TLP : CLEAR

คู่มือการติดตั้ง ใช้งานและการสร้างรายงาน

OWASP ZAP - Zed Attack Proxy (ZAP)

สารบัญ

OWASP ZAP คืออะไร

OWASP ZAP เป็นเครื่องมือที่ใช้สำหรับการทดสอบความปลอดภัยของเว็บแอปพลิเคชัน ซึ่งเป็นกระบวนการที่สำคัญสำหรับการพัฒนาซอฟต์แวร์ที่มีคุณภาพ การทดสอบความปลอดภัยของเว็บแอปพลิเคชันมีวัตถุประสงค์เพื่อค้นหาช่องโหว่หรือจุดอ่อนที่อาจทำให้ผู้ไม่หวังดีสามารถเข้าถึง แก้ไข หรือทำลายข้อมูลที่สำคัญ หรือทำให้เว็บแอปพลิเคชันไม่สามารถทำงานได้

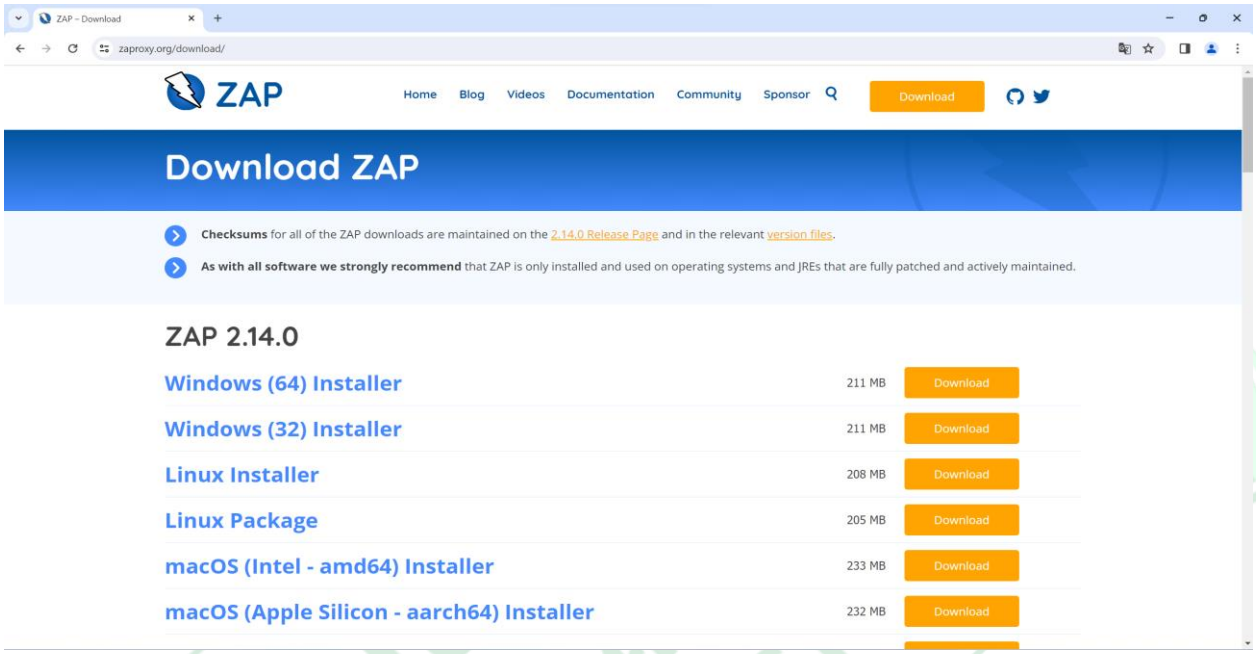
OWASP ZAP เป็นเครื่องมือที่มีความยืดหยุ่นและมีคุณสมบัติที่หลากหลาย เช่น

- Proxy interception : เป็นการดักจับการสื่อสารระหว่างเว็บเบราว์เซอร์และเว็บแอปพลิเคชัน เพื่อวิเคราะห์และแก้ไขคำขอและการตอบกลับ ซึ่งช่วยให้ผู้ใช้สามารถเห็นและเปลี่ยนแปลงข้อมูลที่ถูกส่งไปยังเว็บแอปพลิเคชันได้
- Automated scanning : เป็นการส่งคำขอที่มีการเปลี่ยนแปลงค่าต่างๆ เช่น พารามิเตอร์ หัวข้อ หรือโค้ด เพื่อค้นหาช่องโหว่ที่อาจมีอยู่ในเว็บแอปพลิเคชัน โดยการสแกนอัตโนมัติสามารถทำได้ทั้งแบบแอคทีฟ (active) และแพสซีฟ (passive)
- Fuzzing : เป็นการส่งคำขอที่มีข้อมูลที่ไม่ถูกต้องหรือไม่คาดคิด เช่น อักขระพิเศษ ข้อความยาว หรือข้อมูลที่ไม่เกี่ยวข้อง เพื่อทดสอบว่าเว็บแอปพลิเคชันจะมีการตอบสนองอย่างไร ซึ่งช่วยให้ผู้ใช้สามารถค้นหาช่องโหว่ที่เกี่ยวข้องกับการปฏิเสธการให้บริการ (denial of service) การแทรกแซงโค้ด (code injection) หรือการเปิดเผยข้อมูลสำคัญ (information disclosure)
- Smart card support : เป็นการใช้สมาร์ทการ์ดเพื่อเข้าสู่ระบบเว็บแอปพลิเคชันที่มีการรับรองความถูกต้องด้วยใบรับรอง (certificate) ซึ่งช่วยให้ผู้ใช้สามารถทดสอบความปลอดภัยของเว็บแอปพลิเคชันที่มีการใช้สมาร์ทการ์ดได้
- Add-on extension : เป็นการเพิ่มความสามารถของ OWASP ZAP ด้วยการติดตั้งส่วนขยาย (add-on) ที่มีให้เลือกมากมาย หรือสร้างส่วนขยายของตนเอง ซึ่งช่วยให้ผู้ใช้สามารถปรับแต่ง OWASP ZAP ให้ตรงกับความต้องการและเป้าหมายของการทดสอบความปลอดภัยได้

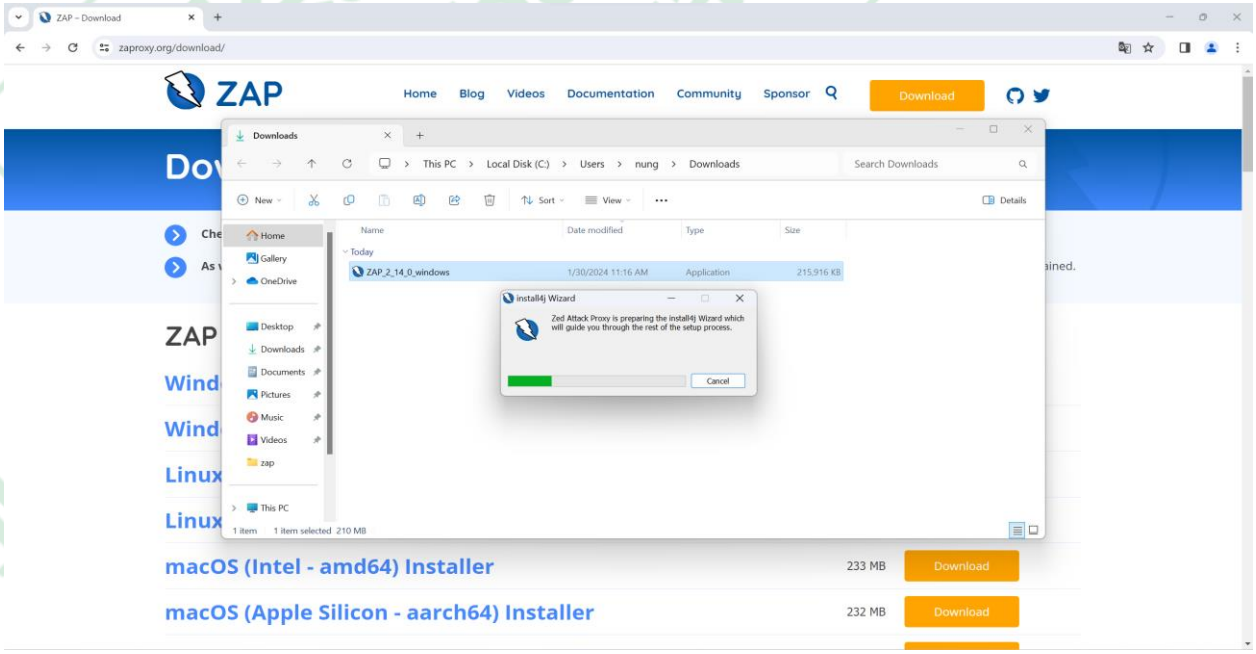
OWASP ZAP เป็นโปรแกรมที่เป็นโอเพ่นซอร์ส ซึ่งหมายความว่าผู้ใช้สามารถดูและแก้ไขโค้ดของโปรแกรมได้ และฟรี ซึ่งหมายความว่าผู้ใช้ไม่ต้องเสียค่าใช้จ่ายใดๆ สำหรับการใช้งานโปรแกรมนี้ โปรแกรมนี้สามารถทำงานได้บนหลายระบบปฏิบัติการ เช่น Windows, Linux, Mac OS และอื่นๆ โดยต้องมี Java Runtime Environment (JRE) เวอร์ชัน 8 หรือสูงกว่า

วิธีการติดตั้งโปรแกรม ZAP Attack Proxy (ZAP) สำหรับผู้ใช้ Windows

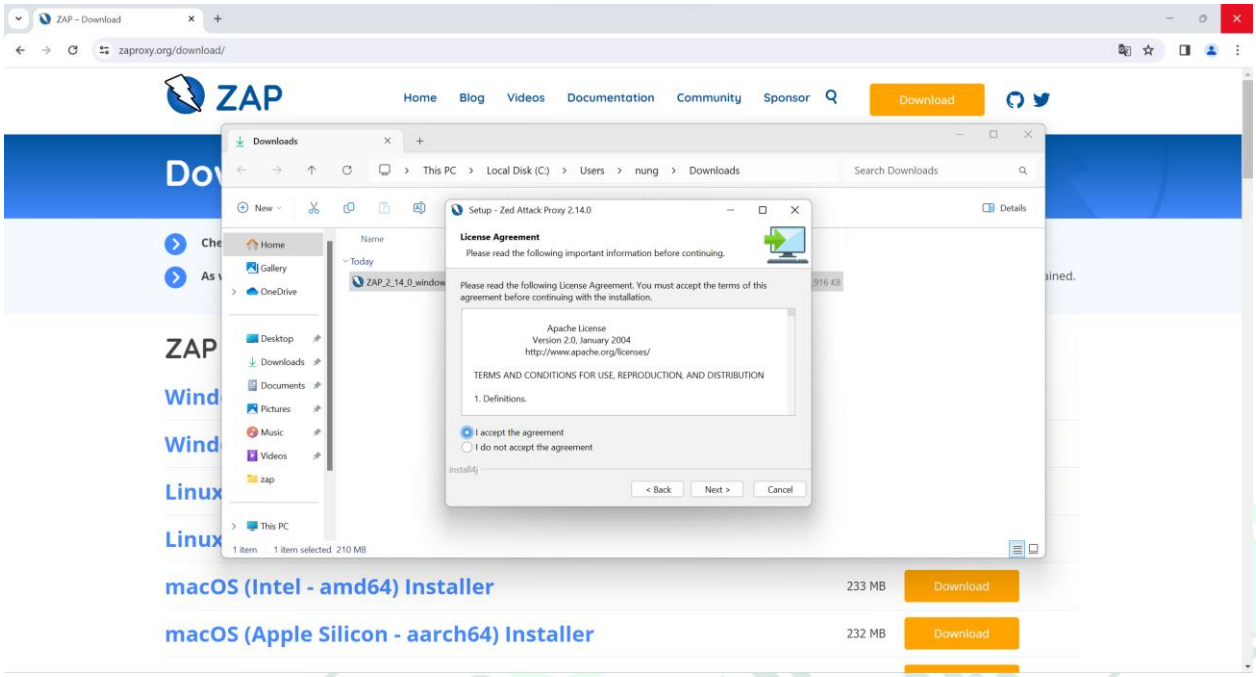
เข้าที่ Website : zaproxy.org และเข้าสู่หน้าของการ Download และ เลือกดาวนโหลดไฟล์ Windows (64) Installer



