



**BUREAU OF DIGITAL
TECHNOLOGY**

WEBSITE SECURITY SCAN

การสแกนความปลอดภัยเว็บไซต์ของหน่วยงาน
ผ่านเครื่องมืออัตโนมัติและการแก้ปัญหาเบื้องต้น

LECTURER :

2LT BANPOT DOLWITHAYAKUL, PH.D

- NCSA CERTIFIED – ETHICAL HACKER (CEH)
- NCSA CERTIFIED – WEB SECURITY (V1.0)
- NCSA CERTIFIED – CYBERSECURITY RESILIENCE



LINE OPEN CHAT



เนื้อหาวันนี้

เนื้อหา 6 ด้านที่เราจะมาคุยกันในวันนี้

01

ประเภทภัยคุกคามเว็บ
ที่โดนบ่อย

03

การป้องกันภัยคุกคาม
ที่โดนบ่อย

05

การแก้ปัญหาเบื้องต้น
ด้วยตนเอง

02

การทำงานเชิงรุก
สำนักดิจิทัลฯ

04

การใช้เครื่องมือสแกน
ZAP และ WP-SCAN

06

แผนด้านความปลอดภัย
เว็บของสำนักดิจิทัล

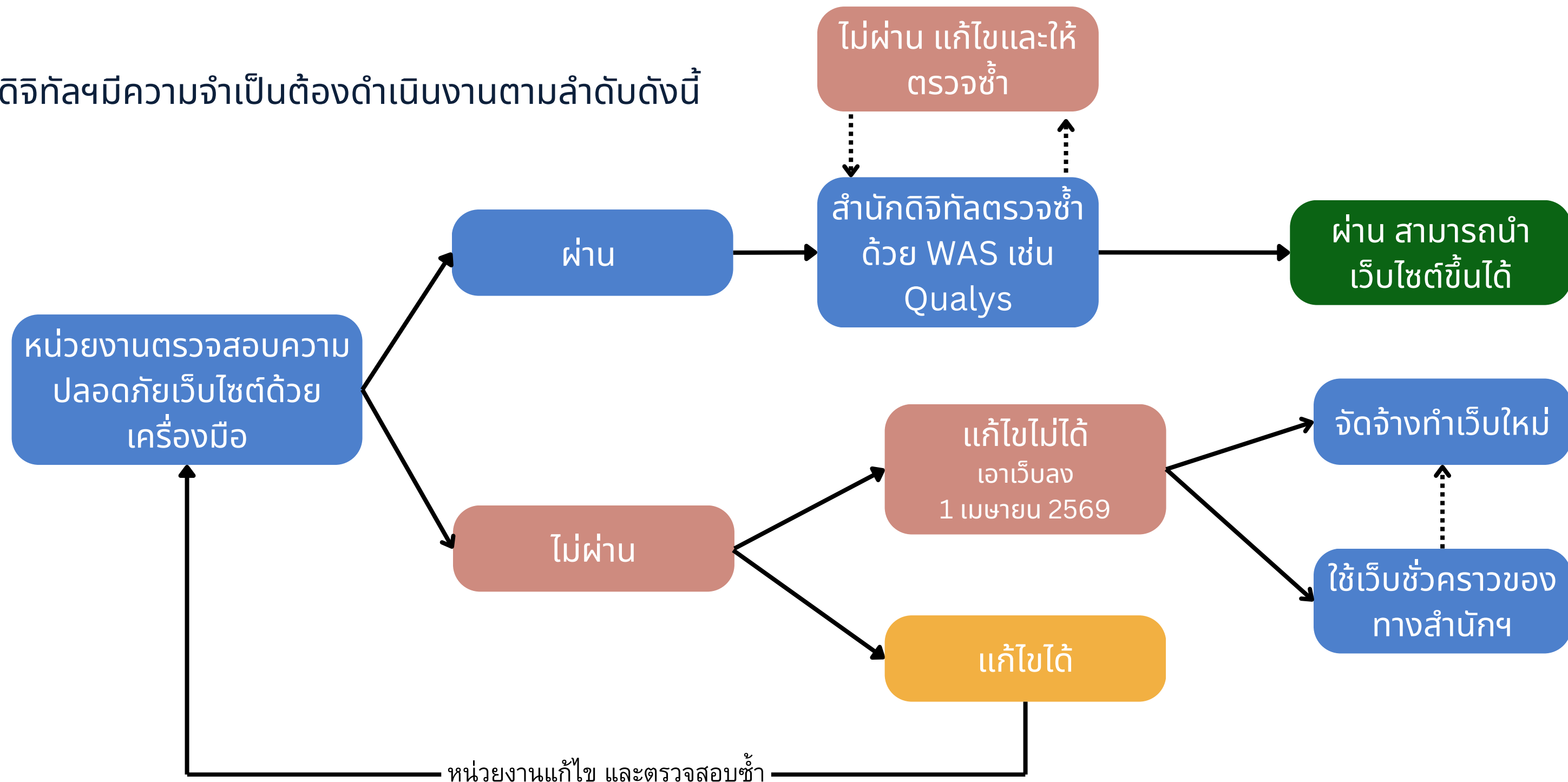
ทำไมถึงนัดวันนี้

- พรบ. ความปลอดภัยเว็บไซต์จะมีผลสิ้นเดือน มีนาคมนี้
- พรบ. PDPA เริ่มเอาจริงในการปรับเงิน กับหน่วยงานต่างๆ
- มหาวิทยาลัย (และหน่วยงานรัฐ) เป็นเป้าหมายแรกๆ ของแฮกเกอร์
- เว็บไซต์มหาวิทยาลัยโดนกันรายวัน
- มีความเชื่อมโยงกับแก๊ง Call Center ที่ระบอบในปัจจุบัน



ลำดับการดำเนินการให้สอดคล้องกับ พรบ. ความปลอดภัยเว็บไซต์

สำนักดิจิทัลฯมีความจำเป็นต้องดำเนินงานตามลำดับดังนี้



ภัยคุกคามที่โดน กันบ่อยที่สุดของ M.เรา



SEO POISONING

คั่นผ่าน Search Engine แล้วขึ้นเป็นเว็บ
อื่น หรือคลิกผ่าน Search Engine แล้ว
เป็นเว็บพนัน ฯลฯ



BACKDOOR / MALWARE

พยายามเข้าเครื่องและติดตั้งโปรแกรม
ลงบนเครื่อง อาจมีการพยายาม scan
เครื่องอื่นในวงเพื่อกระจายต่อ



SQL INJECTION

พยายามฉีดด้วยโค้ด SQL ลงอินพุตเพื่อส่ง
ไป execute คำสั่งบนเซิร์ฟเวอร์ อาจทำให้
แฮกเกอร์เข้าถึงฐานข้อมูลได้ทั้งหมด



