คู่มือการตรวจสอบความมั่นคงปลอดภัยเว็บไซต์

(Website Security Self-Assessment Guide)

สำหรับหน่วยงานภายในมหาวิทยาลัยศิลปากร

(For internal units of Silpakorn University)

สำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร

พฤศจิกายน 2568

สารบัญ

คำนำ

ในปัจจุบันภัยคุกคามทางไซเบอร์ได้ทวีความรุนแรงขึ้น โดยเฉพาะการโจมตีเป้าหมายที่เป็นหน่วยงานภาครัฐและสถาบันการศึกษา ซึ่งส่งผลกระทบต่อความเชื่อมั่นและความปลอดภัยของข้อมูลส่วนบุคคลและข้อมูลราชการ เพื่อให้การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ มหาวิทยาลัยศิลปากรจึงได้กำหนดมาตรการให้ทุกหน่วยงานดำเนินการตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ (Vulnerability Assessment) ด้วยตนเองก่อนการนำขึ้นใช้งานหรือเผยแพร่

คู่มือฉบับนี้จัดทำขึ้นเพื่อให้บุคลากร หรือผู้ดูแลเว็บไซต์ของหน่วยงาน ซึ่งอาจไม่ใช่ผู้เชี่ยวชาญด้านคอมพิวเตอร์โดยตรง สามารถปฏิบัติตามขั้นตอนการตรวจสอบหาช่องโหว่ของระบบเว็บไซต์ได้ด้วยตนเอง โดยใช้เครื่องมือมาตรฐานสากล ได้แก่ SSL Labs, WordPress Scanner และ OWASP ZAP โดยเน้นขั้นตอนที่เข้าใจง่าย ปฏิบัติได้จริง และมีเกณฑ์การวัดผลที่ชัดเจน

สำนักดิจิทัลเทคโนโลยี หวังเป็นอย่างยิ่งว่าคู่มือฉบับนี้จะเป็นประโยชน์ในการยกระดับความปลอดภัยทางไซเบอร์ของมหาวิทยาลัยให้ดียิ่งขึ้น

การเตรียมความพร้อมด้านอุปกรณ์และขั้นตอนสำหรับการตรวจประเมินช่องโหว่ (Vulnerability Assessment Preparation)

เพื่อให้การดำเนินการตรวจหาช่องโหว่ของระบบสารสนเทศ (Vulnerability Assessment) เป็นไปอย่างมีประสิทธิภาพ มีความถูกต้องแม่นยำ และไม่ก่อให้เกิดผลกระทบต่อระบบงานหลัก จำเป็นต้องมีการเตรียมความพร้อมด้านฮาร์ดแวร์ การตั้งค่าระบบ และกระบวนการปฏิบัติงานตามมาตรฐาน ดังรายละเอียดต่อไปนี้

1. คุณสมบัติและข้อกำหนดของเครื่องคอมพิวเตอร์สำหรับสแกน (Scanner Station Requirements)

เครื่องคอมพิวเตอร์ที่ทำหน้าที่รันซอฟต์แวร์สแกนช่องโหว่ (Scanner Node) ต้องมีสมรรถนะที่รองรับการประมวลผลข้อมูลปริมาณมากและการส่งผ่านข้อมูลเครือข่ายอย่างต่อเนื่อง โดยมีข้อกำหนดคุณสมบัติขั้นต่ำ (Minimum Requirements) ดังนี้

อุปกรณ์ (Component)	รายละเอียดคุณสมบัติขั้นต่ำ (Minimum Specification)	เหตุผลความจำเป็น (Rationale)
หน่วยประมวลผลกลาง (CPU)	**4 Cores / 8 Threads** (ความเร็ว 2.0 GHz ขึ้นไป)	การสแกนต้องใช้การประมวลผลแบบ Multi-thread เพื่อวิเคราะห์ Plugin และ Rule ต่าง ๆ หากสมรรถนะต่ำกว่านี้ อาจทำให้โปรแกรมหยุดทำงาน (Freeze) ระหว่างสร้างรายงาน
หน่วยความจำ (RAM)	**16 GB** (แนะนำ 32 GB ขึ้นไป)	โปรแกรมสแกนใช้หน่วยความจำสูงมากในการโหลดฐานข้อมูลช่องโหว่ (Vulnerability Feed) และประมวลผลผลลัพธ์แบบ Real-time
พื้นที่จัดเก็บข้อมูล (Storage)	**SSD 128 GB ขึ้นไป** (พื้นที่ว่างพร้อมใช้งาน > 50 GB)	จำเป็นต้องใช้ SSD เพื่อความเร็วในการเขียน Log และ Database หากใช้ HDD แบบจานหมุนจะเกิดคอขวด (I/O Bottleneck) ทำให้การสแกนล่าช้าอย่างมาก
ระบบเครือข่าย (Network)	**Gigabit Ethernet Port (LAN)**	ต้องเชื่อมต่อผ่านสายสัญญาณ (Wired Connection) เท่านั้น **ไม่แนะนำให้ใช้ Wi-Fi** เนื่องจากความไม่เสถียรและความหน่วง (Latency) ซึ่งอาจส่งผลให้ผลลัพธ์คลาดเคลื่อน
ระบบปฏิบัติการ (OS)	**Windows 10/11 (64-bit)** หรือ **Linux (Kali/Ubuntu)**	รองรับซอฟต์แวร์สแกนมาตรฐานระดับ Enterprise

2. การเตรียมการตั้งค่าเครื่องสแกน (Scanner Configuration & Readiness)

ก่อนเริ่มดำเนินการ เครื่องสแกนต้องได้รับการตั้งค่าและตรวจสอบความพร้อมเพื่อป้องกันข้อผิดพลาดทางเทคนิค ดังนี้

