of searching for domain information by using who.is, 12 findings were obtained, including the following case study information as can be seen in Table 2.

Table 2. Domain Information

1	Hosting provider	Rumahweb
2	Domain id	PANDI-D0665256
3	Created on	08-29-2017
4	Last updated	03-09-2021
5	Expiration date	29-08-2022
6	Service provider	Digital registra
7	Service provider URL	www.digitalregistra.co.id
8	Sponsoring address	Jl. Lempongsari no 39C.
9	Sponsoring city	Sleman.
10	Sponsoring province	Yogyakarta.
11	Postal code	55281.
12	Name Server	nsid1.rumahweb.com nsid2.rumahweb.net nsid3.rumahweb.biz nsid4.rumahweb.org

Source: Processed by the Authors, 2022

   b. SSL Scan (Secure Sockets Layer Scan)
      The results of the SSL Scan using the SSLLabs tool show that the web s1if.ittelkom-pwt.ac.id gets an overall rating of B which means good.

Figure 2. Results from who.is
Source: Processed by the Authors, 2022

      The certificate on the web s1if.ittelkom-pwt.ac.id is very well installed with a 2048 bits RSA certificate (SHA256withRSA).

2. Network Mapping
   The results of the network mapping test on the s1if.ittelkom-pwt.ac.id web show that the domain has a public IP of 180.250.247.93 with 3 open ports, namely ports 80, 443, and 1723.

Vulnerability Identification

1. Using pentest tools
   The results of the vulnerability identification test using pentest-tools.com contained 19 vulnerabilities with details of 1 medium vulnerability, 8 low vulnerability, and 10 info.

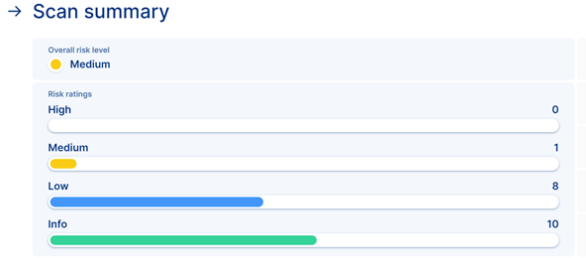


Figure 3. Vulnerability Results Using Pentest Tools
Source: Processed by the Authors through Pentest Tool, 2022

The vulnerability code for this medium is CVE-2019-11358, CVE-2020-11022, and CVE-2020-11023. Where the main problem with this vulnerability is the version of jQuery that has not been updated (Dharma, 2005).

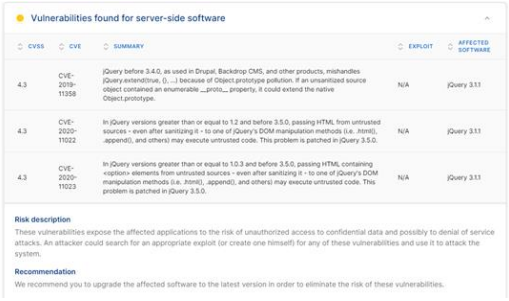


Figure 4. Contents of Medium Vulnerabilities
Source: Processed by the Authors through Vulnerabilities, 2022

a. CVE-2019-11358
It is a vulnerability in jQuery because jQuery is used under the 3.4.0 version which is commonly used in Drupal, CMS backdrops, etc. This version mishandles jQuery.extend(true, { }, ...).
b. CVE-2020-11022
There is a vulnerability in jQuery between version 1.2 and before version 3.5.0 that passes HTML from untrusted sources even after purging to one of jQuery's DOM manipulation methods namely .html(), .append(), and other methods. This vulnerability can be overcome by implementing jQuery version 3.5.0.
c. CVE-2020-11023
There is a vulnerability in jQuery versions above 1.0.3 and before version 3.5.0 that passes <option> elements from trusted sources even after purging to one of the DOM (Document Object Model) models like .html(), .append(), etc. This vulnerability can be overcome with jQuery version 3.5.0 and above.

However, there is 1 vulnerability that goes into the low vulnerability. It is very vulnerable to being exposed to attacks. That is the exposure of the robots.txt file which after being investigated contains user-agent data, site sitemaps, and several website usernames.

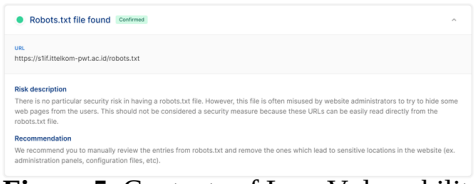


Figure 5. Contents of Low Vulnerability
Source: Processed by the Authors through Robot, 2022

```
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php

Sitemap: https://s1if.ittelkom-pwt.ac.id/wp-sitemap.xml
```

Figure 6. Contents of File Robots.txt
Source: Processed by the Authors through Robot, 2022

2. Using acunetix
Meanwhile, the results of the vulnerability scanning using acunetix, found 1 vulnerability, namely Clickjacking: X-Frame-Options header missing. Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking Web users into clicking on something different from what the user thinks they are clicking, thereby potentially revealing confidential information or taking control of their computer when they click on a web page that seems harmless.

The server does not return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack.

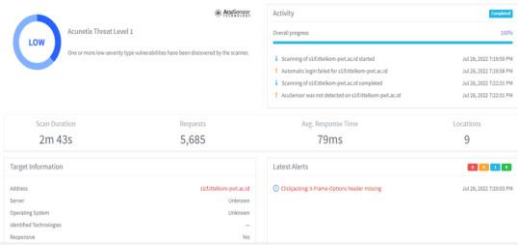


Figure 7. Threat Vulnerabilities in Acunetix
Source: Processed by the Authors through Acunetix, 2022

Meanwhile, other findings from acunetix on web s1if are the site structure as can be seen in Figure 8.

Figure 8. Site Structure from Acunetix
Source: Processed by the Authors through Acunetix, 2022

Penetration

1. DoS Attack
The next step is to conduct penetration testing by using the DoS Attack method. DoS is an activity that can hinder a service so that users who are

entitled/interested cannot use the service. The https://s1if.ittelkom-pwt.ac.id/ website was able to withstand these attacks. This can be known by blocking the attacker's IP automatically after it is indicated that it has flooded the server with many requests in a short time (Samsumar & Gunawan, 2017).

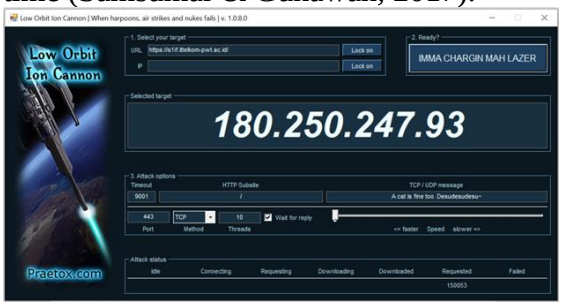


Figure 9. DoS attacks using Low Orbit Ion Cannon (LOIC)
Source: Processed by the Authors through LOIC, 2022

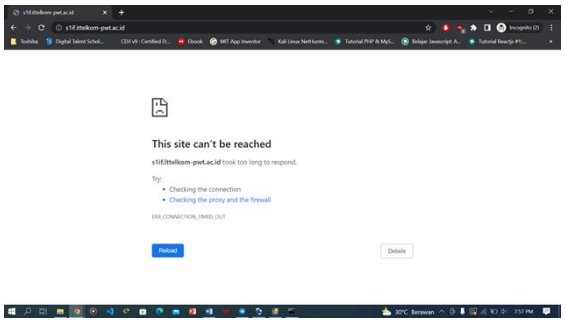


Figure 10. The attacker's PC can't access the website
Source: Processed by the Authors, 2022

Figure 11. The website still can be accessed from other devices
Source: Processed by the Authors through ITTP Website, 2022

2. SQL Injection
   This type of attack attacks by exploiting security loopholes that appear in databases and applications, for SQL Injection attacks, the s1if website cannot be attacked using this method because there is no vulnerability or bug on the website (Bastian, Sujadi, & Abror, 2020).
3. Brute Force
   A brute force is a consequence that can be caused by an attacker that get access rights on the server and the attacker can freely access the information contained in the server (Prasetyo, Idhom, & Wahanani, 2020). For this type of attack, this study uses hydra to attack the logged-in user on the s1if web. As it is known that there is a list of users on the website that allows exploits on the s1if website by using brute-force attacks. This study attacked by initializing the username variable with st3telkomin, and brute force with the wordlist RockYou, but could not find the login password for the usernames st3telkomin, azizah, Bunga, and s1ifadmin.