DDOS ATTACK

แฮกเกอร์พยายามใช้เครื่องจำนวนมาก
เข้ามาเดารหัสผ่าน หรือเข้าเว็บพร้อมๆกัน
เพื่อให้เว็บล่ม



DATA LEAK

แฮกเกอร์พยายามดึงข้อมูล รหัสผ่าน
รายละเอียดผู้ใช้ และ เอกสารต่างๆจาก
เครื่องออกมา และขายในตลาดมืด

SEO POISONING

อาการ

- คืบใน Google แต่ลิงก์ไปอีกเว็บหนึ่ง หรือคำอธิบายเว็บเป็นเว็บพนัน

สาเหตุ

- แฮกเกอร์เข้าถึงเครื่องและวางไฟล์บางอย่างเพื่อหลอก Search Engine ให้ Redirect
- PHP, JS หรือ .htaccess ถูกแก้ไข
- ไฟล์ใหม่คล้ายของเดิม
- ใช้ eval(), base64_decode(), gzinflate()
- CMS เช่น Wordpress, Joomla มีช่องโหว่



SEO POISONING

Home / All / Images / Music / Shopping / News / Specials / More / More



Silpakorn University

<https://suric.su.ac.th> · [Translate this page](#) · [More](#)

บาคาร่าออนไลน์ SA Gaming เว็บตรง Pretty Gaming ไม่ผ่านเอเยนต์ ...

บาคาร่าออนไลน์ คือศูนย์รวมเกมบาคาร่าที่ดีที่สุดในปี 2026 ครบครันด้วยค่ายดังระดับโลก อาทิ - SA Gaming, - Pretty Gaming, - Sexy Baccarat, - AG Baccarat และอีกมากมาย เล่นผ่านมือถือได้ทุกที่ทุกเวลา ... [Read more](#)



Silpakorn University

<https://macicenter-music.su.ac.th> · [Translate this page](#) · [More](#)

GTS89 บาคาร่า สล็อต

GTS89 เว็บบาคาร่าออนไลน์ และ เว็บสล็อตออนไลน์ เว็บตรงไม่ผ่านเอเยนต์ ให้บริการ บาคาร่า จากค่ายดังระดับโลก SA Gaming, Sexy Baccarat, Dream Gaming, WM Casino มาพร้อมระบบฝาก-ถอน ... [Read more](#)



สาธิตศิลปากร

<http://www.satit.su.ac.th> · [Translate this page](#) · [More](#)

สาธิตศิลปากร: ศูนย์วิเคราะห์กีฬา & สล็อตเชิงสถิติ | ทดลองสล็อตฟรี ...

ศูนย์วิเคราะห์เชิงสถิติด้านกีฬาและสล็อต นำเสนอการทดลองสล็อตฟรีในเชิงการเรียนรู้ อธิบายความน่าจะเป็น, RTP, RNG และการจัดการความเสี่ยง เพื่อการศึกษาและการตัดสินใจอย่างมีเหตุผล อัปเดต 2026.

ตัวอย่างเว็บหน่วยงานที่โดนแล้วจริงๆ

SEO POISONING

การป้องกันและแก้ไข

- ถ้าไม่ใช้ .htaccess ให้ปิด โดยกำหนด AllowOverride เป็น None ได้ในระดับ VirtualHost
- เพิ่ม Header เพื่อเป็นเกราะป้องกัน จำนวน 4 ตัว (ดูในไฟล์ที่แจก)
- อย่าลืมเช็ค Config และ Reboot Apache หลังดำเนินการเสร็จ
- ปิดฟังก์ชันอันตรายใน php.ini
- ตรวจสอบเนื้อหาไฟล์สม่ำเสมอ (อย่างน้อยทุก 3-6 เดือน)
- ระงับการใช้งาน CMS เช่น Wordpress



HEADER CHECK

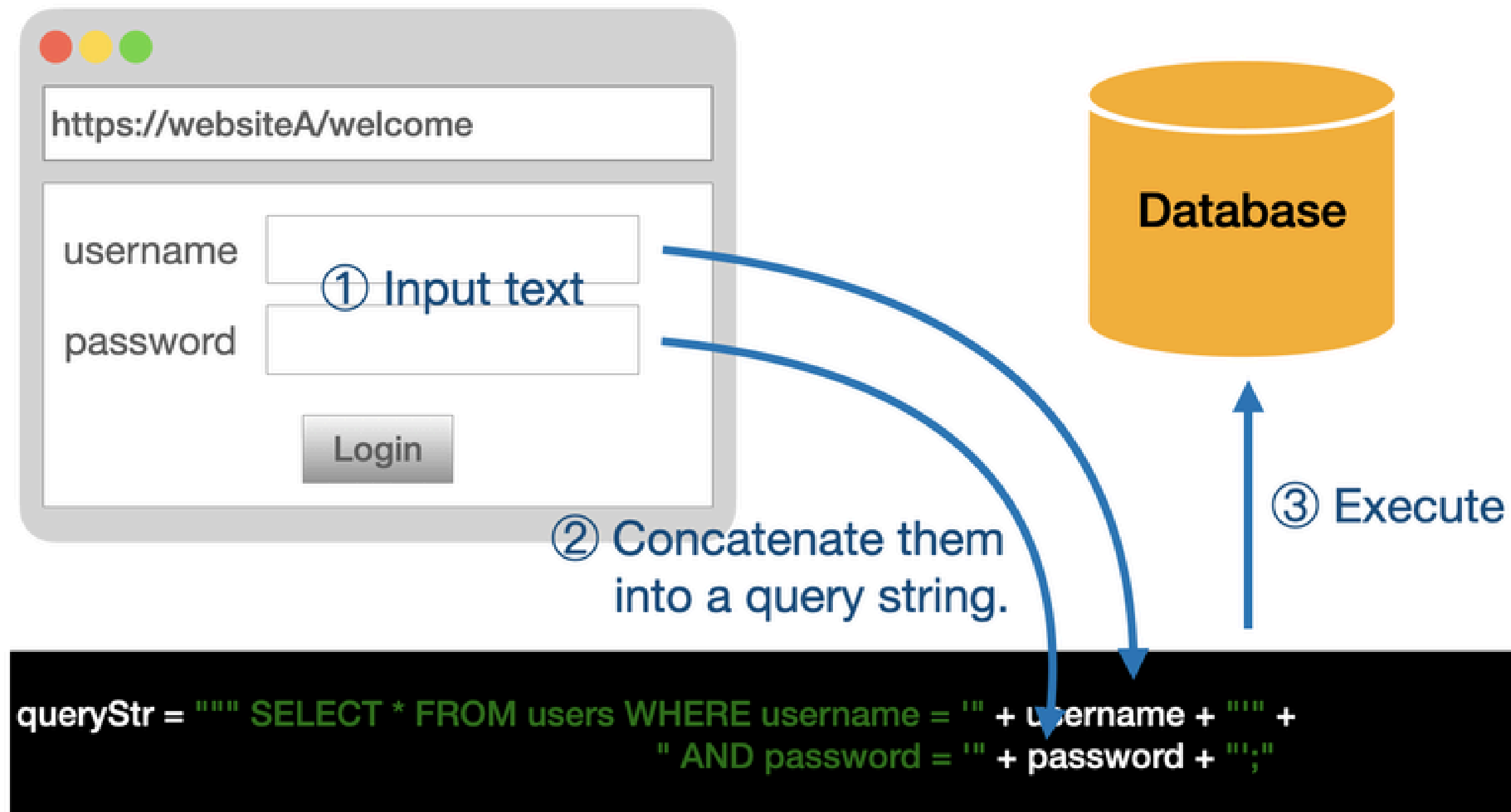
```
[banpot@centos-s-waterbill ~]$ curl -I https://www.su.ac.th
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 03 Feb 2026 08:54:32 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 110
Connection: keep-alive
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Last-Modified: Tue, 30 Dec 2025 08:37:20 GMT
ETag: "6e-6472744951b3c"
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

CONTENT CHECK