1. **การอัปเดตฐานข้อมูล (Signature/Feed Update):** ต้องทำการอัปเดตฐานข้อมูลช่องโหว่ (Vulnerability Database) และ Plugin ของซอฟต์แวร์สแกนให้เป็นเวอร์ชันปัจจุบัน (Latest Version) เพื่อให้สามารถตรวจจับช่องโหว่ใหม่ล่าสุดได้
2. **การจัดการพลังงาน (Power Management):** ต้องตั้งค่า Power Options ของเครื่องให้เป็นโหมด **"Never Sleep"** (ห้ามเข้าสู่โหมดพักหน้าจอหรือ Sleep) ทั้งกรณีเสียบปลั๊กและใช้แบตเตอรี่ เนื่องจากการสแกนอาจใช้เวลานาน หากเครื่องหยุดทำงานกลางคัน การสแกนจะล้มเหลวทันที
3. **การกำหนดค่าเครือข่าย (Network Setup):** ควรกำหนด IP Address ของเครื่องสแกนให้เป็นแบบคงที่ (Static IP) เพื่อสะดวกต่อการตรวจสอบ Log และการทำ Whitelist บนอุปกรณ์ความปลอดภัย
4. **สภาพแวดล้อมซอฟต์แวร์ (Clean Environment):** เครื่องสแกนควรเป็นเครื่องที่ใช้งานเฉพาะทาง (Dedicated Machine) ไม่มีซอฟต์แวร์อื่นรบกวน และต้องปลอดจากมัลแวร์เพื่อป้องกันการแพร่กระจายสู่ระบบเป้าหมาย

3. ขั้นตอนการเตรียมการก่อนเริ่มสแกน (Pre-Scan Operational Workflow)

เพื่อให้กระบวนการสแกนดำเนินไปอย่างปลอดภัยและถูกต้อง ผู้ปฏิบัติงานต้องดำเนินการตามขั้นตอนดังนี้

3.1 การขออนุมัติและกำหนดขอบเขต (Authorization & Scoping)

3.2 การเตรียมระบบเป้าหมาย (Target System Preparation)

3.3 การบริหารจัดการเวลา (Timing Strategy)

ช่วงเวลาดำเนินการ: ควรดำเนินการในช่วงเวลาที่มีผู้ใช้งานน้อยที่สุด (Off-Peak Hours) หรือนอกเวลางาน เพื่อลดผลกระทบด้านประสิทธิภาพ (Performance Impact) ต่อผู้ใช้งานทั่วไป

การแจ้งเตือน: แจ้งผู้ดูแลระบบ (System Admin) หรือศูนย์เฝ้าระวังภัยคุกคาม (SOC) ให้รับทราบแผนการปฏิบัติงาน เพื่อป้องกันความเข้าใจผิดว่าเป็นภัยคุกคามจริง

บทที่ 1: หลักการและเกณฑ์การประเมิน

เพื่อให้การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัยศิลปากรเป็นไปอย่างมีประสิทธิภาพ หน่วยงานจำเป็นต้องตรวจสอบความปลอดภัยของเว็บไซต์ก่อนการเผยแพร่ หรือตรวจสอบประจำปี โดยมีรายละเอียดดังนี้

1.1 เกณฑ์การผ่านการประเมิน

เว็บไซต์ของหน่วยงานจะต้องได้รับการตรวจสอบ และ **ต้องไม่พบ** ช่องโหว่ในระดับความเสี่ยงดังต่อไปนี้:

1. **ระดับวิกฤต (Critical)**
2. **ระดับสูงมาก (Very High)**
3. **ระดับสูง (High)**

หากพบช่องโหว่ในระดับข้างต้น ต้องดำเนินการแก้ไขให้เรียบร้อยก่อนส่งรายงาน

1.2 เครื่องมือที่ใช้ในการตรวจสอบ

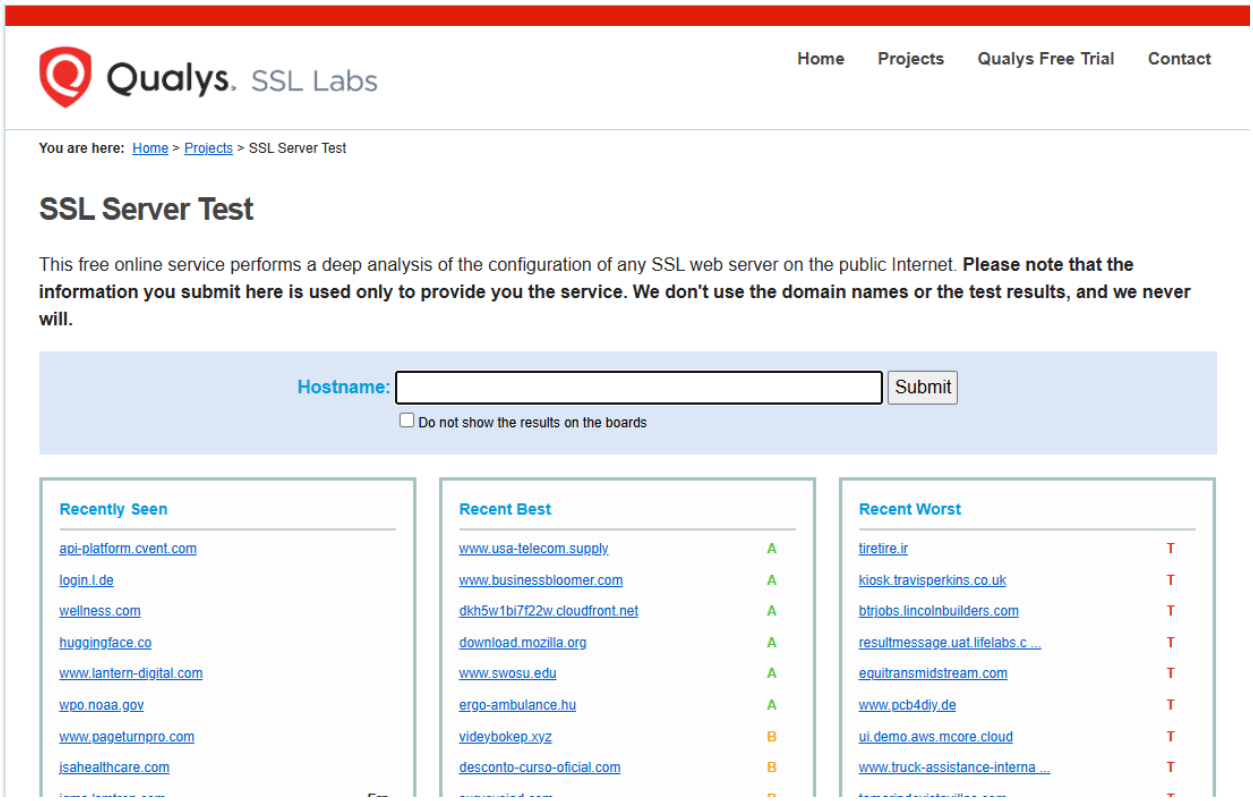
1. **SSL Labs:** ตรวจสอบมาตรฐานความปลอดภัยการเชื่อมต่อ (HTTPS)
2. **WordPress Scanner:** ตรวจสอบความปลอดภัยเฉพาะเว็บไซต์ WordPress (ถ้ามี)
3. **OWASP ZAP:** ตรวจสอบช่องโหว่ของแอปพลิเคชัน (Application Security)

