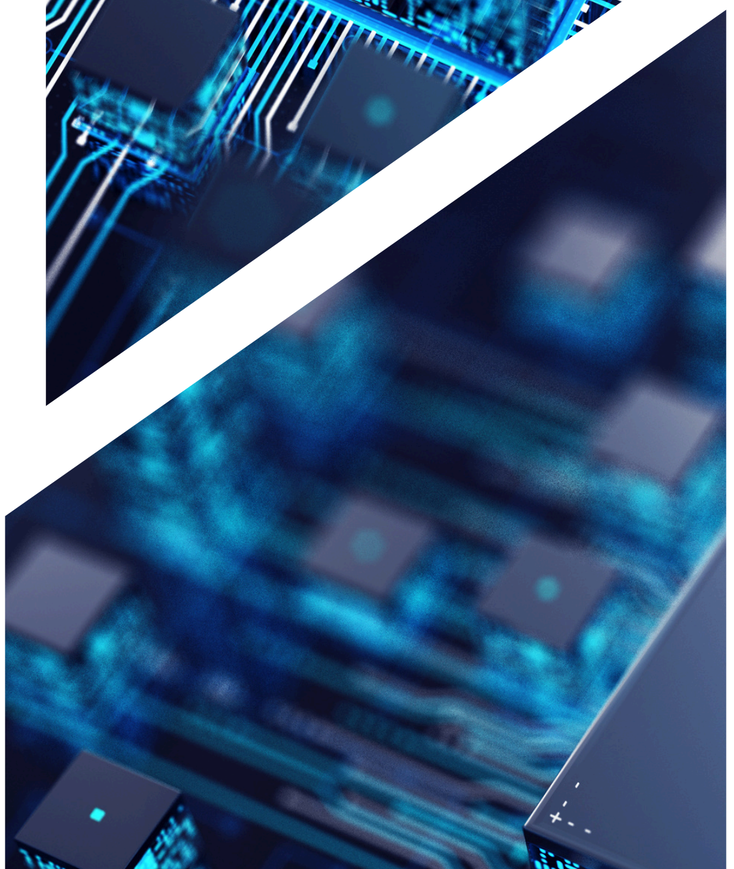
BUREAU OF DIGITAL TECHNOLOGY

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 ประเภทภัยคุกคามเว็บที่โดนบ่อย

02 การทำงานเชิงรุกสำนักดิจิทัลฯ

03 การป้องกันภัยคุกคามที่โดนบ่อย

04 การใช้เครื่องมือสแกน ZAP และ WP-SCAN

05 การแก้ปัญหาเบื้องต้นด้วยตนเอง

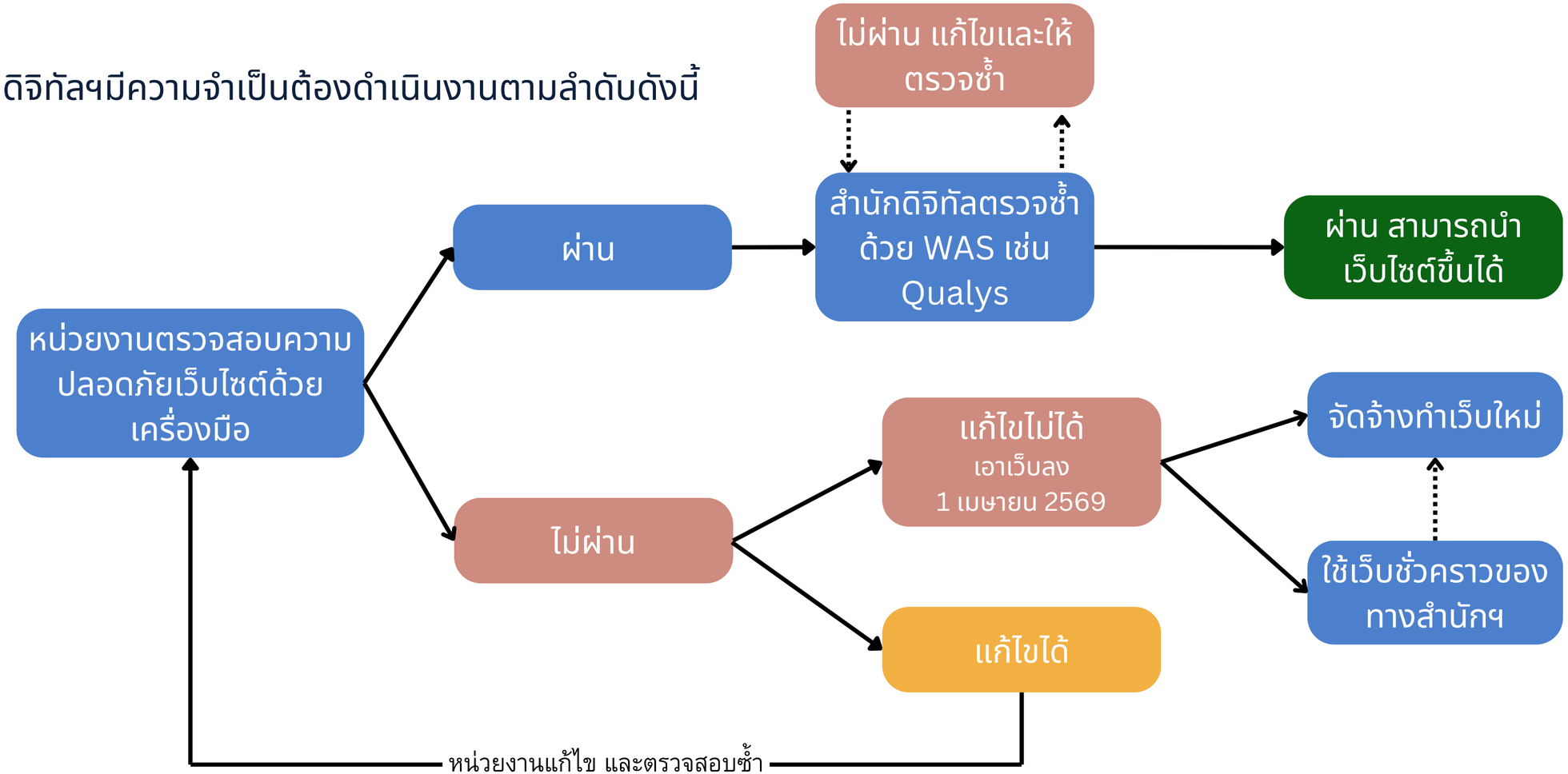
06 แผนด้านความปลอดภัยเว็บของสำนักดิจิทัล

