



THAILAND

นำเสนอ แผนปฏิบัติการ VA SCAN

Vulnerability Assessment Scan



XX-XXX-XX-XX



THAILAND



ผู้จัดทำโครงงาน

1. นางสาววิสาห์ แก้วสาร (สมัยใหม่)
2. นายณัฐพงศ์ เครือเกศ (ผี)
3. นายศักดา อินทะ (พิวส์)
4. นายสุกัลย์ แสงสุวรรณ (ปรีน)
5. นายประทีอง สุภายุรเดช (ปังปอนด์)
6. นายสิรภพ อุตสม (วิว)
7. นายณัฐวัตร ชุ่มเชื้อ (ณัฐวัตร)
8. นายเอกรัตน์ วนะปัญญา (แบงค์)
9. นางสาวอัมพิกา ใจกล้า (ส้มโอ)
10. นายจักรฤทธิ์ ชุมภูชนະภัย (ตุบ)
11. นายคงศร กันทะสาร (นัท)
12. นพ.วันทวัฒน์ สุกธิพงษ์ (บอส)

- สำนักงานเขตสุขภาพที่ 4, เขต 4
โรงพยาบาลสมเด็จพระยุพราชตะพานหิน, เขต 3
- สำนักงานเขตสุขภาพที่ 7, เขต 7
โรงพยาบาลแม่ลาน้อย, เขต 1
- โรงพยาบาลสบเมย, เขต 1
- โรงพยาบาลเวียงหนองล่อง, เขต 1
- โรงพยาบาลสันทราย, เขต 1
สสจ.ลำพูน, เขต 1
- โรงพยาบาลจุน, เขต 1
- โรงพยาบาลเชียงเม่วน, เขต 1
- โรงพยาบาลดอกคำใต้, เขต 1
- โรงพยาบาลนครพิงค์, เขต 1



1. ປັບປາ (Research Problem)

3. **ມີຫຼຸດຫົວໜ້າ**

ໃນສູງ ໄມຕາຍ ໃນປາ



2. ความท้าทาย (Research Challenges)

I <> R

Incident NOT RISK



2. ความท้าทาย (Research Challenges)

2.1 การระบุช่องโหว่ที่ซ่อนเร้น:

ช่องโหว่บางประเภท เช่น Zero-Day Vulnerabilities หรือ Logic Flaws อาจไม่สามารถตรวจสอบได้ด้วยการสแกนพื้นฐาน จึงต้องการวิธีการขั้นสูง เช่น การวิเคราะห์พฤติกรรมหรือ Machine Learning ด้วย tool ที่มีความสามารถจำกัด

2.2 การเชื่อมโยงผลลัพธ์กับการแก้ไข:

แม้ว่าจะสามารถตรวจสอบช่องโหว่ได้สำเร็จ แต่การเชื่อมโยงข้อมูลจากเครื่องมือกับแนวการทำงานป้องกันยังคงเป็นเรื่องท้าทาย เช่น ข้ออยู่กับความรู้ความสามารถของผู้ดูแลระบบ

2.3 การพัฒนาระบบอัตโนมัติในการป้องกัน:

การแปลงข้อมูลจากการสแกนช่องโหว่ไปสู่การป้องกันที่สามารถปรับเปลี่ยนได้อัตโนมัติ เช่น การปรับ Firewall Rules แบบเรียลไทม์



3. ความสำคัญของการแก้ปัญหาเหล่านี้

Know How

Risk Control And Protect

3. ความสำคัญของการแก้ปัญหาเหล่านี้

การเพชร์ญหน้ากับปัญหาและความท้าทายดังกล่าวมีความสำคัญในเชิงวิจัย เนื่องจากสามารถนำไปสู่:

- 1. การพัฒนากระบวนการตรวจสอบช่องโหว่ที่มีความแม่นยำและปลอดภัยยิ่งขึ้น**
- 2. การออกแบบระบบที่มีความยืดหยุ่นและสามารถตอบสนองต่อภัยคุกคามได้รวดเร็ว**
- 3. การสร้างองค์ความรู้ใหม่ที่ช่วยยกระดับความปลอดภัยทางไซเบอร์ในระดับองค์กรและสังคมโดยรวม**



