Evaluation Security Web-Based Information System Application Using ISSAF Framework (Case Study: SIMAK-NG Udayana University)

Ni Kade Mega Handayani[a1], Gusti Made Arya Sasmita[a2], Anak Agung Ketut Agung Cahyawan Wiranatha [b3]

[a]Information Technology Department, Udayana University, Indonesia
[b]Information Technology Department, Udayana University, Indonesia
[c]Information Technology Department, Udayana University, Indonesia
e-mail: [1]megahandayani95@gmail.com, [2]aryasasmita88@gmail.com,
[3]agung.cahyawan@gmail.com

Abstrak

Pendidikan merupakan salah satu bidang yang memanfaatkan teknologi informasi dalam mendukung kegiatan baik akademik maupun operationalnya. Teknologi yang banyak digunakan dalam bidang pendidikan adalah teknologi yang berbasis aplikasi web. Teknologi berbasis web memiliki kelemahan yang dapat dimanfaatkan oleh para penyerang untuk melakukan eksploitasi terhadap suatu sistem berbasis web. Sistem berbasis web perlu mempunyai jaminan keamanan yang baik dapat memberikan rasa aman bagi penggunanya. Universitas Udayana sebagai organisasi pendidikan juga menggunakan aplikasi berbasis web yang dikenal dengan SIMAK-NG. SIMAK-NG sebagai sistem berbasis web perlu dilakukan uji keamanan. Uji kemanan dapat dilakukan dengan penetration test. Penetration test dapat dilakukan dengan kerangka kerja ISSAF. penetration test berdasarkan kerangka kerja ISSAF ada 9 tahapan, meliputi information gathering, network mapping , vulnerability identification, peneitration, gainning acces and privilage escalation, enumerating further, maintain access dan covering tracks. Hasil pengujian penetration SIMAK-NG pada tahap identifikasi celah ditemukan beberapa kerentanan sistem. Hasil akhir pengujian pada semua tahapan ISSAF pada SIMAK-NG hanya ditemukan 11 kerentanan diantaranya 3 kerentanan level medium, 6 kerentanan level low dan 2 kerentanan level informational. Kerentanan yang sukses diuji diberikan rekomendasi perbaikan untuk menutup celah kerentanan sehingga tidak terdapat lagi kerentanan yang bisa digunakan oleh penyerang.

Kata kunci: *Pendidikan, Evaluasi Keamanan, Uji Penetrasi, ISSAF, Website, Kerentanan, Keamanan*

Abstract

Education is one of the fields that utilize information technology to support both academic and operational activities. Technology that is widely used in education is technology based on web applications. Web-based technology has weaknesses that can be used to exploited by attackers. Web-based systems need to have a good security guarantee to provide a sense of security for its users. Udayana University as an educational organization also uses a web-based application known as SIMAK-NG. SIMAK-NG as a web-based system needs a security test. Security tests with penetration tests. Penetration tests with the ISSAF framework. The penetration test based on the ISSAF framework consists of 9 stages, including information gathering, network mapping, vulnerability identification, penetration, gainning access and privilege escalation, enumerating further, maintaining access and covering tracks. The results of SIMAK-NG penetration testing at the gap identification stage found several system vulnerabilities. The final results of testing at all stages of ISSAF at SIMAK-NG only found 11 vulnerabilities including 3 medium level vulnerabilities, 6 low level vulnerabilities and 2 informational level vulnerabilities. Vulnerabilities that are successfully tested are given recommendations for fixes to close vulnerabilities so that no more vulnerabilities can be used by the attacker

Keywords: *Education, Assessment Security, Penetration Testing, ISSAF, Website, Vulnerability*

1. Introduction

Udayana University is a college in the education field. Udayana University implements a web-based information system known as SIMAK-NG (Sistem Informasi Manajemen Akademik Kampus-New Generation). SIMAK-NG is a web-based information system application that is integrated with the single sign-on method on the IMISSU system (Integrated Management Information System, the Strategic of UNUD) which is a portal for all information systems at UNUD. SIMAK-NG was built to support business processes in the academic field of the University which need to be guaranteed from a security side.

SIMAK-NG system security is based on the gap identification stage carried out, there is still some vulnerability in the system. The vulnerabilities found are still in the high threat level category. This shows that SIMAK-NG still needs to do a security evaluation. This security evaluation is necessary because every web application has a security vulnnerability that can be exploited by attaker.