ทำไมถึงนัดวันนี้

- พรบ. ความปลอดภัยเว็บไซต์จะมีผลสิ้นเดือนมีนาคมนี้
- พรบ. PDPA เริ่มเอาจริงในการปรับเงิน กับหน่วยงานต่างๆ
- มหาวิทยาลัย (และหน่วยงานรัฐ) เป็นเป้าหมายแรกๆ ของแฮกเกอร์
- เว็บไซต์มหาวิทยาลัยโดนกันรายวัน
- มีความเชื่อมโยงกับแก๊ง Call Center ที่ระบาดในปัจจุบัน

ลำดับการดำเนินการให้สอดคล้องกับ พรบ. ความปลอดภัยเว็บไซต์

สำนักดิจิทัลฯมีความจำเป็นต้องดำเนินงานตามลำดับดังนี้



ภัยคุกคามที่โดนกันบ่อยที่สุดของ ม.เรา

SEO POISONING

ค้นผ่าน Search Engine แล้วขึ้นเป็นเว็บอื่น หรือคลิกผ่าน Search Engine แล้วเป็นเว็บพนัน ฯลฯ

BACKDOOR / MALWARE

พยายามเข้าเครื่องและติดตั้งโปรแกรมลงบนเครื่อง อาจมีการพยายาม scan เครื่องอื่นในวงเพื่อกระจายต่อ

SQL INJECTION

พยายามฉีดด้วยโค้ด SQL ลงอินพุตเพื่อส่งไป execute คำสั่งบนเซิร์ฟเวอร์ อาจทำให้แฮกเกอร์เข้าถึงฐานข้อมูลได้ทั้งหมด

DDOS ATTACK

แฮกเกอร์พยายามใช้เครื่องจำนวนมากเข้ามาเดารหัสผ่าน หรือเข้าเว็บพร้อมๆกันเพื่อให้เว็บล่ม

DATA LEAK

แฮกเกอร์พยายามดึงข้อมูล รหัสผ่าน รายละเอียดผู้ใช้ และ เอกสารต่างๆจากเครื่องออกมา และขายในตลาดมืด

