Souphanouvong University Journal of Multidisciplinary Research and Development
2026, Vol. 12, No. 02, 244-250
https://doi.org/10.69692/SUJMRD1202244

Enhancing the Security Efficiency of the Souphanouvong University Journal Website

Thongphet KHONGKETH[1*], Vinath MEKTHANAVANH[2], Xayxavath SOUKCHALEUN[3], Bounthanome VILAISACK[4], Sangvang KITTIKHOUN[5]

Faculty of Engineering, Souphanouvong University, Lao PDR

***Correspondence:** Thongphet KHONGKETH*, Faculty of Engineering, Souphanouvong University, Tel +8562052354556, E-mail: khongketh.tp@su.edu.la

Article Info:
Submitted: April 27, 2026
Revised: May 19, 2026
Accepted: May 25, 2026

Abstract

This research is a study on the security of the Souphanouvong University Journal website with the aim of testing security checks, detecting flaws and vulnerabilities. The current problem is that the Souphanouvong University Journal website is in an insecure mode, which is at high risk of being hacked or attacked by hackers. Each time you access the website, you will be forced to view the website in an insecure mode, which may cause damage to personal information and lead to attacks on financial transactions. The research method is to analyze the structure of the website, check the SSL/TLS in use, check the Key Certificate, Security Certificate, Server version, and use Command Line commands and advanced programs to detect flaws and vulnerabilities on the website. Through research, we can conclude that: The website code still has weaknesses, SSL/TLS has not been upgraded, the Key Certificate has expired, the Security Certificate has expired, the Server version does not have Secure. Http Only, there are 13 ports open in low security mode, and there are 6 ports with a high risk of being easily attacked. The way to fix and protect the website for security is to update the Source Code with weaknesses, Upgrade SSL/TLS to Version 1.3, Update Key Certificate, Update Security Certificate, Close ports with low security and no services, Install Web Application Firewall, create a security monitoring table, Backup and update the system.

Keywords: Cybersecurity, Vulnerability Assessment, SSL/TLS Encryption, Web Application Firewall (WAF), Network Port Security, Data Protection

1. ພາກສະເໜີ

ປະຈຸບັນເວັບໄຊ້ແມ່ນມີບົດບາດ ແລະ ມີການຕອບໂຕ້ຫຼາຍຂຶ້ນ ຈາກຜູ້ໃຊ້ງານຢູ່ບັນດາອົງກອນທຸກລະດັບ ແລະ ບໍລິສັດຕ່າງໆ ເພື່ອເປັນຕົວຊ່ວຍໃນການແບ່ງປັນຂໍ້ມູນຂ່າວສານ ແລະ ການຕະຫຼາດທີ່ມີຄວາມທັນສະໄໝ ຈຶ່ງເຮັດໃຫ້ມີການພັດທະນາເວັບໄຊ້ອອກມາຫຼາຍຮູບແບບ ເຊັ່ນ: ເວັບບລ໋ອກ (Web block), ເວັບສື່ສັງຄົມ (social media), ແລະ ເວັບແອັບ (Web Application) ເຊິ່ງໄດ້ພັດທະນາເວັບໄຊ້ໂດຍໃຊ້ພາສາ JavaScript, Asynchronous JavaScript and XML (AJAX) ແລະ Cascading Style Sheets (CSS) ເຂົ້າມາຊ່ວຍຕື່ມ (Lane et al., 2017 & Sudianto, A., & Sugiantara, 2020). ປີ 2010 ເວັບໄຊ້ໄດ້ຖືກອອກແບບໃຫ້ສາມາດນຳໃຊ້ກັບອຸປະກອນເຄື່ອນທີ່ໄດ້ (Responsive Web & Mobile-First) ແລະ ມີການພັດທະນາ Framework ເຂົ້າມາຊ່ວຍຕື່ມ ເຊັ່ນ: Bootstrap, React, Angular (Aklesh Kumar, 2022). ປີ 2020 ໄດ້ມີການພັດທະນາເວັບໄຊ້ເວີຊັນ (Web 3.0 ແລະ Artificial Intelligence (AI) ຫຼື Integration) ໂດຍການໃຊ້ Blockchain ເພື່ອເຮັດທຸລະກຳດ້ວຍ Crypto ແລະ ປັນຍາປະດິດ (AI) ເພື່ອໃຫ້ຜູ້ໃຊ້ງານເວັບໄຊ້ເຂົ້າໃຈຂໍ້ມູນຢ່າງເລິກເຊິ່ງ (Ghelani & Hua, 2022 & Lei et al., 2023).

Dynamic (Dynamic Website) ແມ່ນເວັບໄຊທີ່ເນື້ອຫາບໍ່ຄົງທີ່ ແລະ ສາມາດປ່ຽນແປງໄດ້ໂດຍອັດຕະໂນມັດຕາມສະຖານະ ຫຼື