```
[banpot@centos-s-waterbill ~]$ cd /var/www/html
[banpot@centos-s-waterbill html]$ grep -R "base64_decode" /var/www
/var/www/html/pppma/composer.lock:         "base64_decode",
/var/www/html/pppma/libraries/classes/Url.php:use function base64_decode;
/var/www/html/pppma/libraries/classes/Url.php:         return $crypto->decrypt(base64_decode(strtr($query, '-_', '+/')));
/var/www/html/pppma/libraries/classes/Navigation/NavigationTree.php:use function base64_decode;
/var/www/html/pppma/libraries/classes/Navigation/NavigationTree.php:
$path[$key] = base64_decode($value);
/var/www/html/pppma/libraries/classes/Plugins/Auth/AuthenticationCookie.php:use function base64_decode;
/var/www/html/pppma/libraries/classes/Plugins/Auth/AuthenticationCookie.php:
        base64_decode($data['iv'])
/var/www/html/pppma/libraries/classes/Plugins/Auth/AuthenticationCookie.php:
        $cipher->setIV(base64_decode($data['iv']));
/var/www/html/pppma/libraries/classes/Plugins/Auth/AuthenticationCookie.php:
        $result = $cipher->decrypt(base64_decode($data['payload']));
/var/www/html/pppma/libraries/classes/Plugins/Auth/AuthenticationHttp.php:use function base64_decode;
/var/www/html/pppma/libraries/classes/Plugins/Auth/AuthenticationHttp.php:
        $usr_pass = base64_decode(substr($this->user, 6));
```

ตัวอย่างเว็บหน่วยงานที่โดนแล้วจริงๆ

SQL INJECTION



ถ้าใส่รหัสผ่านเป็น " OR 1=1 --' "

จะได้QUERYSTR = "" SELECT * FROM USERS WHERE USERNAME = 'JACK' AND PASSWORD = " OR 1= 1 --';"

SQL INJECTION

อาการ

- มักเชื่อมโยงกับการถูกขโมยข้อมูลในฐานข้อมูลออกไป และการทำผิด พรบ. PDPA
- อาจพบอักขระแปลกๆ ในบางตารางบนฐานข้อมูล แสดงว่าโดนโจมตีสำเร็จแล้ว

สาเหตุ

- ไม่มีการ Sanitize Input ก่อนเข้าระบบ หรือยัง Sanitize ไม่ดีพอ
- แนวการเขียน PHP ยังเป็นแบบเก่าอยู่ (ไม่มี prepare)
- เวอร์ชัน PHP หรือ MySQL เก่าเกินไป



SQL INJECTION + XSS

```
←T→ USER_ID
 แก้ไข  คัดลอก  ลบ
 แก้ไข  คัดลอก  ลบ !(&&!|*|
 แก้ไข  คัดลอก  ลบ "%>dfb<%=98991*97996%>xca
 แก้ไข  คัดลอก  ลบ "%}dfb{{98991*97996}}xca
 แก้ไข  คัดลอก  ลบ ")dfb@(98991*97996)xca
 แก้ไข  คัดลอก  ลบ "+A".concat(70-3).concat(22*4).concat(103).concat...
 แก้ไข  คัดลอก  ลบ "+A".concat(70-3).concat(22*4).concat(106).concat...
 แก้ไข  คัดลอก  ลบ "+A".concat(70-3).concat(22*4).concat(107).concat...
 แก้ไข  คัดลอก  ลบ "+response.write(9258439*9224371)+"
 แก้ไข  คัดลอก  ลบ "+response.write(9732219*9234094)+"
 แก้ไข  คัดลอก  ลบ "+response.write(9912373*9292660)+"
 แก้ไข  คัดลอก  ลบ ".gethostbyname(lc("hitfv"."dbgqlpqm291f8.bxss.me....
 แก้ไข  คัดลอก  ลบ ".gethostbyname(lc("hittk"."phxzisql9153f.bxss.me....
 แก้ไข  คัดลอก  ลบ ".gethostbyname(lc("hitub"."hheybxgf02f59.bxss.me....
 แก้ไข  คัดลอก  ลบ "98991*97996*98991*97996
 แก้ไข  คัดลอก  ลบ ";print(md5(31337));$a="
 แก้ไข  คัดลอก  ลบ "dfb__${98991*97996}__::x
 แก้ไข  คัดลอก  ลบ "print("dfb" . 98991*97996 . "xca");
 แก้ไข  คัดลอก  ลบ "}dfbzxxxxzzzbbccccdddeexca".replace("z","o")
 แก้ไข  คัดลอก  ลบ "}#{98991*97996*98991*97996}
 แก้ไข  คัดลอก  ลบ "}dfb#set($x=98991*97996)${x}xca
 แก้ไข  คัดลอก  ลบ "}dfb#{98991*97996}xca
 แก้ไข  คัดลอก  ลบ "}dfb#{xca}=123
```

ถูกใส่สคริปต์ JAVA SCRIPT เพื่อทำ XSS

SQL INJECTION

การป้องกันและแก้ไข

- ใช้ SQL Prepare Statement เพื่อความปลอดภัย (PHP 7+)
- อัปเดตเป็น PHP เวอร์ชันล่าสุด (8.3+)
- หมั่นตรวจสอบข้อมูลในตารางคร่าวๆ เป็นระยะ
- ไม่เก็บรหัสผ่านที่ไม่ได้ถูกเข้ารหัส ควรเข้าด้วย SHA-256 หรืออย่างน้อย PASSWORD() และ MD5/SHA (ไม่ค่อยปลอดภัยแล้ว)
- กรองข้อมูลใน GET และ POST request เสมอ
- ปิดการแสดงผล Error ของสคริปต์บน Server เมื่อเป็น Production แล้ว



SQL INJECTION

