โรงพยาบาลน้ำเกลี้ยงได้จัดทำ Penetration Testing: การทดสอบการเจาะระบบเพื่อให้ทราบถึงจุดอ่อนหรือช่องโหว่ของระบบงาน

ดำเนินการทดสอบความมั่นคงปลอดภัยระบบสารสนเทศ (Penetration Testing) ของโรงพยาบาล เพื่อประเมินระดับความเสี่ยงเบื้องต้นของระบบ Web Server และบริการเครือข่ายที่เกี่ยวข้อง

การทดสอบดำเนินการภายใต้ขอบเขตที่ได้รับอนุญาต และมุ่งเน้นการประเมินเชิงป้องกัน (Preventive Assessment) โดยไม่มีการดำเนินการโจมตีเชิงทำลายระบบ

เครื่องมือที่ใช้ (Tools & Methodology)

- **Burp Suite CE**
  Burp Suite CE เป็นเครื่องมือ Web Security Testing
  ใช้วิเคราะห์ทราฟฟิกระหว่าง Browser ↔ Web Application เพื่อหาช่องโหว่ เช่น
  - SQL Injection
  - XSS
  - IDOR
  - Authentication / Session issue

ผลการทดสอบด้านความปลอดภัยระบบสารสนเทศ

(Penetration Testing Report)