ການຮ້ອງຂໍຂອງຜູ້ໃຊ້, ເວັບປະເພດນີ້ມັກຈະໃຊ້ server-side scripting ຕ່າງໆ ເຊັ່ນ: PHP, Python, Node.js, Java ແລະໃຊ້ຂໍ້ມູນຈາກ database ດ້ວຍ (Guttikonda et al., 2025 & Truong et al., 2025), ມີຄຸນສົມບັດຂອງການປ່ຽນແປງໄດ້ຕາມຜູ້ໃຊ້, ຂໍ້ມູນໃນລະບົບ, ຫຼື ເວລາຈິງ, ໃຊ້ Database (MySQL, PostgreSQL, MongoDB), ໃຊ້ server ປະມວນຜົນກ່ອນສົ່ງໄປຫາຜູ້ໃຊ້, ການໂຕຕອບຕໍ່ຜູ້ໃຊ້ຕ້ອງໃຊ້ຟອມ, ລະບົບ login, ຄົ້ນຫາ, ແລະ ອື່ນໆ. ນິຍົມໃຊ້ກັບເວັບຂ່າວສານ (ຫຼື blog) ທີ່ເນື້ອຫາອັບເດດເລື້ອຍໆ, ເວັບ e-commerce (ຮ້ານຄ້າອອນລາຍ), ເວັບທີ່ມີການ login/logout ແລະ ຈັດການຂໍ້ມູນສ່ວນຕົວ, ລະບົບການຈ່ອງ ແລະ ການຈັດຕາຕະລາງ ເປັນຕົ້ນ. ເທັກໂນໂລຢີທີ່ນິຍົມໃຊ້ໃນເວັບ Dynamic ຄື: Front-end: HTML, CSS, JavaScript (ກັບຟຣຽມເວີກ Angular, React, Vue.js), Back-end: PHP, Node.js, Python (Django/Flask), Ruby on Rails, Database: MySQL, PostgreSQL, MongoDB. ຄວາມປອດໄພທີ່ຈຳເປັນໃນ Dynamic Web ຄື: ປ້ອງກັນ SQL Injection, ການເຂົ້າລະຫັດຂໍ້ມູນຜ່ານ HTTPS, ການເຂົ້າລະບົບຢ່າງປອດໄພ (authentication & authorization) (Esposito et al., 2021 & Mohammad et al., 2022) ແລະ ເກັບລະຫັດຜ່ານດ້ວຍ b-crypt, s-crypt (Provos, 2023) .

(OJS) ແມ່ນເຄື່ອງມືການພິມເຜີຍແຜ່ໃນຍຸກສະໄໝໃໝ່ ສຳລັບຜູ້ຂຽນ, ຜູ້ທົບທວນ ແລະ ບັນນາທິການໄດ້ຮັບຄວາມນິຍົມຫຼາຍໃນຊ່ວງເວລາທີ່ຜ່ານມາ ຍ້ອນວ່າຊອບແວນີ້ສາມາດຕິດຕັ້ງ ແລະ ນຳໃຊ້ໄດ້ໂດຍບໍ່ເສຍຄ່າບໍລິການ, ສຳລັບການນຳໃຊ້ ແລະ ການເຜີຍແຜ່ວາລະສານທາງອອນລາຍ. ໃນຂະນະທີ່ລະບົບ ແລະ ເຄື່ອງມືນີ້ສາມາດຊ່ວຍໃຫ້ຜູ້ໃຊ້ສາມາດກວດສອບ, ສະໜັບສະໜູນ, ຄວບຄຸມ, ຕິດຕາມ ສິ່ງພິມຕ່າງໆ, ແລະ ອື່ນໆ, ເຊິ່ງມີຫຼາຍໆອົງກອນໄດ້ນຳມາໃຊ້ຢ່າງກວ້າງຂວາງ ແຕ່ຍັງຕ້ອງມີຄວາມກັງວົນຫຼາຍກ່ຽວກັບຄວາມປອດໄພຂອງຂໍ້ມູນ ເນື່ອງຈາກເປັນການບໍລິການຟຼີສຳລັບການນຳໃຊ້ ແຕ່ຍັງບໍ່ທັນມີບໍລິການດ້ານຄວາມປອດໄພຂອງລະບົບນີ້ (Em, 2024 & Tabatadze, 2024).

ປະຈຸບັນ ເວັບໄຊ້ວາລະສານ ມະຫາວິທະຍາໄລ ສຸພານຸວົງ ແມ່ນຢູ່ໃນໂໝດບໍ່ມີຄວາມປອດໄພ ເຊິ່ງມີຄວາມສ່ຽງສູງທີ່ຈະເຮັດໃຫ້ເວັບໄຊ້ຖືກແຮັກເກີລັກລອບເອົາຂໍ້ມູນ ຫຼື ໂຈມຕີເວັບໄຊ້ໂດຍການປ່ຽນແປງ ຫຼື ແກ້ໄຂຂໍ້ມູນ ບໍ່ໃຫ້ສາມາດໃຊ້ງານໄດ້, ເຊິ່ງແຕ່ລະຄັ້ງນັກຄົ້ນຄວ້າວິທະຍາສາດ ຫຼື ຜູ້ສົນໃຈທົ່ວໄປ ທີ່ຈະເຂົ້າໄປເບິ່ງເວັບໄຊ້ແມ່ນຈະຖືກບັງຄັບໃຫ້ເຂົ້າເບິ່ງເວັບໄຊ້ໃນໂໝດທີ່ບໍ່ປອດໄພ ອາດເຮັດເກີດຄວາມເສຍຫາຍທາງດ້ານຂໍ້ມູນສ່ວນຕົວ ແລະ ນຳໄປສູ່ການຖືກໂຈມຕີທາງທຸລະກຳການເງິນໄດ້. ສາເຫດແມ່ນເນື່ອງຈາກປະຈຸບັນ ມະຫາວິທະຍາໄລ ສຸພານຸວົງ ໄດ້ນຳໃຊ້ Framework (OJS) ມາພັດທະນາ ຈຶ່ງເຮັດໃຫ້ມີຄວາມປອດໄພຕ່ຳ, ເພາະຕ້ອງໄດ້ຕິດຕັ້ງ Plugin ເພີ່ມຫຼາຍຢ່າງ ຈຶ່ງເຮັດໃຫ້ມີຊ່ອງທາງໃນການຖືກໂຈມຕີທາງ Cyber ຈາກຜູ້ບໍ່ຫວັງດີ.