```
<?php
$conn = mysqli_connect("localhost", "root", "password", "testdb");

$username = $_POST['username'];
$password = $_POST['password'];

$sql = "SELECT * FROM users
      WHERE username = '$username'
      AND password = '$password'";

$result = mysqli_query($conn, $sql);

if (mysqli_num_rows($result) > 0) {
    echo "Login success";
} else {
    echo "Login failed";
}
```

แบบเก่า ง่ายต่อ INJECTION

```
<?php
$conn = mysqli_connect("localhost", "root", "password", "testdb");

$username = $_POST['username'];
$password = $_POST['password'];

$sql = "SELECT * FROM users WHERE username = ? AND password = ?";

$stmt = mysqli_prepare($conn, $sql);
mysqli_stmt_bind_param($stmt, "ss", $username, $password);
mysqli_stmt_execute($stmt);

$result = mysqli_stmt_get_result($stmt);

if (mysqli_num_rows($result) > 0) {
    echo "Login success";
} else {
    echo "Login failed";
}
```

แบบใหม่ ป้องกัน SQL INJECTION

แผนเชิงรุกของ สำนักดิจิทัลฯ



WEB APPLICATION FIREWALL

หรือ WAF ใช้เทคโนโลยี AI เพื่อตรวจจับ
คาดเดาการโจมตีและบล็อกการเข้าถึง
เว็บ แบบไม่เหมาะสม



การสแกนเชิงรุก

ส่งเจ้าหน้าที่สำนัก ออกไปตามคณะต่างๆ
เพื่อสอนการสแกน การลงโปรแกรมสแกน
และการจัดการช่องโหว่ต่างๆ



การอัปเดตเซิร์ฟเวอร์ครั้งใหญ่

สำนักทยอยย้ายหรืออัปเดตเซิร์ฟเวอร์
จำนวนมากที่ใช้ OS ที่ End-of-Life และ
Wordpress ที่เวอร์ชันเก่า



NEXT-GEN FIREWALL

เป็น Firewall รุ่นใหม่ ไม่ใช่ Signature แต่ใช้
Machine Learning และ Deep Learning คัด
กรองพฤติกรรมผู้ใช้ปกติและแฮกเกอร์



ACTIVE WEB SCAN

สำนักจัดซื้อซอฟต์แวร์สแกนระดับสูง
เช่น Qualys เพื่อสแกนช่องโหว่เว็บไซต์
และเร่งเตือนหน่วยงานหากมีช่องโหว่

การเตรียมตัว

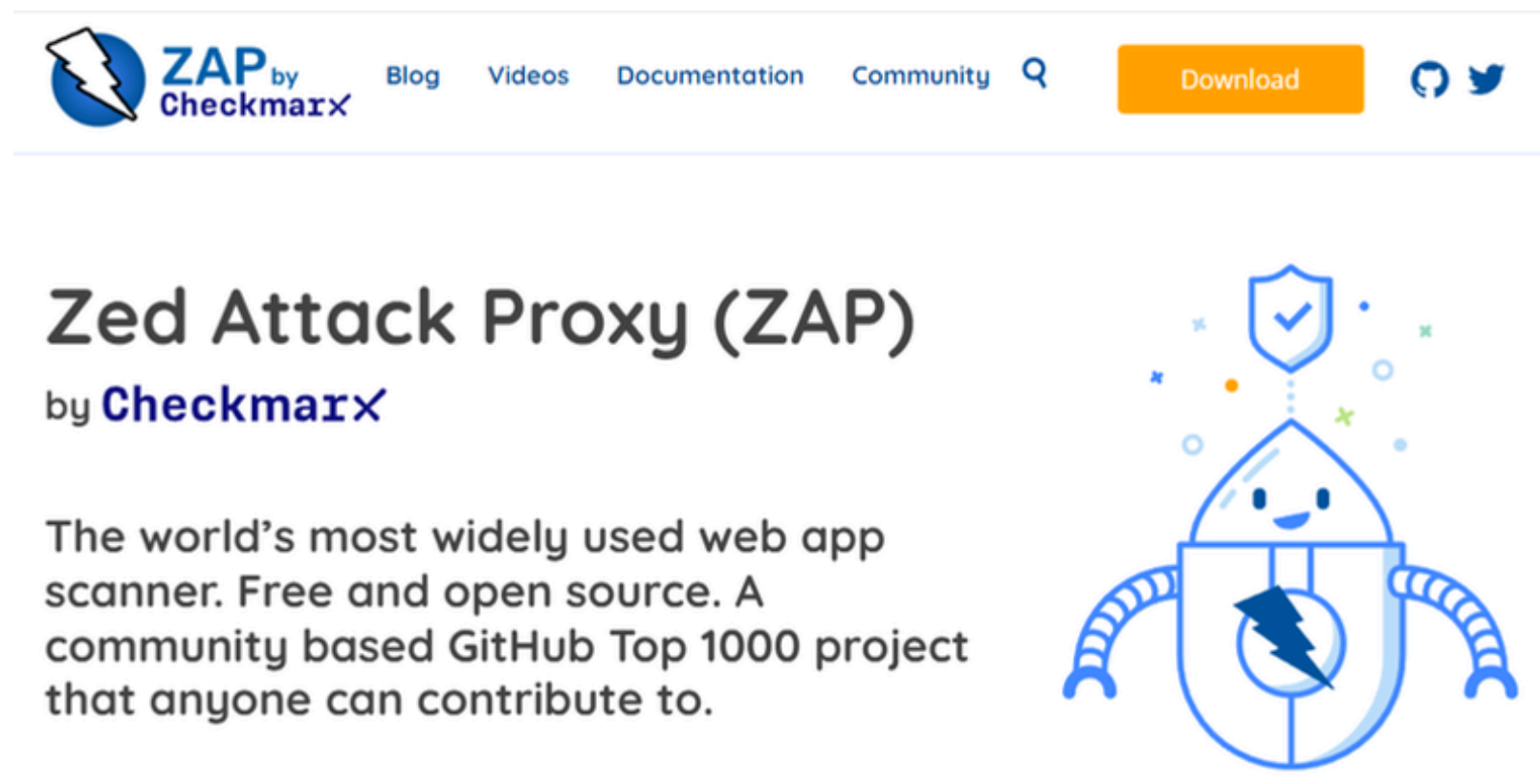
- การเตรียมตัวก่อนสแกนความปลอดภัย
 - ขออนุญาต และแจ้งเจ้าของ Server หรือผู้ดูแลเซิร์ฟเวอร์ให้ทราบเป็นลายลักษณ์อักษร
 - เลือกเวลาที่คาดว่าคนใช้เซิร์ฟเวอร์ไม่มาก
 - สำรองข้อมูลถ้าเป็นไปได้
 - ใช้เครื่องคอมพิวเตอร์หน่วยความจำอย่างน้อย 16GB
 - ใช้สาย LAN ความเร็วอย่างน้อย 1Gbps เพื่อความรวดเร็ว (ไม่แนะนำ WiFi)



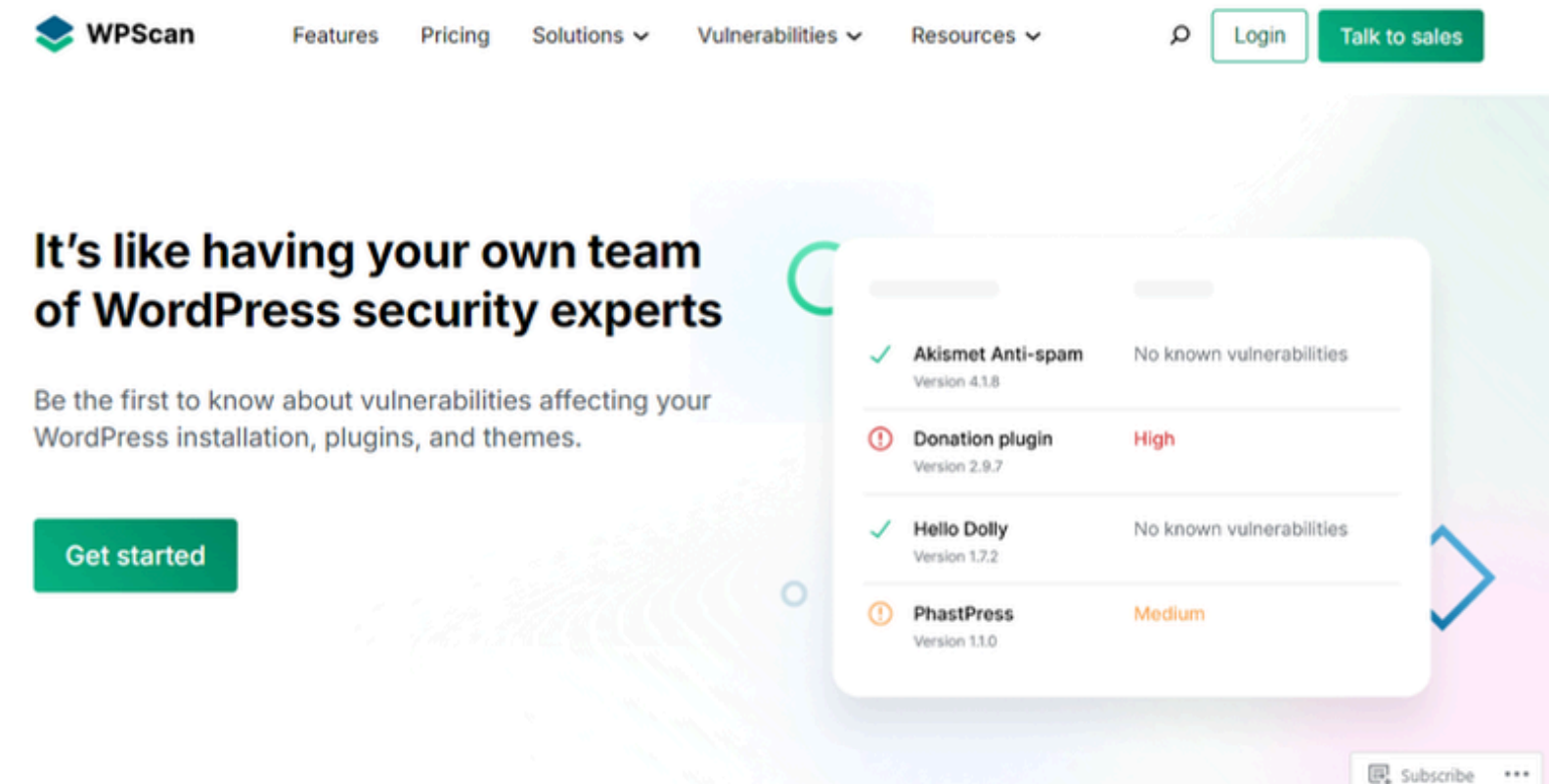