SEO POISONING

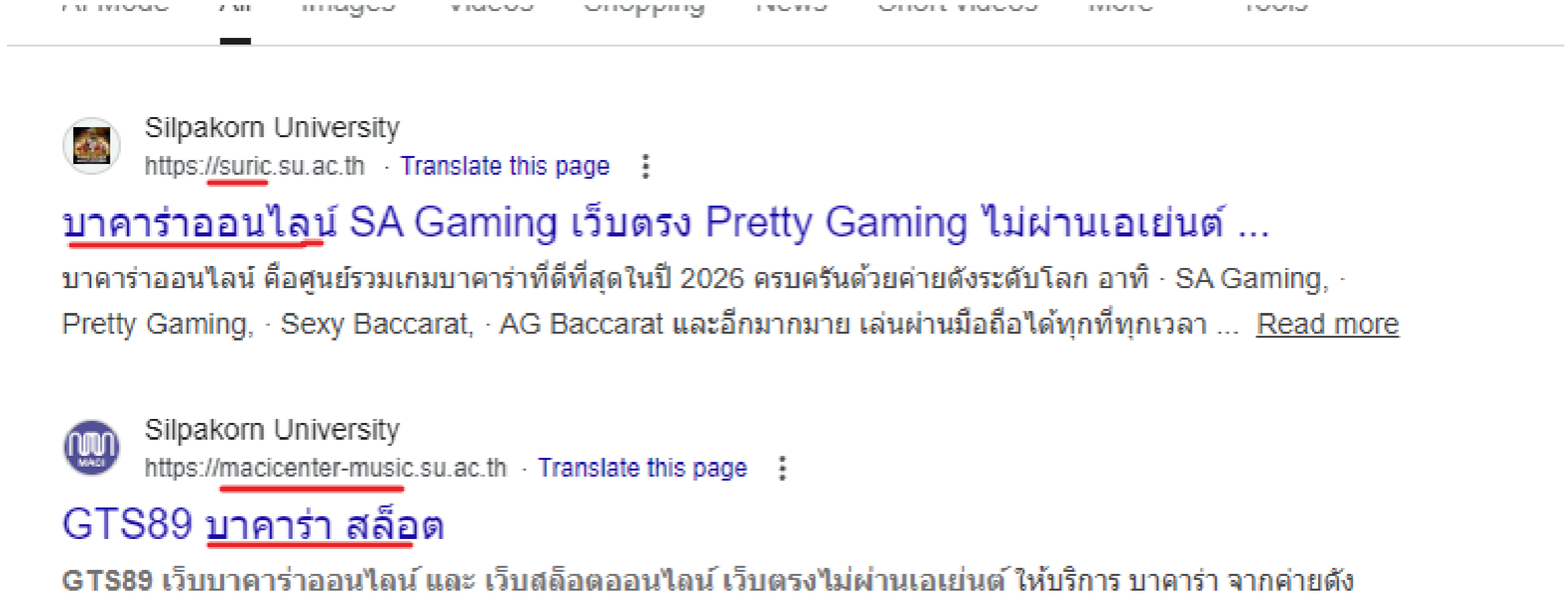
อาการ

- ค้นใน 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



ตัวอย่างเว็บหน่วยงานที่โดนแล้วจริงๆ

SEO POISONING

การป้องกันและแก้ไข

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

HEADER CHECK

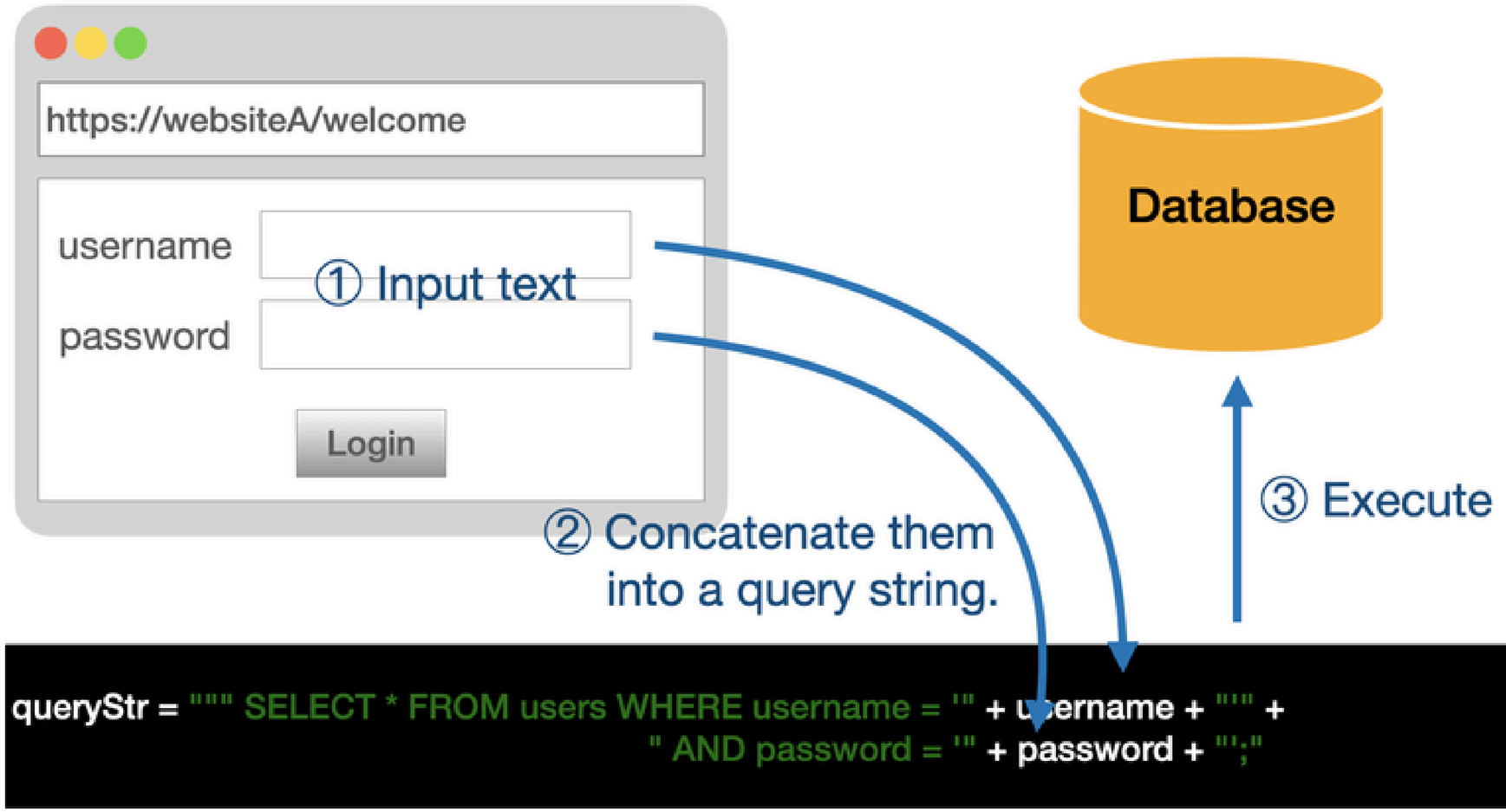
```
[banpot@centos-s-waterbill ~]$ curl -I https://www.su.ac.th
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 03 Feb 2026 08:54:32 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 110
Connection: keep-alive
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
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 $crypto->decrypt(ba
se64_decode(strtr($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 fu
nction 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

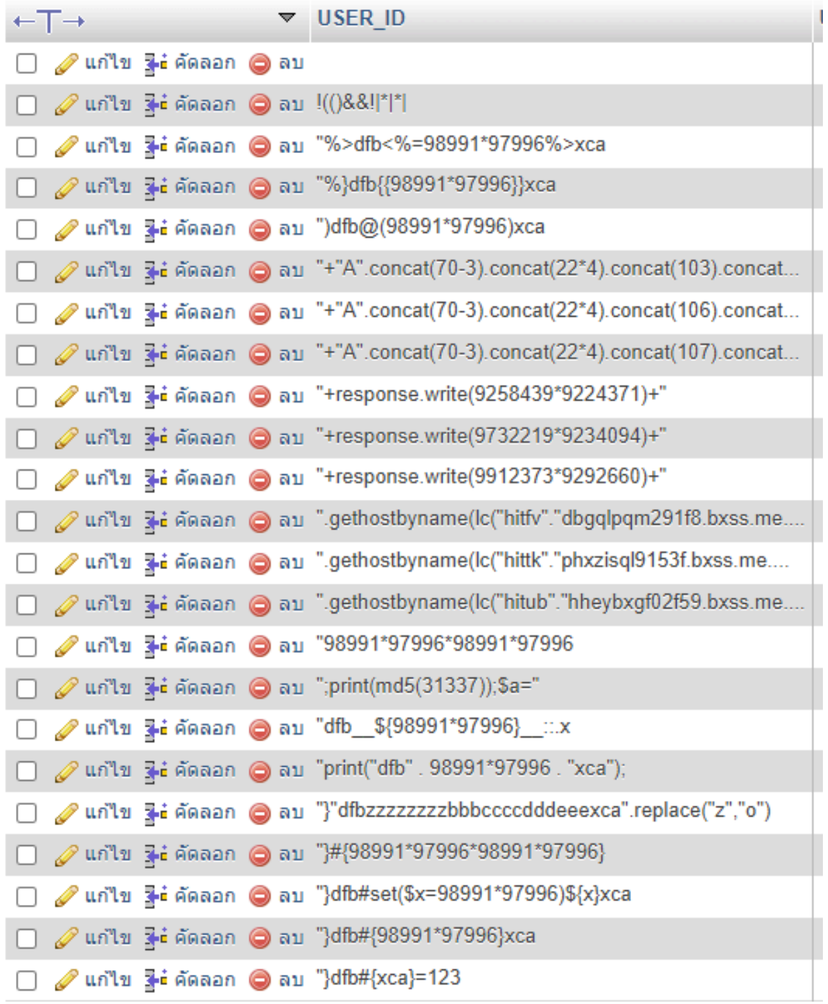
อาการ

- มักเชื่อมโยงกับการถูกขโมยข้อมูลในฐานข้อมูลออกไป และการทำผิด พรบ. PDPA
- อาจพบอักขระแปลกๆ ในบางตารางบนฐานข้อมูล แสดงว่าโดนโจมตีสำเร็จแล้ว

สาเหตุ

- ไม่มีการ Sanitize Input ก่อนเข้าระบบ หรือยัง Sanitize ไม่ดีพอ
- แนวการเขียน PHP ยังเป็นแบบเก่าอยู่ (ไม่มี prepare)
- เวอร์ชั่น 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	"}"dfbzzzzzzzzbbbccccdddeeexca".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+)
- อัพเดทเป็น PHP เวอร์ชั่นล่าสุด (8.3+)
- หมั่นตรวจสอบข้อมูลในตารางคร่าวๆ เป็นระยะ
- ไม่เก็บรหัสผ่านที่ไม่ได้ถูกเข้ารหัส ควรเข้าด้วย SHA-256 หรืออย่างน้อย PASSWORD() และ MD5/SHA (ไม่ค่อยปลอดภัยแล้ว)
- กรองข้อมูลใน GET และ POST request เสมอ
- ปิดการแสดง Error ของสคริปต์บน Server เมื่อเป็น Production แล้ว

SQL INJECTION