Table 3. ISSAF Test Results

Stages	Tools	Results
Information Gathering	Who. is	Success
	SSL Scan	Success
Network Mapping	Legion	Success
Vulnerability Identification	Pentest Tools	Success
	Acunetix	Success
	DoS Attack	Not Successful
	SQL Injection	Not Successful
	Brute Force	Not Successful

Source: Processed by the Authors, 2022

The test results using ISSAF show that the s1if website still has basic weaknesses, especially in Jquery which has not yet received the latest updates which are very

vulnerable to exploiting certain attacks. The s1if website has been equipped with an auto-blocking mechanism if it is found that suspicious website access is simultaneously and in a short time which aims to bring down the website, the attacker's IP will be blocked for a while.

Testing the Open Web Application Security Project (OWASP) Method

Authentication Testing

This process is trying to authenticate/verify the correct identity of the sender of information. The stages of Authentication Testing carried out by researchers are as (Dirgahayu, Prayudi, & Fajaryanto, 2015).

Authorization Testing

Testing for authorization means understanding how the authorization process works and using that information to circumvent authorization mechanisms. Authorization is a process that comes after successful authentication, so the tester will verify this point once he holds a valid identity (Hidayatulloh & Saptadiaji, 2021).

From the Table 4, it can be seen that research using OWASP 4.0 was successfully carried out, but several points were not successfully carried out due to the lack of further information about the contents of the S1if website. Web s1if is considered safe from simple attacks and

Table 4. OWASP test results

Stage	Parameter	Tools	Results
Authentication Testing	Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001)	Web Scarab	Success
	Testing for default credentials (OTG-AUTHN-002)	Mozilla Firefox	Success
	Testing for Weak lock-out mechanism (OTG-AUTHN003)	Mozilla Firefox	Not Successful
	Testing for bypassing authentication schema (OTGAUTHN-004)	Web Scarab	Success
	Test remember password functionality (OTG-AUTHN005)	Mozilla	Not Successful
	Testing for Browser cache weakness (OTG-AUTHN006)	Mozilla	Not Successful
	Testing for Weak password policy (OTG-AUTHN-007)	Mozilla	Not Successful
	Testing for Weak security question/answer (OTGAUTHN-008)	Mozilla	Not Successful
	Testing for weak password change or reset functionalities (OTG- AUTHN-009)	Mozilla	Not Successful
	Testing for Weaker authentication in the alternative channel (OTG-AUTHN-010)	-	Not Successful
Authorization Testing	Testing Directory traversal/file includes (OTGAUTHZ-001)	Wfuzz	Success
	Testing for bypassing authorization schema (OTGAUTHZ-002)	-	Not Successful
	Testing for Privilege Escalation (OTG-AUTHZ-003)	-	Not Successful
	Testing for Insecure Direct Object References (OTGAUTHZ-004)	Mozilla Firefox	Success

Source: Processed by the Authors, 2022

bypass security when viewed from the OWASP 4.0 research, but there are several points from OWASP 4.0 that cannot be investigated further.

CONCLUSIONS, RECOMMENDATION AND LIMITATION

In penetration testing using the ISSAF and OWASP frameworks, it was quite effective in detecting the types of vulnerabilities on the S1 Informatics website. It has been tested for the types of vulnerabilities detected with moderate and low vulnerabilities shown in the discussion above. This study recommends that further research not only use the ISSAF and OWASP frameworks but using other techniques such as using tools MALTEGO, NCRACK, SQLMAP on Kali Linux to find profound weaknesses in the system.

REFERENCES

Alfidzar, H., & Zen, B. P. (2022). Implementasi HoneyPy dengan Malicious Traffic Detection System (Maltrail) Menggunakan Analisis Deskriptif guna untuk Mendeteksi Serangan DDOS pada Server. *Journal of Informatics Information System Software Engineering and Applications (INISTA)*, *4*(2), 32–45. https://doi.org/10.20895/inista.v4I2.534

Bastian, A., Sujadi, H., & Abror, L. (2020). Analisis Keamanan Aplikasi Data Pokok Pendidikan (Dapodik) Menggunakan Penetration Testing dan SQL Injection. *Infotech Journal*, *6*(2), 65–70. https://doi.org/10.31949/infotech.v6I2.848

Bolanio, J. B., Paredes, R. K., Yoldan, J. A. L., & Acapulco II, R. E. (2021). Network Security Policy for Higher Education Institutions based on ISO Standards. *Mediterranean Journal of Basic and Applied Sciences*, *5*(1), 1–17. https://doi.org/10.1016/S1353-4858(10)70039-8

CNN Indonesia. (2022, January 20). Sistem Keamanan Siber BI Ditembus, Berikut Data yang Dicuri. Retrieved November 8, 2022, from https://www.cnnindonesia.com/teknologi/20220120175527-185-749252/sistem-keamanan-siber-bi-ditembus-berikut-data-yang-dicuri

Dharma, M. A. J. (2005). *DOS, DDOS & Cara Penanggulangannya.* Universitas Sriwijaya. https://fdokumen.com/document/dos-denial-of-service-halaman-utama-viewbisa-di-tebak-situs-yang.html?page=1

Darmawan, B. I. (2019). *Simulasi dan Analisis Encryption Based Ransomware untuk Memetakan Evolusi Ransomware*. Universitas Islam Indonesia, Yogyakarta.

Dirgahayu, R. T., Prayudi, Y., & Fajaryanto, A. (2015). Penerapan Metode ISSAF dan OWASP Versi 4 untuk Uji Kerentanan Web Server. *Network Engineering Research Operation*, *1*(3), 190–197. https://doi.org/10.21107/nero.v1I3.29

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., … Baker, T. (2018). Security Threats to Critical Infrastructure: the Human Factor. *Journal of Supercomputing*, *74*, 4986–5002. https://doi.org/10.1007/s11227-018-2337-2/tables/1

Haeruddin, & Kurniadi, A. (2021). Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6). *Conference on Management, Business, Innovation, Education and Socal Sciences*, 508–515. Batam: Universitas Internasional Batam.