ขั้นตอนทดสอบเจาะระบบ

ขั้นตอนที่ 1

จำลองเครือข่าย สำหรับ
ทดสอบภายใน VM
WorkStation

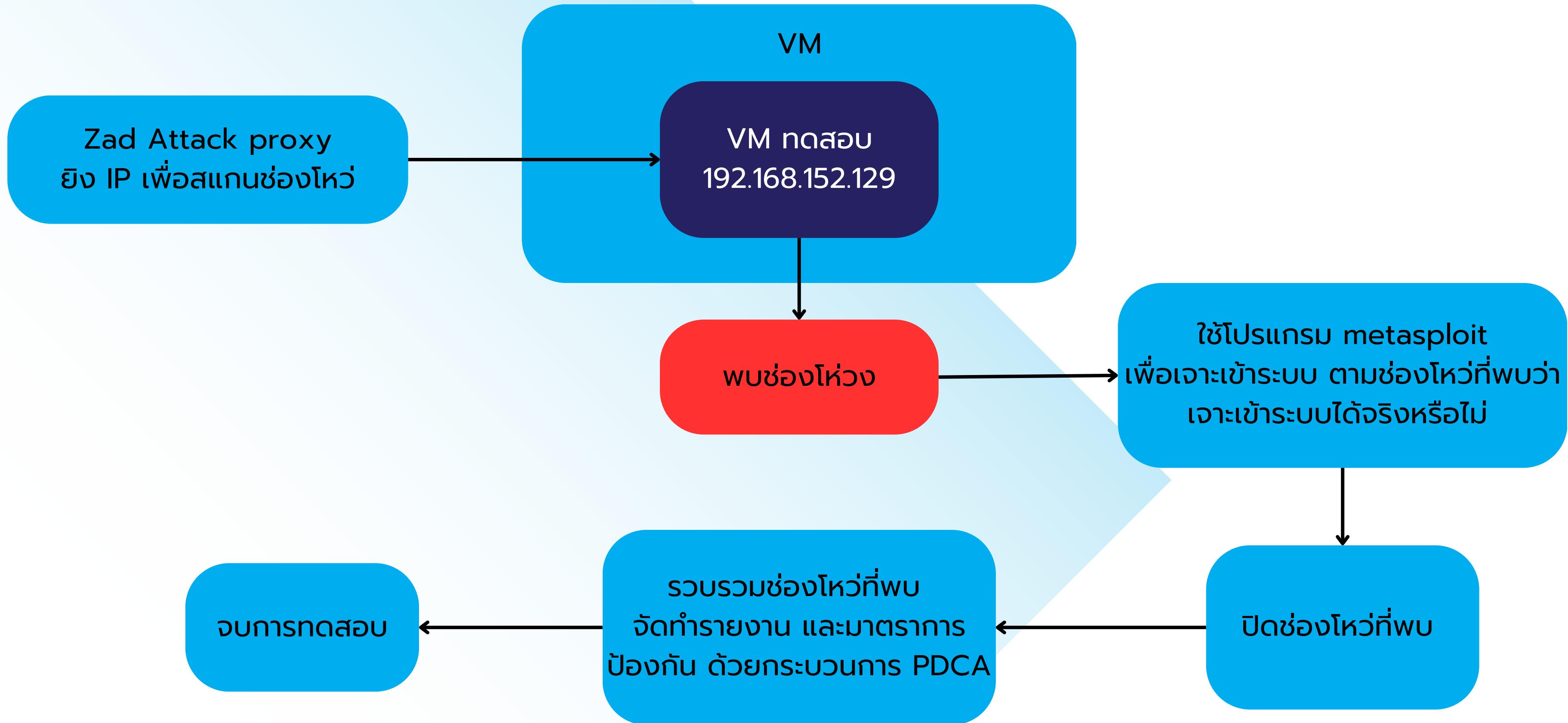
ขั้นตอนที่ 2

การสแกนระบบเป้าหมาย
หาช่องโหว่จำลองการ
เจาะข้อมูลจาก
metasploit

ขั้นตอนที่ 3

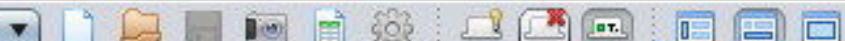
ตรวจสอบผลจาก log
เครื่องที่ถูกโอบตี และทำรี
พอกรายการ และสร้าง
มาตรการป้องกัน จาก
ช่องโหว่ที่พบ