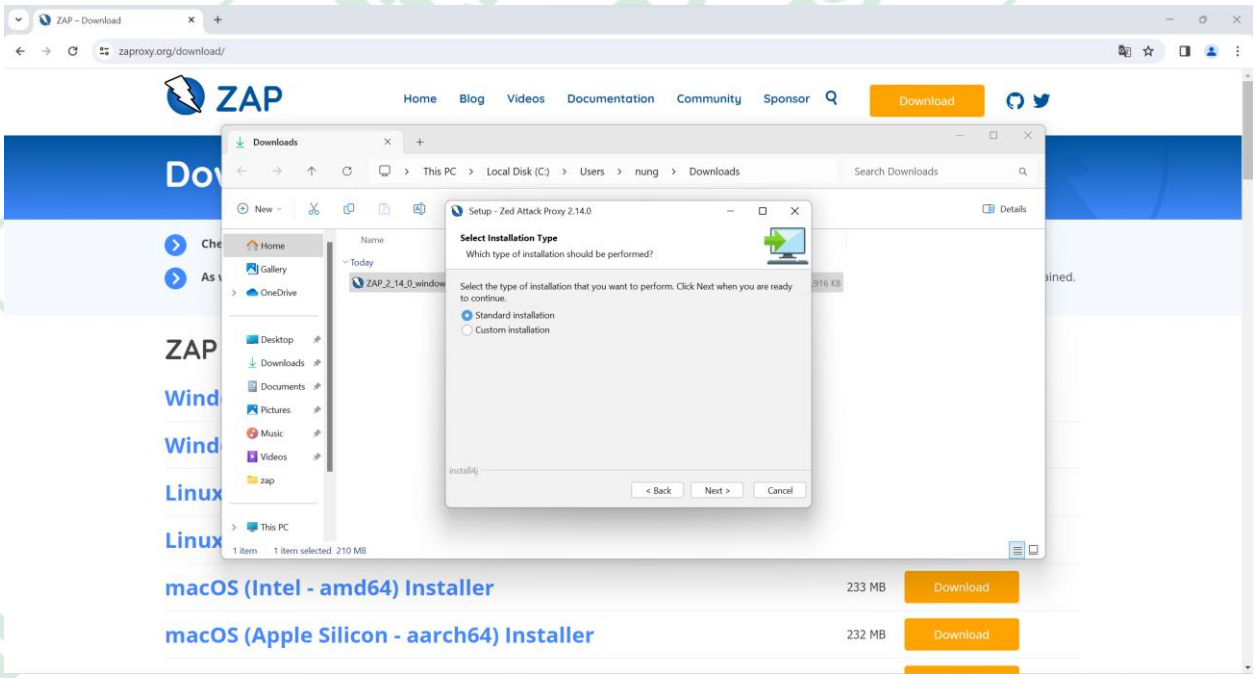
ทำการตรวจสอบไฟล์ที่ดาวน์โหลดและ Double Click เพื่อติดตั้งโปรแกรม



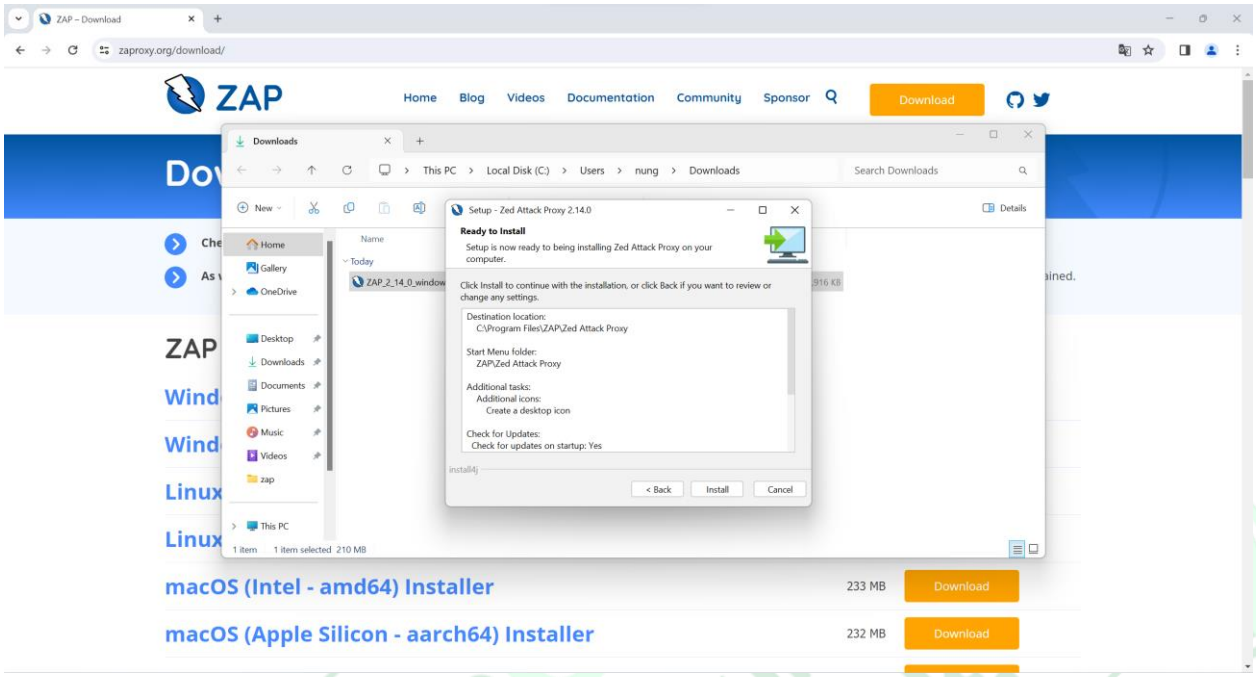
กด Next ไปจนกระทั่งแสดงหน้า License Agreement ให้เลือก Accept และกด Next



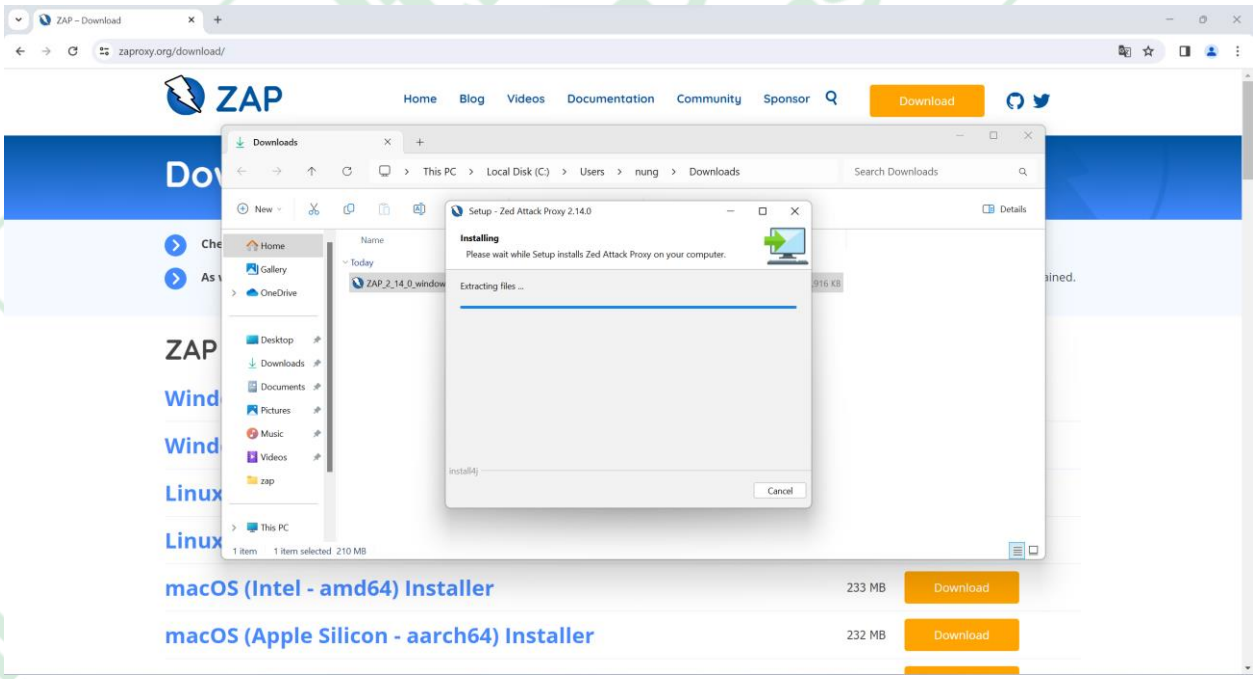
เลือก Standard Installation และไปสู่ขั้นตอนต่อไปโดยการเลือก Next