บทที่ 2: การตรวจสอบการเข้ารหัสข้อมูล (SSL Labs)

เป้าหมาย: เพื่อตรวจสอบใบรับรองความปลอดภัย (Certificate) และการเข้ารหัสข้อมูล

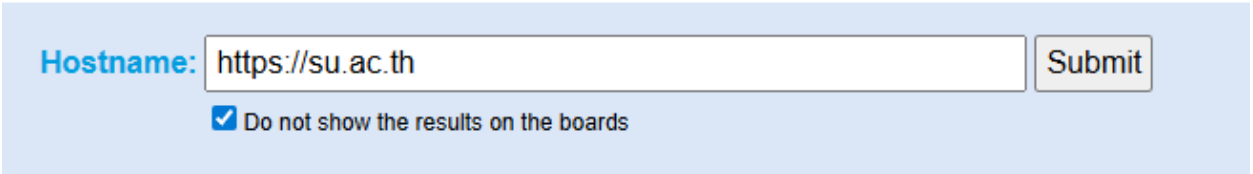
ขั้นตอนการปฏิบัติ

1. เปิดเว็บเบราว์เซอร์ และเข้าไปที่: https://www.ssllabs.com/ssltest/



[ภาพที่ 1 แสดงหน้าแรกของเว็บไซต์ SSL Labs]

2. ในช่อง Hostname ให้พิมพ์ชื่อเว็บไซต์ของหน่วยงาน (เช่น www.yoursite.su.ac.th) แล้วกด Submit

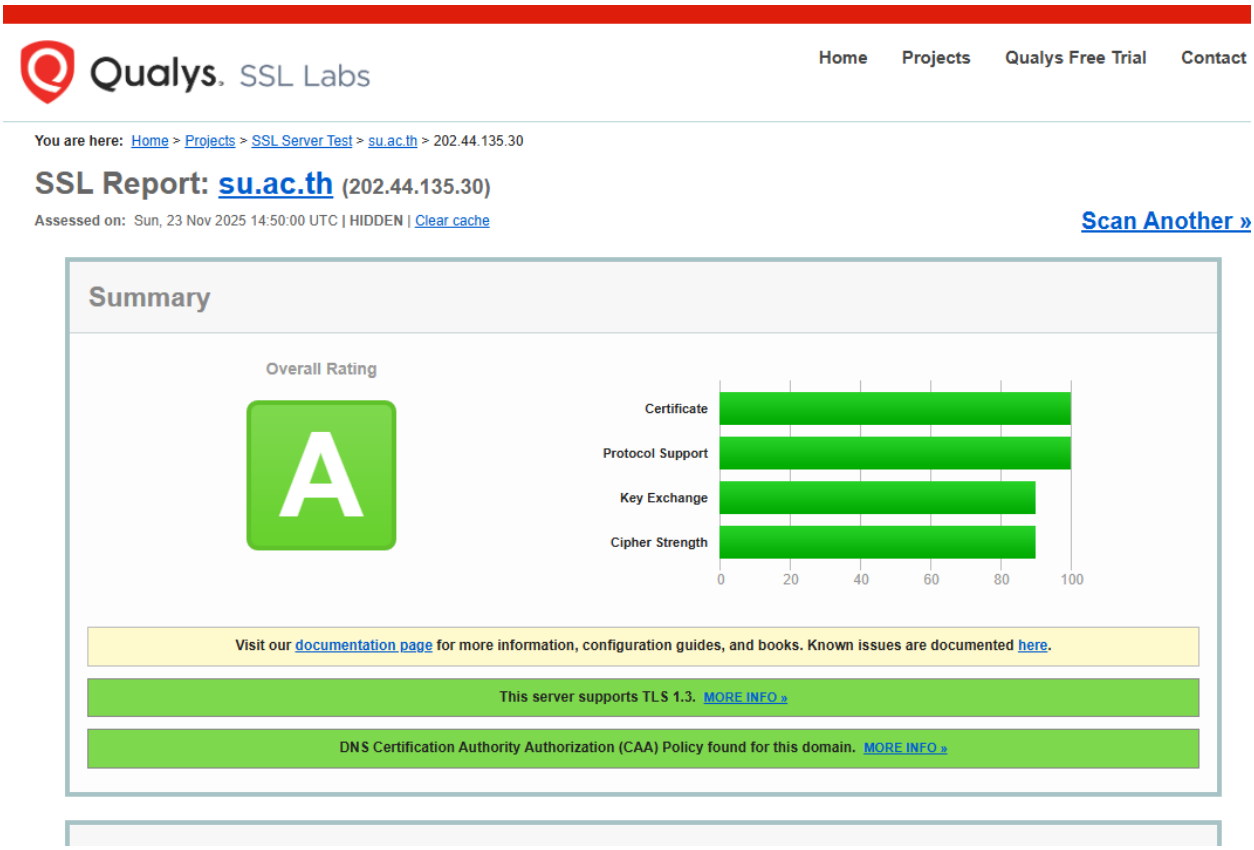


[ภาพที่ 2 แสดงตัวอย่างการกรอกชื่อเว็บแล้วกดปุ่ม]

3. รอระบบประมวลผล (ประมาณ 3 นาที)