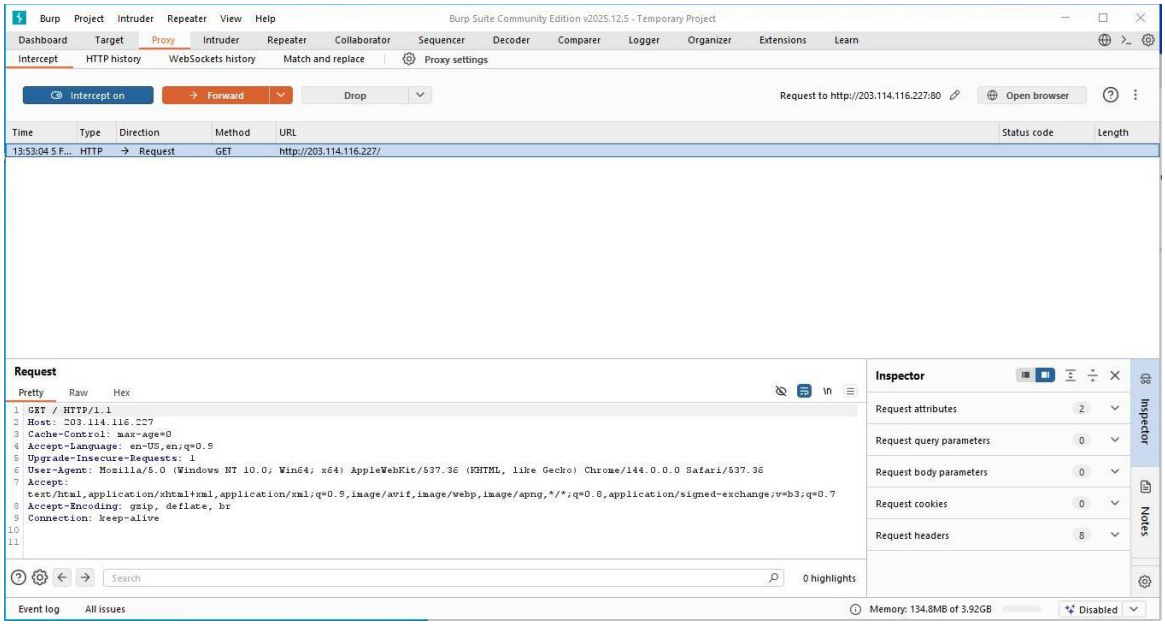
ชื่อระบบ: เว็บไซต์โรงพยาบาลน้ำเกลี้ยง

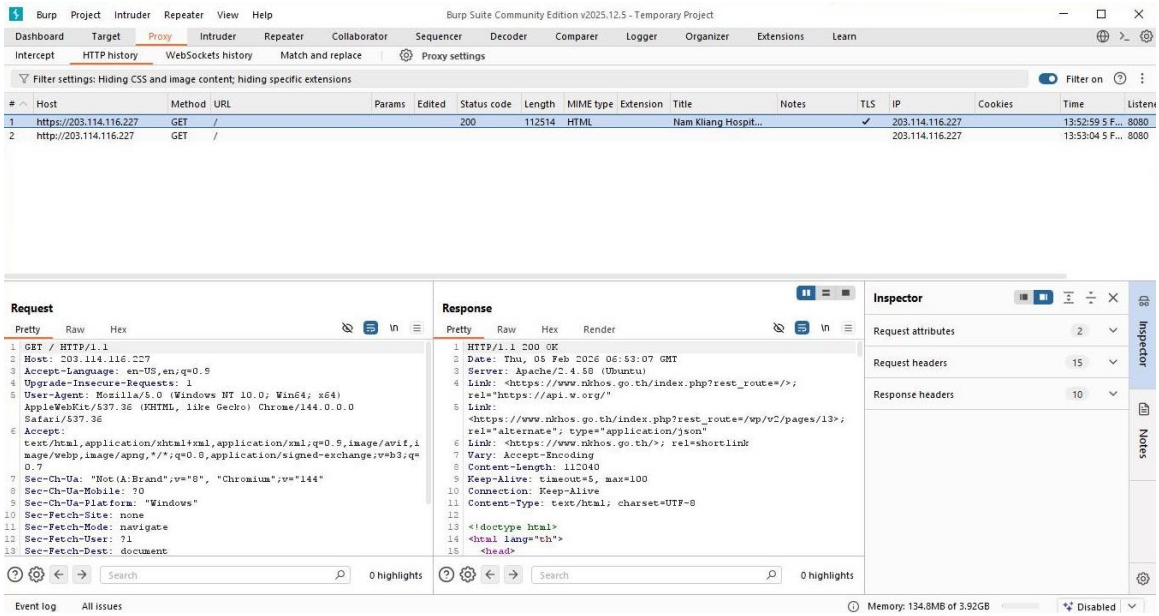
URL: https://www.nkhos.go.th

ประเภทระบบ: Web Application (WordPress)

วิธีการทดสอบ: ตรวจสอบ HTTP Response Header และ Source Code

วันที่ทดสอบ: กุมภาพันธ์ 2569





การทดสอบเว็บไซต์ พบว่าระบบมีการเปิดเผยข้อมูลเวอร์ชันของซอฟต์แวร์ผ่าน HTTP Response Header และใน Source Code ของหน้าเว็บ รวมถึงไม่พบการตั้งค่า Security Header ที่สำคัญหลายรายการ ซึ่งอาจเพิ่มความเสี่ยงต่อการถูกโจมตี เช่น Clickjacking, Cross-Site Scripting (XSS) และการโจมตีแบบเจาะจงเวอร์ชันซอฟต์แวร์

ระดับความเสี่ยงโดยรวมของระบบ: ปานกลาง (Medium)

รายละเอียดช่องโหว่

Information Disclosure via Server Header

ระดับความรุนแรง: Medium

ประเภทช่องโหว่: Information Disclosure / Security Misconfiguration

มาตรฐานอ้างอิง:

- OWASP Top 10:2021 – A05: Security Misconfiguration
- CWE-200: Information Exposure

รายละเอียดช่องโหว่

จากการตรวจสอบ HTTP Response Header พบว่าระบบมีการเปิดเผยข้อมูลเวอร์ชันของ Web Server ดังนี้

- Server: Apache/2.4.58 (Ubuntu)

ข้อมูลดังกล่าวสามารถถูกใช้เพื่อ:

- ระบุชนิดของเซิร์ฟเวอร์
- ค้นหาช่องโหว่ที่ตรงกับเวอร์ชันดังกล่าว
- ใช้ในการโจมตีแบบเจาะจงเป้าหมาย

หลักฐาน (Evidence)

ตัวอย่าง HTTP Response:

HTTP/1.1 200 OK
Server: Apache/2.4.58 (Ubuntu)

ผลกระทบ (Impact)