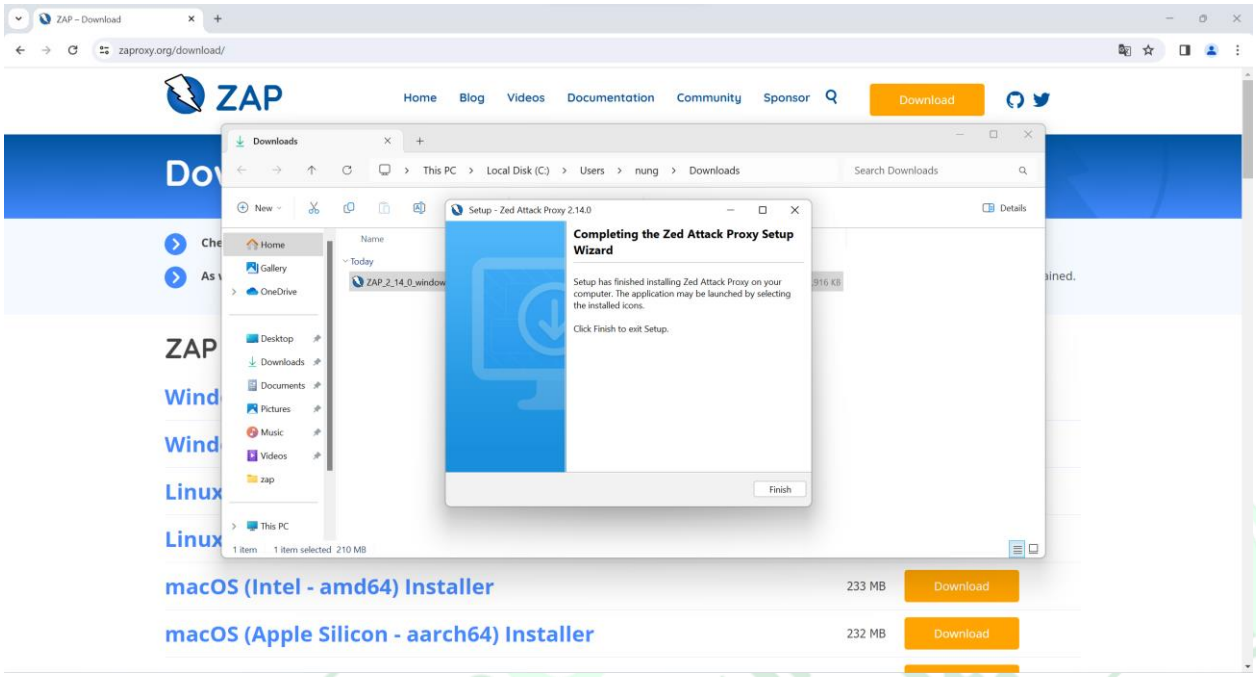
ทำการเลือก Install เพื่อติดตั้งโปรแกรม



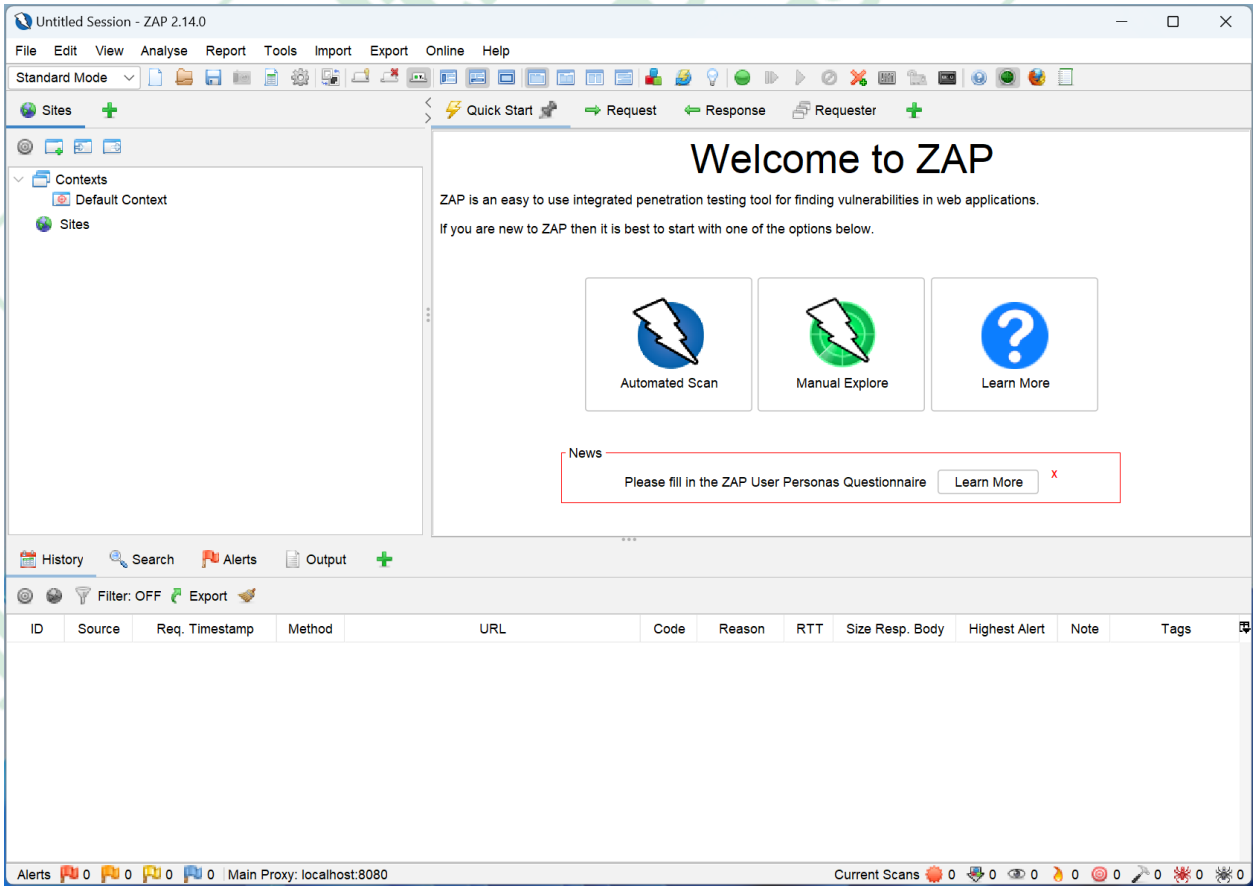
รอจนกว่าจะติดตั้งโปรแกรมสำเร็จ



แสดงหน้าเสร็จสิ้นขั้นตอนการติดตั้งโปรแกรมให้คลิกปุ่ม Finish

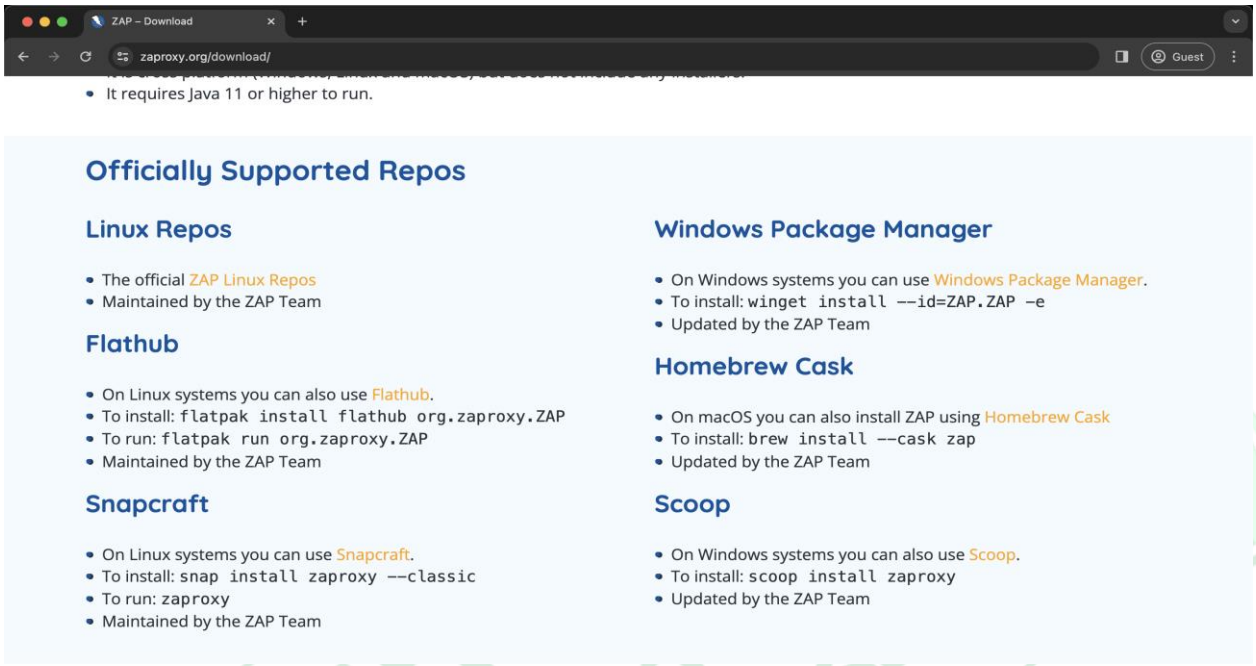


เปิดโปรแกรมเพื่อใช้งาน

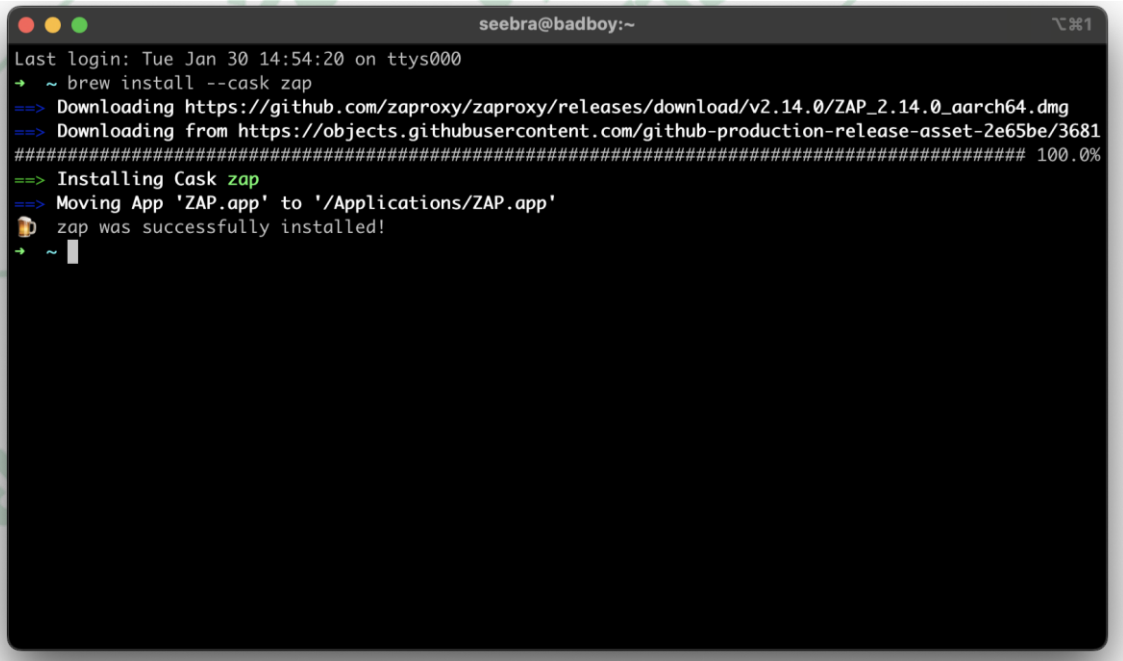


วิธีการติดตั้งโปรแกรม Zed Attack Proxy (ZAP) สำหรับผู้ใช้ Mac

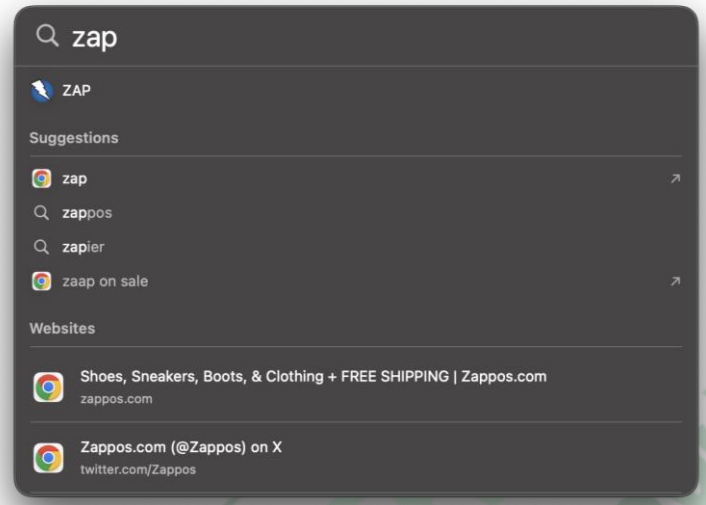
เข้าที่ Website : zaproxy.org และเข้าสู่หน้าของการ Download และค้นหาที่มีคำว่า Homebrew Cask



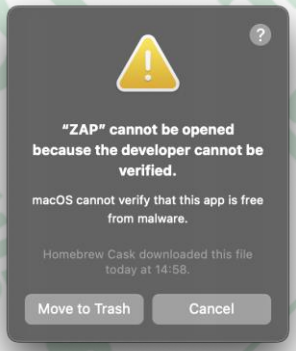
เปิด Terminal และใช้คำสั่ง brew install –cask zap และรอจนกว่าจะติดตั้งโปรแกรมเสร็จ