การสแกนช่องโหว่เบื้องต้น

ทางสำนักดิจิทัลฯ แนะนำ 3 เครื่องมือในการสแกนเว็บไซต์เบื้องต้น คือ

- **Zed Attack Proxy (ZAP)** ดาวน์โหลดที่ <https://www.zaproxy.org/>
- **WP-Scan** (สำหรับเว็บไซต์ที่ใช้ WordPress) ที่ <https://hackertarget.com/wordpress-security-scan/>
- **Qualys SSL Labs** ที่ <https://www.ssllabs.com/ssltest/>



The screenshot shows the ZAP website homepage. At the top, there is a navigation bar with the ZAP logo (a lightning bolt in a circle) and the text "ZAP by CheckmarX". To the right of the logo are links for "Blog", "Videos", "Documentation", and "Community", followed by a search icon and a yellow "Download" button. Below the navigation bar, the main heading reads "Zed Attack Proxy (ZAP) by CheckmarX". To the right of the heading is a cartoon robot character with a shield on its head and a lightning bolt on its chest. Below the heading, the text states: "The world's most widely used web app scanner. Free and open source. A community based GitHub Top 1000 project that anyone can contribute to."

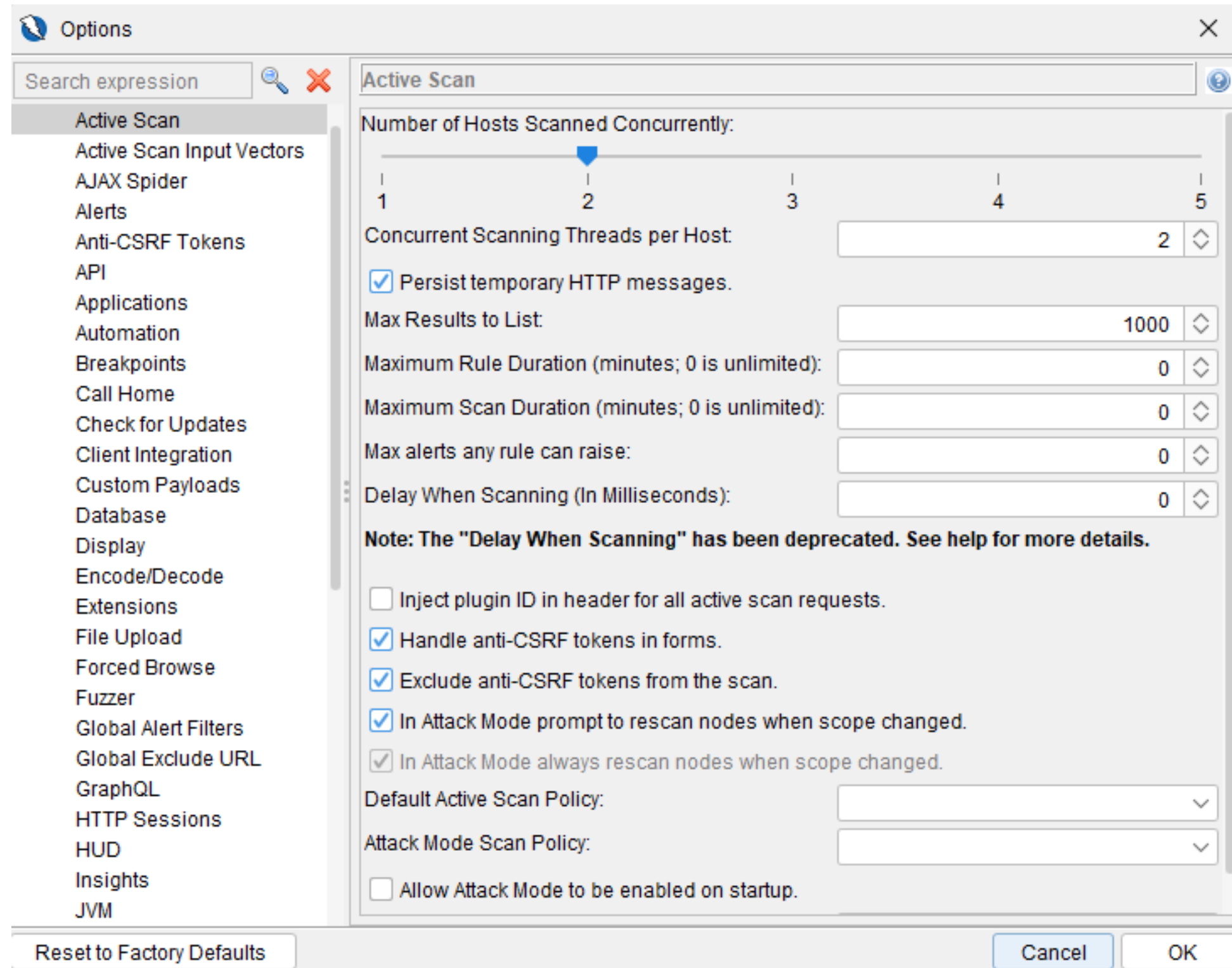


The screenshot shows the WPScan website homepage. At the top, there is a navigation bar with the WPScan logo (a green shield) and the text "WPScan". To the right of the logo are links for "Features", "Pricing", "Solutions", "Vulnerabilities", and "Resources", followed by a search icon, a "Login" button, and a "Talk to sales" button. Below the navigation bar, the main heading reads "It's like having your own team of WordPress security experts". Below the heading, the text states: "Be the first to know about vulnerabilities affecting your WordPress installation, plugins, and themes." Below this text is a green "Get started" button. To the right of the heading is a screenshot of the WPScan interface showing a list of plugins and their vulnerability status. The list includes:

Plugin	Version	Vulnerability Status
Akismet Anti-spam	Version 4.1.8	No known vulnerabilities
Donation plugin	Version 2.9.7	High
Hello Dolly	Version 1.7.2	No known vulnerabilities