ສະນັ້ນ, ການຄົ້ນຄວ້າວິໄຈຄັ້ງນີ້ແມ່ນວິໄຈກ່ຽວກັບຄວາມປອດໄພເວັບໄຊ້ວາລະສານ ມະຫາວິທະຍາໄລ ສຸພານຸວົງ ໂດຍມີຈຸດປະສົງໃນການທົດລອງຄົ້ນຫາຈຸດບົກຜ່ອງ ແລະ ຊ່ອງໂຫວ່ຂອງເວັບໄຊ

2. ອຸປະກອນ ແລະ ວິທີການ

ໃນບົດວິໄຈຄັ້ງນີ້ຜູ້ຄົ້ນຄວ້າຈະໄດ້ເຮັດຕິດຕັ້ງລະບົບປະຕິບັດການ Kali Linux ແລະ ຊອບແວຂັ້ນສູງ ເພື່ອກວດຄົ້ນຫາຈຸດບົກຜ່ອງ ແລະ ຊ່ອງໂຫວ່ຂອງເວັບໄຊ.

2.1 ເຄື່ອງມືທີ່ໃຊ້ໃນການຄົ້ນຄວ້າ

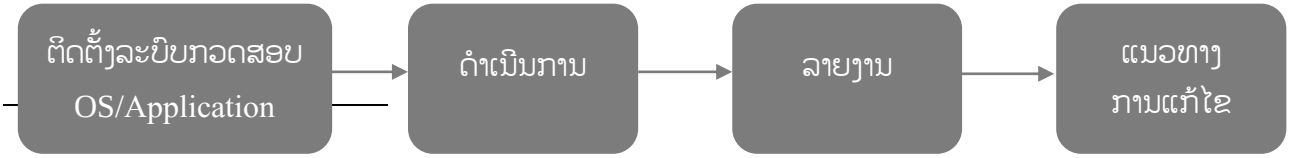
ເຄື່ອງມືຫຼັກທີ່ນຳໃຊ້ໃນການຄົ້ນຄວ້າວິໄຈຄັ້ງນີ້ປະກອບມີ: ລະບົບປະຕິບັດການ Kali Linux, Application, Database ແລະ Command Line.

ຕາຕາລາງທີ 1. ເຄື່ອງມືທີ່ໃຊ້ໃນການເຮັດການຄົ້ນຄວ້າວິໄຈ

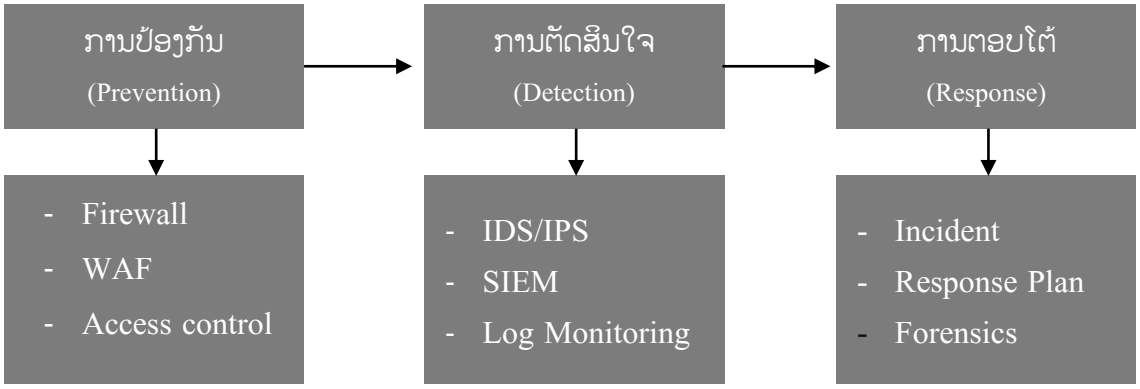
ລາຍການ	ປະເພດ	ໜ້າທີ່
Kali Linux	Operating System	Web Security and Detect
Nmap, Wireshark, Metasploit, Burp Suit, Nessus	Application	Network, Detect, Analyze Vulnerability Scanning
Visual Studio Code	Application	Text Editor
WinSCP	Application	File Upload
AppServ 9.3.0	Database	Database Design
Command Line	Command	Vulnerability Scanning

ເວັບໄຊ້ຕົວຢ່າງສຳລັບເຮັດການວິໄຈ ແມ່ນໄດ້ກຳນົດເອົາເວັບໄຊ້ວາລະສານ ມະຫາວິທະຍາໄລ ສຸພານຸວົງ ມາວິໄຈ ເຊິ່ງຈະໄດ້ເຮັດການທົດລອງເອົາຊື່ໂດເມນ[1] ມາກວດສອບ, ກວດຄົ້ນຫາຈຸດບົກຜ່ອງ ແລະ ຕິດຕາມລະດັບຄວາມປອດໄພເວັບໄຊ້ ແລ້ວນຳເອົາຜົນທີ່ໄດ້ມາ ລາຍງານຕໍ່ຄະນະຮັບຜິດຊອບ ເພື່ອເຮັດການແກ້ໄຂບັນຫາດັ່ງກ່າວ ແລະ ປັບປຸງເວັບໄຊ້ໃຫ້ມີຄວາມປອດໄພ ດ້ວຍການນຳໃຊ້ເຕັກໂນໂລຊີດ້ານຄວາມປອດໄພເຂົ້າມາຊ່ວຍ.