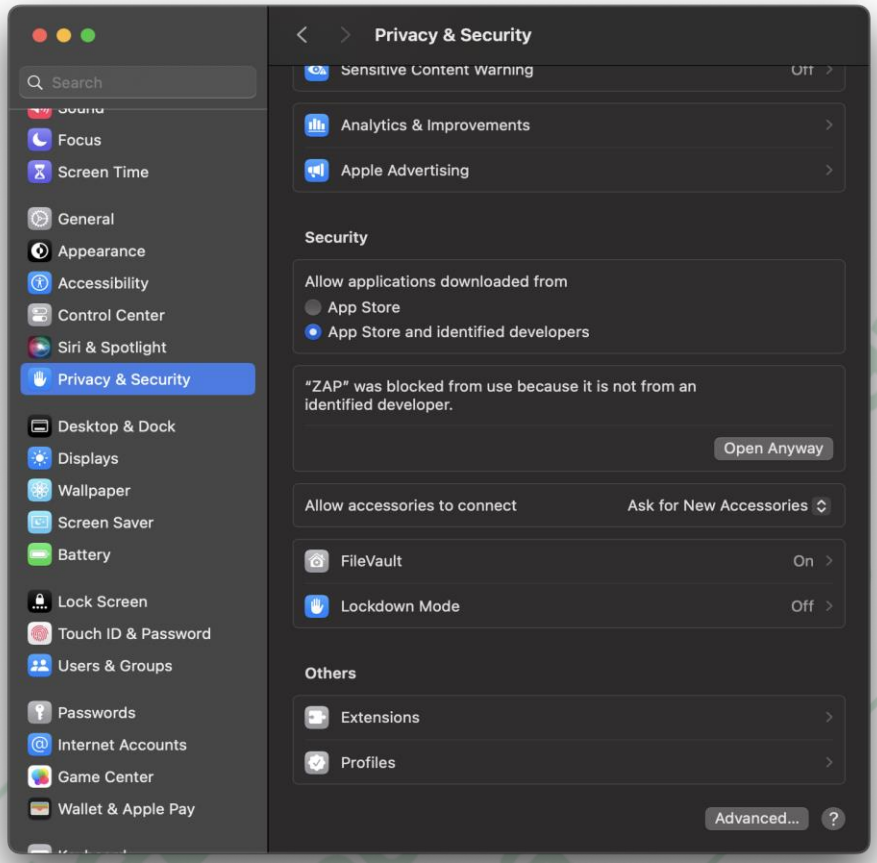
ทำการเปิดโปรแกรม ZAP



กรณีที่มีข้อความแจ้งเตือนเกี่ยวกับเรื่องความปลอดภัย ให้เลือก Cancel

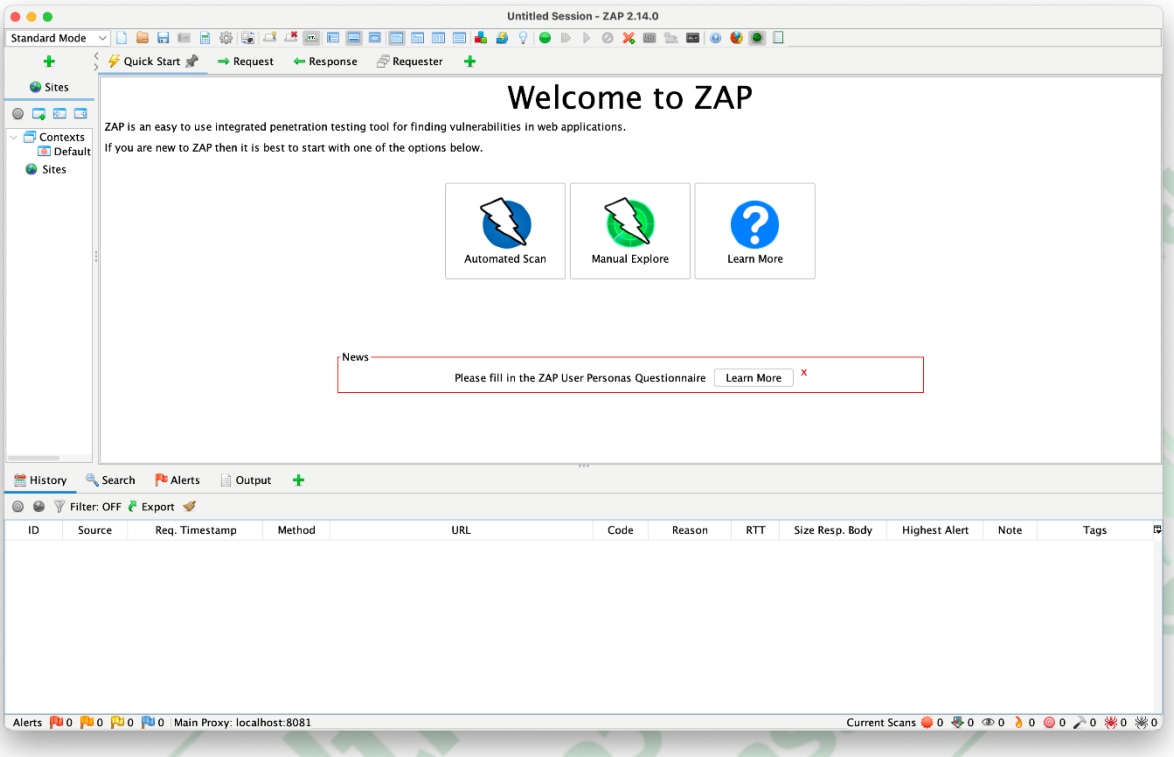


เข้าที่ setting -> Privacy & Security ดูที่ส่วนของ “ZAP” was blocked ….. และเลือก Open Anyway



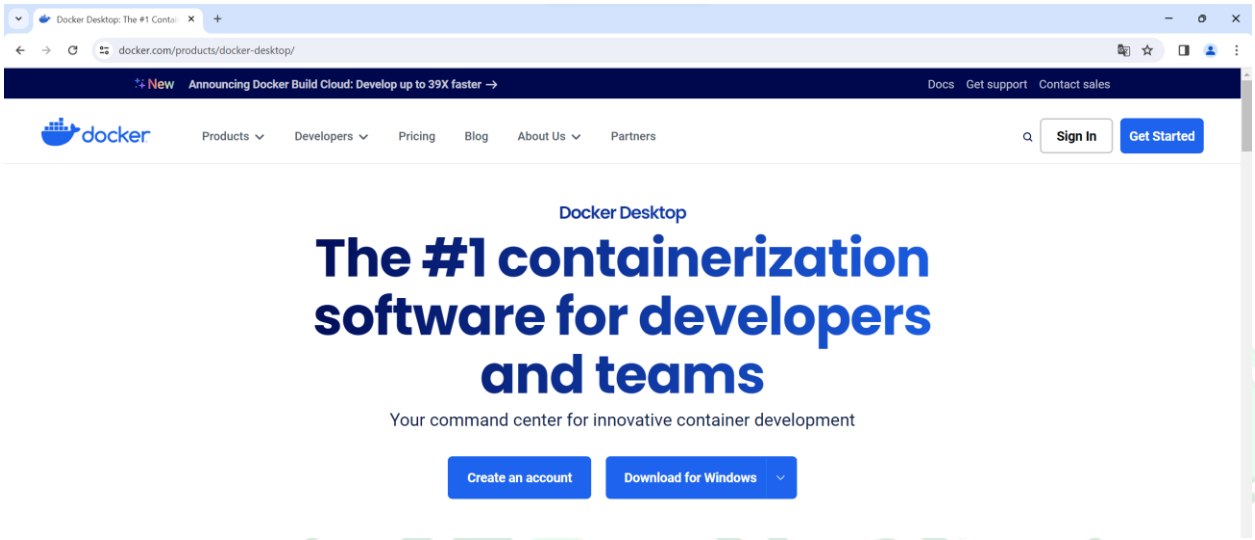
แสดงหน้าต่างการยืนยันการเปิดโปรแกรม zap ให้เลือก Open