```php
<?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
<?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

แผนเชิงรุกของสำนักดิจิทัลฯ

การสแกนเชิงรุก

ส่งเจ้าหน้าที่สำนัก ออกไปตามคณะต่างๆ เพื่อสอนการสแกน การลงโปรแกรมสแกน และการจัดการช่องโหว่ต่างๆ

WEB APPLICATION FIREWALL

หรือ WAF ใช้เทคโนโลยี AI เพื่อตรวจจับคาดเดาการโจมตีและบล็อกการเข้าถึงเว็บ แบบไม่เหมาะสม

การอัพเดทเซิร์ฟเวอร์ครั้งใหญ่

สำนักทยอยย้ายหรืออัพเดทเซิร์ฟเวอร์จำนวนมากที่ใช้ OS ที่ End-of-Life และ Wordpress ที่เวอร์ชั่นเก่า

NEXT-GEN FIREWALL

เป็น Firewall รุ่นใหม่ ไม่ใช้ Signature แต่ใช้ Machine Learning และ Deep Learning คัดกรองพฤติกรรมผู้ใช้ปกติและแฮกเกอร์

ACTIVE WEB SCAN

สำนักจัดซื้อซอฟต์แวร์สแกนระดับสูง เช่น Qualys เพื่อสแกนช่องโหว่เว็บไซต์ และเร่งเตือนหน่วยงานหากมีช่องโหว่