PhastPress	Version 1.1.0	Medium

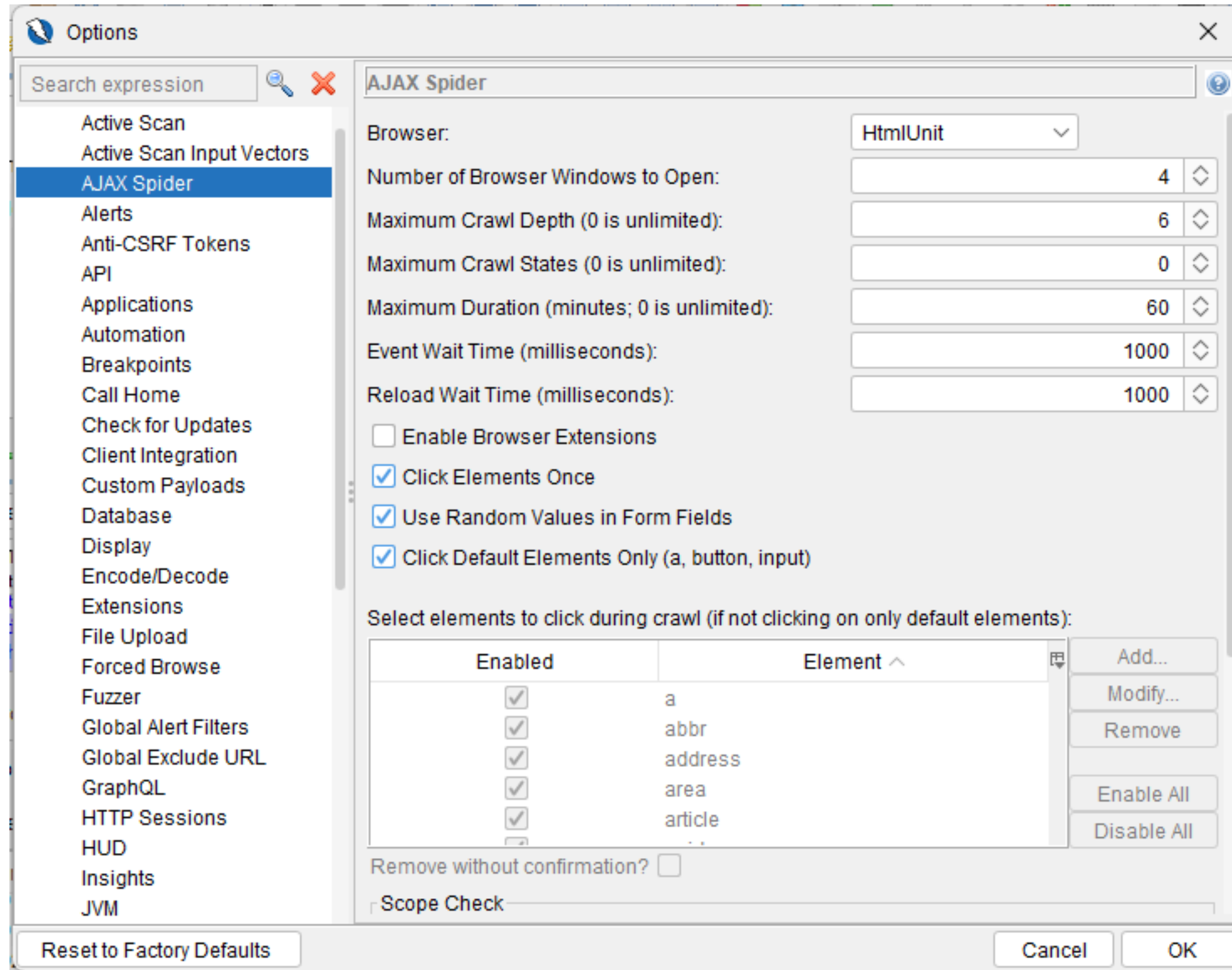
At the bottom right of the screenshot, there is a "Subscribe" button.

ตั้งค่าสำหรับ ZAP



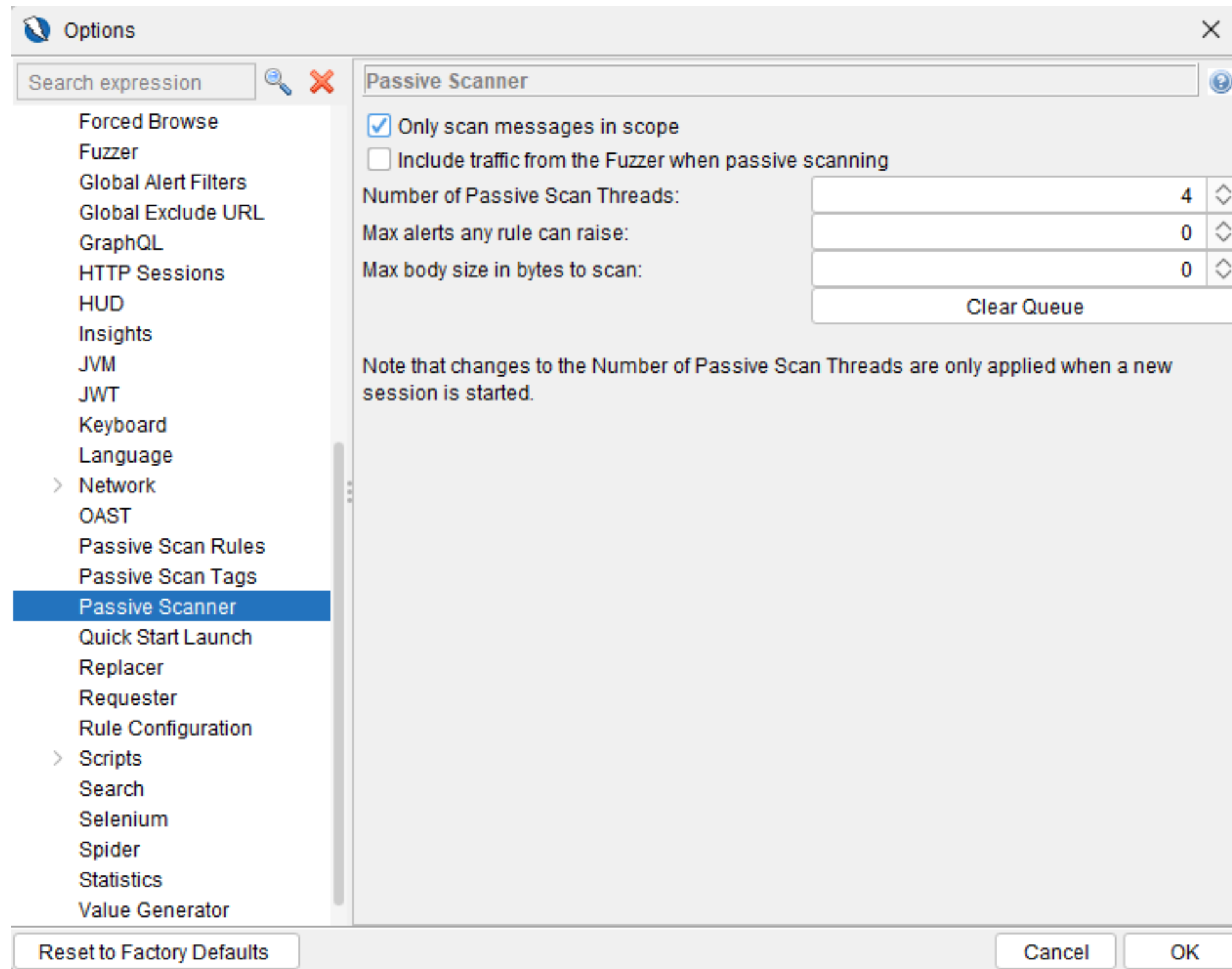
ลดการประมวลผล และลดหน่วยความจำ

ตั้งค่าสำหรับ ZAP



ลดหน่วยความจำที่ใช้

ตั้งค่าสำหรับ ZAP



ลดหน่วยความจำและ CPU ที่จะใช้

ปัญหาการสแกนที่พบบ่อย

ปัญหาที่พบบ่อย #1

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page – covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

สาเหตุและวิธีการแก้ไข

เว็บสมัยใหม่ และเบราว์เซอร์สมัยใหม่มีระบบความปลอดภัย เรียกว่า CSP ซึ่งต้องกำหนดใน HEADER แต่ไม่ได้กำหนด

ใช้เพื่อป้องกัน CROSS-SITE SCRIPTING

เพิ่ม HEADER จากไฟล์ HEADER.TXT ที่แจกให้ในกลุ่ม

หลังเพิ่มทดสอบเรียก `CURL -I HTTPS://.....` และดูว่ามีเพิ่ม

ปัญหาที่พบบ่อย #2

The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options

สาเหตุและวิธีการแก้ไข

เว็บสมัยใหม่ และเบราว์เซอร์สมัยใหม่มีระบบความปลอดภัย เรียกว่า CSP ซึ่งต้องกำหนดใน HEADER แต่ไม่ได้กำหนด

ใช้เพื่อป้องกัน CLICKJACKING

เพิ่ม HEADER ดูกจากไฟล์ HEADER.TXT ที่แจกให้ในกลุ่ม

หลังเพิ่มทดสอบเรียก
CURL -I HTTPS://..... และดูว่ามีเพิ่ม

ปัญหาที่พบบ่อย #3

The identified library appears to be vulnerable
eg.

<https://xxxxx.su.ac.th/js/jquery.min.js>

หรือ

Vulnerable JS Library

The identified library appears to be vulnerable.

<https://xxxxxx.su.ac.th/app-assets/vendors/js/pickers/dateTime/moment-with-locales.min.js>

สาเหตุและวิธีการแก้ไข

ไลบรารี JAVASCRIPT เก่าเกินไปและพบว่าเวอร์ชันที่ใช้งานอยู่มีช่องโหว่ให้ทำการโจมตีได้

สำรองข้อมูลโค้ดเว็บทั้งหมด และดาวน์โหลด JAVASCRIPT ตัวใหม่

อัปเดตกับตัวเก่า และตรวจสอบดูว่าเว็บไซต์ยังทำงานได้ตามปกติอยู่หรือไม่

ปัญหาที่พบบ่อย #4

The integrity attribute is missing on a script or link tag served by an external server. The integrity tag prevents an attacker who have gained access to this server from injecting a malicious content.

สาเหตุและวิธีการแก้ไข

ตัว JAVASCRIPT ไม่มีการตรวจ HASH ทำให้แฮกเกอร์มีโอกาส REDIRECT หรือไปถึง JS จากที่อื่นมารันบนเว็บไซต์ได้