ถ้าทำถูกต้องทุกขั้นตอนแล้วจะสามารถใช้งานโปรแกรม zap ได้

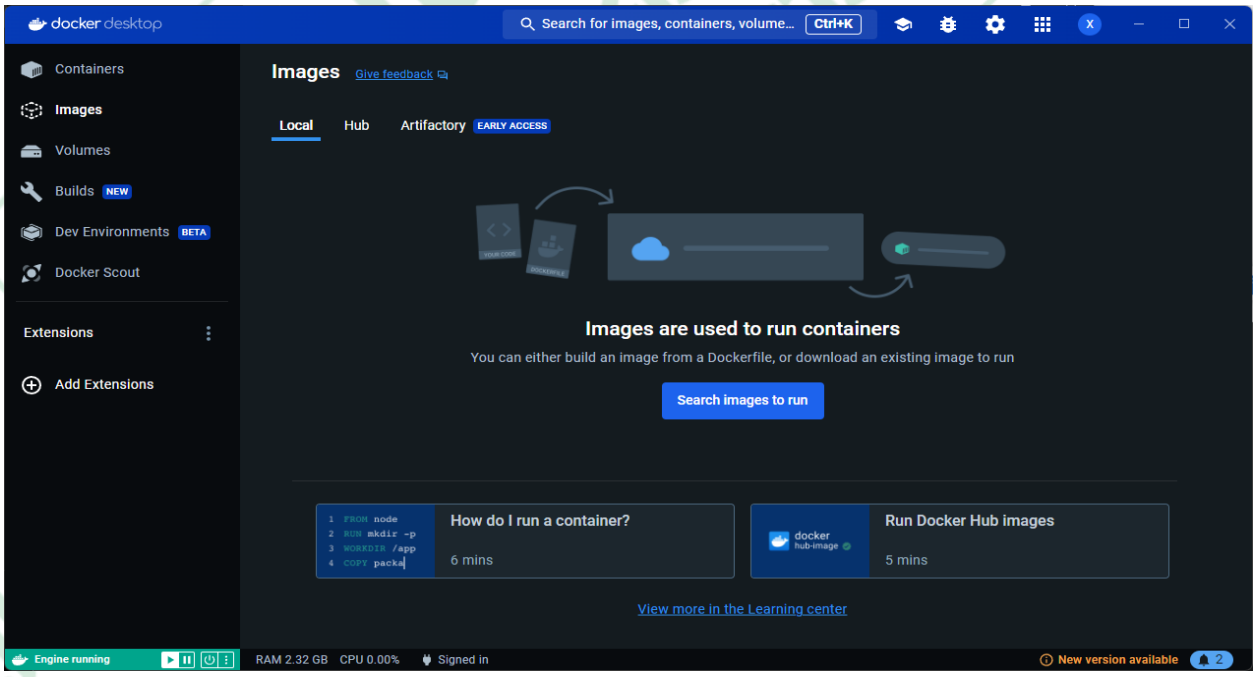


วิธีการติดตั้งโปรแกรม Zed Attack Proxy (ZAP) สำหรับผู้ใช้ Docker

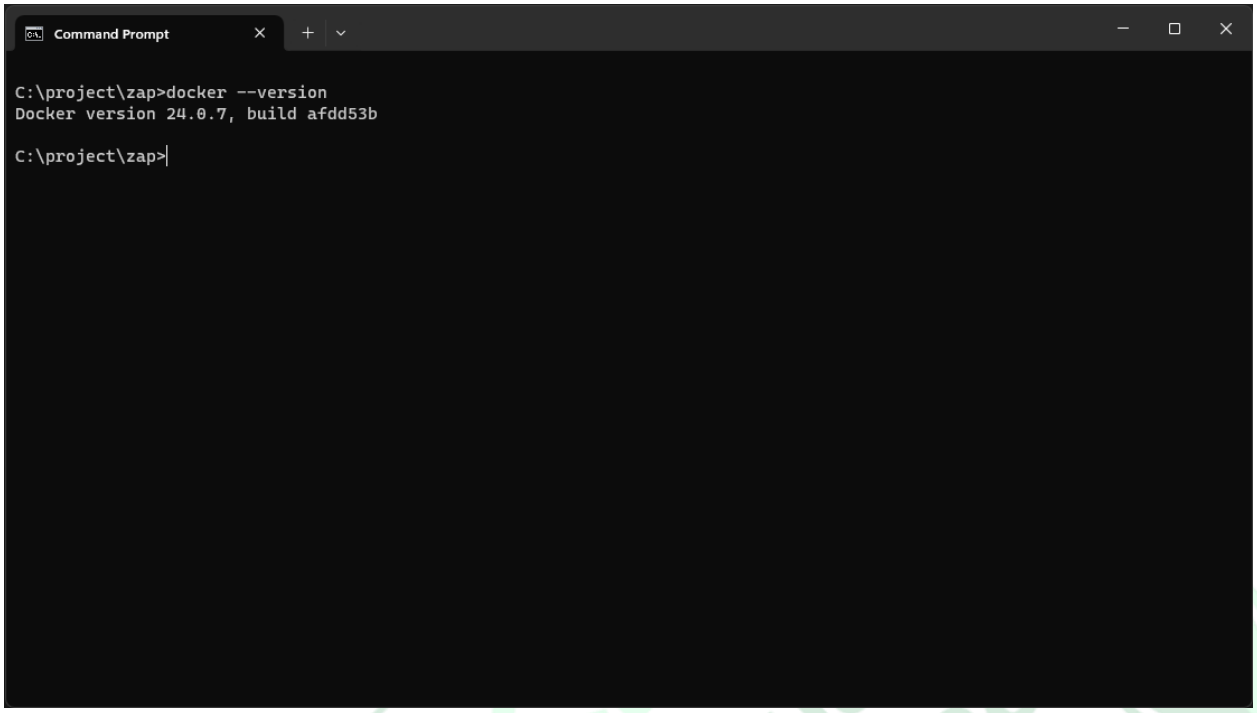
เข้าสู่เว็บไซต์ของ Website: docker.com/products/docker-desktop เพื่อทำการดาวน์โหลดโปรแกรม docker desktop โดยเลือก Download for Windows



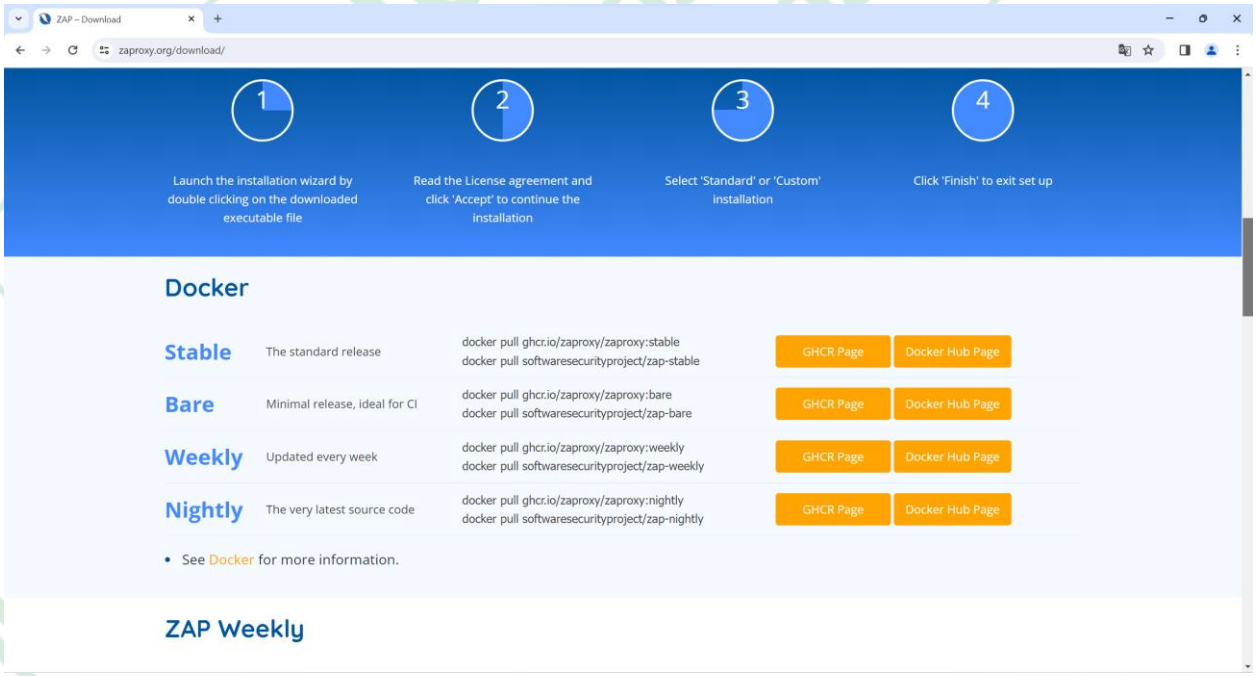
ทำการติดตั้งโปรแกรม Docker Desktop ให้เรียบร้อย



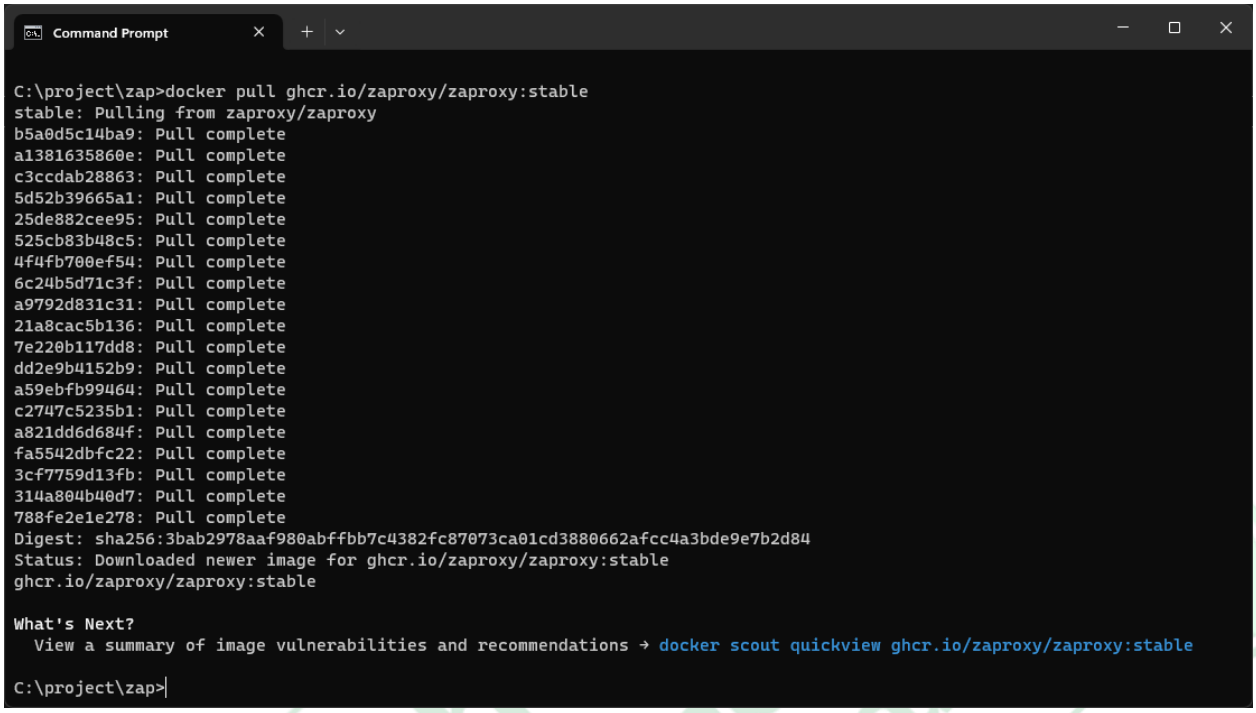
เปิด command prompt และทำการตรวจสอบว่าใช้ docker ได้หรือไม่โดยการใช้คำสั่ง docker --version



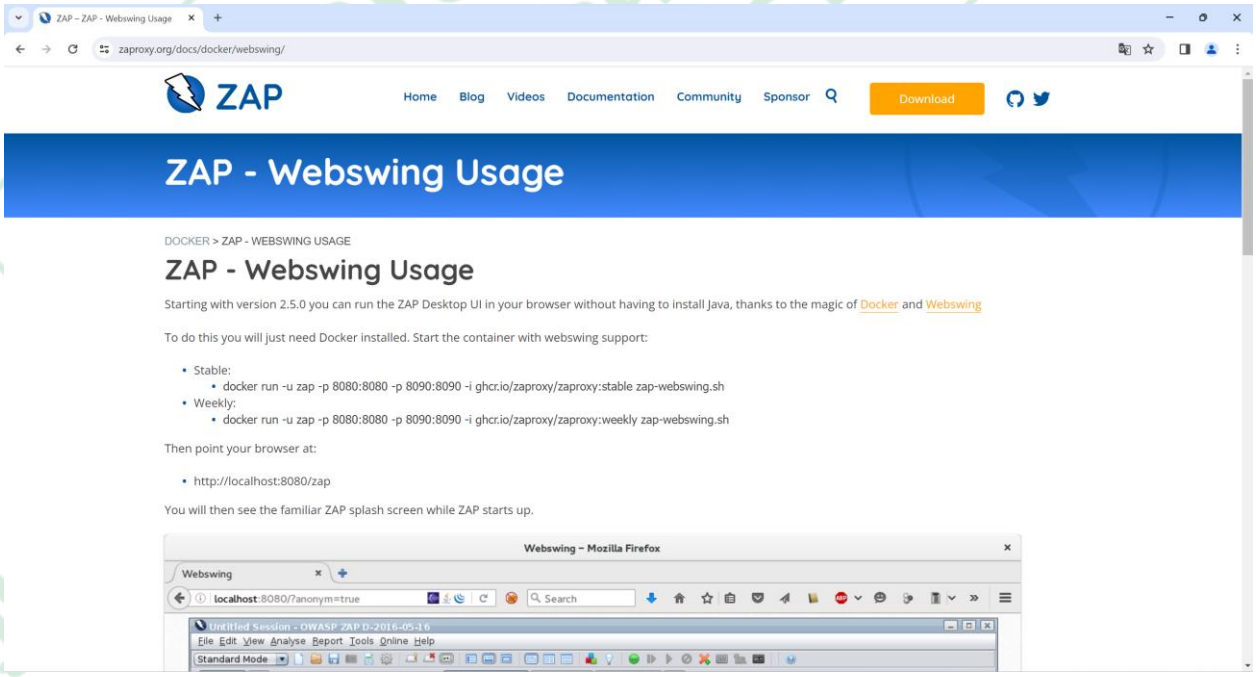
เข้าที่หน้า Website: zaproxy.org ดาวน์โหลดของ zap ในส่วนของ Docker และเลือกใช้คำสั่งเพื่อ pull images ของ docker โดยเลือก Stable