4. การตรวจสอบผล: เว็บไซต์ที่ผ่านเกณฑ์ต้องได้เกรด A+, A หรือ A- เท่านั้น

	Server	Test time	Grade
1	2001:3c8:2107:0:0:0:0:30 Unable to connect to the server	Sun, 23 Nov 2025 14:48:12 UTC Duration: 16.333 sec	-
2	202.44.135.30 www.su.ac.th Ready	Sun, 23 Nov 2025 14:48:29 UTC Duration: 91.286 sec	A



[ภาพที่ 3 แสดงผลลัพธ์เกรด A สีเขียว และหลังคลิกดูรายละเอียด]

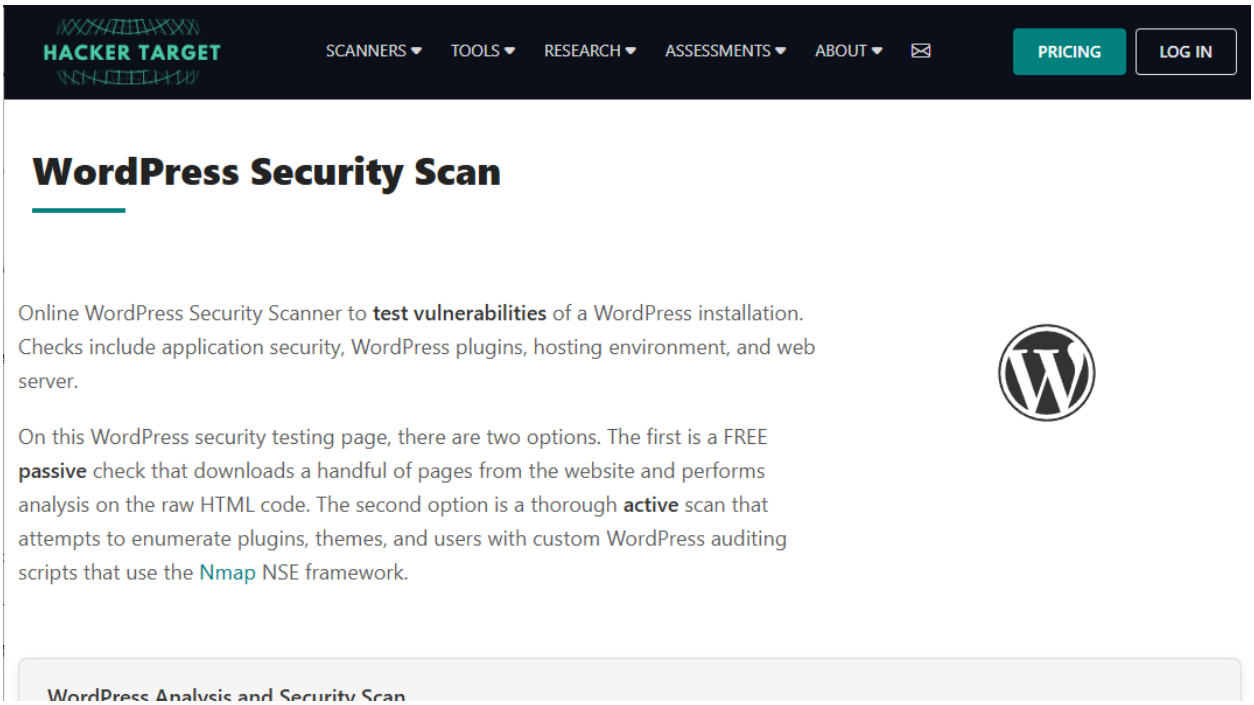
5. **การบันทึกข้อมูล:** ให้จับภาพหน้าจอ (Screenshot) ที่เห็นเกรดชัดเจนเพื่อแนบรายงาน

บทที่ 3: การตรวจสอบเว็บไซต์ประเภท WordPress

*(หากเว็บไซต์ของท่าน **ไม่ได้** พัฒนาด้วย WordPress ให้ข้ามไปทำบทที่ 4)*

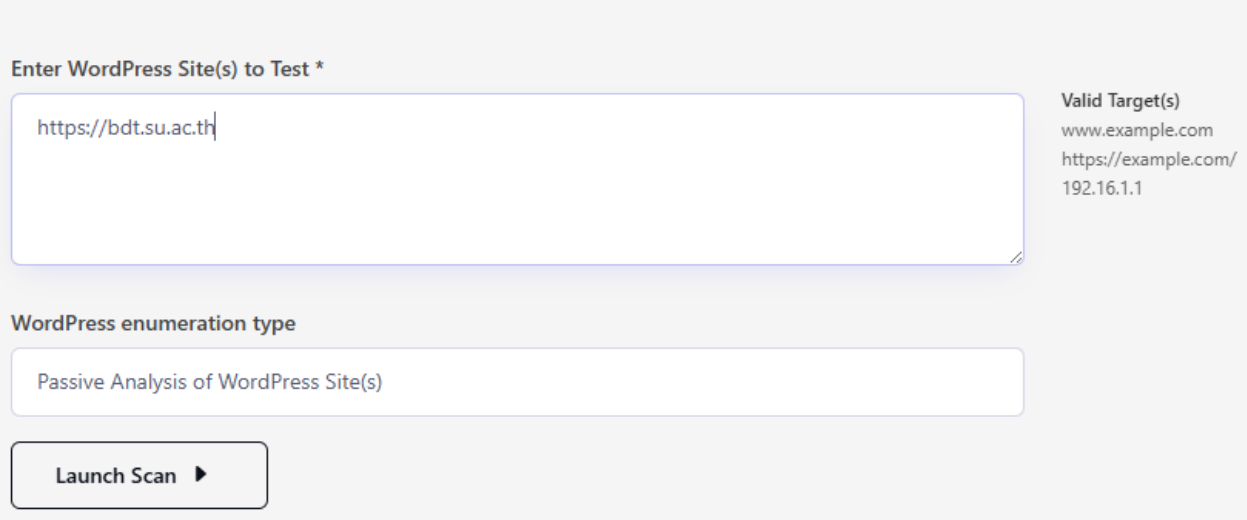
ขั้นตอนการปฏิบัติ

1. เข้าไปที่เว็บไซต์สำหรับสแกนออนไลน์ เช่น https://hackertarget.com/wordpress-security-scan/