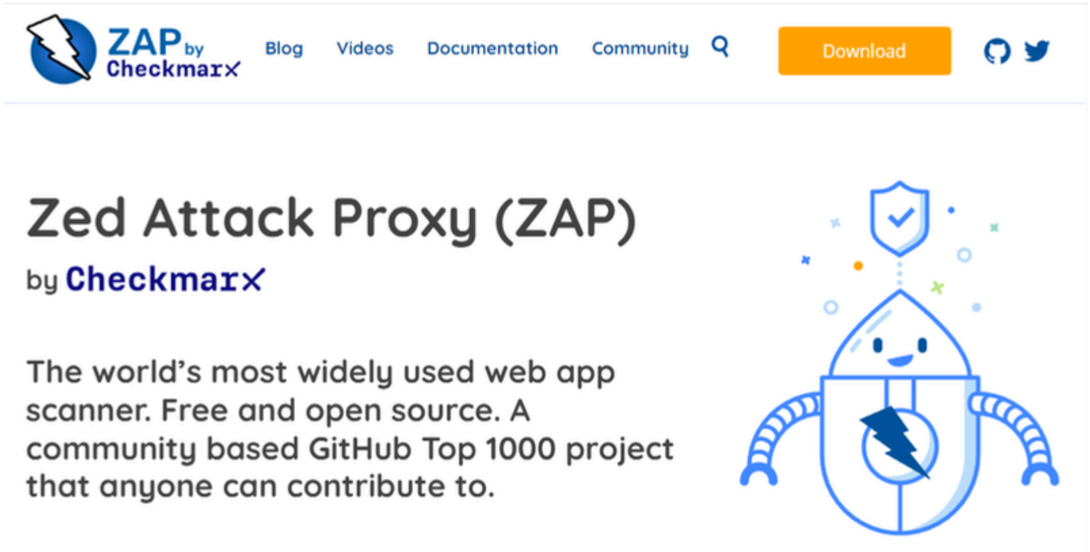
การเตรียมตัว

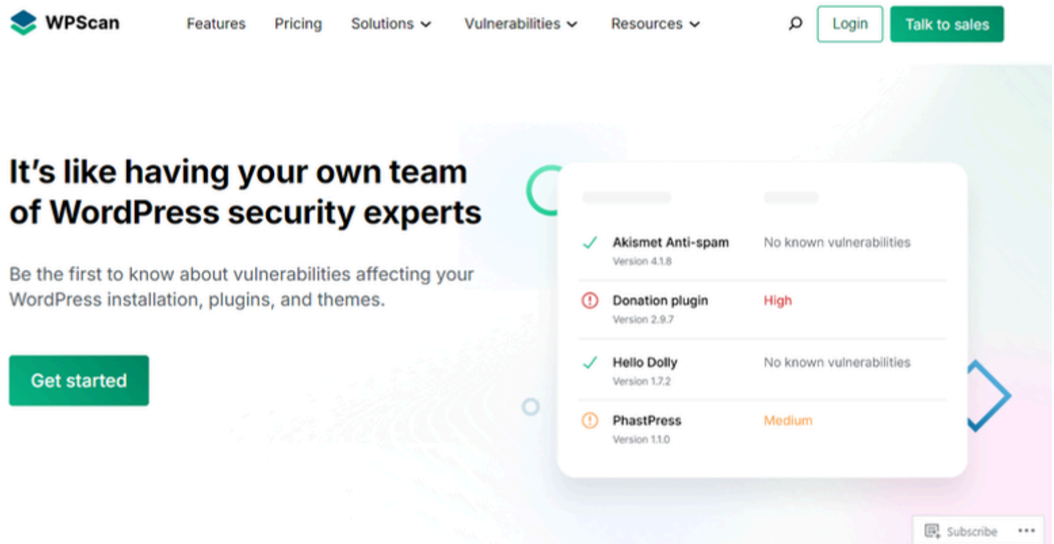
- **การเตรียมตัวก่อนสแกนความปลอดภัย**
  - ขออนุญาต และแจ้งเจ้าของ Server หรือผู้ดูแลเซิร์ฟเวอร์ให้ทราบเป็นลายลักษณ์อักษร
  - เลือกเวลาที่คาดว่าคนใช้เซิร์ฟเวอร์ไม่มาก
  - สำรองข้อมูลถ้าเป็นไปได้
  - ใช้เครื่องคอมพิวเตอร์หน่วยความจำอย่างน้อย 16GB
  - ใช้สาย LAN ความเร็วอย่างน้อย 1Gbps เพื่อความรวดเร็ว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

การสแกนช่องโหว่เบื้องต้น

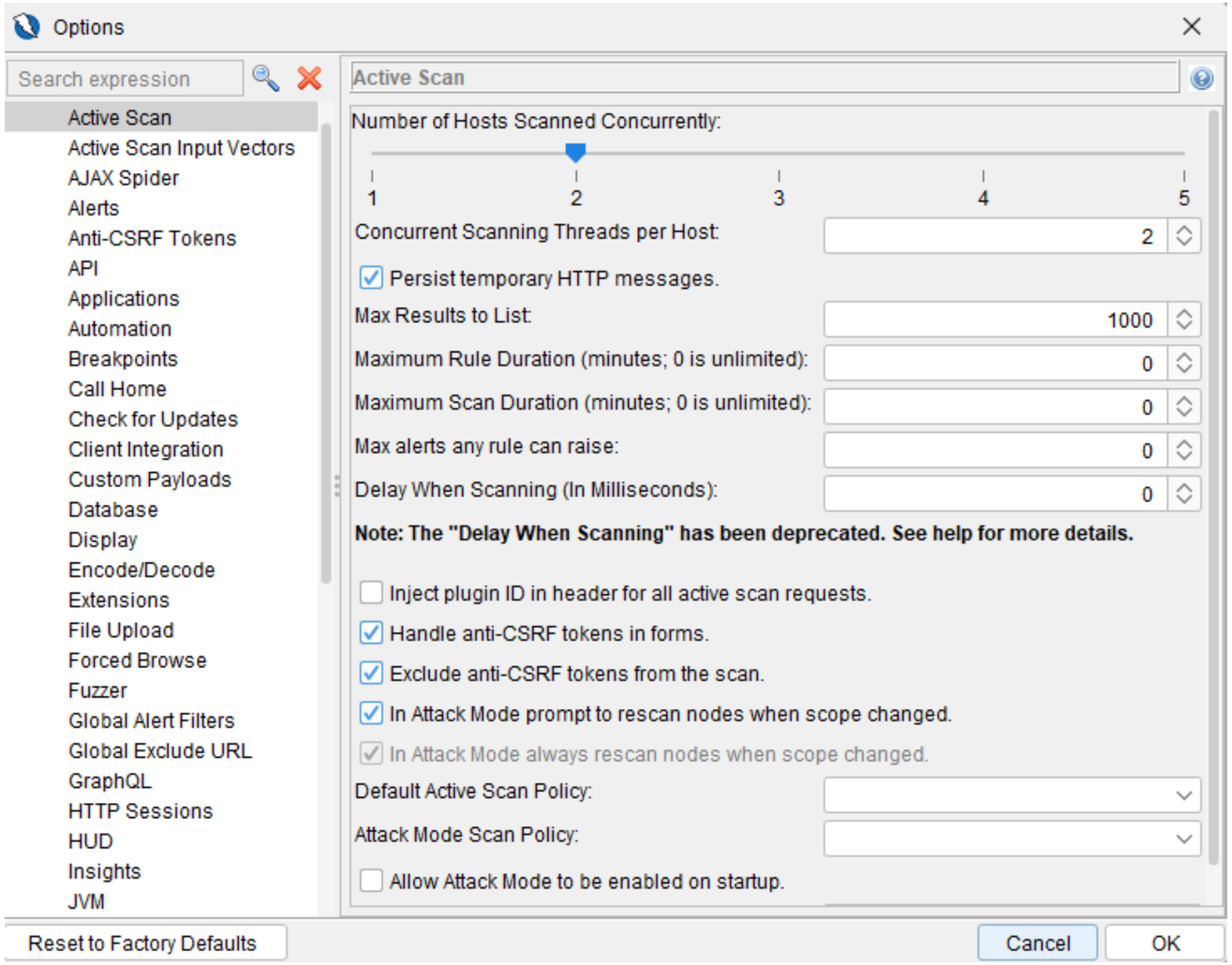
ทางสำนักดิจิทัลฯ แนะนำ 3 เครื่องมือในการสแกนเว็บไซต์เบื้องต้น คือ