Penetration testing is an attempt by an attacker to exploit a system directly [1]. There are many penetration testing frameworks, one of which is the ISSAF used in this study. The ISSAF framework is a structured penetration testing framework for testing system weaknesses in depth to find as many vulnerabilities as possible[2]. There nine step of ISSAF framework of penetration testing, but this studi will ekplain only 4 step, that is information gathering, network mapping, vulnerability identification.

2. Research Method / Proposed Method

The research method used is based on the ISSAF framework. Penetration testing consists of 3 phases, covering the preparation and planning phases, the assessment and reporting phases, the cleaning and destruction of evidence [3]. The assessment stage is divided into 9 main processes. The preparatory and planning phase begins by requesting research permission from USDI as the SIMAK-NG application developer.

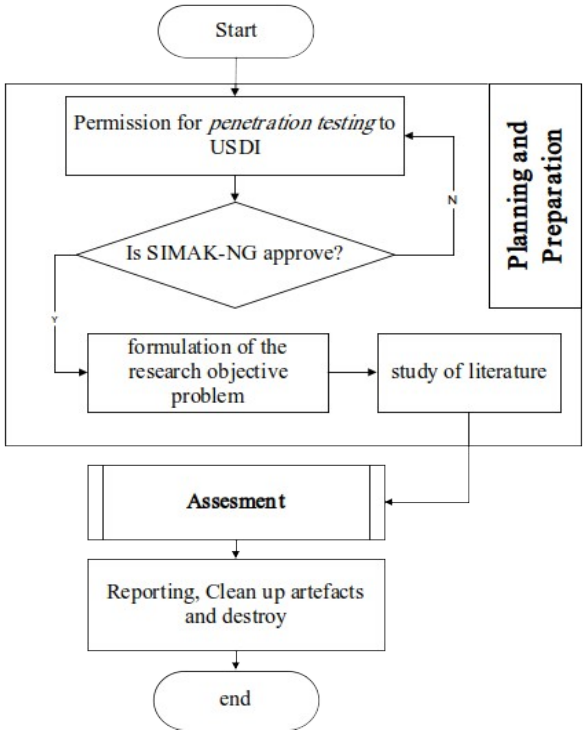

Figure 1. Data flow diagram general step of ISSAF Framework

Figure 1 show general step of ISSAF Framework that we should follow before we can do penetration, the first phase preparation dan planning include request permition to the target that will be attack, for SIMAK-NG depelover in USDI (Unit Sumber Daya Informasi) Udayana

University. The next phase is is assessment, for this phase in this study we only explain step, that is information gathering, network mapping, vulnerability identification.

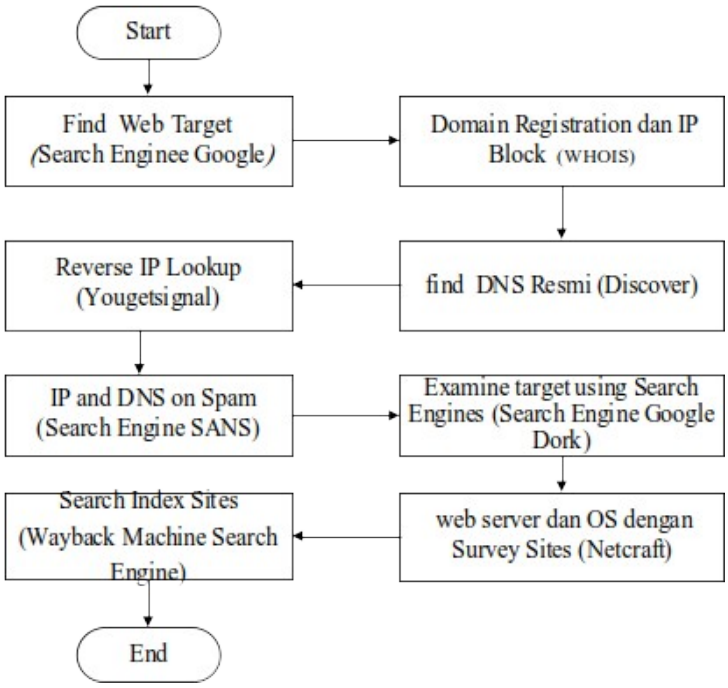

Figure 2. Data flow diagram information gathering

Figure 2 is diagram flow processes include obtaining target name information, identifying domain registration, target DNS identification, reverse DNS, getting more information using the help of a search engine, getting web server information from netcraft and getting web mirror results that are in historical web data [4].