- เพิ่มโอกาสการโจมตีแบบ Targeted Attack
- ช่วยให้ผู้โจมตีค้นหา Exploit ที่ตรงกับเวอร์ชันระบบได้

ความเป็นไปได้ในการโจมตี

ปานกลาง (ตรวจสอบได้จากภายนอกโดยไม่ต้องยืนยันตัวตน)

WordPress Version Disclosure

ระดับความรุนแรง: Medium

ประเภทช่องโหว่: Information Disclosure

มาตรฐานอ้างอิง:

- OWASP A05: Security Misconfiguration
- CWE-200

รายละเอียดช่องโหว่

พบการเปิดเผยเวอร์ชันของ WordPress ภายใน Source Code ของหน้าเว็บ:

ver=6.5.5

ผลกระทบ

ผู้โจมตีสามารถค้นหาช่องโหว่ที่ตรงกับเวอร์ชัน WordPress

เพิ่มความเสี่ยงต่อการโจมตีผ่าน Plugin หรือ Theme

Missing Security Headers

ระดับความรุนแรง: Medium

ประเภทช่องโหว่: Security Misconfiguration

มาตรฐานอ้างอิง:

OWASP Top 10:2021 – A05

รายละเอียดช่องโหว่

จากการตรวจสอบ HTTP Response Header ไม่พบ Security Header ที่สำคัญ เช่น

X-Frame-Options
X-Content-Type-Options
Content-Security-Policy
Strict-Transport-Security

ผลกระทบ

อาจทำให้ระบบเสี่ยงต่อ:

Header ที่ขาด	ความเสี่ยง
X-Frame-Options	Clickjacking
X-Content-Type-Options	MIME sniffing
CSP	Cross-Site Scripting (XSS)
HSTS	SSL stripping

4. ตารางสรุปความเสี่ยง

ลำดับ	ช่องโหว่	Impact	Likelihood	Risk
1	Server Version Disclosure	Medium	Medium	Medium
2	WordPress Version Disclosure	Medium	Medium	Medium

3 Missing Security Headers Medium Medium Medium

ระดับความเสี่ยงรวมของระบบ: Medium

ข้อเสนอแนะในการแก้ไข (Recommendations)

ซ่อนข้อมูลเวอร์ชันเซิร์ฟเวอร์

แก้ไขไฟล์ Apache config

ServerTokens Prod
ServerSignature Off

เพิ่ม Security Headers

ตัวอย่างการตั้งค่าใน Apache:

Header always set X-Frame-Options "SAMEORIGIN"
Header always set X-Content-Type-Options "nosniff"
Header always set X-XSS-Protection "1; mode=block"
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Header always set Content-Security-Policy "default-src 'self' https: data: 'unsafe-inline' 'unsafe-eval'"

ซ่อนเวอร์ชัน WordPress

เพิ่มใน functions.php

remove_action('wp_head', 'wp_generator');

ระดับความเสี่ยงโดยรวม : Medium

ผลการทดสอบความมั่นคงปลอดภัยระบบสารสนเทศ

ชื่อช่องโหว่	ประเภท	Impact	Likelihood	ระดับความเสี่ยง (Risk)	มาตรฐานอ้างอิง
Information Disclosure via Server Header	Security Misconfiguration	Medium	Medium	Medium	OWASP A05, CWE-200
WordPress Version Disclosure	Information Exposure	Medium	Medium	Medium	OWASP A05, CWE-200
Missing Security Headers	Security Misconfig	Medium	Medium	Medium	OWASP A05

ระดับความเสี่ยงโดยรวม (Overall Risk Summary)

ระดับความเสี่ยง	จำนวนรายการ
Critical	0
High	0
Medium	3
Low	0

Penetration Test Report

1. General Information

- **Target System:** Nam Kliang Hospital Website
- **URL:** https://www.nkhos.go.th
- **System Type:** Web Application (WordPress)
- **Testing Method:** HTTP Response Header and Source Code Analysis
- **Test Date:** 05 February 2026

---

2. Executive Summary

A security assessment of the target web application identified several configuration weaknesses. The system exposes server and application version information and lacks critical HTTP security headers.