- **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/



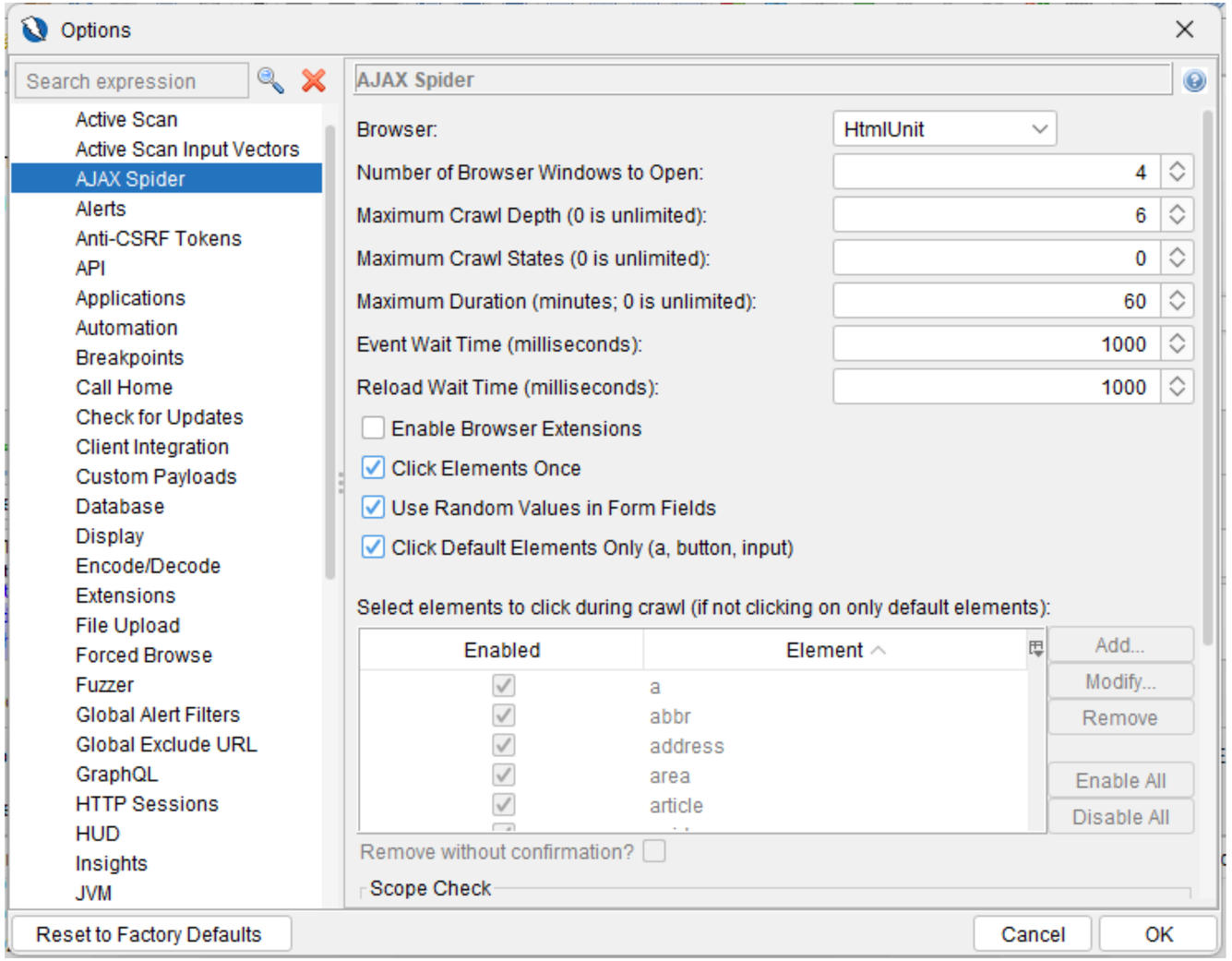


ตั้งค่าสำหรับ ZAP



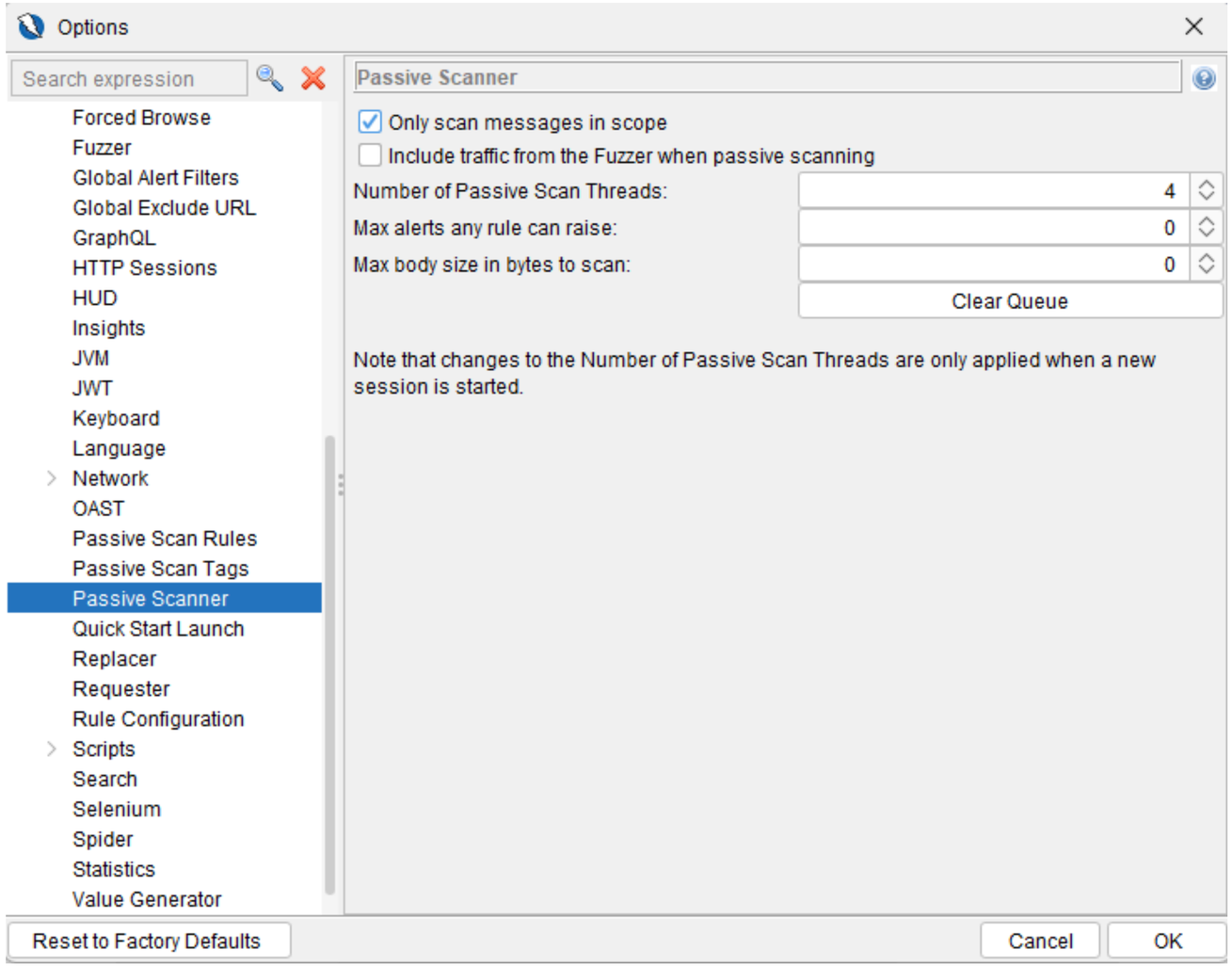
ลดการประมวลผล และลดหน่วยความจำ

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 และเบราเซอร์สมัยใหม่มีระบบความปลอดภัย เรียกว่า CSP ซึ่งต้องกำหนดใน HEADER แต่ไม่ได้กำหนด
- ใช้เพื่อป้องกัน CROSS-SITE SCRIPTING
- เพิ่ม HEADER ดูจากไฟล์ 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 และเบราเซอร์สมัยใหม่มีระบบความปลอดภัย เรียกว่า CSP ซึ่งต้องกำหนดใน HEADER แต่ไม่ได้กำหนด
- ใช้เพื่อป้องกัน CLICKJACKING
- เพิ่ม HEADER ดูจากไฟล์ 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

- ไลบรารี่ JAVASCRIPT เก่าเกินไปและพบว่าเวอร์ชั่นที่ใช้งานอยู่มีช่องโหว่ให้ทำการโจมตีได้
- สำรองข้อมูลโค้ดเว็บทั้งหมด และดาวน์โหลด JAVASCRIPT ตัวใหม่