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

Mulyanto, Y., Haryanti, E., & Jumirah. (2021). Analisis Keamanan Website SMAN 1 Sumbawa Menggunakan Metode Vulnerability Asesement. *Jurnal Informatika Teknologi Dan Sains*, *3*(3), 394–400. https://doi.org/10.51401/jinteks.v3I3.1260

Prasetyo, K. A., Idhom, M., & Wahanani, H. E. (2020). Sistem Pencegahan Serangan Bruteforce pada Multiple Server dengan Menggunakan Fail2ban. *Jurnal Informatika Dan Sistem Informasi*, *1*(3), 709–715. https://doi.org/10.33005/jifosi.v1I3.205

Pratama, I. P. A. E., & Wiradarma, A. A. B. A. (2019). Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study: X Company). *International Journal of Computer Network and Information Security*, *11*(7), 8–12. https://doi.org/10.5815/ijcnis.2019.07.02

Rochman, A., Salam, R. R., & Maulana, S. A. (2021). Analisis Keamanan Website dengan Information System Security Assessment Framework (Issaf) dan Open Web Application Security Project (Owasp) di Rumah Sakit Xyz. *Jurnal Indonesia Sosial Teknologi*, *2*(4), 506–519. https://doi.org/10.36418/jist.v2i4.124

Samsumar, L. D., & Gunawan, K. (2017). Analisis dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless LAN); Studi Kasus di Kampus STMIK Mataram. *Jurnal Ilmiah Teknologi Infomasi Terapan*, *4*(1), 73–82. https://doi.org/10.33197/jitter.vol4.iss1.2017.152

Sanjaya, I. G. A. S., Sasmita, G. M. A., & Arsa, D. M. S. (2020). Evaluasi Keamanan Website Lembaga X melalui Penetration Testing Menggunakan Framework ISSAF. *Jurnal Ilmiah Merpati*, *8*(2), 113–124. https://doi.org/10.24843/jim.2020.v08.i02.p05

Sari, W. P., & Putra, I. N. A. P. (2015). Analisis Serangan Hacker Menggunakan Honeypot High Interaction. *Jurnal Tiarsie*, *14*(1). https://doi.org/10.32816/tiarsie.v14i1.16

Sun, C.-C., Hahn, A., & Liu, C.-C. (2018). Cyber Security of a Power Grid: State-of-the-Art. *International Journal of Electrical Power & Energy Systems*, *99*, 45–56. https://doi.org/10.1016/j.ijepes.2017.12.020

Zen, B. P., Gultom, R. A. G., & Reksoprodjo, A. H. S. (2020). Analisis Security Assessment Menggunakan Metode Penetration Testing dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara. *Jurnal Teknologi Penginderaan*, *2*(1), 105–122. https://doi.org/10.5121/csit.2018.81714

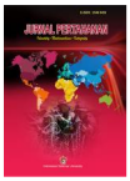
SECURITY ANALYSIS ON WEBSITES USING THE INFORMATION SYSTEM ASSESSMENT FRAMEWORK (ISSAF) AND OPEN WEB APPLICATION SECURITY VERSION 4 (OWASPv4) USING THE PENETRATION TESTING METHOD

By Bita Parga Zen

WORD COUNT 4136 TIME SUBMITTED 08-AUG-2023 03:36PM
PAPER ID 101841203

Jurnal Pertahanan

Media Informasi tentang Kajian dan Strategi Pertahanan
yang Mengedepankan *Identity*, *Nationalism* dan *Integrity*
e-ISSN: 2549-9459
http://jurnal.idu.ac.id/index.php/DefenseJournal



SECURITY ANALYSIS ON WEBSITES USING THE INFORMATION SYSTEM ASSESSMENT FRAMEWORK (ISSAF) AND OPEN WEB APPLICATION SECURITY VERSION 4 (OWASPv4) USING THE PENETRATION TESTING METHOD

Ditya Putri Anggraeni
Institut Teknologi Telkom Purwokerto
D.I Panjaitan Street No.128, Purwokerto, Central Java, Indonesia 53147
18102047@ittelkom-pwt.ac.id

Bita Parga Zen
Institut Teknologi Telkom Purwokerto
D.I Panjaitan Street No.128, Purwokerto, Central Java, Indonesia 53147
Corresponding Email: bita@ittelkom-pwt.ac.id

Mega Pranata
Institut Teknologi Telkom Purwokerto
D.I Panjaitan Street No.128, Purwokerto, Central Java, Indonesia 53147
mega@ittelkom-pwt.ac.id

Article Info

Article history:
Received : September 13, 2022
Revised : October 19, 2022
Accepted : December 21, 2022

Keywords:
Penetration Testing
ISSAF
OWASPv4
Cyber Security
Website

DOI:
http://dx.doi.org/10.33172/jp.v8i3.1777

Abstract

At this time in the rapid development of technology, there must be advantages and disadvantages of a system or technology that was created. Within the scope of the website, there are also many security holes that irresponsible parties can enter. The state of the website at the Telkom Purwokerto Institute of Technology, both University and Faculty websites, already uses Hypertext Transfers Protocol Secure (HTTPS). This study used the Information System Security Assessment Framework (ISSAF) and Open Web Application Project (OWASP) frameworks with the Penetration Testing method. This study aims to determine vulnerabilities on the website s1if.ittelkom-pwt.ac.id. The result of performing vulnerabilities is several vulnerabilities to the Institut Teknologi Telkom Purwokerto (ITTP) Informatics Study Program website, including not updating jquery on the ITTP website. Ten tests have been carried out, five tests using ISSAF and five tests using OWSP version 4. When performing vulnerabilities in the ISSAF framework, found robots files.txt on the S1 Informatics website which is quite crucial for s1if.ittelkom-pwt.ac.id website which contains an exploitable sitemap.

INTRODUCTION

In the modern era, technological developments experience very rapid changes. This can be seen by the number of users and website developers with different interests, such as education, organizations, agencies, and personal needs (Ghafir et al., 2018). Website is one of the information services that is widely accessed by users in the world of information technology that is connected to the internet (Sari & Putra, 2015).

A website is required to be able to meet the demands of many users with good results. In building a website, it is common for security holes to be breached by irresponsible users. In the world of information technology, security is an essential requirement in maintaining and ensuring the confidentiality, integrity, and availability of data or information (Mulyanto, Haryanti, & Jumirah, 2021).

To improve efficiency and reliability, a significant investment has been made by industry and government to build a smarter and more automated/connected power system. With the support of information and communications technology (ICT), power system operators can perform operation and control tasks based on data acquired from remote facilities, for example the advanced automation system isolates a faulted segment by opening switching devices (e.g., circuit breakers and automated reclosers) and sends the fault information back to the control center (Sun, Hahn, & Liu, 2018). Since power grids span a wide geographic area, public and private networks (e.g., fiber optics, RF/microwave, cellular) can provide a communication path between remote sites and a control center. These capabilities also open doors for attackers to access a power grid and cause disruptions to the normal operation of the grid. Cyber attackers also can access power system communication networks and connect to remote access points at a power system infrastructure. This can lead to serious and harmful consequences. As a result, the cyber security of smart grids has been recognized as a critical issue (Sanjaya, Sasmita, & Arsa, 2020).

Within the website, there are many security holes that can be entered by other parties or hackers. They hack websites by being exposed (disseminated) and not exposed (not disseminated). One of the recent problems is that the security system of Bank Indonesia was hacked by Ransomware. Ransomware is malware and malware has a habit to stop processes on the design and retain data by using an encryption system that can harm the data (Bolanio, Paredes, Yoldan, & Acapulco II, 2021; Darmawan, 2019). The data was taken from one employee's data on laptop loans and event proposals (CNN Indonesia, 2022).

The state of the website at the Telkom Purwokerto Institute of Technology, both University and Faculty websites, already uses Hypertext Transfers Protocol Secure (HTTPS). That way, perform a pre-emptive vulnerability to the website of the Faculty of Informatics (Haeruddin & Kurniadi, 2021). There are several recommended frameworks for conducting penetration testing, including ISSAF (Information System Security Assessment Framework), a structured penetration testing framework that categorizes information system security in various domains and details evaluation criteria or specific tests for each part. Then there is the Open Web Application Security Project (OWASP) which is an organization that focuses on improving software security (Pratama & Wiradarma, 2019).