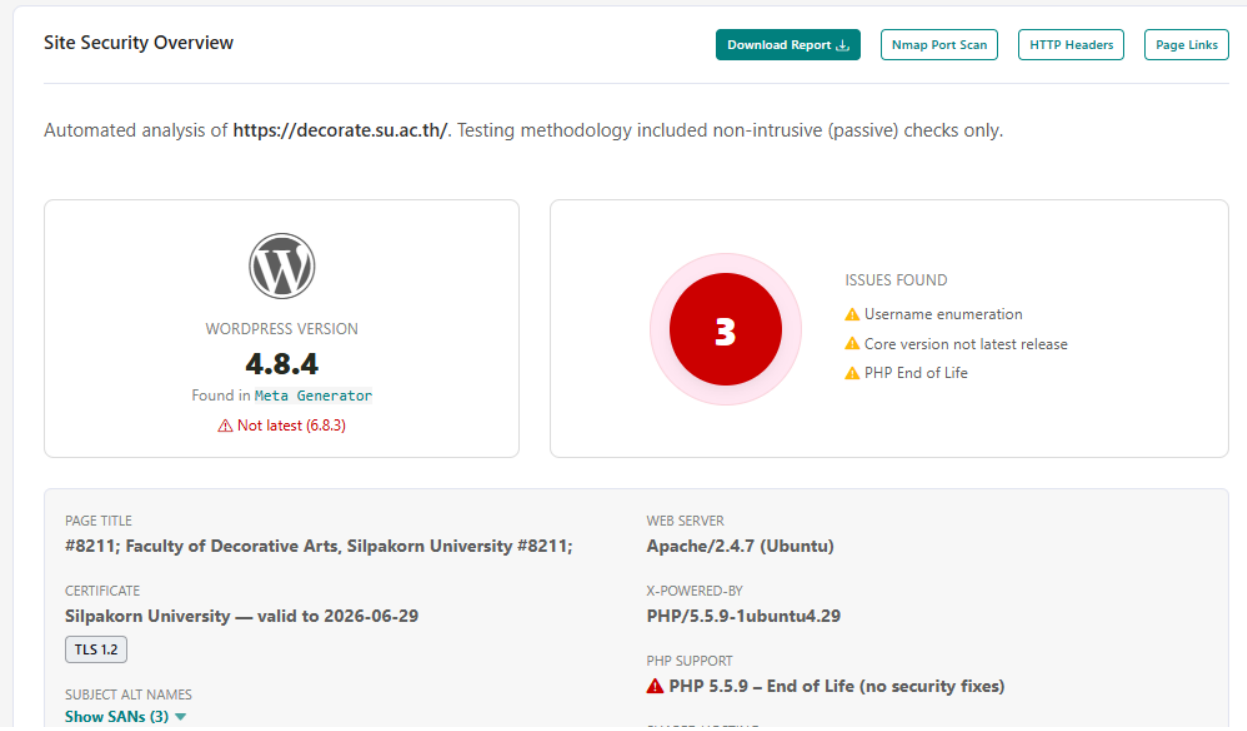


[ภาพที่ 4 แสดงหน้าเว็บไซต์สำหรับสแกน WordPress]

2. กรอก URL เว็บไซต์ของท่าน แล้วกดปุ่ม Start Scan



[ภาพที่ 5 แสดงการกดปุ่มสแกน]



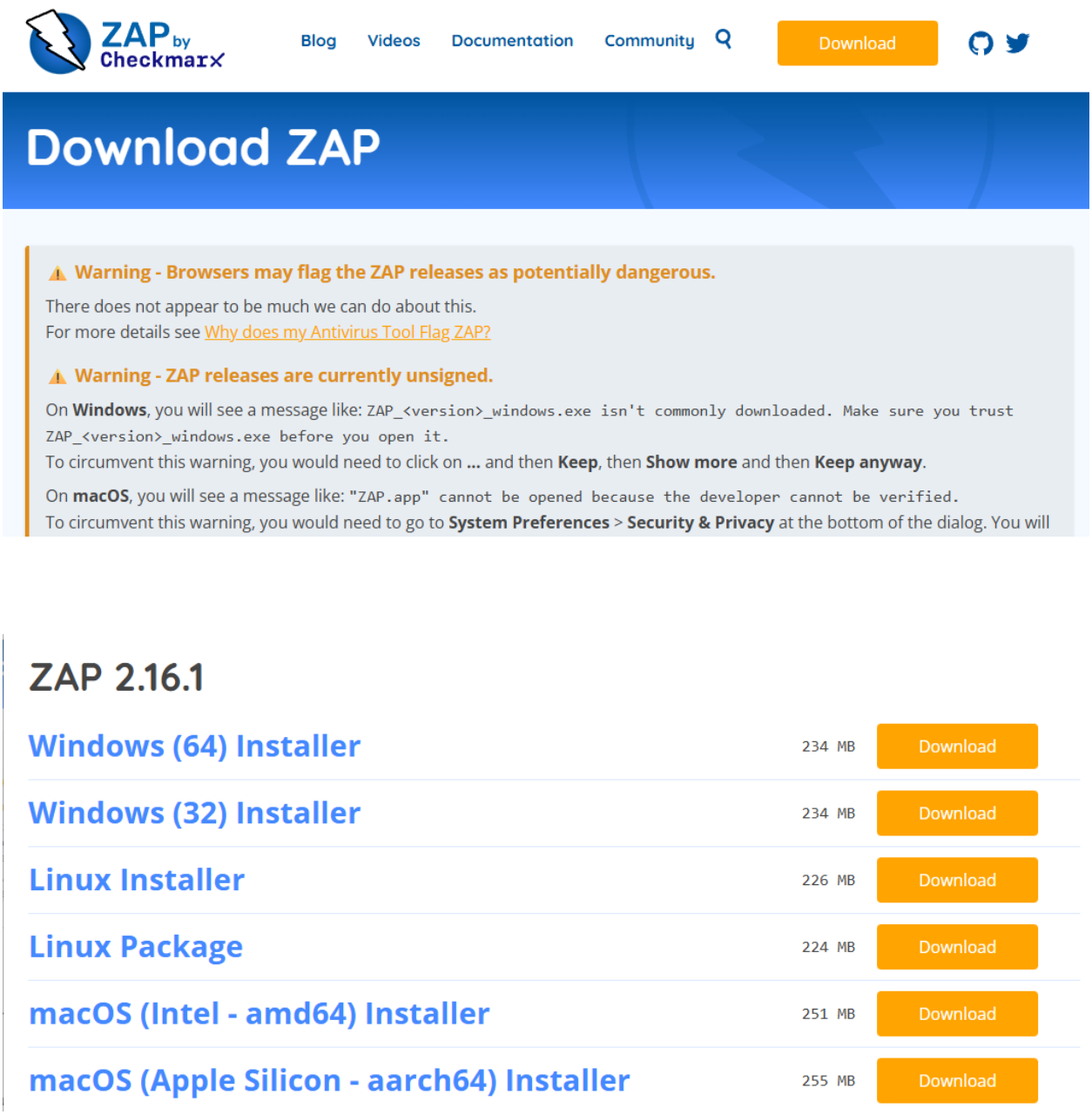
[ภาพที่ 5.1 แสดงรายละเอียดการสแกน โดยที่ส่วน Issues Found ต้องไม่มีสีแดงและจำนวนต้องเป็น 0]