เพิ่ม ATTRIBUTE INTEGRITY เมื่อมีการ INCLUDE ไฟล์จาก REMOTE ทุกครั้ง

ใช้เครื่องมือจาก
[HTTPS://SRIHASH.ORG/](https://srihash.org/)
[HTTPS://CDNJS.COM/LIBRARIES/SRI-GENERATOR](https://cdnjs.com/libraries/sri-generator)

ปัญหาที่พบบ่อย #5

Hidden file found

A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts

https://xxxxxx.su.ac.th/.DS_Store

สาเหตุและวิธีการแก้ไข

เกิดจากมีไฟล์เดออร์หรือไฟล์สำคัญระหว่างการพัฒนาที่อาจเปิดเผยโค้ด ถูกอัปโหลดพร้อมเว็บไซต์มาด้วย

ตรวจสอบชื่อไฟล์และลบไฟล์ตามที่แจ้งออก
จากเซิร์ฟเวอร์

ปัญหาที่พบบ่อย #6

Absence of Anti-CSRF Tokens

cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL /form actions in a

สาเหตุและวิธีการแก้ไข

- เว็บไซต์มีฟอร์มหรือ URL ที่ไม่มีตัวตรวจสอบว่าเป็นคำสั่งจากผู้ใช้จริง

- ผู้ไม่หวังดีสามารถหลอกให้ผู้ใช้ที่ LOGIN อยู่ ส่งคำสั่งแทนตนเองได้โดยไม่รู้ตัว (CSRF)

- วิธีการง่ายสุดคือสร้าง RANDOM_STRING ในทุกหน้าที่มีแบบฟอร์ม ดูใน CSRF.TXT

ปัญหาที่พบบ่อย #7

HTTP to HTTPS Insecure Transition in Form Post
หรือ

Secure Pages Include Mixed Content

This check looks for insecure HTTP pages that host HTTPS forms. The issue is that an insecure HTTP page can easily be hijacked through MITM and the secure HTTPS form can be replaced or spoofed.

สาเหตุและวิธีการแก้ไข

เกิดจากการเรียกทรัพยากร หรือส่งแบบฟอร์ม จาก HTTPS ไป HTTP ทำให้การเข้ารหัสสูญหายไป

ข้อมูลอาจถูกดักจับกลางทาง

ปรับ ACTION หรือการเรียกภาพ เสียง ไฟล์ ให้ถูกต้อง ต้องมี HTTPS ทุกครั้ง ไม่ใช่ HTTP

การสแกน WORDPRESS

HACKER TARGET SCANNERS ▾ TOOLS ▾ RESEARCH ▾ ASSESSMENTS ▾ ABOUT ▾ ✉

WordPress Analysis and Security Scan

Perform a Free WordPress Security Scan with a **low impact test**.

Check any WordPress based site and get a high level overview of the sites security posture. Once you see how easy it is grab a **membership** and test **WordPress + Server Vulnerabilities** with Nmap WordPress NSE Scripts, Nikto, OpenVAS and more.

Items checked in the FREE scan

- Attempt to detect version of WordPress Core
- Find Plugins & Theme in HTML response