2.2 ວິທີການທົດລອງ



ຮູບພາບທີ 1: Security Audit Methods



ຮູບພາບທີ 2: ແນວທາງແກ້ໄຂ Security Monitoring Diagram

2.3 ການວິເຄາະຂໍ້ມູນ

ຂັ້ນຕອນການວິເຄາະຂໍ້ມູນແມ່ນເອົາຜົນການນຳໃຊ້ເຕັກນິກໃນການກວດສອບໂດເມນ ໂດຍສະເລ່ຍຄວາມໄວໃນການກວດສອບ ແລະ ເອົາຜົນໄດ້ຮັບທີ່ແຕກຕ່າງກັນ ເຊິ່ງໄດ້ນຳໃຊ້ເຕັກນິກທັງໝົດ 7 ຂັ້ນຕອນ ສາມາດສະຫຼຸບຂໍ້ມູນດັ່ງນີ້:

ຕາຕາລາງທີ 2. ການວິເຄາະຜົນການນຳໃຊ້ເຕັກນິກທີ່ແຕກຕ່າງກັນ

ຂັ້ນຕອນ	ເຕັກນິກ	ໃຊ້ເວລາ(ວິນາທີ)	ຜົນໄດ້ຮັບ
1	Ping Scan	0.14s	ຢືນຢັນເຊີບເວີໃຊ້ງານປົກກະຕິ
2	DNS Resolution	0.17s	ໄດ້ IP 27.254.146.20
3	SYN Stealth Scan	5.07s	ພົບ 13 ພອດເປີດ
4	Service Scan	162.31s	ລະບຸເວີຊັນບໍລິການ
5	OS Detection	~3-5s ຕໍ່ຄັ້ງ	ລະບຸ OS (ບໍ່ສະແດງ)
6	Traceroute	3.03s	ເສັ້ນທາງເຄືອຂ່າຍປົກະຕິ
7	NSE Scripts	5.03s	ພົບເຫັນຊ່ອງໂຫວ່ໂຈມຕີ

3. ຜົນໄດ້ຮັບ

ຈາກການກວດສອບຄວາມປອດໄພຂອງເວັບໄຊ້ວາລະສານດ້ວຍເຄື່ອງມື ແລະ ເທັກນິກການທົດສອບຊ່ອງໂຫວ່ ແລະ ຈຸດອ່ອນທົ່ວໄປ ໄດ້ພົບຈຸດບົກຜ່ອງດ້ານຄວາມປອດໄພທີ່ສຳຄັນດັ່ງນີ້:

ການໃຊ້ງານ SSL/TLS ທີ່ບໍ່ປອດໄພ, ເວັບເຊີເວີ (Web Server) ຍັງໃຊ້ SSL/TLS ແບບເກົ່າທີ່ມີຊ່ອງໂຫວ່ຄວາມປອດໄພທີ່ບໍ່ໄດ້ອັບເດດຈາກ TLS 1.2 ເປັນ TLS 1.3 ຢ່າງເຕັມທີ່. ເຮັດໃຫ້ຂໍ້ມູນທີ່ໂອນລະຫວ່າງຜູ້ໃຊ້ ແລະ ເຊີເວີມີຄວາມສ່ຽງຕໍ່ການຖືກດັກຈັບ (Eavesdropping) ແລະ ການໂຈມຕີ "Man-in-the-Middle". ການຈັດການໃບຢັ້ງຢືນດິຈິຕອນບໍ່ຖືກຕ້ອງ ເຊິ່ງກວດສອບພົບ Key Certificate ແລະ Security Certificate ບາງສ່ວນໝົດອາຍຸແລ້ວ ເຮັດໃຫ້ການເຊື່ອມຕໍ່ທີ່ (HTTPS) ສູນເສຍຄວາມໜ້າເຊື່ອຖື, ຕົວບຣາວເຊີຈະແຈ້ງເຕືອນຜູ້ໃຊ້ວ່າເຊື່ອມຕໍ່ "ບໍ່ປອດໄພ", ຫຼຸດຄວາມໜ້າເຊື່ອຖືຂອງເວັບໄຊ້ວາລະສານ ມະຫາວິທະຍາໄລ ສຸພານຸວົງ

ການຕັ້ງຄ່າເວັບເຊີເວີທີ່ມີຊ່ອງໂຫວ່ການນຳໃຊ້ Server Version ທີ່ບໍ່ ມີຄຸນລັກສະນະ Secure ແລະ HttpOnly ສຳລັບ Cookies, ເຮັດໃຫ້ Cookies ມີຄວາມສ່ຽງຕໍ່ການຖືກເກັບຂໍ້ມູນໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ (Cross-site Scripting - XSS), ຂໍ້ມູນການເຂົ້າລະບົບ ຫຼື session ຂອງຜູ້ໃຊ້ອາດຖືກລັກລອບນຳໄປສູ່ການລັກເຂົ້າໃຊ້ບັນຊີໂດຍບຸກຄົນອື່ນ.

ການເປີດ Port ເຊີເວີທີ່ມີຄວາມສ່ຽງ, ຜົນການສະແກນ Port ພົບວ່າມີ Port ທັງໝົດ 13 Port ທີ່ເປີດໃຊ້ຢູ່ໃນນັ້ນ, 6 Port ຈັດຢູ່ໃນກຸ່ມທີ່ມີຄວາມສ່ຽງສູງ ເນື່ອງຈາກເປັນບໍລິການທີ່ເກົ່າ ຫຼື ມີຂໍ້ບົກຜ່ອງດ້ານຄວາມປອດໄພ ເຊິ່ງຮູ້ຈັກກັນດີ (ເຊັ່ນ: Telnet, FTP, ບໍລິການທີ່ມີຄວາມປອດໄພຕ່ຳ).

ຈຸດອ່ອນຈາກ Source Code ແລະ ການພັດທະນາເວັບໄຊ ເຊິ່ງການວິເຄາະ Source Code ແລະ ເອີ້ນໃຊ້ຟັງຊັນພົບວ່າມີຈຸດອ່ອນ ເຊັ່ນ: ການບໍ່ກວດສອບຂໍ້ມູນນຳເຂົ້າ (Input Validation), ຄວາມສ່ຽງຕໍ່ SQL Injection, ແລະ Cross-Site Scripting (XSS) ອາດເປີດຊ່ອງທາງໃຫ້ແຮັກເກີ ຫຼື ຜູ້ບໍ່ຫວັງດີໃສ່ຄຳສັ່ງອັນຕະລາຍ ຫຼື ສະຄຣິບເພື່ອເຂົ້າເຖິງຖານຂໍ້ມູນ ແລະ ຄວບຄຸມເວັບໄຊ້ (ຕາຕາລາງທີ 3).