3. **การตรวจสอบผล:** อ่านผลในส่วนต่าง ๆ ดังนี้
    - **WordPress Version:** ต้องเป็นสีเขียว (เวอร์ชันล่าสุด) หรือไม่ขึ้นเตือนว่า Outdated
    - **Plugins/Themes:** ต้องไม่มีรายการแจ้งเตือนสีแดง (Vulnerable)
    - **User Enumeration:** ไม่ควรแสดงรายชื่อ Admin
4. **การบันทึกข้อมูล:** จับภาพหน้าจอผลการสแกนเพื่อแนบรายงาน หรือคลิกที่ปุ่ม Download Report สีเขียวด้านบน

บทที่ 4: การตรวจสอบช่องโหว่ด้วย OWASP ZAP

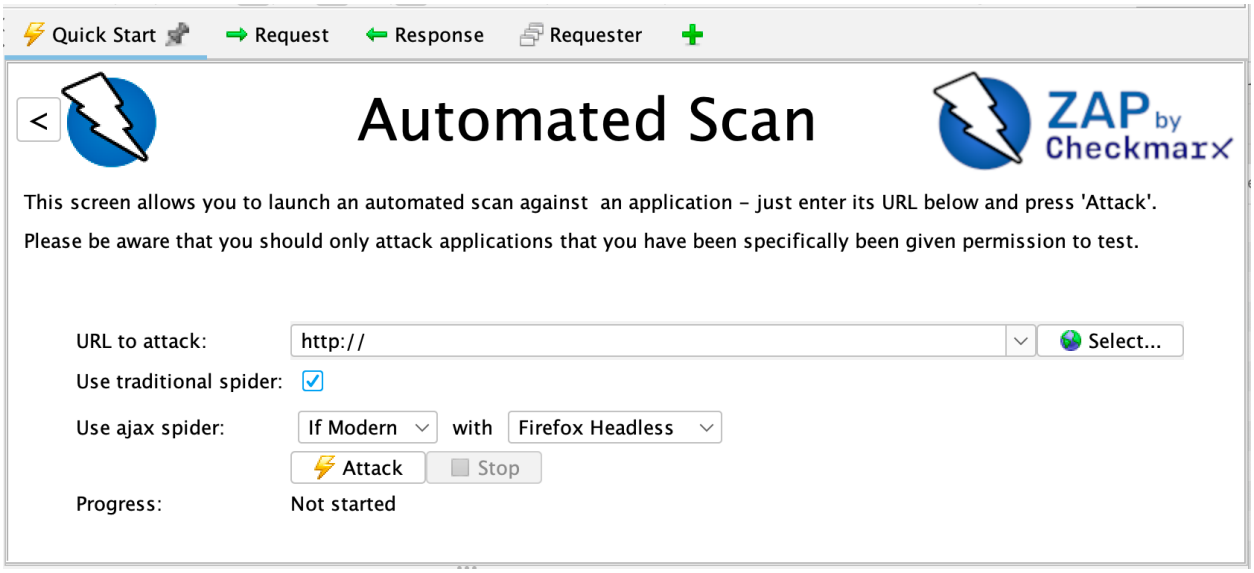
ขั้นตอนการปฏิบัติ

1. ดาวน์โหลดโปรแกรมที่ https://www.zaproxy.org/download/ และติดตั้งลงในคอมพิวเตอร์ เลื่อนหน้าจอลงมาด้านล่าง ให้เลือกดาวน์โหลดตามระบบปฏิบัติการที่ใช้อยู่ หลังจากนั้นก็ติดตั้งให้เรียบร้อย



[ภาพที่ 6 แสดงหน้าดาวน์โหลด OWASP ZAP]

2. เปิดโปรแกรม เลือกเมนู "Automated Scan" บริเวณแท็บ Quick Start ด้านขวาของหน้าจอ