A previous study entitled Security Assessment Analysis Using the Penetration Testing Method in Maintaining the Security Capability of National Defense Information Technology tries to improve computer system security from illegal data theft with security breaches on computer networks in testing the security enhancement of the firewall defense system (Alfidzar & Zen, 2022). When conducting a penetration test at the security

assessment stage by using the standard OWASP and CVSS (Common Vulnerability Scoring System) vulnerability stages, the most basic things a network needs are routers and servers. In the results of this study, several gaps can be exploited by irresponsible parties (Zen, Gultom, & Reksoprodjo, 2020). The next research is entitled Website Security Analysis With Information System Security Assessment Framework (ISSAF) and Open Web Application Security Project (OWASP) in 2021 by Agus Rochman, Rizal Rohian Salam, and Sandi Agus Maulana. Computer security systems are increasingly needed to avoid cyber crimes by irresponsible parties. The test results can be a solution to overcome problems on the information system web server, where there are several gaps that irresponsible parties can exploit. One of the gaps that can be accessed is the target website activates a public HTML page. This allows direct access to the phpMyAdmin database page without logging into Cpanel (Rochman, Salam, & Maulana, 2021). The purpose of this study is to find out the security gaps on the s1if.ittelkom-pwt.ac.id website, and find out the effect of penetration testing on the website s1if.ittelkom-pwt.ac.id.

METHODS

In the flow of this research, this study describes the stages of work to be carried out with the object of research, namely the website s1if.ittelkom-pwt.ac.id. In the ISSAF method, there are three stages, namely:

1. Planning and Preparation. This phase contains steps to exchange information, plan, and prepare for tests.
2. Assessment. This phase is the phase of conducting penetration tests. In the assessment phase, a multilevel approach is carried out. Each tier will provide broader access to the desired information assets.
3. Clean-up and Destroy Artefacts. All information created or stored on the tested system must be deleted.

Then in the OWASP version 4 method, there are several stages as follows:

1. Authentication Testing. Authentication is the act of constructing and confirming something that the claim made is true. Authorization Testing.
2. Authorization is a concept that allows access to resources for those who are allowed to use them.
3. Session Management Testing is defined as the set of all controls that set full state interaction between users and web-based applications.

This research flow will be used as a guideline during the research so that the results of the research carried out do not deviate from the objectives in the background. In this study using the penetration testing method (Prasad, Abraham, Suhas, & Kumar, 2011), before penetration testing the authors conducted vulnerability testing first.

The first stage of the study is the analysis of the problem. Then a literature study is carried out. The next stage is to prepare the device. Next is the system configuration, namely installing and configuring the software that will be used in this study. The next stage is to attack or test the s1if.ittelkom-pwt.ac.id website. The next stage is data collection and analysis. Penetration testing is a method for evaluating the security of computer systems and networks. Evaluation is carried out by simulating an attack. The next stage is to conclude.

In this era of sophisticated and all-digital technology, there must be advantages or disadvantages of a system or technology that was created, especially in the scope of the website. The website also has security, one of which is the Open Web Application Security Project (OWASP). The security of this website has different encryption, and also has different security holes that hackers can enter. If the hacker has managed to enter the website's

system or database, then it will take data or illegally hijack the website (Rochman et al., 2021).

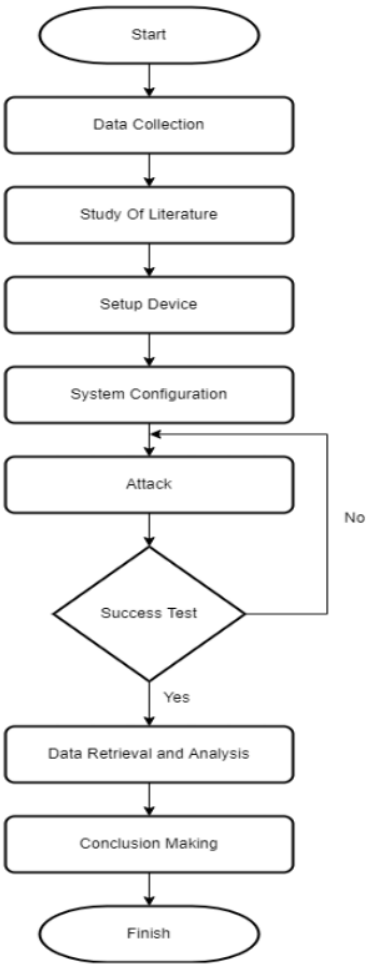


Figure 1. Research flowchart
Source: Processed by the Authors, 2022

Starting from the problem above, there is a method called penetration testing. Penetration testing is a method that can find open security loopholes or loopholes that will be entered by hackers (Haeruddin & Kurniadi, 2021). the attacks carried out in this study are Denial of Service (DoS), SQL Injection and Brute Force attacks. Penetration testing methods can be done using ISSAF and OWASP tools, Information System Security Assessment Framework (ISSAF) is a structured penetration testing framework that has the advantage of security control with stages of Planning and Preparation, Evaluation, Vulnerability Identification, and Penetration. Open Web Application Security Project (OWASP) aims to create software security from unauthorized parties with stages of Authentication Testing, Authorization Testing. This research uses the penetration testing (pentest) method to test the s1if.ittelkom-pwt.ac.id website, the pentest method is also widely used.

RESULT AND DISCUSSION

Types of preprocessing that in the results and discussion, the carried out 2 methods, namely testing the Information System Assessment Framework (ISSAF) approach and testing the Open Web Application Security Project (OWASP) method. What is explained in the ISSAF and OWASP methods are the stages of testing. In this case study, the implementation was carried out on the s1if.ittelkom-pwt.ac.id website which is known to still have vulnerabilities that can be exploited by irresponsible parties. This method can be done on other websites, to find out the security system of a website.

Testing the Information System Assessment Framework (ISSAF) Method

Planning and Preparation

Table 1. Case Study Information

No	Case	Information
1	The web used In this study	https://s1if.ittelkom-pwt.ac.id/
2	Web IP Address	IP 180.250.247.93
3	Date of Testing Web	stages from July 17, 2022, to July 31, 2022.
4	Permission	Have done permission on the agency (Lawful Penetration)

Source: Website S1IF IT Telkom, 2022

Assessment

1. Information Gathering
   a. Domain Info
   During the stage of searching for domain information by using who.is, 12 findings were obtained, including the following case study information as can be seen in Table 2.

Table 2. Domain Information

1	Hosting provider	Rumahweb
2	Domain id	PANDI-D0665256
3	Created on	08-29-2017
4	Last updated	03-09-2021
5	Expiration date	29-08-2022
6	Service provider	Digital registra
7	Service provider URL	www.digitalregistra.co.id
8	Sponsoring address	Jl. Lempongsari no 39C.
9	Sponsoring city	Sleman.
10	Sponsoring province	Yogyakarta.
11	Postal code	55281.
12	Name Server	nsid1.rumahweb.com nsid2.rumahweb.net nsid3.rumahweb.biz nsid4.rumahweb.org

Source: Processed by the Authors, 2022

   b. SSL Scan (Secure Sockets Layer Scan)
   The results of the SSL Scan using the SSLLabs tool show that the web s1if.ittelkom-pwt.ac.id gets an overall rating of B which means good.

Figure 2. Results from who.is
Source: Processed by the Authors, 2022

   The certificate on the web s1if.ittelkom-pwt.ac.id is very well installed with a 2048 bits RSA certificate (SHA256withRSA).

2. Network Mapping
   The results of the network mapping test on the s1if.ittelkom-pwt.ac.id web show that the domain has a public IP of 180.250.247.93 with 3 open ports, namely ports 80, 443, and 1723.