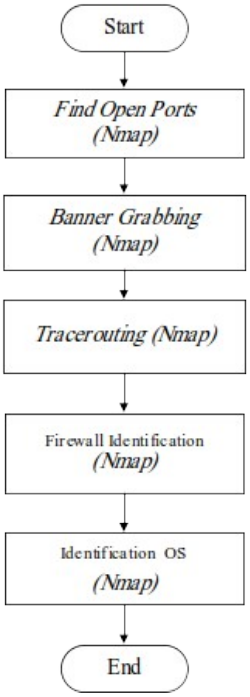

Figure 3. Data flow diagram network mapping

Figure 3 show proses that we do on stage of network mapping is get information open ports target, banners version of the technology used as consideration for further exploitation, perform tracerouting to get information on the closest router that is on the target, prove the existence of the firewall and identify the type of operating system target server [5] .

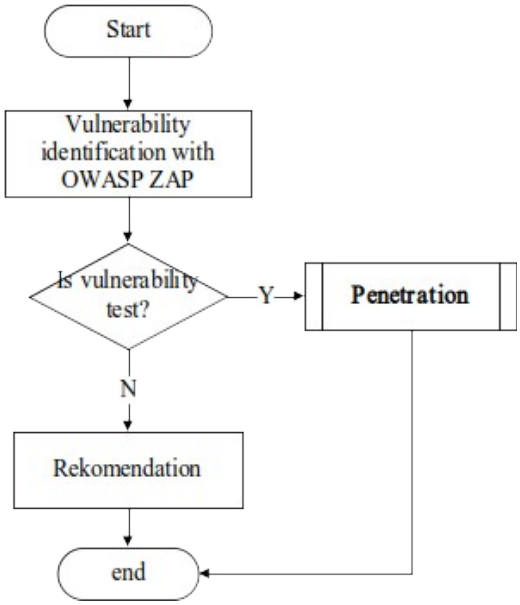

Figure 4. Data flow diagram vulnerability identification

Figure 4 show process in the stage of vulnerability identification, in this study we use OWASP ZAP as tool for scanning vulnerability. The ZAP tool combine with information that we have on stage of information gathering and network mapping, after vulnerability list is complete we go to the next stage is penetration.

3. Literature Study

The theory uses in this study is about penetration testing research using ISSAF framework from books and journals as a support in the research.

3.1 Information Security

Information security is step keep information from possible threats, as a guarantee for business continuity, minimizing business risk (reduce business risk) and maximizing profits and business opportunities [6].

3.2 Vulnerability

Vulnerability is a flaw that allows to reduce the information security assurance of a system. Vulnerability Assessment is a method that tests the security of interactive applications [7].

3.3 Penetration Testing

Penetration testing is a security testing activity that is permitted and legal to exploit the system as an effort to increase the level of system security. The results of the pentration testing are system security gaps that are the recommendation for the repair of the system [8].

3.4 Blackbox Testing

Black-Box Testing is a testing technique that focuses on the functional specifications of software. Blackbox Testing works by ignoring control structures so that attention is focused on domain information. Blackbox Testing allows software developers to create a set of input conditions that will exercise all of the functional requirements of a program [9].

3.5 OWASP ZAP

OWASP ZAP (Open Web Application Security Project Zed Attack Proxy) biasa juga dikenal dengan sebutan Zaproxy, fungsinya sama dengan Burp Suite dimana kita dapat menggunakannya sebagai proxy [10].

4. Result and Discussion

This section will describe a process and result for each testing for information gathering, network mapping and vulnerability identification on this research.

4.1. Information Gathering

The result of information gathering process of system SIMAK-NG Udayana, that is shows on the table above. The status is for show that proses is success if the tools founds the evidence, and fail if the process is not found any a proof.