These issues do not represent an immediate compromise but may assist attackers in identifying known vulnerabilities and executing targeted attacks such as clickjacking or cross-site scripting.

Overall Risk Level: Medium

---

3. Findings

3.1 Server Version Disclosure

Severity: Medium
Category: Information Disclosure
OWASP Reference: A05:2021 – Security Misconfiguration
CWE: CWE-200
Description

The HTTP response header reveals the web server software and version:
Server: Apache/2.4.58 (Ubuntu)
This information allows attackers to:

- Identify the server type
- Search for known vulnerabilities
- Launch targeted attacks based on version-specific exploits

Evidence
HTTP/1.1 200 OK
Server: Apache/2.4.58 (Ubuntu)
Impact

- Facilitates targeted attacks
- Assists in vulnerability enumeration

Likelihood
Medium (information is publicly accessible)
Risk Rating
Medium

3.2 WordPress Version Disclosure
Severity: Medium
Category: Information Disclosure
OWASP Reference: A05:2021 – Security Misconfiguration
CWE: CWE-200
Description
The WordPress version is exposed in the page source:
ver=6.5.5
Attackers may use this information to:

- Identify known WordPress vulnerabilities
- Target specific plugins or themes

Impact

- Increased risk of targeted exploitation
- Easier vulnerability discovery

Likelihood
Medium
Risk Rating
Medium

3.3 Missing Security Headers

Severity: Medium
Category: Security Misconfiguration
OWASP Reference: A05:2021

Description

The application does not include important HTTP security headers, such as:

- X-Frame-Options
- X-Content-Type-Options
- Content-Security-Policy
- Strict-Transport-Security

Impact

The absence of these headers may expose the system to:

Missing Header	Potential Attack
X-Frame-Options	Clickjacking
X-Content-Type-Options	MIME sniffing
Content-Security-Policy	Cross-Site Scripting (XSS)
HSTS	SSL stripping

Likelihood

Medium

Risk Rating

Medium

---

4. Risk Summary

ID	Finding	Impact	Likelihood	Risk
1	Server Version Disclosure	Medium	Medium	Medium
2	WordPress Version Disclosure	Medium	Medium	Medium
3	Missing Security Headers	Medium	Medium	Medium

Overall System Risk: Medium

---

5. Recommendations

5.1 Hide Server Version Information

Update Apache configuration:

```
ServerTokens Prod
ServerSignature Off
```

5.2 Implement Security Headers

Example Apache configuration:

```
Header always set X-Frame-Options "SAMEORIGIN"
Header always set X-Content-Type-Options "nosniff"
Header always set X-XSS-Protection "1; mode=block"
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Header always set Content-Security-Policy "default-src 'self' https: data: 'unsafe-inline' 'unsafe-eval'"
```

5.3 Hide WordPress Version

Add the following to the functions.php file:

```
remove_action('wp_head', 'wp_generator');
```

การดำเนินงาน ด้านการตรวจสอบความปลอดภัยและช่องโหว่ของระบบ หน่วยงานได้รับการสนับสนุนจากเครือข่าย ซึ่งเป็นผู้ที่ได้รับการอบรมหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์

- หลักสูตรการอบรมเชิงปฏิบัติการ “การตรวจวิเคราะห์ภัยคุกคามและแนวทางในการรับมือต่อเหตุการณ์ภัยคุกคาม” (หลักสูตรที่ ศทส.สป.สธ.จัดร่วมกับ สกมช.)

- หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ ระดับชี่ยวชาญ (ของ สกมช.)