Vulnerability Identification

1. Using pentest tools
   The results of the vulnerability identification test using pentest-tools.com contained 19 vulnerabilities with details of 1 medium vulnerability, 8 low vulnerability, and 10 info.

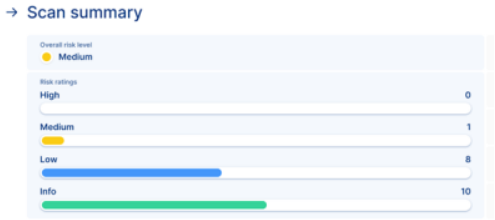


Figure 3. Vulnerability Results Using Pentest Tools
Source: Processed by the Authors through Pentest Tool, 2022

   The vulnerability code for this medium is CVE-2019-11358, CVE-2020-11022, and CVE-2020-11023. Where the main problem with this vulnerability is the version of jQuery that has not been updated (Dharma, 2005).

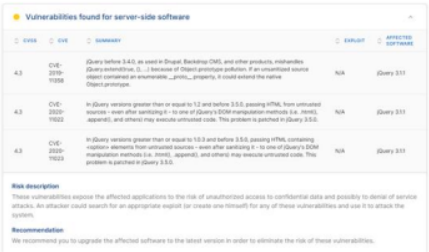


Figure 4. Contents of Medium Vulnerabilities
Source: Processed by the Authors through Vulnerabilities, 2022

a. CVE-2019-11358
It is a vulnerability in jQuery because jQuery is used under the 3.4.0 version which is commonly used in Drupal, CMS backdrops, etc. This version mishandles jQuery.extend(true, { }, ...).

b. CVE-2020-11022
There is a vulnerability in jQuery between version 1.2 and before version 3.5.0 that passes HTML from untrusted sources even after purging to one of jQuery's DOM manipulation methods namely .html(), .append(), and other methods. This vulnerability can be overcome by implementing jQuery version 3.5.0.

c. CVE-2020-11023
There is a vulnerability in jQuery versions above 1.0.3 and before version 3.5.0 that passes <option> elements from trusted sources even after purging to one of the DOM (Document Object Model) models like .html(), .append(), etc. This vulnerability can be overcome with jQuery version 3.5.0 and above.

However, there is 1 vulnerability that goes into the low vulnerability. It is very vulnerable to being exposed to attacks. That is the exposure of the robots.txt file which after being investigated contains user-agent data, site sitemaps, and several website usernames.

Figure 5. Contents of Low Vulnerability
Source: Processed by the Authors through Robot, 2022

```
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php

Sitemap: https://s1if.ittelkom-pwt.ac.id/wp-sitemap.xml
```

Figure 6. Contents of File Robots.txt
Source: Processed by the Authors through Robot, 2022

2. Using acunetix
Meanwhile, the results of the vulnerability scanning using acunetix, found 1 vulnerability, namely Clickjacking: X-Frame-Options header missing. Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking Web users into clicking on something different from what the user thinks they are clicking, thereby potentially revealing confidential information or taking control of their computer when they click on a web page that seems harmless.

The server does not return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack.

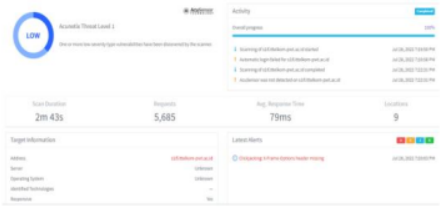


Figure 7. Threat Vulnerabilities in Acunetix
Source: Processed by the Authors through Acunetix, 2022

Meanwhile, other findings from acunetix in web s1if are the site structure as can be seen in Figure 8.

Figure 8. Site Structure from Acunetix
Source: Processed by the Authors through Acunetix, 2022

Penetration

1. DoS Attack
The next step is to conduct penetration testing by using the DoS Attack method. DoS is an activity that can hinder a service so that users who are

entitled/interested cannot use the service. The https://s1if.ittelkom-pwt.ac.id/ website was able to withstand these attacks. This can be known by blocking the attacker's IP automatically after it is indicated that it has flooded the server with many requests in a short time (Samsumar & Gunawan, 2017).

Figure 9. DoS attacks using Low Orbit Ion Cannon (LOIC)
Source: Processed by the Authors through LOIC, 2022

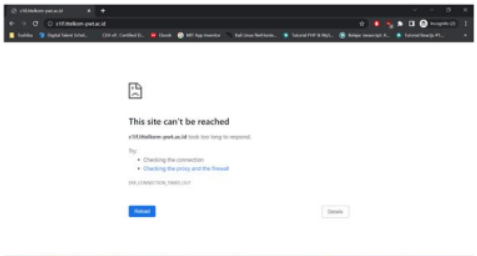


Figure 10. The attacker's PC can't access the website
Source: Processed by the Authors, 2022

Figure 11. The website still can be accessed from other devices
Source: Processed by the Authors through ITTP Website, 2022

2. SQL Injection
   This type of attack attacks by exploiting security loopholes that appear in databases and applications, for SQL Injection attacks, the s1if website cannot be attacked using this method because there is no vulnerability or bug on the website (Bastian, Sujadi, & Abror, 2020).
3. Brute Force
   A brute force is a consequence that can be caused by an attacker that get access rights on the server and the attacker can freely access the information contained in the server (Prasetyo, Idhom, & Wahanani, 2020). For this type of attack, this study uses hydra to attack the logged-in user on the s1if web. As it is known that there is a list of users on the website that allows exploits on the s1if website by using brute-force attacks. This study attacked by initializing the username variable with st3telkomin, and brute force with the wordlist RockYou, but could not find the login password for the usernames st3telkomin, azizah, Bunga, and s1ifadmin.

Table 3. ISSAF Test Results

Stages	Tools	Results
Information Gathering	Who. is	Success
	SSL Scan	Success
Network Mapping	Legion	Success
Vulnerability Identification	Pentest Tools	Success
	Acunetix	Success
	DoS Attack	Not Successful
	SQL Injection	Not Successful
	Brute Force	Not Successful

Source: Processed by the Authors, 2022

The test results using ISSAF show that the s1if website still has basic weaknesses, especially in Jquery which has not yet received the latest updates which are very

vulnerable to exploiting certain attacks. The s1if website has been equipped with an auto-blocking mechanism if it is found that suspicious website access is simultaneously and in a short time which aims to bring down the website, the attacker's IP will be blocked for a while.

Testing the Open Web Application Security Project (OWASP) Method

Authentication Testing

This process is trying to authenticate/verify the correct identity of the sender of information. The stages of Authentication Testing carried out by researchers are as (Dirgahayu, Prayudi, & Fajaryanto, 2015).

Authorization Testing

Testing for authorization means understanding how the authorization process works and using that information to circumvent authorization mechanisms. Authorization is a process that comes after successful authentication, so the tester will verify this point once he holds a valid identity (Hidayatulloh & Saptadiaji, 2021).