- Attempt to enumerate first 2 WP users
- List page resources including js & iframes
- Test for directory indexing enabled on key locations
- Check Google Safe Browse for reputation

Enter WordPress Site(s) to Test *

Valid Target(s)
www.example.com
https://example.com/
192.16.1.1

WordPress enumeration type

Site Security Overview

[HTTPS://HACKERTARGET.COM/WORDPRESS-SECURITY-SCAN/](https://hackertarget.com/wordpress-security-scan/)


ผลการสแกน WORDPRESS



WordPress Security Analysis

<https://president.su.ac.th/legal/>

This report presents the results of a passive analysis of HTTP responses for the target WordPress site.

 <p>WORDPRESS VERSION</p> <p>5.9.2</p> <p>Version not latest release (6.9)</p> <p>Update Now (see releases)</p>	<p>ISSUES FOUND</p> <p>4</p> <ul style="list-style-type: none">Wordpress version has security vulnerabilitiesPlugin needs updatingCore version not latest release										
<table border="0"><tr><td>Page Title: -</td><td>Web Server: Apache/2.4.58 (Ubuntu)</td></tr><tr><td>Certificate: Silpakorn University - valid to: 2026-06-29</td><td>Shared Hosting: 1 sites found on IP</td></tr><tr><td>TLS 1.2 TLS 1.3</td><td></td></tr><tr><td>IP Address: 202.28.75.126 (202.28.75.0/24)</td><td></td></tr><tr><td>Hosting Provider: UNINET-AS-SU-AP Silpakorn University, TH (AS140618)</td><td></td></tr></table>		Page Title: -	Web Server: Apache/2.4.58 (Ubuntu)	Certificate: Silpakorn University - valid to: 2026-06-29	Shared Hosting: 1 sites found on IP	TLS 1.2 TLS 1.3		IP Address: 202.28.75.126 (202.28.75.0/24)		Hosting Provider: UNINET-AS-SU-AP Silpakorn University, TH (AS140618)	
Page Title: -	Web Server: Apache/2.4.58 (Ubuntu)										
Certificate: Silpakorn University - valid to: 2026-06-29	Shared Hosting: 1 sites found on IP										
TLS 1.2 TLS 1.3											
IP Address: 202.28.75.126 (202.28.75.0/24)											
Hosting Provider: UNINET-AS-SU-AP Silpakorn University, TH (AS140618)											

จะผ่านได้ต้องเป็นสีเขียวเท่านั้น

การสแกน SSL