- อัพโหลดทับตัวเก่า 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 หรือไปดึง JS จากที่อื่นมารันบนเว็บไซต์ได้
- เพิ่ม ATTRIBUTE INTEGRITY เมื่อมีการ INCLUDE ไฟล์จาก REMOTE ทุกครั้ง
- ใช้เครื่องมือจาก HTTPS://SRIHASH.ORG/ 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://xxxxxxx.su.ac.th/.DS_Store

สาเหตุและวิธีการแก้ไข

- เกิดจากมีโฟลเดอร์หรือไฟล์สำคัญระหว่างการพัฒนาที่อาจเปิดเผยโค้ด ถูกอัพโหลดพร้อมเว็บไซต์มาด้วย
- ตรวจสอบชื่อไฟล์และลบไฟล์ตามที่แจ้งออกจากเซิร์ฟเวอร์

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 ที่ ไม่มีตัวตรวจสอบว่าเป็นคำสั่งจากผู้ใช้จริง
- ผู้ไม่หวังดีสามารถหลอกให้ผู้ใช้ที่ LOGIN อยู่ ส่งคำสั่งแทนตนเองได้โดยไม่รู้ตัว (CSRF)
- วิธีการง่ายสุดคือสร้าง RANDOM_STRING ในทุกหน้าที่มีแบบฟอร์ม ดูใน CSRF.TXT

ปัญหาที่พบบ่อย #7

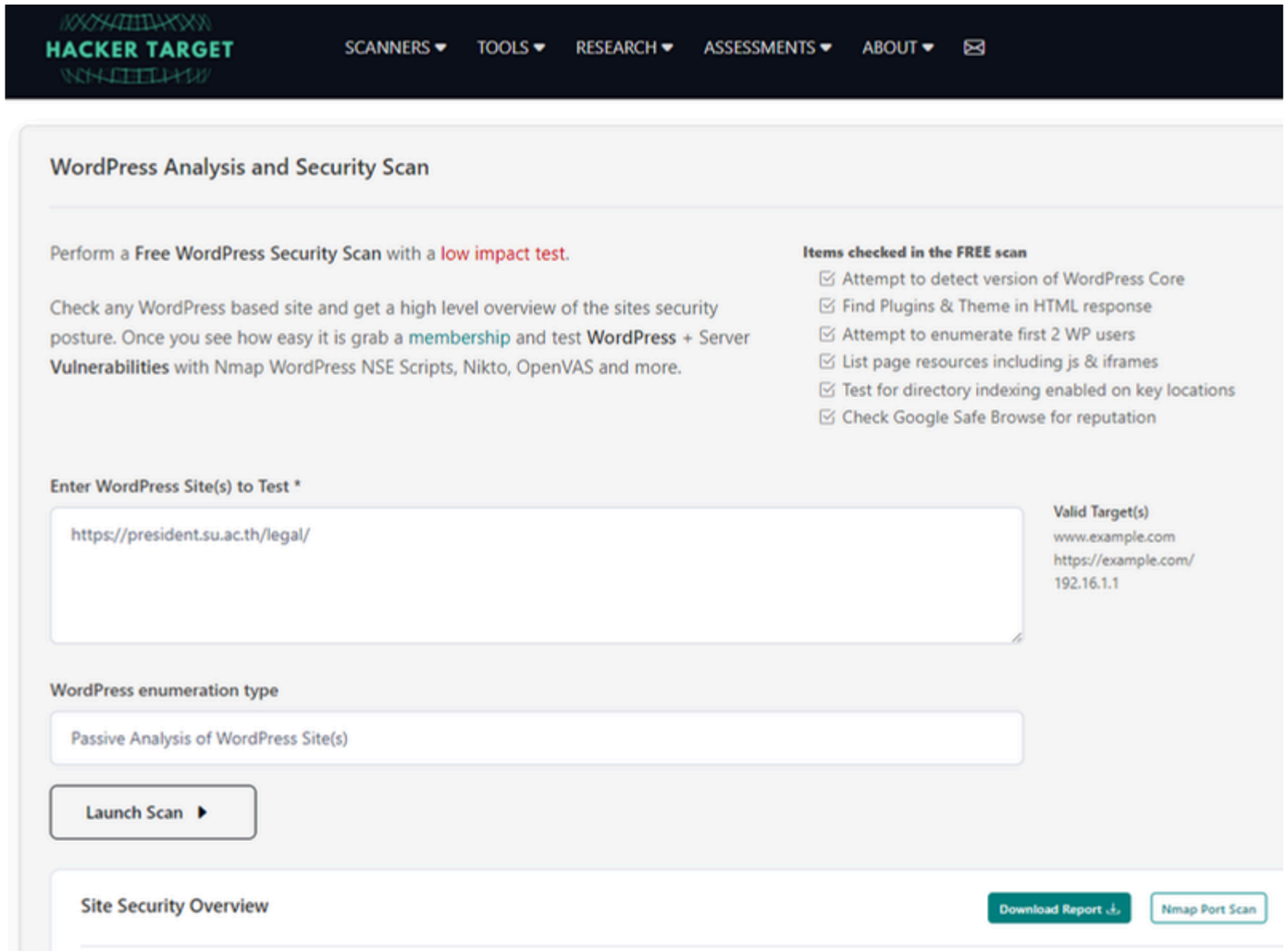
HTTP to HTTPS Insecure Transition in Form Post
หรือ
Secure Pages Include Mixed Content