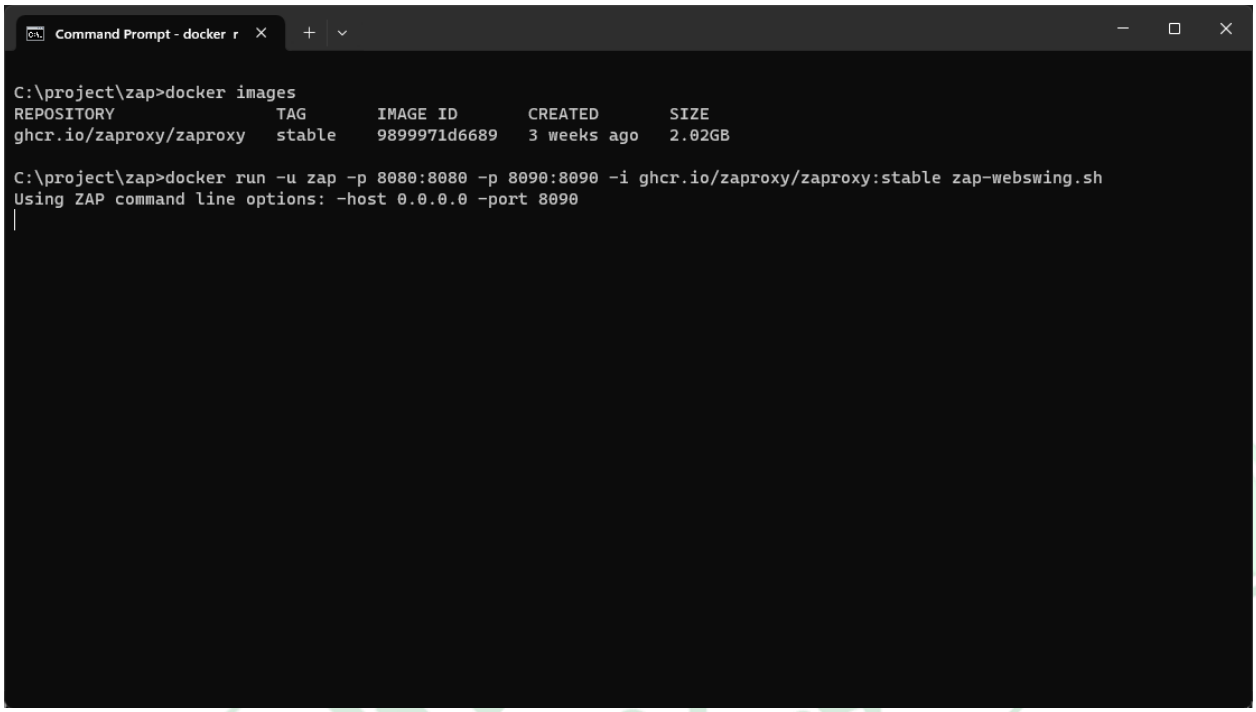
เข้าที่ command prompt ใช้คำสั่ง docker pull ghcr.io/zaproxy/zaproxy:stable และรอจนกว่าจะติดตั้งเสร็จ



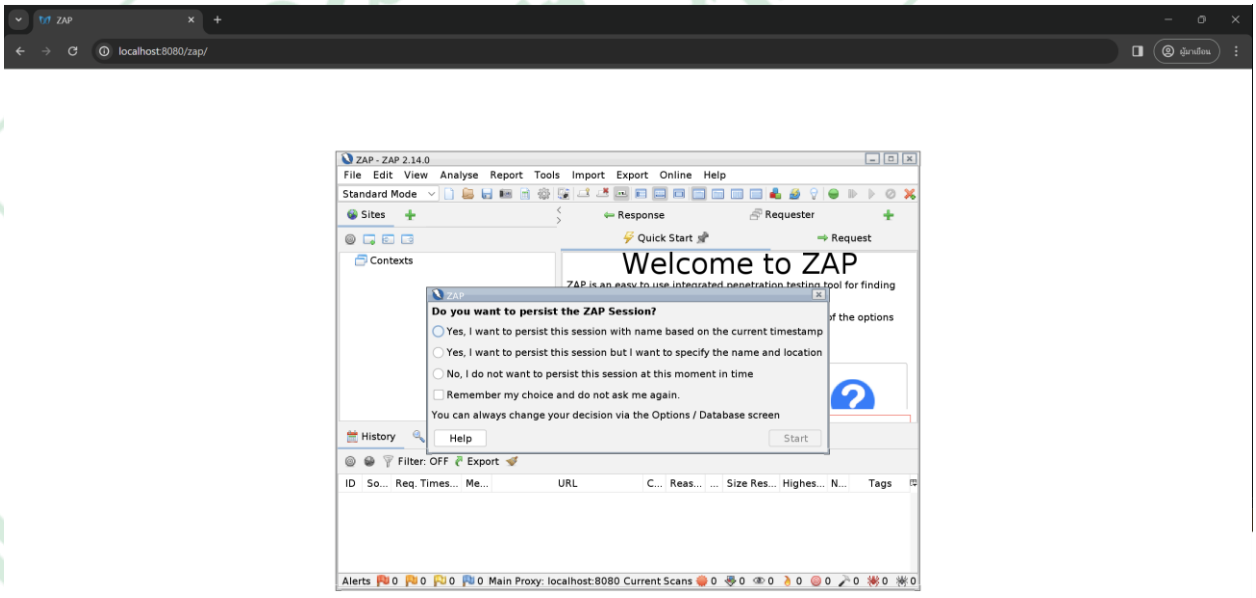
เข้าที่หน้า Document ในส่วน ZAP – Webswing Usage



ทำการใช้คำสั่ง docker run -u zap -p 8080:8080 -p 8090:8090 -i ghcr.io/zaproxy/zaproxy:stable zap-webswing.sh ที่หน้า command prompt