Table 1. Result of Information Gathering

No	Proses	Tools	Status	Result
1	Locate The Target Web Presence	*Seach enginge* Google	Success	website SIMAK-NG URL simak-ng.unud.ac.id Location Jimbaran, Badung
2	Examine Domain Name System / Find Out Domain Registration Info and IP Block Owned	Whois	Success	Block IP 103.29.196.0 - 103.29.196.255. email Linawati Linawati, email linawati@unud.ac.id
3	Examine Domain Name System - Check for the Authoritative Name Servers	Discover	Success	IP domain pada 103.29.196.139
4	Examine Domain Name System - Check for Reverse DNS lookup presence	Yougetsignal	Success	2 domain beasiswa.unud.ac.id dan simak-ng.unud.ac.id
5	Examine Domain Name System - Check Spam/Attackers databases lookup	SANS *search engine*	Fail	Not found
6	*Examine target using Search Engines*	Google dork	Fail	Not found
7	Search System/Network Survey Sites	Netcraft	Success	OS Linux dengan web server ngix/1.14.0
8	*Search Index Sites*	Wayback Machine	Fail	Not found

Table 1 is a summary of the results of the information gathering stage testing with the main web address simak-ng.unud.ac.id. Important information at this stage includes the IP address of the web, the target domain name server, found OS information that can be used for testing the next network mapping stage.

4.2. Network Mapping

The result of network mapping process of system SIMAK-NG Udayana, that is shows on the table above. The status is for show that proses is success if the tools founds the evidence, and fail if the process is not found any a proof.

Table 2. Result of Network Mapping

No	Proses	Tools	Status	Result
1	Find Open Ports	Nmap	success	domain :simak-ng.unud.ac.id IP :(103.29.196.139)

				Port State Service 21/tcp Open ftp 22/tcp Open ssh 80/tcp Open http 110/tcp Open pop3 143/tcp Open imap 443/tcp open https 993/tcp open imaps 995/tcp open pop3s 3306/tcpopen mysql 8081/tcpopen blackice-icecap
2	Banner Grabbing	Nmap	Success	• 21/tcp open ftp Pure-FTPd banner: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------\x • 22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0) banner: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3. • 110/tcp open pop3 Dovecot pop3d banner: +OK Dovecot (Ubuntu) ready. • 143/tcp open imap Dovecot imapd (Ubuntu) banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID. • 993/tcp open ssl/imap Dovecot imapd (Ubuntu) banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID. • 3306/tcp open mysql MySQL (unauthorized) banner: H\x00\x00\x00\xFFj\x04Host '180.249.119.114' is not allowed to |_connect to this MySQL server.
3	Identify Perimeter Network – Tracerouting	Nmap	Success	Found
4	Identify Firewall	Nmap	Sukses	open|filtered. PORT STATE SERVICE 21/tcp open|filtered ftp 22/tcp open|filtered ssh 53/tcp open|filtered domain 80/tcp open|filtered http 110/tcp open|filtered pop3 123/tcp open|filtered ntp 143/tcp open|filtered imap 993/tcp open|filtered imaps 995/tcp open|filtered pop3s

5	Identify Os	Nmap	Sukses	3306/tcp open|filtered mysql Running: Linux 4.X OS CPE: cpe:/o:linux:linux_kernel:4.9 OS details: Linux 4.9

Table 2 is summary of the test results of the network mapping stage with the main web address simak-ng.unud.ac.id. Important information on the ports on the server from SIMAK-NG, there are many types of service ports, there are UDP, TCP, SMTP, SSH, HTTP and others.

4.3. Vulnerability Identification

The result of vulnerability identification with owasp zap tools process of system SIMAK-NG Udayana, that is shows on the table above. The status is for show that proses is success if the tools founds the evidence, and fail if the process is not found any a proof.

Table 3. Result of Vulnerability Identification

No	Vulnerability	Level	Status
1	Anti CSRF Tokens Scanner	High	Test
2	Remote Code Execution - Shell Shock	High	Test
3	Remote OS Command Injection	High	Test
4	SQL Injection	High	Test
5	Backup File Disclosure	Medium	Test
	Buffer Overflow	Medium	Test
7	Integer Overflow Error	Medium	Test
8	Source Code Disclosure - SVN	Medium	Test
9	X-Frame-Options Header Not Set	Medium	Test
10	Absence of Anti-CSRF Tokens	Low	Test
11	Application Error Disclosure	Low	Test
12	Big Redirect Detected (Potential Sensitive Information Leak)	Low	Test
13	Content Security Policy (CSP) Header Not Set	Low	Test
14	Cookie No HttpOnly Flag	Low	Test
15	Cookie Without Secure Flag	Low	Test
16	Cross-Domain JavaScript Source File Inclusion	Low	Test
17	Incomplete or No Cache-control and Pragma HTTP Header Set	Low	Test
18	Information Disclosure - Debug Error Messages	Low	Test
19	Strict-Transport-Security Header Not Set	Low	Test
20	Web Browser XSS Protection Not Enabled	Low	Test
21	Cookie Slack Detector	informational	-
22	User Agent Fuzzer	informational	-

Table 3 is The results of the identification of vulnerabilities contained in SIMAK-NG, this vulnerability is only the possibility of being detected by OWASP ZAP, but to get certainty that the vulnerability may or may not impact the system, it is necessary to carry out the next stage, namely penetration. Vulnerability status which is not tested because it is in an informational threat level only.