4. ວິພາກ

ຜົນການວິໄຈສະແດງໃຫ້ເຫັນເຖິງ ສະພາບຄວາມປອດໄພໃນລະດັບຕ່ຳຂອງເວັບໄຊ້ວາລະສານ. ສາເຫດຫຼັກແມ່ນເວັບໄຊ້ມີຈຸດບົກຜ່ອງໃນຂັ້ນຕອນການຕິດຕັ້ງ Framework OJS (Paulina, 2023) ທີ່ກຳນົດການຕັ້ງຄ່າໃຫ້ເປັນ Default ໃນການກຳນົດສິດເຂົ້າເຖິງຂໍ້ມູນໃນເບື້ອງຕົ້ນ ຈຶ່ງເຮັດໃຫ້ໂຄງສ້າງຂອງເວັບໄຊ້ມີຊ່ອງຫວ່າງໃນການເຂົ້າ

ເຖິງລະບົບ, ສ່ວນຊ່ອງໂຫວ່ແມ່ນເກີດຈາກຂາດການບຳລຸງຮັກສາ ແລະ ອັບເດດລະບົບຢ່າງຕໍ່ເນື່ອງໂດຍສະເພາະແມ່ນການ Update Plug in ຕ່າງໆ ເນື່ອງຈາກ Framework OJS ແມ່ນສາມາດຕິດຕັ້ງ ແລະ ໃຊ້ງານຟຼີ ແຕ່ຍັງມີຄວາມປອດໄພຕ່ຳ ຖ້າຫາກຂາດການອັບເດດລະບົບ.

ໃບຢັ້ງຢືນດ້ານຄວາມປອດໄພໝົດອາຍຸ Security Certificate ແລະ ບໍ່ຍົກລະດັບມາດຕະຖານຄວາມປອດໄພຂອງ SSL/TLS ຢູ່ໃນເຊີເວີ (Server) (Adha, & Muhammad, 2023). ທີ່ເປັນຕົວປ້ອງກັນຂໍ້ມູນຂອງເວັບໄຊ ສະແດງໃຫ້ເຫັນເຖິງການຂາດກົນໄກການຕິດຕາມຄວາມປອດໄພຂອງລະບົບ. ຈຶ່ງເຮັດໃຫ້ຂາດຄວາມໜ້າເຊື່ອຖືຂອງຜູ້ໃຊ້ລະບົບ ແລະ ສະຖາບັນໃນທັນທີ.

ການເປີດ Port ຫຼາຍ Port ທີ່ບໍ່ຈຳເປັນໃນເບື້ອງຂອງ (Server) ຈຶ່ງເຮັດໃຫ້ມີຄວາມສ່ຽງສູງ ເນື່ອງຈາກຫລັກດັ່ງກ່າວເປັນເຕັກໂນໂລຊີແບບເກົ່າ ຄວນເປີດພຽງ Port ສິ່ງທີ່ຈຳເປັນ (Principle of Least Privilege) ເຊິ່ງເຊີເວີ (Server) ຖືກເປີດບໍລິການຫຼາຍກວ່າຄວາມຈຳເປັນ ອາດເພີ່ມພື້ນທີ່ໂຈມຕີ (Attack Surface) ໃຫ້ແກ່ຜູ້ບໍ່ຫວັງດີ ຫຼື ແຮັກເກີ.

ຈຸດອ່ອນຂອງລະບົບໃນ Framework OJS ຍັງມີ Source Code ທີ່ເປັນບັນຫາທີ່ມີຄວາມສັບຊ້ອນ ແລະ ຕ້ອງໃຊ້ເວລາໃນການແກ້ໄຂ ເຊິ່ງສະທ້ອນໃຫ້ເຫັນວ່າ ຂະບວນການພັດທະນາເວັບໄຊ (SDLC) ອາດຈະຂາດຂັ້ນຕອນການທົດສອບຄວາມປອດໄພ (Security Testing) ເຊັ່ນ: Static Application Security Testing (SAST) ຫຼື Dynamic Application Security Testing (DAST) (Arromdoni et al., 2024)

ຈຸດດີຂອງ Framework OJS ຖ້າຫາກຕິດຕັ້ງຖືກວິທີ, ເອົາໃສ່ໃນການບຳລຸງຮັກສາ ແລະ ອັບເດດລະບົບຢູ່ເປັນປະຈຳ ຈະເຮັດໃຫ້ລະບົບມີປະສິດທິພາບ ແລະ ມີຄວາມປອດໄພສູງ. ເນື່ອງຈາກເປັນລະບົບທີ່ນິຍົມໃຊ້ຫຼາຍໃນວຽກງານກ່ຽວກັບວາລະສານຂອງສະຖາບັນ ເຊິ່ງປະຈຸບັນແມ່ນນິຍົມໃຊ້ເຕັກໂນໂລຊີຂັ້ນສູງ ແລະ AI ເຂົ້າມາຊ່ວຍບໍລິຫານ ແລະ ຄຸ້ມຄອງລະບົບ (Tabatadze, 2024).

ໂດຍລວມແລ້ວ ເວັບໄຊ້ວາລະສານໃນປະຈຸບັນແມ່ນມີຄວາມສ່ຽງສູງຕໍ່ການໂຈມຕີຫຼາຍຮູບແບບ ເຊັ່ນ: ການເຂົ້າເຖິງລະບົບຖານຂໍ້ມູນ, ການລັກຂໍ້ມູນສ່ວນຕົວຂອງນັກສຶກສາ, ອາຈານ ແລະ ນັກຄົ້ນຄວ້າທົ່ວໄປ ແລະ ອາດເປັນຊ່ອງທາງໃນການໂຈມຕີຕໍ່ລະບົບອື່ນໆ ພາຍໃນມະຫາວິທະຍາໄລ ສຸພານະວົງ (ຮູບພາບທີ 3).