From the Table 4, it can be seen that research using OWASP 4.0 was successfully carried out, but several points were not successfully carried out due to the lack of further information about the contents of the S1if website. Web s1if is considered safe from simple attacks and

Table 4. OWASP test results

Stage	Parameter	Tools	Results
Authentication Testing	Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001)	Web Scarab	Success
	Testing for default credentials (OTG-AUTHN-002)	Mozilla Firefox	Success
	Testing for Weak lock-out mechanism (OTG-AUTHN003)	Mozilla Firefox	Not Successful
	Testing for bypassing authentication schema (OTGAUTHN-004)	Web Scarab	Success
	Test remember password functionality (OTG-AUTHN005)	Mozilla	Not Successful
	Testing for Browser cache weakness (OTG-AUTHN006)	Mozilla	Not Successful
	Testing for Weak password policy (OTG-AUTHN-007)	Mozilla	Not Successful
	Testing for Weak security question/answer (OTGAUTHN-008)	Mozilla	Not Successful
	Testing for weak password change or reset functionalities (OTG- AUTHN-009)	Mozilla	Not Successful
	Testing for Weaker authentication in the alternative channel (OTG-AUTHN-010)	-	Not Successful
Authorization Testing	Testing Directory traversal/file includes (OTGAUTHZ-001)	Wfuzz	Success
	Testing for bypassing authorization schema (OTGAUTHZ-002)	-	Not Successful
	Testing for Privilege Escalation (OTG-AUTHZ-003)	-	Not Successful
	Testing for Insecure Direct Object References (OTGAUTHZ-004)	Mozilla Firefox	Success

Source: Processed by the Authors, 2022

bypass security when viewed from the OWASP 4.0 research, but there are several points from OWASP 4.0 that cannot be investigated further.

CONCLUSIONS, RECOMMENDATION AND LIMITATION

In penetration testing using the ISSAF and OWASP frameworks, it was quite effective in detecting the types of vulnerabilities on the S1 Informatics website. It has been tested for the types of vulnerabilities detected with moderate and low vulnerabilities shown in the discussion above. This study recommends that further research not only use the ISSAF and OWASP frameworks but using other techniques such as using tools MALTEGO, NCRACK, SQLMAP on Kali Linux to find profound weaknesses in the system.

REFERENCES

Alfidzar, H., & Zen, B. P. (2022). Implementasi HoneyPy dengan Malicious Traffic Detection System (Maltrail) Menggunakan Analisis Deskriptif guna untuk Mendeteksi Serangan DDOS pada Server. *Journal of Informatics Information System Software Engineering and Applications (INISTA)*, *4*(2), 32–45. https://doi.org/10.20895/inista.v4I2.534

Bastian, A., Sujadi, H., & Abror, L. (2020). Analisis Keamanan Aplikasi Data Pokok Pendidikan (Dapodik) Menggunakan Penetration Testing dan SQL Injection. *Infotech Journal*, *6*(2), 65–70. https://doi.org/10.31949/infotech.v6I2.848

Bolanio, J. B., Paredes, R. K., Yoldan, J. A. L., & Acapulco II, R. E. (2021). Network Security Policy for Higher Education Institutions based on ISO Standards. *Mediterranean Journal of Basic and Applied Sciences*, *5*(1), 1–17. https://doi.org/10.1016/S1353-4858(10)70039-8

CNN Indonesia. (2022, January 20). Sistem Keamanan Siber BI Ditembus, Berikut Data yang Dicuri. Retrieved November 8, 2022, from https://www.cnnindonesia.com/teknologi/20220120175527-185-749252/sistem-keamanan-siber-bi-ditembus-berikut-data-yang-dicuri

Dharma, M. A. J. (2005). *DOS, DDOS & Cara Penanggulangannya*. Universitas Sriwijaya. https://fdokumen.com/document/dos-denial-of-service-halaman-utama-viewbisa-di-tebak-situs-yang.html?page=1

Darmawan, B. I. (2019). *Simulasi dan Analisis Encryption Based Ransomware untuk Memetakan Evolusi Ransomware*. Universitas Islam Indonesia, Yogyakarta.

Dirgahayu, R. T., Prayudi, Y., & Fajaryanto, A. (2015). Penerapan Metode ISSAF dan OWASP Versi 4 untuk Uji Kerentanan Web Server. *Network Engineering Research Operation*, *1*(3), 190–197. https://doi.org/10.21107/nero.v1I3.29

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., … Baker, T. (2018). Security Threats to Critical Infrastructure: the Human Factor. *Journal of Supercomputing*, *74*, 4986–5002. https://doi.org/10.1007/s11227-018-2337-2/tables/1

Haeruddin, & Kurniadi, A. (2021). Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6). *Conference on Management, Business, Innovation, Education and Socal Sciences*, 508–515. Batam: Universitas Internasional Batam.

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

Mulyanto, Y., Haryanti, E., & Jumirah. (2021). Analisis Keamanan Website SMAN 1 Sumbawa Menggunakan Metode Vulnerability Asesement. *Jurnal Informatika Teknologi Dan Sains*, *3*(3), 394–400. https://doi.org/10.51401/jinteks.v3I3.1260

Prasetyo, K. A., Idhom, M., & Wahanani, H. E. (2020). Sistem Pencegahan Serangan Bruteforce pada Multiple Server dengan Menggunakan Fail2ban. *Jurnal Informatika Dan Sistem Informasi*, *1*(3), 709–715. https://doi.org/10.33005/jifosi.v1I3.205

Pratama, I. P. A. E., & Wiradarma, A. A. B. A. (2019). Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study: X Company). *International Journal of Computer Network and Information Security*, *11*(7), 8–12. https://doi.org/10.5815/ijcnis.2019.07.02

Rochman, A., Salam, R. R., & Maulana, S. A. (2021). Analisis Keamanan Website dengan Information System Security Assessment Framework (Issaf) dan Open Web Application Security Project (Owasp) di Rumah Sakit Xyz. *Jurnal Indonesia Sosial Teknologi*, *2*(4), 506–519. https://doi.org/10.36418/jist.v2i4.124

Samsumar, L. D., & Gunawan, K. (2017). Analisis dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless LAN); Studi Kasus di Kampus STMIK Mataram. *Jurnal Ilmiah Teknologi Infomasi Terapan*, *4*(1), 73–82. https://doi.org/10.33197/jitter.vol4.iss1.2017.152

Sanjaya, I. G. A. S., Sasmita, G. M. A., & Arsa, D. M. S. (2020). Evaluasi Keamanan Website Lembaga X melalui Penetration Testing Menggunakan Framework ISSAF. *Jurnal Ilmiah Merpati*, *8*(2), 113–124. https://doi.org/10.24843/jim.2020.v08.i02.p05

Sari, W. P., & Putra, I. N. A. P. (2015). Analisis Serangan Hacker Menggunakan Honeypot High Interaction. *Jurnal Tiarsie*, *14*(1). https://doi.org/10.32816/tiarsie.v14i1.16

Sun, C.-C., Hahn, A., & Liu, C.-C. (2018). Cyber Security of a Power Grid: State-of-the-Art. *International Journal of Electrical Power & Energy Systems*, *99*, 45–56. https://doi.org/10.1016/j.ijepes.2017.12.020

Zen, B. P., Gultom, R. A. G., & Reksoprodjo, A. H. S. (2020). Analisis Security Assessment Menggunakan Metode Penetration Testing dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara. *Jurnal Teknologi Penginderaan*, *2*(1), 105–122. https://doi.org/10.5121/csit.2018.81714

SECURITY ANALYSIS ON WEBSITES USING THE INFORMATION SYSTEM ASSESSMENT FRAMEWORK (ISSAF) AND OPEN WEB APPLICATION SECURITY VERSION 4 (OWASPv4) USING THE PENETRATION TESTING METHOD

ORIGINALITY REPORT

14%
SIMILARITY INDEX

PRIMARY SOURCES

1	jurnal.stkippgritulungagung.ac.id Internet	75 words — 2%
2	www.researchgate.net Internet	57 words — 1%
3	123docz.net Internet	52 words — 1%
4	es.slideshare.net Internet	47 words — 1%
5	epdf.pub Internet	45 words — 1%
6	Submitted to Telkom University Your Indexed Documents	30 words — 1%
7	pdfs.semanticscholar.org Internet	27 words — 1%
8	I Putu Agus Eka Pratama, Alvin Maulana Rhusuli. "Penetration Testing on Web Application Using	26 words — 1%