5. Conclusion

Final result is the correct results of vulnerability identification exist after passing through the next stage including pentration, gainning access and privilege escalation, enumerating futher, maintaining access and covering track with recommendations.

Table 4 Final Result Test

No	Vunerability	Level	Rekomendation
1	Buffer Overflow	Medium	Rewrite the background program using proper return length checking
2	Interger Overflow Error	Medium	Rewrite the background program using proper checking of the size of integer being input to prevent overflows and

			divide by 0 errors.
3	X-Frame-Options Header Not Set	Medium	Setting X-frame-Option Header on • Apache web: Header always append X-Frame-Options SOMEORIGIN and Header set X-Frame-Options DENY. • Nginx set X-Frame-Options on http, server, or web konfiguration: add_header X-Frame-Options SAMEORIGIN.
4	Big Redirect Detected (Potential Sensitive Information Leak)	Low	Ensure that no sensitive information is leaked via redirect responses. Redirect responses should have almost no content.
5	Content Security Policy (CSP) Header Not Set	Low	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support
6	Cookie Without Secure Flag	Low	File htaccess atau httpd.conf sebagai berikut. Set-Cookie: <PHPSEDDID>=<cookie-value>; Domain=<simak-ng.unuc.ac.id>; Secure; HttOnly
7	Cross-Domain Javascript Source File Inclusion	Low	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
8	Incomplete or No Cache-control and Pragma HTTP Header Set	Low	Possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.
9	Web Browser XSS Protection Not Enabled	Low	Setting htaccess: X-XSS-Protection; 1, mode=block.

The conclusion of this research is that vulnerabilities that have been found and tested can be overcome with recommendations for improvement based on the ISSAF framework.

The vulnerabilities that were successfully tested at the penetration stage became 11 vulnerabilities including 3 vulnerabilities with medium threat levels, 6 vulnerabilities with low threat levels and 2 vulnerabilities with informational levels only. The recommendation to fix the vulnerability given succeeded in closing the existing vulnerabilities in SIMAK-NG. The vulnerabilities that were found and successfully implemented did not have a major impact on the SIMAKNG system and it can be said that SIMAK-NG is in the safe category.

References

[1] J. N. Goel and B. M. Mehtre, “Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology,” *Procedia Comput. Sci.*, vol. 57, pp. 710–715, 2015.

[2] A. F. Zulfi, “Evaluasi Keamanan Aplikasi Sistem Informasi Mahasiswa Menggunakan Framework Vapt (Studi Kasus : Sister Universitas Jember).,” Institut Teknologi Sepuluh Nopember, 2017.

[3] R. E. L. De Jimenez, “Pentesting on web applications using ethical - Hacking,” *2016 IEEE 36th Cent. Am. Panama Conv. CONCAPAN 2016*, no. 503, 2017.

[4] E. Pratama and A. Wiradarma, “Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study : X Company),” *MECS*, vol. 7, no. July, pp. 8–12, 2019.

[5] R. H. Hutagalung, L. E. Nugroho, and R. Hidayat, “Analisis Uji Penetrasi Menggunakan ISSAF (Kasus di Server DTETI UGM),” *Hacking Digit. Forensics Expo.*, pp. 32–40, 2017.

[6] M. Parasian, “Audit Keamanan Sistem Informasi Automatic Meter Reading (AMR)

Menggunakan Framework Cobit 4.1 Dengan Standar ISO 27002:2005," Udayana, 2015.
[7] S. Nagpure and S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," *2017 Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2017*, pp. 1–6, 2018.
[8] P. Engrebeston, *The Basics of Hacking and Penetration Testing*. Massachusetts: Elsevier Inc, 2011.
[9] T. S. Jaya, "Pengujian Aplikasi dengan Metode Blackbox Testing Boundary Value Analysis (Studi Kasus: Kantor Digital Politeknik Negeri Lampung)," *J. Inform. Pengemb. IT*, vol. 3, no. 2, pp. 45–46, 2018.
[10] Mr.Doel, "Panduan Hacking Website dengan Kali Linux." p. 229, 2016.