5. ສະຫຼຸບ

ການວິໄຈຄັ້ງນີ້ໄດ້ເປີດເຜີຍ ຈຸດອ່ອນດ້ານຄວາມປອດໄພທີ່ເປັນອັນຕະລາຍຮ້າຍແຮງ ໃນດ້ານປະສິດທິພາບຄວາມປອດໄພຕ່ຳ ຢູ່ໃນເວັບໄຊ້ວາລະສານ ມະຫາວິທະຍາໄລ ສຸພານຸວົງ, ຕັ້ງແຕ່ບັນຫາພື້ນຖານດ້ານໂຄງລ່າງ ເຊັ່ນ: ໃບຢັ້ງຢືນ ແລະ ພັດທະນາການລະບົບ, ໄປຈົນເຖິງບັນຫາທີ່ລະອຽດອ່ອນກວ່າເຊັ່ນ: ການຕັ້ງຄ່າເຊີບເວີ ແລະ ຊ່ອງໂຫວ່ຈາກການພັດທະນາໂປຣແກຣມ. ສະພາບເຫຼົ່ານີ້ເຮັດໃຫ້ເວັບໄຊ້ມີຄວາມສ່ຽງສູງ ແລະ ຈຳເປັນຕ້ອງໄດ້ມີການແກ້ໄຂຢ່າງຮີບດ່ວນ ແລະ ເປັນລະບົບ.

ປັບປຸງ SSL/TLS ແລະ ໃບຢັ້ງຢືນ ເພື່ອຍົກລະດັບການພັດທະນາການເຂົ້າລະຫັດເປັນ TLS 1.3, ຕິດຕັ້ງ ແລະ ກວດສອບໃບຢັ້ງຢືນ (Key Certificate ແລະ Security Certificate) ໃຫມ່ທີ່ຍັງບໍ່ໝົດອາຍຸ ແລະ ປິດ Port ທີ່ບໍ່ຈຳເປັນ ໂດຍເຮັດການສຳຫຼວດ ແລະ ປິດທັນທີ Port ທັງ 6 Port ທີ່ມີຄວາມສ່ຽງສູງ ແລະ ບໍ່ມີການໃຊ້ງານໃນປັດຈຸບັນ, ຕັ້ງຄ່າເຊີເວີໃຫ້ມີ Secure ແລະ HttpOnly flags ສຳລັບ cookies.

ສ້າງຊັ້ນການປ້ອງກັນເພີ່ມເຕີມ ໂດຍການຕິດຕັ້ງ Web Application Firewall (WAF) ເພື່ອເປັນກຳແພງດ່ານການໂຈມຕີແບບເທັກນິກສູງ ເຊັ່ນ: SQL Injection, XSS, ມີການກວດສອບ ແລະ ປັບປຸງ Source Code ໃນຈຸດທີ່ມີຊ່ອງໂຫວ່, ໂດຍສະເພາະດ້ານ Input Validation ແລະ ການເຂົ້າລະຫັດຂໍ້ມູນ, ສຳຮອງຂໍ້ມູນແບບປົກກະຕິ ໂດຍຕັ້ງເວລາການສຳຮອງຂໍ້ມູນອັດຕະໂນມັດ ແລະ ທົດສອບການກູ້ຂໍ້ມູນ, ສ້າງຕາຕະລາງການຕິດຕາມ ແລະ ປະເມີນຄວາມປອດໄພຢ່າງເປັນປົກກະຕິ (ເຊັ່ນ: ປະຈຳເດືອນ ຫຼື ທຸກໆ 3 ເດືອນ) ແລະ ຈັດການຝຶກອົບຮົມດ້ານຄວາມປອດໄພໃຫ້ແກ່ທີມງານພັດທະນາ ແລະ ບໍລິຫານລະບົບ.

6. ຂໍ້ຂັດແຍ່ງ

ຂ້າພະເຈົ້າໃນນາມຜູ້ຄົ້ນຄວ້າວິທະຍາສາດ ຂໍປະຕິຍານຕົນວ່າ ຂໍ້ມູນທັງໝົດທີ່ມີໃນບົດຄວາມວິຊາການດັ່ງກ່າວນີ້ ແມ່ນບໍ່ມີຂໍ້ຂັດແຍ່ງທາງຜົນປະໂຫຍດກັບພາກສ່ວນໃດ ແລະ ບໍ່ໄດ້ເອື້ອປະໂຫຍດໃຫ້ກັບພາກສ່ວນໃດພາກສ່ວນໜຶ່ງ, ກໍລະນີມີການລະເມີດ ໃນຮູບການໃດໜຶ່ງ ຂ້າພະເຈົ້າມີຄວາມຍິນດີ ທີ່ຈະຮັບຜິດຊອບແຕ່ພຽງຜູ້ດຽວ.

7. ເອກະສານອ້າງອີງ

Adha, M., KWA, Z. D., & Muhammad, A. H. (2023). Website security test at the university of mataram using vulnerability assessment. *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, *8*(2), 647-655

Aklesh Kumar, B. (2022). Mobile-first usability guideline for responsive e-commerce websites. *International Journal of Web Portals (IJWP)*, *14*(1), 1–12.

Arromdoni, B. U. H., Kusuma, M., & Sugiantoro, B. (2024). Web application vulnerability analysis using the owasp method (case study: ojs csfd uin sunan kalijaga yogyakarta). *Engineering Headway*, *6*, 211-218

Em, S. (2024). Management of Scientific Journals Using Open Journal System (OJS). *CJESS Online Library*, 1-21.

Esposito, C., Ficco, M., & Gupta, B. B. (2021). Blockchain-based authentication and authorization for smart city applications. *Information Processing & Management*, *58*(2), 102468. https://doi.org/10.1016/j.ipm.2020.102468

Ghelani, D., & Hua, T. K. (2022). Conceptual framework of Web 3.0 and impact on marketing, artificial

intelligence, and blockchain. *International Journal of Information and Communication Sciences*, *7*(1), 10.