ขั้นตอนปฎิบัติงาน



ผลการปฏิบัติงาน ตามขั้นตอน VA SCAN





Category	URI
GET:Category:SAMM-ST-2	
GET:Category:OWASP_Tool	
GET:Category:OWASP_Release_Quality_Tool	
GET:2015-08-ZAP-ScriptingCompetition	
About_OWASP	
GET:File:ZAP-ScreenShotSearchTab.png	
GET:File:ZAP-ScreenShotHistoryFilter.png	
GET:File:ZAP-ScreenShotHelp.png	
GET:File:ZAP-ScreenShotAddAlert.png	
GET:File:Zap128x128.png	
GET:Category:Popular	
GET:Contributions	

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack:

http://www.owasp.org

Select...



Attack



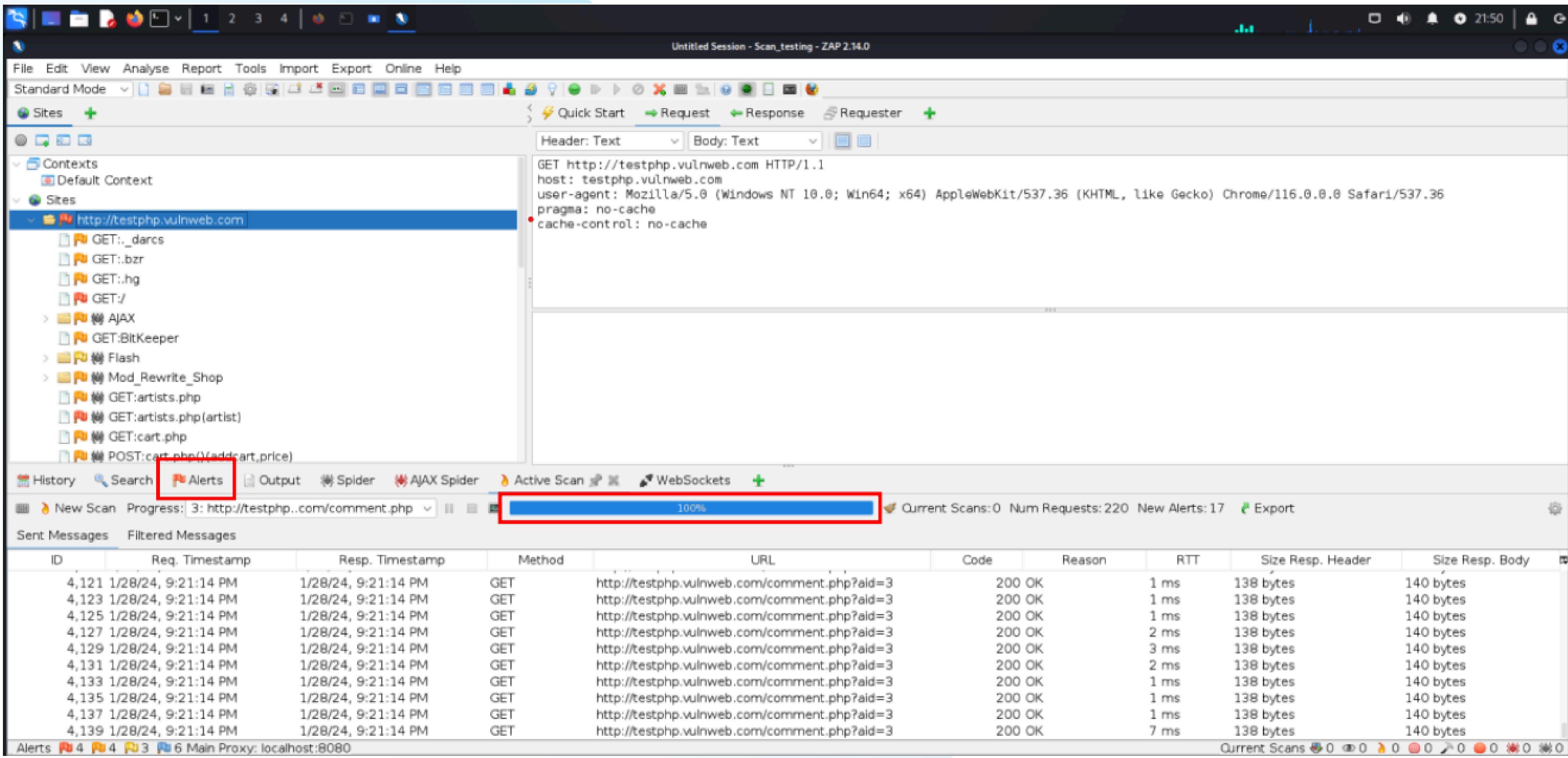
Stop

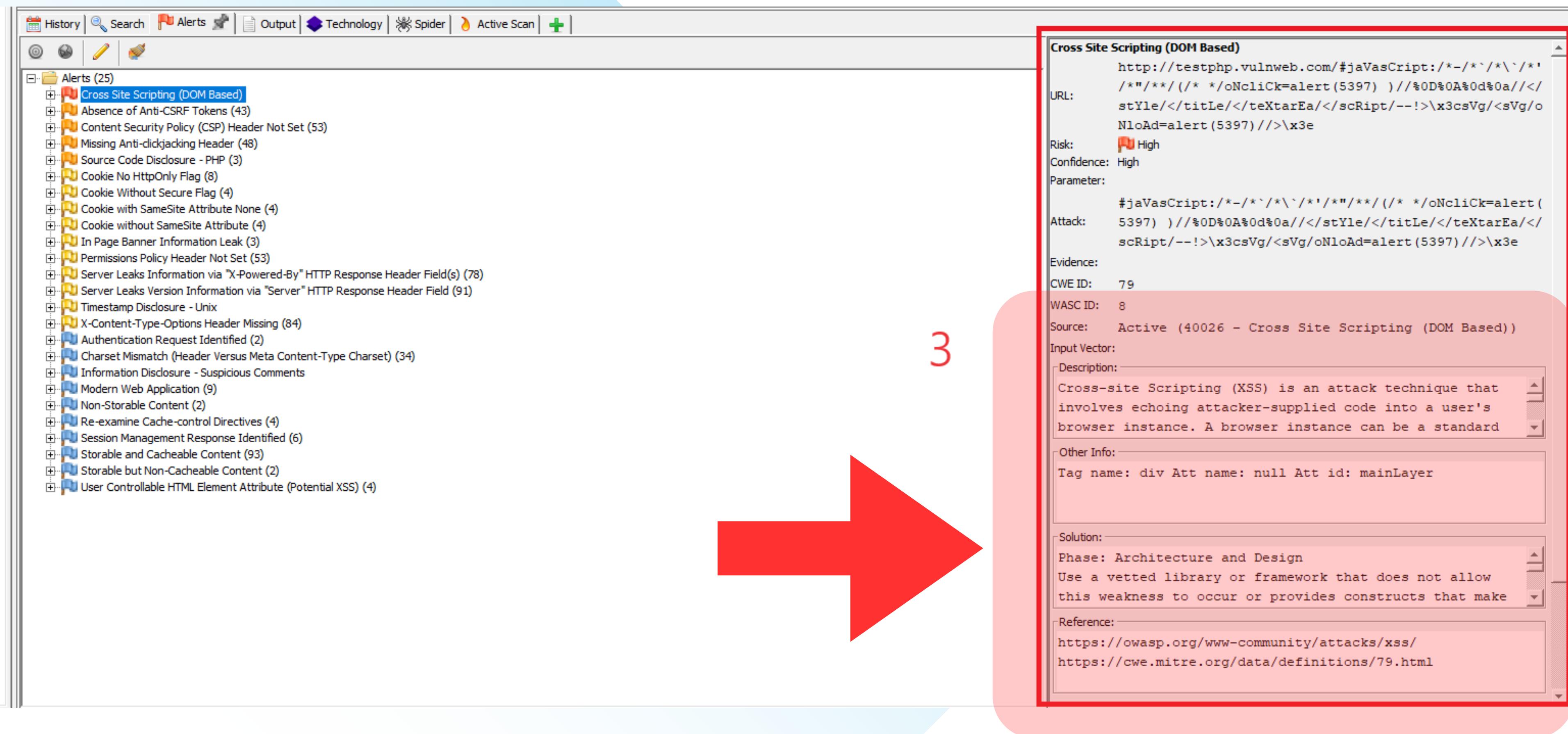
Progress:

Spidering the URL to discover the content



Processed	Method	URI	Flags
●	GET	https://www.owasp.org/index.php/Mohd_Fazli_Azran	
●	GET	https://www.owasp.org/index.php/John_Vargas	
●	GET	https://docs.google.com/spreadsheets/d/1m00e983giNVwhbuQ96cmb79t...	OUT_OF_SCOPE
●	GET	https://www.owasp.org/images/d/da/WASPY_2015_Sponsorship_Docume...	
●	GET	http://owasp.blogspot.com/2015/06/2015-waspy-award-nominations.html	OUT_OF_SCOPE
●	GET	https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e21153b3fe690d&ui...	OUT_OF_SCOPE
●	GET	https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e211c0353117cd&ui...	OUT_OF_SCOPE
●	GET	https://twitter.com/owasp/status/613372502698532864	OUT_OF_SCOPE
●	GET	https://www.facebook.com/groups/owaspfoundation/permalink/798497196...	OUT_OF_SCOPE
●	GET	https://plus.google.com/116933056486234813396/posts/EFTauUZjyuE	OUT_OF_SCOPE
●	GET	https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e3182abfd79146&ui...	OUT_OF_SCOPE
●	GET	https://twitter.com/owasp/status/614528448325771266	OUT_OF_SCOPE
●	GET	https://plus.google.com/116933056486234813396/posts/1JcQN92vZHA	OUT_OF_SCOPE
●	GET	http://owasp.blogspot.com/2015/06/nominate-your-waspy-candidates-today...	OUT_OF_SCOPE
●	GET	https://www.facebook.com/groups/owaspfoundation/permalink/800341350...	OUT_OF_SCOPE
●	GET	https://twitter.com/owasp/status/624676858127368194	OUT_OF_SCOPE





ZAP Scanning Report

Generated with  ZAP on Sat 27 Jan 2024, at 11:33:32

ZAP Version: 2.14.0

Contents

- [About this report](#)
 - [Report parameters](#)
- [Summaries](#)
 - [Alert counts by risk and confidence](#)
 - [Alert counts by site and risk](#)
 - [Alert counts by alert type](#)
- [Alerts](#)
 - [Risk=High, Confidence=Medium \(2\)](#)
 - [Risk=Medium, Confidence=High \(1\)](#)
 - [Risk=Medium, Confidence=Medium \(2\)](#)
 - [Risk=Medium, Confidence=Low \(1\)](#)
 - [Risk=Low, Confidence=High \(1\)](#)

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- <http://testphp.vulnweb.com>

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: High, Medium, Low, Informational

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

สรุปผล

การกำกับ Vulnerability Assessment Scan (VA Scan) คือกระบวนการตรวจสอบช่องโหว่ในระบบสารสนเทศ เช่น ระบบปฏิบัติการ ซอฟต์แวร์ หรืออุปกรณ์เครือข่าย โดยใช้เครื่องมือ เพื่อค้นหาช่องโหว่และประเมินความรุนแรงตามมาตรฐาน CVE และ CVSS การกำกับ VA ช่วยให้รู้จุดอ่อนของระบบและสามารถแก้ไขได้ก่อนการโจมตีจากแฮกเกอร์ ซึ่งทำให้ระบบมีความปลอดภัยสูงขึ้น และสามารถปฏิบัติตามข้อกำหนด Cybersecurity เช่น HIPAA และ PCI DSS โดย ขั้นตอนการกำกับ VA ควรมีกระบวนการดังนี้

- (PLAN)** กำหนดขอบเขตและค้นหาช่องโหว่ในระบบ
- (DO)** วิเคราะห์สาเหตุของช่องโหว่
- (CHECK)** ประเมินความรุนแรงและจัดลำดับความสำคัญ
- (Action)** แก้ไขช่องโหว่และปิดจุดอ่อน

การกำกับ VA อย่างสม่ำเสมออย่างน้อยปีละ 2 ครั้งช่วยลดความเสี่ยงจากภัยคุกคามต่างๆ ทำให้ระบบเครือข่ายขององค์กรมีความปลอดภัยอยู่เสมอ.



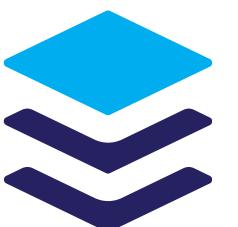
GROUP 6

គ្រូប៊ែន





 GROUP 6
Q & A



GROUP 6

ขอขอบคุณ จับการนำเสนอ