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ขอมอบประกาศนียบัตรเพื่อแสดงว่า

เสริมศิลป์ สินศิริ

เป็นผู้สำเร็จการอบรมในหลักสูตร

ด้านความมั่นคงปลอดภัยไซเบอร์ ระดับผู้เชี่ยวชาญ
(Cybersecurity Professional Course)
ผ่านระบบ NCSA e-Learning จำนวน 20 ชั่วโมง

ให้ไว้ ณ วันที่ 20 เมษายน พ.ศ. 2568

พลอากาศตรี
(อมร ชมเชย)
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

Advanced

Verification Code
908185137755

แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ประจำปี

(Cybersecurity Audit Plan)

วัตถุประสงค์: เพื่อประเมินความพร้อม ตรวจสอบช่องโหว่ และรับประกันความปลอดภัยของระบบสารสนเทศตามมาตรฐาน

ความถี่ในการตรวจสอบ: อย่างน้อยปีละ 1 ครั้ง (ช่วงเดือนที่แผนกำหนด: เดือนกุมภาพันธ์ ของทุกปี)

เฟส / ขั้นตอน	รายละเอียดกิจกรรมหลัก (Key Activities)	ผู้รับผิดชอบ	สถานะ
ระยะ1 วางแผน	1. กำหนดขอบเขตการตรวจ (Audit Scope): ครอบคลุมห้อง Server, ระบบโครงข่าย (Network), ระบบงานสำคัญ และฐานข้อมูล	IT / Auditor	✓
	2. จัดตั้งทีมตรวจ: ระบุผู้ตรวจสอบภายใน หรือผู้เชี่ยวชาญจากภายนอกเพื่อความโปร่งใส	IT / Auditor	✓
ระยะ2 ประเมินความเสี่ยง	3. ตรวจสอบสิทธิ์การเข้าถึง (Access Control): เช็คสิทธิ์สิทธิ์ User/Admin, นโยบายรหัสผ่าน (Password Policy) และระบบยืนยันตัวตน 2 ชั้น (MFA)	IT Security	✓
	4. ตรวจระบบสำรองข้อมูล (Backup): ทดสอบการกู้คืนข้อมูล (Disaster Recovery Test) ว่าใช้งานได้จริงและปลอดภัยจาก Ransomware	IT Security	✓
	5. ตรวจสอบการอัปเดตระบบ (Patch Management): เช็คประวัติการอัปเดต OS, Firewall, และโปรแกรมแอนตี้ไวรัสให้เป็นเวอร์ชันล่าสุดเสมอ	IT Security	✓
ระยะ3 ทดสอบระบบ	6. ประเมินช่องโหว่ (Vulnerability Assessment): สแกนหาช่องโหว่ของระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server)	ทีม Audit / ผู้เชี่ยวชาญ	✓
	7. ตรวจสอบความปลอดภัยกายภาพ: ตรวจบันทึกการเข้า-ออกห้อง Server และระบบบันทึกของกล้องวงจรปิด (CCTV)	ทีม Audit / ผู้เชี่ยวชาญ	✓
ระยะ4 สรุปผล	8. จัดทำรายงานผล (Audit Report): รวบรวมข้อบกพร่อง ช่องโหว่ และระดับความรุนแรงที่ตรวจพบในการประเมินทั้งหมด	Auditor / ผู้บริหาร	✓
	9. แผนปรับปรุง (Remediation Plan): กำหนดมาตรการแก้ไข ผู้รับผิดชอบ และกรอบระยะเวลาในการปิดช่องโหว่	Auditor / ผู้บริหาร	✓
	10. รายงานผู้บริหาร: นำเสนอผลการตรวจสอบและแผนปรับปรุงต่อผู้บริหารระดับสูงเพื่อขอมุมติงบประมาณและทรัพยากร	Auditor / ผู้บริหาร	✓

[✓] **แผนรองรับกรณีฉุกเฉิน** (Incident Response Review):

มีการทบทวนและซักซ้อมแผนแก้ปัญหาภัยคุกคามทางไซเบอร์ (เช่น การซ้อมรับมือสถานการณ์ข้อมูลรั่วไหล หรือระบบถูกโจมตี ฯลฯ) อย่างน้อยปีละ 1 ครั้ง

ข้อเสนอแนะเพิ่มเติม:

_____

_____

ลงชื่อผู้จัดทำแผน: _____ นายธีระวัฒน์ ศิละพันธ์
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
(ตำแหน่ง): _____

ลงชื่อผู้อนุมัติแผน: _____ นางสาวศิริลักษณ์ สมศิริ
(ตำแหน่ง): นักวิชาการสาธารณสุขปฏิบัติการ