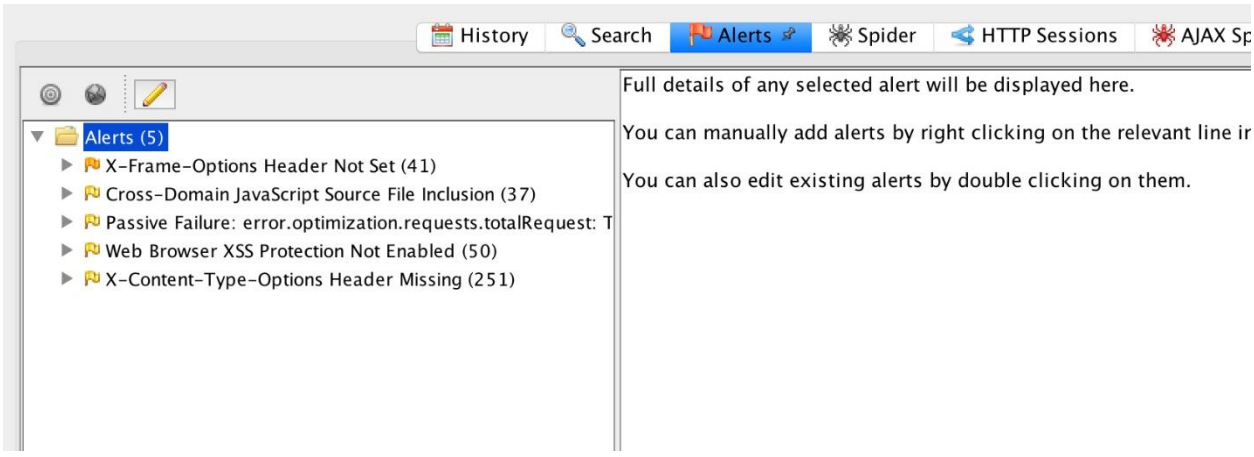


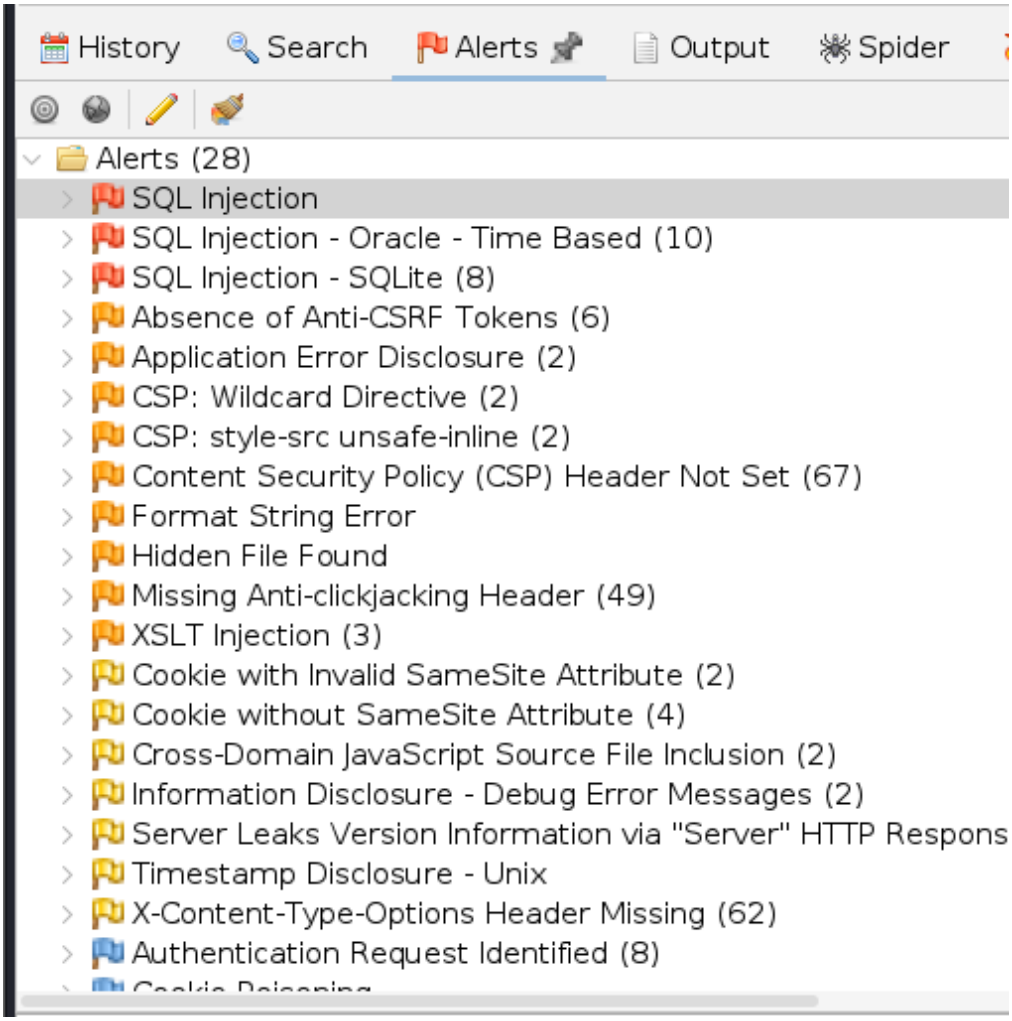
[ภาพที่ 7 แสดงปุ่ม Automated Scan บนหน้าจอหลัก]

3. ใส่ชื่อเว็บไซต์ในช่อง URL to attack แล้วกดปุ่ม Attack

4. รอจนแถบสถานะด้านล่างทำงานจนครบ 100% อาจใช้เวลาเกิน 1 ชั่วโมง

5. ตรวจสอบผลที่แท็บ "Alerts" (รูปธงด้านล่างซ้าย)





[ภาพที่ 9 แสดงรายการแจ้งเตือนในแท็บ Alerts]

- **ต้องไม่มี** ธงสีแดง (High/Critical)

6. การสร้างรายงาน: คลิกเมนู Report > Generate Report เลือกเป็นไฟล์ PDF หรือ HTML

ZAP Scanning Report

Generated on Fri, 4 Feb 2022 12:07:12

Summary of Alerts

Risk Level	Number of Alerts
High	2
Medium	4
Low	8
Informational	6

Alerts

Name	Risk Level	Number of Instances
Anti-CSRF Tokens Check	High	10
Cross Site Scripting (Reflected)	High	2
Buffer Overflow	Medium	529
Content Security Policy (CSP) Header Not Set	Medium	58
Example Passive Scan Rule: Denial of Service	Medium	7
X-Frame-Options Header Not Set	Medium	55
Absence of Anti-CSRF Tokens	Low	73
Application Error Disclosure	Low	1
Cookie No HttpOnly Flag	Low	1
Cookie without SameSite Attribute	Low	2
In Page Banner Information Leak	Low	3
Information Disclosure - Debug Error Messages	Low	1
Permissions Policy Header Not Set	Low	59
X-Content-Type-Options Header Missing	Low	62
Information Disclosure - Suspicious Comments	Informational	58
Loosely Scoped Cookie	Informational	3
Modern Web Application	Informational	33
Non-Storable Content	Informational	2
Storable and Cacheable Content	Informational	64
User Controllable HTML Element Attribute (Potential XSS)	Informational	32