Guttikonda, B. S., Sachan, R. C., & Veeramachaneni, V. (2025). LLM-GA: A hybrid framework to build dynamic websites for optimizing web performance. *International Journal of Information Technology*, 1–7. https://doi.org/10.1007/s41870-025-02089-1

Lane, J., Barker, T., Lewis, J. R., & Moscovitz, M. (2017). *Foundation website creation with HTML5, CSS3, and JavaScript*. Apress.

Lei, X., Li, S., & Ning, H. (2023). Concept, connotation, technology and development status of Web 3.0. *Chinese Journal of Engineering*, *45*(5), 774–786.

Mohammad, A., Al-Refai, H., & Alawneh, A. A. (2022). User authentication and authorization framework in IoT protocols. *Computers*, *11*(10), 147. https://doi.org/10.3390/ computers11100147

Paulina, K. (2023). PENETRATION TESTING OPEN JOURNAL SYSTEMS (OJS) PADA APLIKASI WEB JURNAL JI-TECH. *Jurnal Teknologi Informasi, Manajemen dan Bisnis Digital*, 37-45.

Provos, N. (2023). Bcrypt at 25: A retrospective on password security.

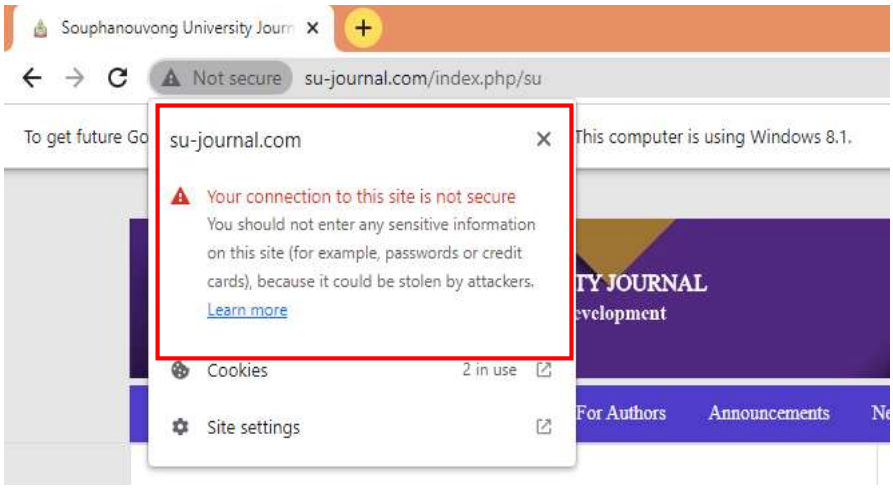
Sudianto, A., & Sugiantara, J. (2020). Website as foundation information media under the auspices of Nahdlatul Wathan. *Journal of Physics: Conference Series*, *1539*(1), 012001. IOP Publishing. https://doi.org/10.1088/1742-6596/1539/1/012001

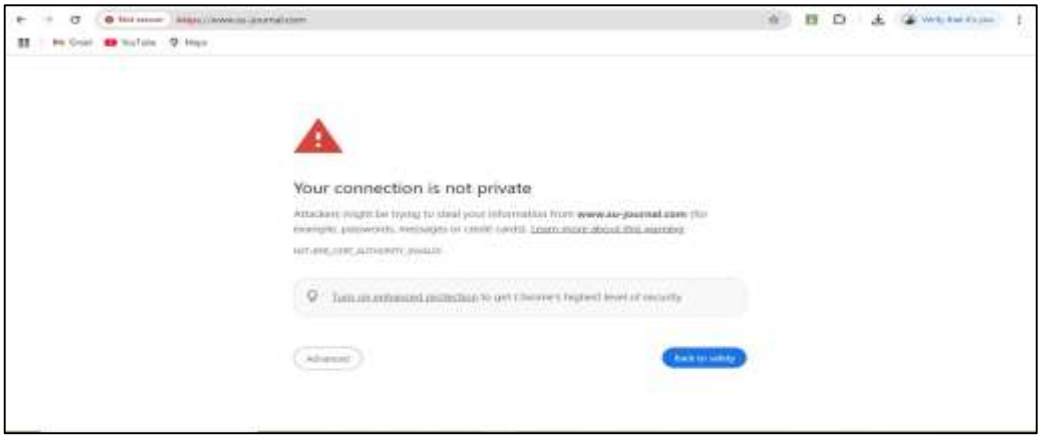
Truong, V., Nguyen, L., Pham, P. & Vo, B. (2025). HTMLDownloader: An open-source tool for dynamic web scraping and archiving using WebView2. *SoftwareX. 32.* 10.1016/j.softx.2025.102373.

Tabatadze, B. (2024). Technological Aspects of Open Journal Systems (OJS). *Journal of Technical Science and Technologies*, *8*(1), 23-29.