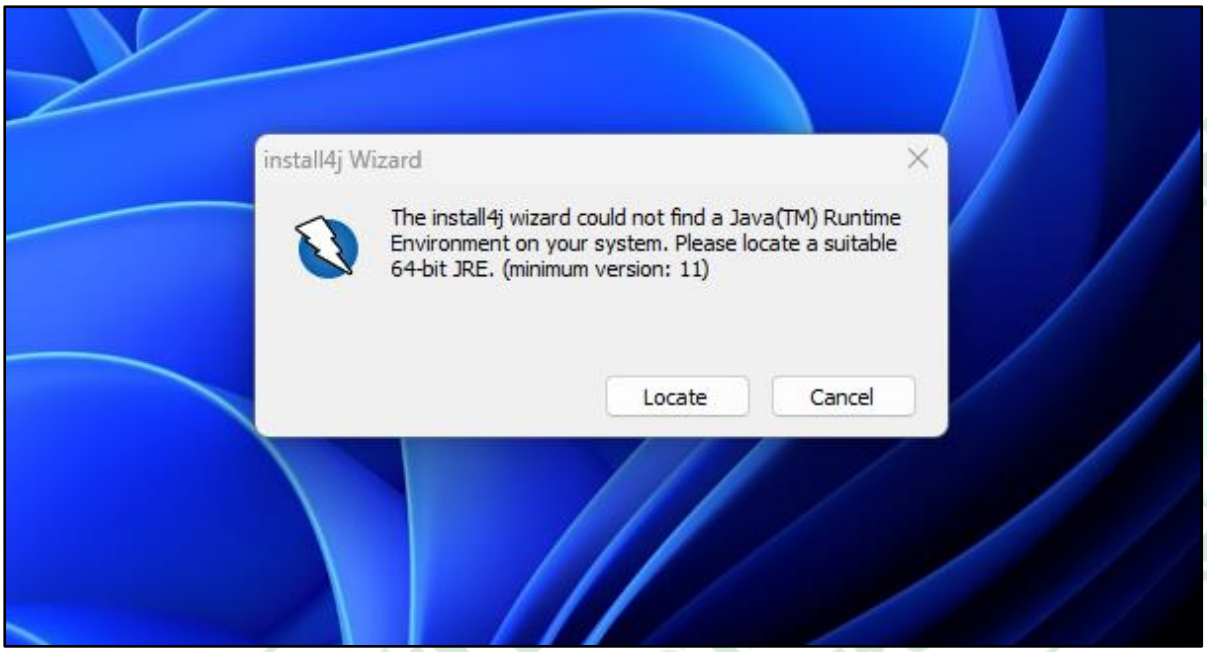


เปิด Browser และเข้า url : http://localhost:8080/zap

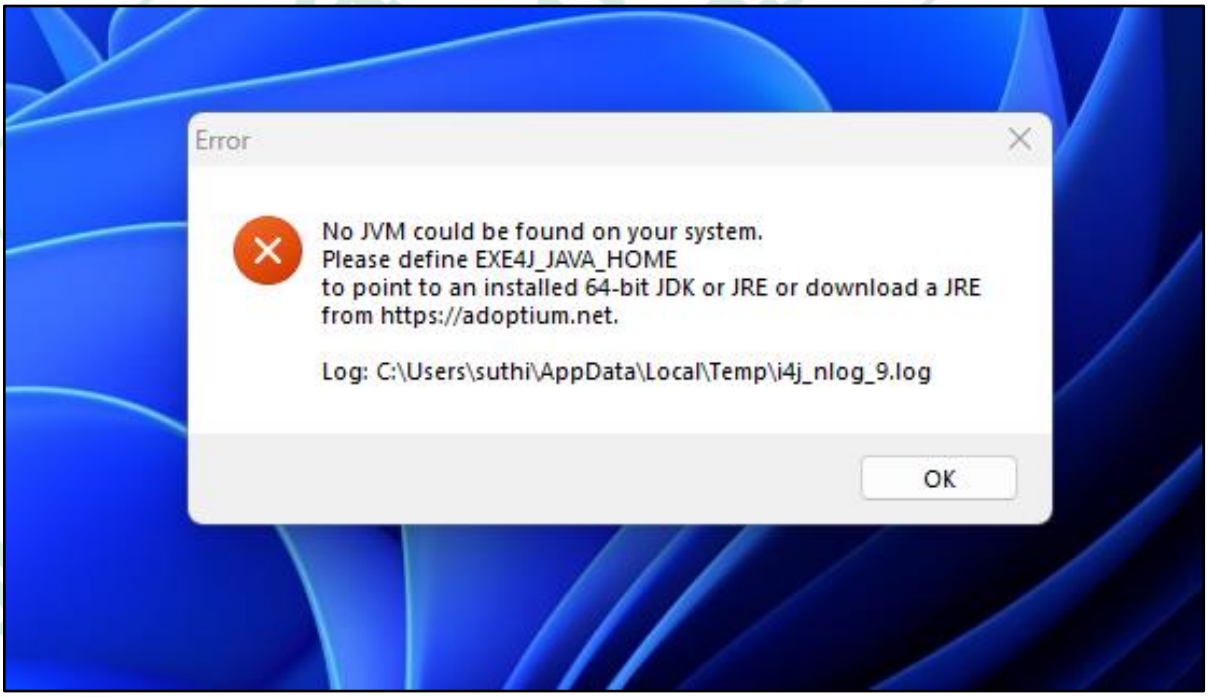


วิธีการติดตั้ง JAVA ก่อนการติดตั้งโปรแกรม ZAP

ภาพแสดง Error การติดตั้งโปรแกรม ZAP

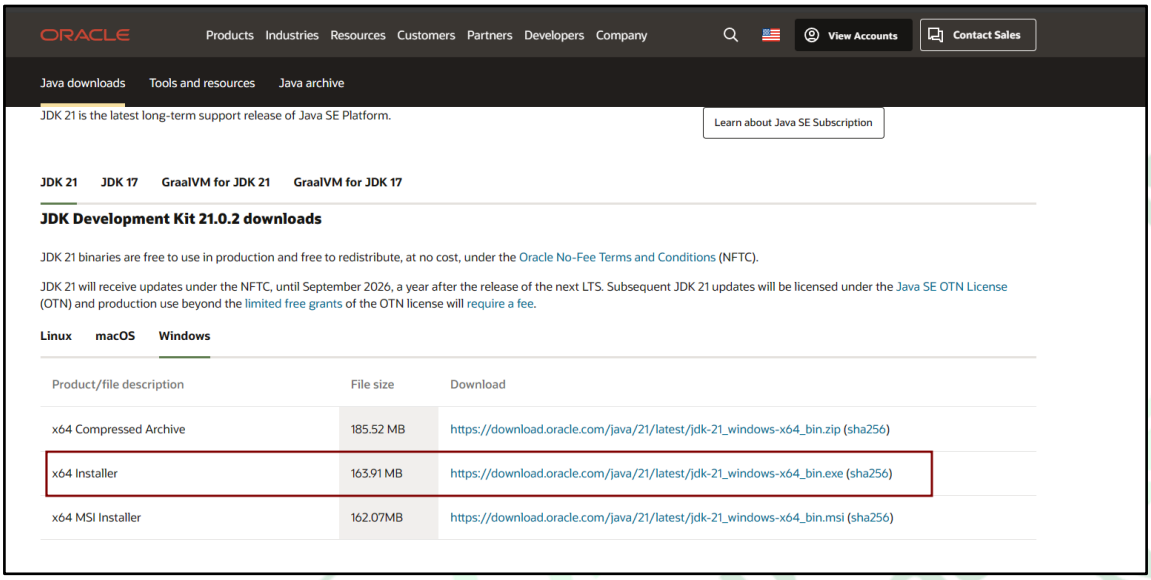


ภาพแสดง Error การติดตั้งโปรแกรม ZAP

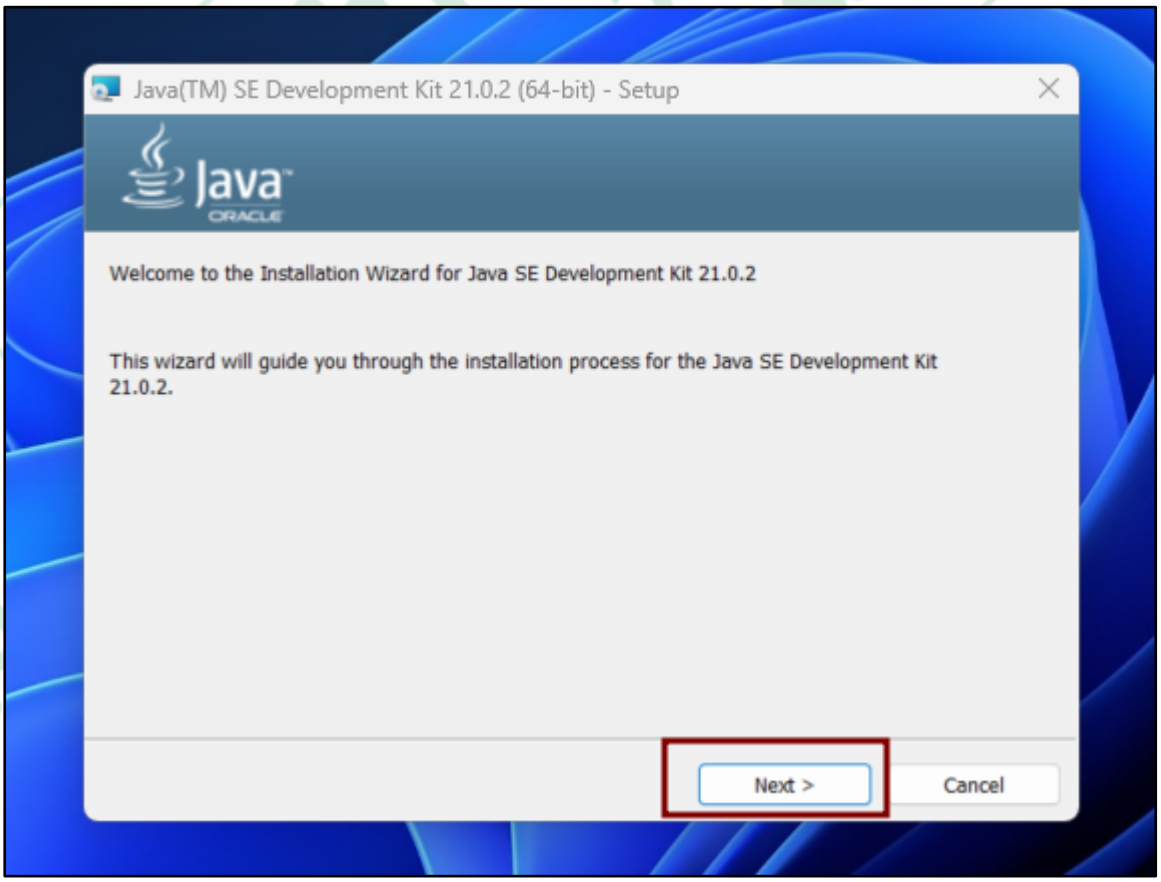


ให้หน่วยงานทำการดาวน์โหลด JDK ตาม OS ของตนเองที่ใช้งาน ที่ลิงก์

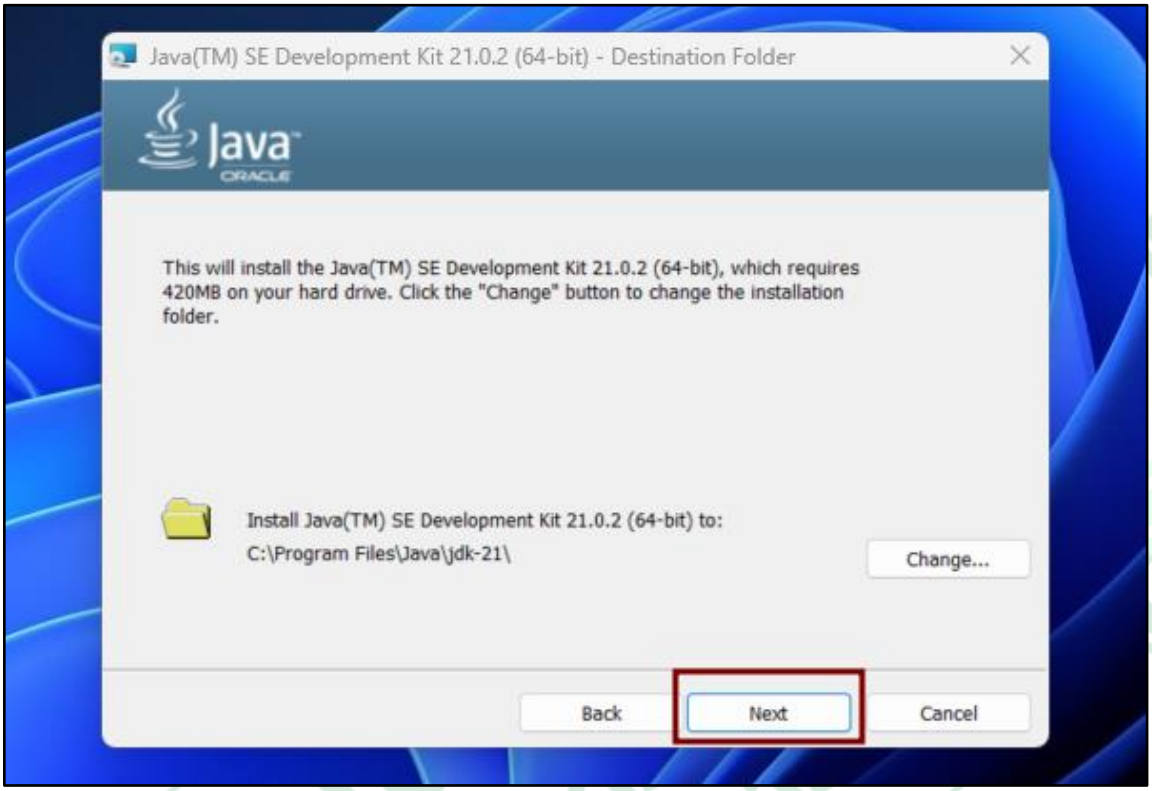
Website : https://www.oracle.com/java/technologies/downloads/#jdk21-windows



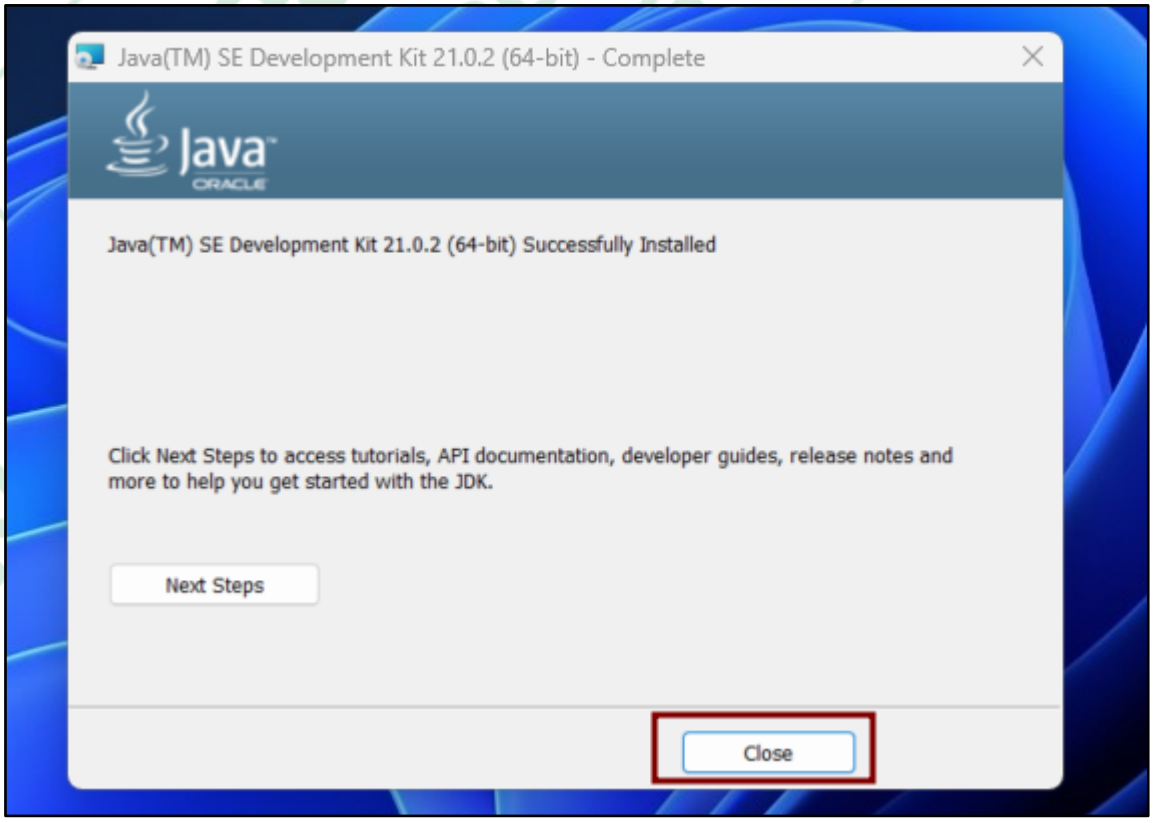
กดติดตั้งไฟล์ที่ได้รับมา คลิก Next



คลิกปุ่ม Next



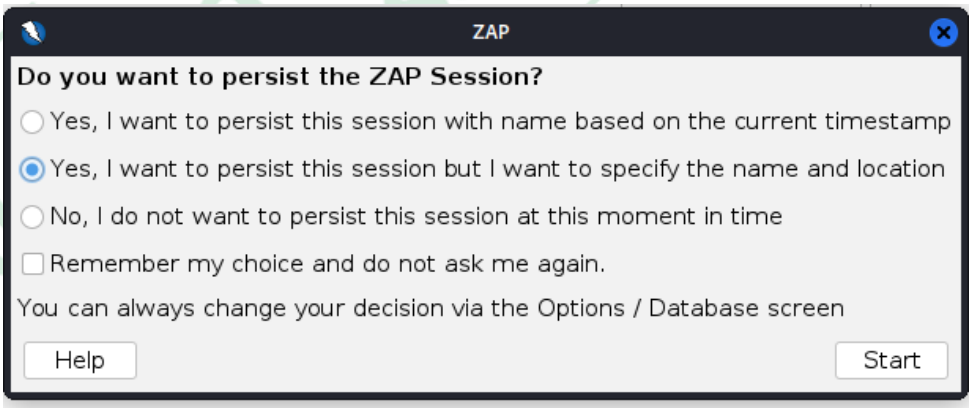
การติดตั้ง JAVA เสร็จเรียบร้อย ทดสอบเปิดโปรแกรม ZAP