Insecure Direct Object References (IDOR) Method", 2022 International Conference on ICT for Smart Society (ICISS), 2022
Crossref

9	developer.tenable.com Internet	19 words — < 1%
10	jartel.polinema.ac.id Internet	18 words — < 1%
11	jptam.org Internet	17 words — < 1%
12	Abdallah A. Smadi, Babatunde Tobi Ajao, Brian K. Johnson, Hangtian Lei, Yacine Chakhchoukh, Qasem Abu Al-Haija. "A Comprehensive Survey on Cyber-Physical Smart Grid Testbed Architectures: Requirements and Challenges", Electronics, 2021 Crossref	16 words — < 1%
13	Wahyu Adi Prabowo, Yudha Saintika. "Perancangan IT Balanced Scorecard dalam Penyusunan Strategic Map Perguruan Tinggi (Studi kasus: Institut Teknologi Telkom Purwokerto)", JRST (Jurnal Riset Sains dan Teknologi), 2018 Crossref	16 words — < 1%
14	theses.lib.sfu.ca Internet	16 words — < 1%
15	pdfcoffee.com Internet	15 words — < 1%
16	www.rumahweb.com Internet	14 words — < 1%
17	eprints.unm.ac.id Internet	

12 words — < 1%

18	Power Systems, 2015. Crossref	11 words — < 1%
19	journal.lembagakita.org Internet	11 words — < 1%
20	Vargas Moya, Edgardo. "Security and Privacy Risks Associated of Cloud Computing: A Correlational Study", Capella University, 2021 ProQuest	10 words — < 1%
21	ojs.unud.ac.id Internet	10 words — < 1%
22	www.idealhost.eu Internet	9 words — < 1%
23	Mohamed Gaber, Ashraf Khalaf, Imbaby Mahmoud, Mohamed El_Tokhy. "Advanced Protection Scheme For Information Monitoring in Internet of Things Environment", Research Square Platform LLC, 2021 Crossref Posted Content	8 words — < 1%
24	silo.tips Internet	8 words — < 1%

EXCLUDE QUOTES	ON	EXCLUDE SOURCES	OFF
EXCLUDE BIBLIOGRAPHY	ON	EXCLUDE MATCHES	OFF

Proses submission

Indonesia Defense University

E-ISSN: 2549-9459

HOME ABOUT USER HOME SEARCH CURRENT ARCHIVES ANNOUNCEMENTS
EDITORIAL BOARD REVIEWERS PUBLICATION ETHICS AUTHOR GUIDELINES & SUBMISSION FOCUS AND SCOPE EDITORIAL POLICIES CONTACT

Home > User > Author > Submissions > #1777 > **Summary**

#1777 Summary

SUMMARY REVIEW EDITING

Submission

Authors	Ditya Putri Anggraeni, Bita Parga Zen, Mega Pranata
Title	SECURITY ANALYSIS ON WEBSITES USING THE INFORMATION SYSTEM ASSESSMENT FRAMEWORK (ISSAF) AND OPEN WEB APPLICATION SECURITY VERSION 4 (OWASPv4) USING THE PENETRATION TESTING METHOD
Original file	1777-7145-1-SM.DOCX 2022-09-13
Supp. files	None
Submitter	BITA PARGA ZEN
Date submitted	September 13, 2022 - 04:23 AM
Section	Articles
Editor	Prof. Tutut Herawan, BEd, MSc, PhD
Author comments	Kepada editor, mohon untuk di proses ya
Abstract Views	0

USER
You are logged in as...
bitapargazen
- My Journals
- My Profile
- Log Out

ABOUT THE JOURNAL
- Focus and Scope
- Editorial Board
- List of Reviewers
- Author Guidelines & Submissions
- Section Policies
- Peer Reviewed Process
- Open Access Policy
- Archiving
- Article Processing Charges (APCs)
- Publication Ethics
- Ethics Statement
- Plagiarism
- Publication Frequency
- Creative Commons Licensing

NEW SUBMISSION

Proses Review

Indonesia Defense University

E-ISSN: 2549-9459

HOME ABOUT USER HOME SEARCH CURRENT ARCHIVES ANNOUNCEMENTS
EDITORIAL BOARD REVIEWERS PUBLICATION ETHICS AUTHOR GUIDELINES & SUBMISSION FOCUS AND SCOPE EDITORIAL POLICIES CONTACT

Home > User > Author > Submissions > #1777 > **Review**

#1777 Review

SUMMARY **REVIEW** EDITING

Submission

Authors	Ditya Putri Anggraeni, Bita Parga Zen, Mega Pranata
Title	SECURITY ANALYSIS ON WEBSITES USING THE INFORMATION SYSTEM ASSESSMENT FRAMEWORK (ISSAF) AND OPEN WEB APPLICATION SECURITY VERSION 4 (OWASPv4) USING THE PENETRATION TESTING METHOD
Section	Articles
Editor	Prof. Tutut Herawan, BEd, MSc, PhD

Peer Review

Round 1

Review Version	1777-7146-1-RV.DOCX 2022-09-13
Initiated	2022-10-25
Last modified	2022-12-09
Uploaded file	Reviewer B 1777-7489-1-RV.DOC 2022-12-09

Editor Decision

Decision	Accept Submission 2022-12-21
Notify Editor	Editor/Author Email Record 2022-12-09
Editor Version	None
Author Version	1777-7262-1-ED.DOCX 2022-10-19 DELETE 1777-7262-2-ED.DOCX 2022-11-11 DELETE 1777-7262-3-ED.DOCX 2022-12-05 DELETE 1777-7262-4-ED.DOC 2022-12-12 DELETE

USER
You are logged in as...
bitapargazen
- My Journals
- My Profile
- Log Out

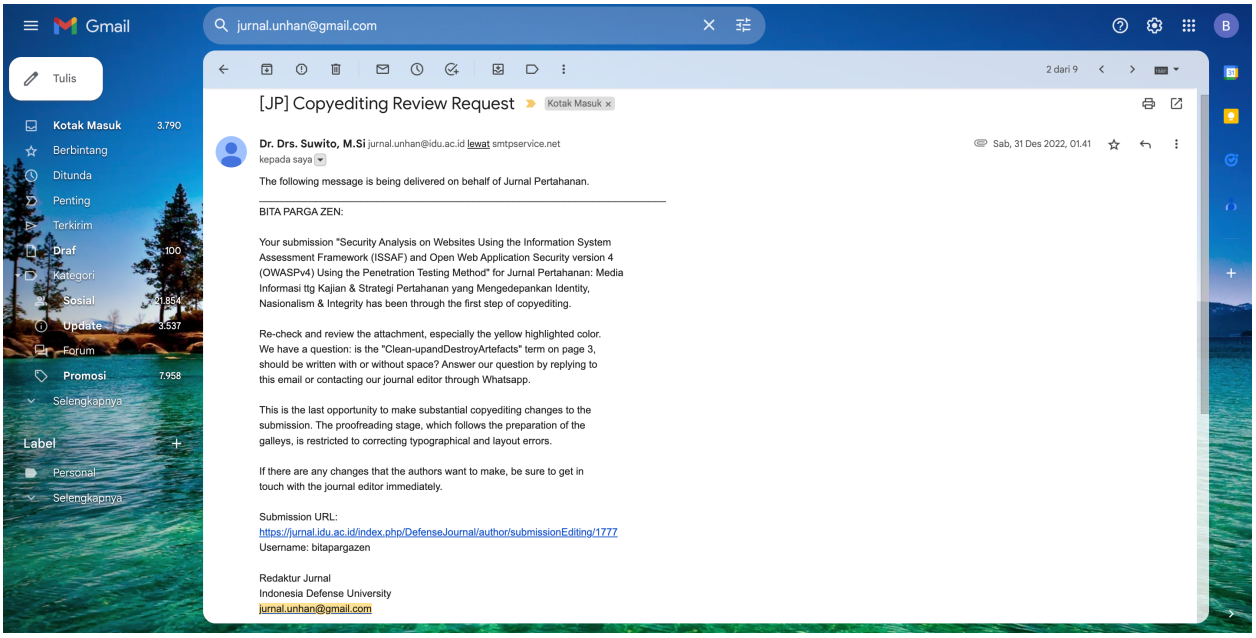
ABOUT THE JOURNAL
- Focus and Scope
- Editorial Board
- List of Reviewers
- Author Guidelines & Submissions
- Section Policies
- Peer Reviewed Process
- Open Access Policy
- Archiving
- Article Processing Charges (APCs)
- Publication Ethics
- Ethics Statement
- Plagiarism
- Publication Frequency
- Creative Commons Licensing