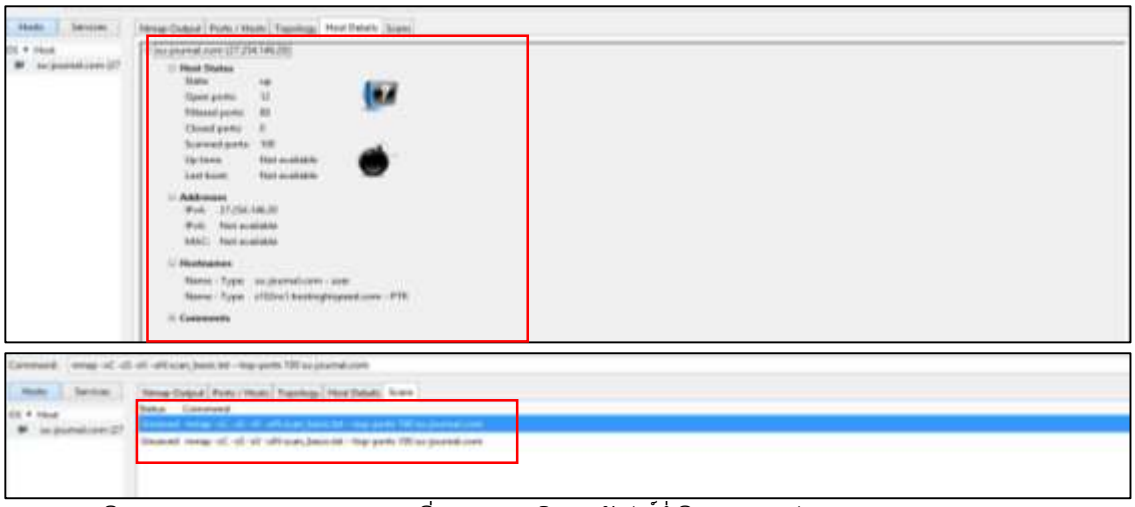
Tabatadze, B. (2024). Prospects of Using AI Technologies in Open Journal Systems (OJS). *Journal of Technical Science and Technologies*, *8*(2), 68-74.

ຮູບພາບທີ 3: ການແຈ້ງເຕືອນທີ່ບົ່ງບອກວ່າເວັບໄຊນີ້ບໍ່ປອດໄພກັບຜູ້ໃຊ້





ຮູບພາບທີ 5 ໜ້າເວັບໄຊ້ວາລະສານ ມະຫາວິທະຍາໄລ ສຸພານຸວົງ ຢູ່ໃນໂໝດບໍ່ປອດໄພ



ຮູບພາບທີ 6 ກວດສອບ Port, Host ແລະ ຊື່ Domain ພົບວ່າເວັບໄຊ້ບໍ່ມີຄວາມປອດໄພ (Unsaved)

```
Scanning www.su-journal.com (27.254.146.20) [1000 ports]
Discovered open port 80/tcp on 27.254.146.20
Discovered open port 995/tcp on 27.254.146.20
Discovered open port 587/tcp on 27.254.146.20
Discovered open port 993/tcp on 27.254.146.20
Discovered open port 443/tcp on 27.254.146.20
Discovered open port 110/tcp on 27.254.146.20
Discovered open port 21/tcp on 27.254.146.20
Discovered open port 25/tcp on 27.254.146.20
Discovered open port 143/tcp on 27.254.146.20
Discovered open port 53/tcp on 27.254.146.20
Discovered open port 8083/tcp on 27.254.146.20
Discovered open port 8443/tcp on 27.254.146.20
Discovered open port 465/tcp on 27.254.146.20
Completed SYN Stealth Scan at 13:28, 5.07s elapsed (1000 total ports)
Initiating Service scan at 13:28
Scanning 13 services on www.su-journal.com (27.254.146.20)
Completed Service scan at 13:30, 162.31s elapsed (13 services on 1 host)
Initiating OS detection (try #1) against www.su-journal.com (27.254.146.20)
Retrying OS detection (try #2) against www.su-journal.com (27.254.146.20)
```

```
Starting Nmap 7.70 ( https://nmap.org ) at 2025-09-30 10:14 SE Asia Standard Time
Nmap scan report for su-journal.com (27.254.146.20)
Host is up (0.47s latency).
rDNS record for 27.254.146.20: s102ns1.hostinghispeed.com

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 4096) - A
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (dh 4096) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 4096) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 4096) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 4096) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       Key exchange (ecdh_x25519) of lower strength than certificate key
|_  least strength: A
```

TLS 1.3 ສ່ວນ Key exchange ແລະ Security Certificate ມີຄວາມປອດໄພຕ່ຳ ແລະ ຫມົດອາຍຸ

ຕາຕາລາງທີ 3. ຜົນການກວດພົບ Port ທີ່ເປີດຢູ່ໃນໂໝດທີ່ມີຄວາມສ່ຽງສູງ

ເນື້ອໃນ	ໜ້າທີ່	ຄຳແນະນຳ
Port 80	ເຊື່ອມຕໍ່ລະຫວ່າງ ເວັບບຣາວເຊີ ແລະ ເວັບເຊີເວີ	
Port 995	ຮັບສົ່ງອີເມວ ຈາກເມວເຊີເວີ	
Port 587	ການສົ່ງອີເມວແບບປອດໄພ	
Port 993	ການຈັດການອີເມວໃຫ້ປອດໄພດ້ວຍຜ່ານ SSL/TLS	
Port 443	ການເຊື່ອມຕໍ່ເວັບໄຊແບບປອດໄພ ຜ່ານ SSL/TLS	
Port 110	ການດຶງອີເມວຈາກ ເມວເຊີເວີມາຫາລູກຄ່າຍ	
Port 21	ການຮັບ-ສົ່ງຟາຍລະຫວ່າງລູກຂ່າຍ ແລະ ເຊີເວີ ແບບບໍ່ເຂົ້າລະຫັດ	ຖ້າໃຊ້ຄວນມີ TLS 1.3
Port 25	ການສົ່ງເມວຈາກເມວເຊີເວີ ຫາ ເມວເຊີເວີ	ຄວນປິດ
Port 143	ການຈັດການອີເມວ ຢູ່ໃນເມວເຊີເວີ	ຄວນປິດ
Port 53	ການບໍລິການ dns server	ຄວນປິດ
Port 8083	ໃຊ້ສະເພາະ http	ຄວນປິດ
Port 8443	ການເຊື່ອມຕໍ່ຄວາມປອດໄພ	ຖ້າໃຊ້ຄວນມີ TLS 1.3
Port 465	ການສົ່ງເມວຈາກລູກຂ່າຍ ຫາ ເຊີເວີ	