Passing Rules

Name	Rule Type	Threshold	Strength
Remote Code Execution - Shell Shock	Active	MEDIUM	MEDIUM
Directory Browsing	Active	MEDIUM	MEDIUM
CRLF Injection	Active	MEDIUM	MEDIUM
Path Traversal	Active	MEDIUM	MEDIUM
Remote File Inclusion	Active	MEDIUM	MEDIUM
Parameter Tampering	Active	MEDIUM	MEDIUM
Server Side Include	Active	MEDIUM	MEDIUM
Session Fixation	Active	MEDIUM	MEDIUM
Cross Site Scripting (Persistent)	Active	MEDIUM	MEDIUM
Script Active Scan Rules	Active	MEDIUM	MEDIUM
Cross Site Scripting (Persistent) - Prime	Active	MEDIUM	MEDIUM
Cross Site Scripting (Persistent) - Spider	Active	MEDIUM	MEDIUM
SQL Injection	Active	MEDIUM	MEDIUM
SQL Injection - MySQL	Active	MEDIUM	MEDIUM
SQL Injection - Hypersonic SQL	Active	MEDIUM	MEDIUM
ELMAH Information Leak	Active	MEDIUM	MEDIUM
.htaccess Information Leak	Active	MEDIUM	MEDIUM
Server Side Code Injection	Active	MEDIUM	MEDIUM
Remote OS Command Injection	Active	MEDIUM	MEDIUM
Source Code Disclosure - Git	Active	MEDIUM	MEDIUM
Source Code Disclosure - File Inclusion	Active	MEDIUM	MEDIUM

[ภาพที่ 10 ตัวอย่างรายงานที่สร้าง]

บทที่ 5: การสรุปผลและส่งรายงาน

เมื่อดำเนินการตรวจสอบครบถ้วนแล้ว ให้ผู้ดูแลเว็บไซต์ดำเนินการดังนี้:

1. พิมพ์ **"แบบฟอร์มรายงานผลการตรวจสอบ (หน้าถัดไป)"**
2. กรอกข้อมูลลงในแบบฟอร์มให้ครบถ้วน
3. ลงลายมือชื่อผู้ตรวจสอบ และหัวหน้าหน่วยงาน
4. แนบหลักฐานประกอบ (ไฟล์รายงาน ZAP, ภาพหน้าจอ SSL, ภาพหน้าจอ WordPress)

ส่งเอกสารทั้งหมดมายัง **สำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร** เพื่อทำการตรวจสอบยืนยันความถูกต้อง

แบบฟอร์มรายงานผลการตรวจสอบความมั่นคงปลอดภัยเว็บไซต์

สำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร

1. ข้อมูลทั่วไป

- **หน่วยงาน / คณะวิชา:** .....
- **วันที่ตรวจสอบ:** .....
- **URL ที่ตรวจสอบ:** .....
- **ระบบที่ใช้พัฒนา (CMS):** ☐ WordPress ☐ อื่น ๆ (ระบุ).....

2. ผลการตรวจสอบด้วยตนเอง (Self-Assessment Checklist)

(โปรดทำเครื่องหมาย ✓ ลงในช่องสี่เหลี่ยม และกรอกข้อมูลตามความเป็นจริง)

ส่วนที่ 1: การเข้ารหัสข้อมูล (SSL Labs)

ผลการตรวจสอบเกรด SSL: ..... (เช่น A+, A, B, C)

☐ **ผ่าน** (ได้เกรด A-, A หรือ A+)

☐ **ไม่ผ่าน** และต้องการให้สำนักดิจิทัลเทคโนโลยีเข้าช่วยหรือให้คำปรึกษา

ส่วนที่ 2: เว็บไซต์ WordPress (เลือก "ไม่เกี่ยวข้อง" หากไม่ได้ใช้ WordPress)

☐ **ผ่าน** (ไม่พบ Plugins/Themes ที่มีช่องโหว่ และ WordPress เป็นเวอร์ชันปัจจุบัน)

☐ **ไม่ผ่าน** และต้องการให้สำนักดิจิทัลเทคโนโลยีเข้าช่วยหรือให้คำปรึกษา

☐ **ไม่เกี่ยวข้อง** (ไม่ได้ใช้ WordPress)

ส่วนที่ 3: การสแกนช่องโหว่ด้วย OWASP ZAP

สรุปจำนวนช่องโหว่ที่พบ (ดูจากแท็บ Alerts)

ระดับความรุนแรง (Risk Level)	**จำนวนที่พบ (รายการ)**	**ผลการประเมิน**
Critical / High (ธงสีแดง)	.....	*ต้องเท่ากับ 0 จึงจะผ่าน*
Medium (ธงสีส้ม)	.....	*ควรแก้ไขถ้าทำได้*
Low (ธงสีเหลือง)	.....	*ยอมรับความเสี่ยงได้*
Informational (ธงสีฟ้า)	.....	*ข้อมูลทั่วไป*

การรับรองผลการตรวจสอบ

ข้าพเจ้าขอรับรองว่า เว็บไซต์ดังกล่าวได้รับการตรวจสอบและแก้ไขช่องโหว่ระดับ High และ Critical จนหมดสิ้นแล้ว พร้อมกันนี้ได้แนบเอกสารประกอบมาด้วย ดังนี้:

☐ ภาพหรือไฟล์ภาพหน้าจอผลการตรวจ SSL Labs

☐ ภาพหรือไฟล์ภาพหน้าจอผลการตรวจ WordPress (ถ้ามี)

☐ ไฟล์รายงานฉบับเต็มจาก OWASP ZAP (PDF/HTML)

ลงชื่อ .....

(.....)

ผู้ตรวจสอบ/ผู้ดูแลเว็บไซต์

ตำแหน่ง .....