NEW SUBMISSION

Article template

JOURNAL CONTENT

Bukti Copyediting dan Accept



[JP] Copyediting Review Request

Dr. Drs. Suwito, M.Si jurnal.unhan@idu.ac.id lewat smtpservice.net
kepada saya

Sab, 31 Des 2022, 01.41

The following message is being delivered on behalf of Jurnal Pertahanan.

BITA PARGA ZEN:

Your submission "Security Analysis on Websites Using the Information System Assessment Framework (ISSAF) and Open Web Application Security version 4 (OWASPv4) Using the Penetration Testing Method" for Jurnal Pertahanan: Media Informasi ttg Kajian & Strategi Pertahanan yang Mengedepankan Identity, Nasionalism & Integrity has been through the first step of copyediting.

Re-check and review the attachment, especially the yellow highlighted color. We have a question: is the "Clean-upandDestroyArtefacts" term on page 3, should be written with or without space? Answer our question by replying to this email or contacting our journal editor through Whatsapp.

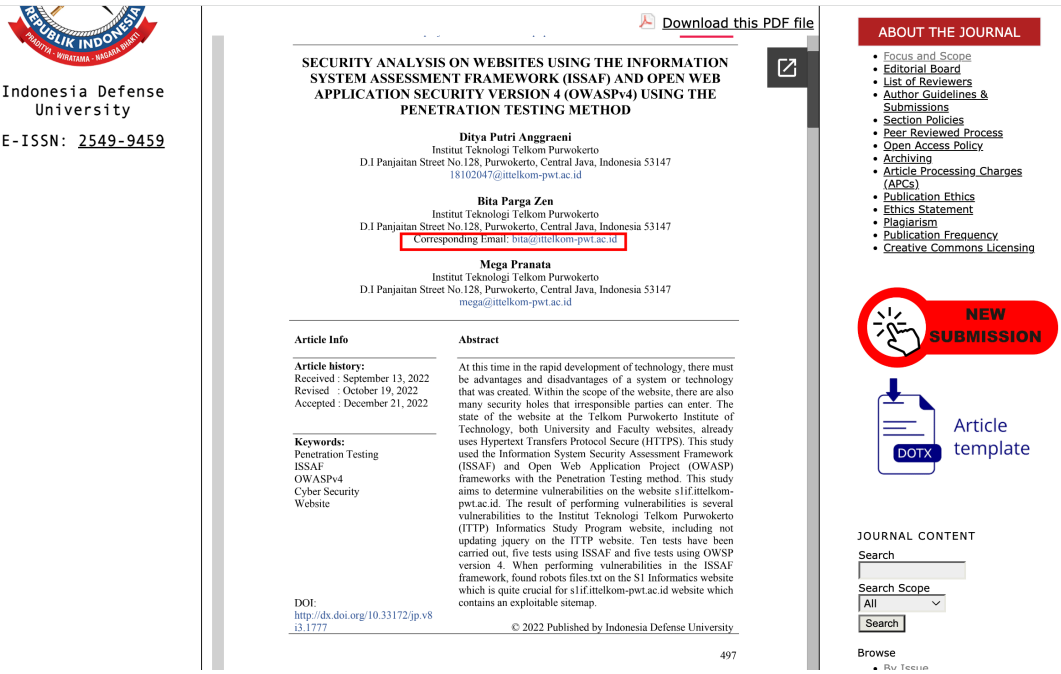
This is the last opportunity to make substantial copyediting changes to the submission. The proofreading stage, which follows the preparation of the galleys, is restricted to correcting typographical and layout errors.

If there are any changes that the authors want to make, be sure to get in touch with the journal editor immediately.

Submission URL:
https://jurnal.idu.ac.id/index.php/DefenseJournal/author/submissionEditing/1777
Username: bitapargazen

Redaktur Jurnal
Indonesia Defense University
jurnal.unhan@gmail.com

Bukti Korespondensi pada naskah



Indonesia Defense University

E-ISSN: 2549-9459

Download this PDF file

SECURITY ANALYSIS ON WEBSITES USING THE INFORMATION SYSTEM ASSESSMENT FRAMEWORK (ISSAF) AND OPEN WEB APPLICATION SECURITY VERSION 4 (OWASPv4) USING THE PENETRATION TESTING METHOD

Ditya Putri Anggraeni
Institut Teknologi Telkom Purwokerto
D.I Panjaitan Street No.128, Purwokerto, Central Java, Indonesia 53147
18102047@ittelkom-pwt.ac.id

Bita Parga Zen
Institut Teknologi Telkom Purwokerto
D.I Panjaitan Street No.128, Purwokerto, Central Java, Indonesia 53147
Corresponding Email: bita@ittelkom-pwt.ac.id

Mega Pranata
Institut Teknologi Telkom Purwokerto
D.I Panjaitan Street No.128, Purwokerto, Central Java, Indonesia 53147
mega@ittelkom-pwt.ac.id

Article Info

Article history:
Received : September 13, 2022
Revised : October 19, 2022
Accepted : December 21, 2022

Keywords:
Penetration Testing
ISSAF
OWASPv4
Cyber Security
Website

DOI:
http://dx.doi.org/10.33172/jp.v8i3.1777

Abstract

At this time in the rapid development of technology, there must be advantages and disadvantages of a system or technology that was created. Within the scope of the website, there are also many security holes that irresponsible parties can enter. The state of the website at the Telkom Purwokerto Institute of Technology, both University and Faculty websites, already uses Hypertext Transfers Protocol Secure (HTTPS). This study used the Information System Security Assessment Framework (ISSAF) and Open Web Application Project (OWASP) frameworks with the Penetration Testing method. This study aims to determine vulnerabilities on the website s1if.ittelkom-pwt.ac.id. The result of performing vulnerabilities is several vulnerabilities to the Institut Teknologi Telkom Purwokerto (ITTP) Informatics Study Program website, including not updating jquery on the ITTP website. Ten tests have been carried out, five tests using ISSAF and five tests using OWSP version 4. When performing vulnerabilities in the ISSAF framework, found robots files.txt on the S1 Informatics website which is quite crucial for s1if.ittelkom-pwt.ac.id website which contains an exploitable sitemap.

ABOUT THE JOURNAL

- Focus and Scope
- Editorial Board
- List of Reviewers
- Author Guidelines & Submissions
- Section Policies
- Peer Reviewed Process
- Open Access Policy
- Archiving
- Article Processing Charges (APCs)
- Publication Ethics
- Ethics Statement
- Plagiarism
- Publication Frequency
- Creative Commons Licensing

NEW SUBMISSION

Article template

JOURNAL CONTENT

Search

Search Scope
All

Search

Browse