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

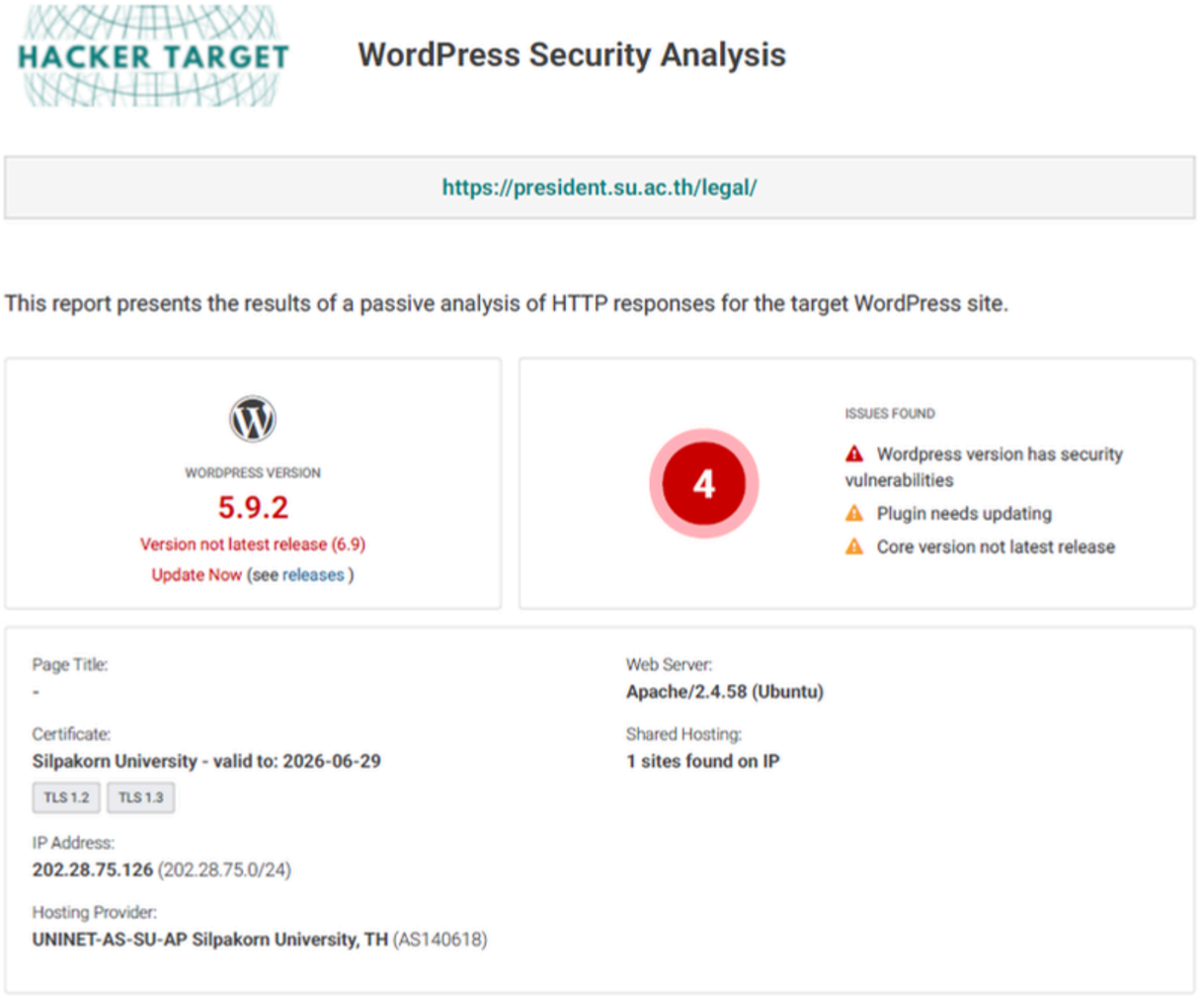
- เกิดจากมีการเรียกทรัพยากร หรือส่งแบบฟอร์ม จาก HTTPS ไป HTTP ทำให้การเข้ารหัสสูญเสียไป
- ข้อมูลอาจถูกดักจับกลางทาง
- ปรับ ACTION หรือการเรียกภาพ เสียง ไฟล์ ให้ถูกต้อง ต้องมี HTTPS ทุกครั้ง ไม่ใช่ HTTP

การสแกน WORDPRESS



HTTPS://HACKERTARGET.COM/WORDPRESS-SECURITY-SCAN/

ผลการสแกน WORDPRESS



จะผ่านได้ต้องเป็นสีเขียวเท่านั้น

การสแกน SSL