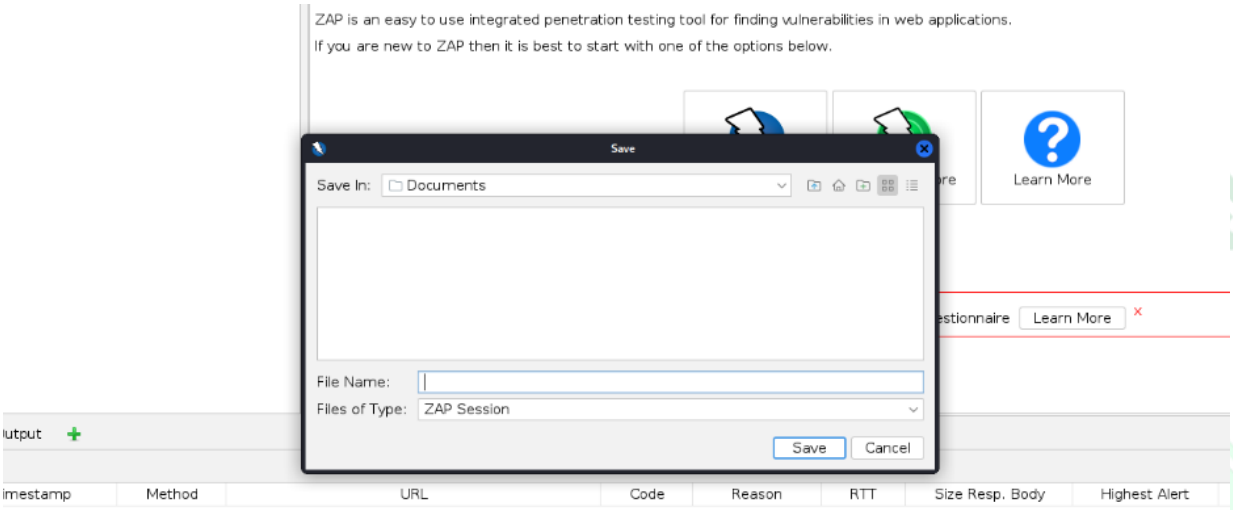
การใช้งานโปรแกรมเบื้องต้น

เปิดโปรแกรม ZAP ที่ทำการติดตั้งสำเร็จเรียบร้อยแล้ว

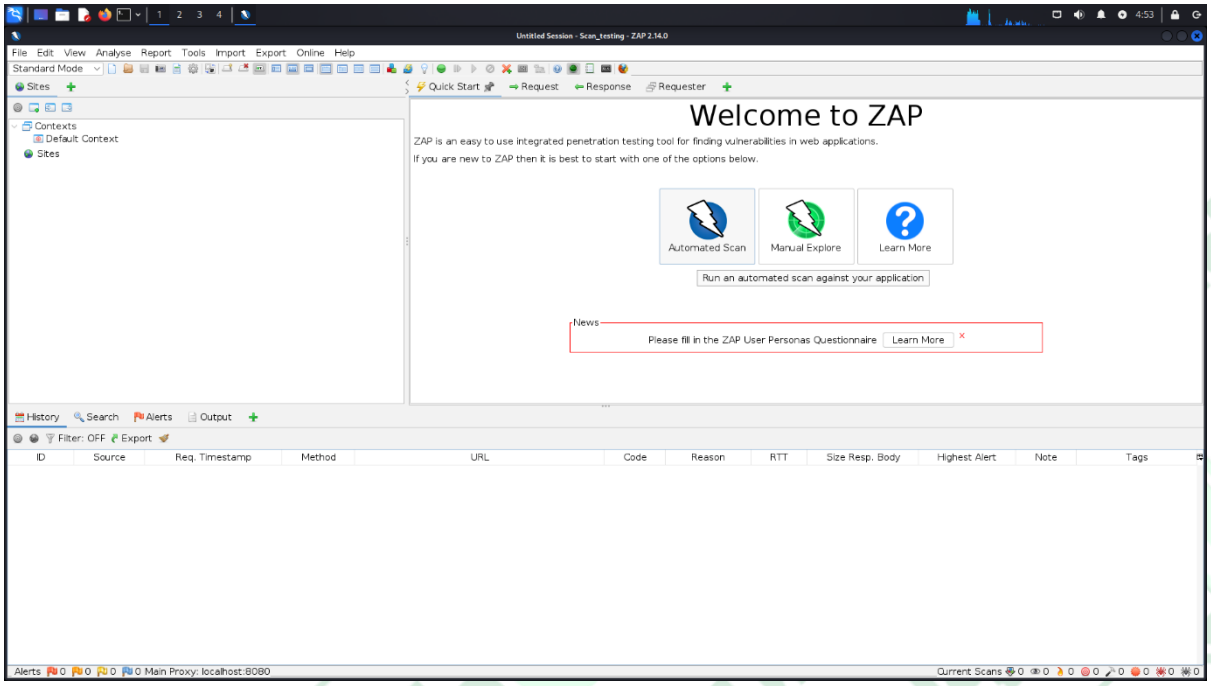
เลือก Yes, I want to persist this session but I want to specify the name and location และคลิก Start



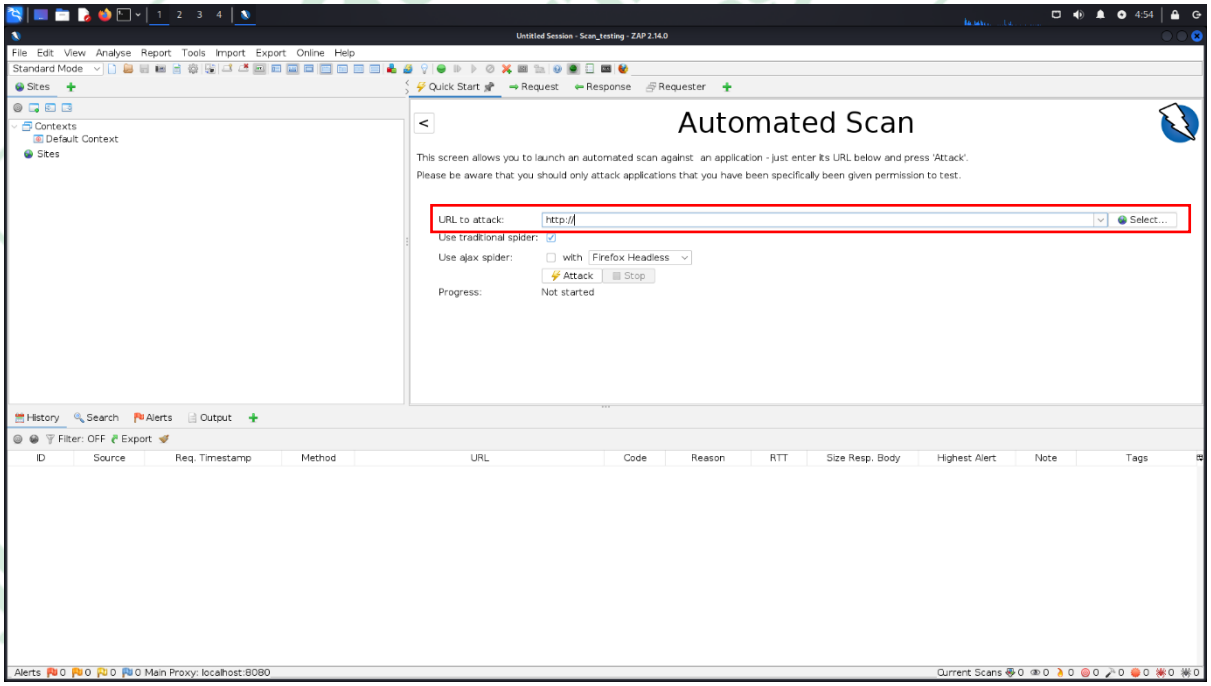
เลือก Folder และตั้งชื่อไฟล์ที่ต้องการ Save



เข้าสู่หน้าต่างโปรแกรมคลิกเลือก Automated Scan



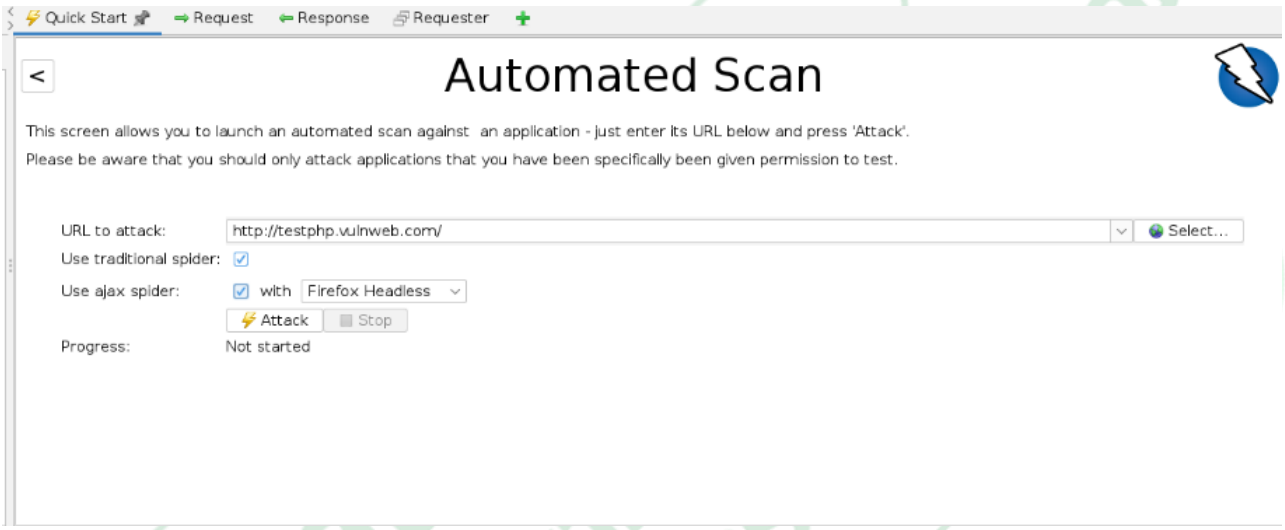
ใส่ URL Website ที่ต้องการตรวจสอบช่องโหว่ลงในช่อง URL to attack เช่น https://xxxx.moph.go.th



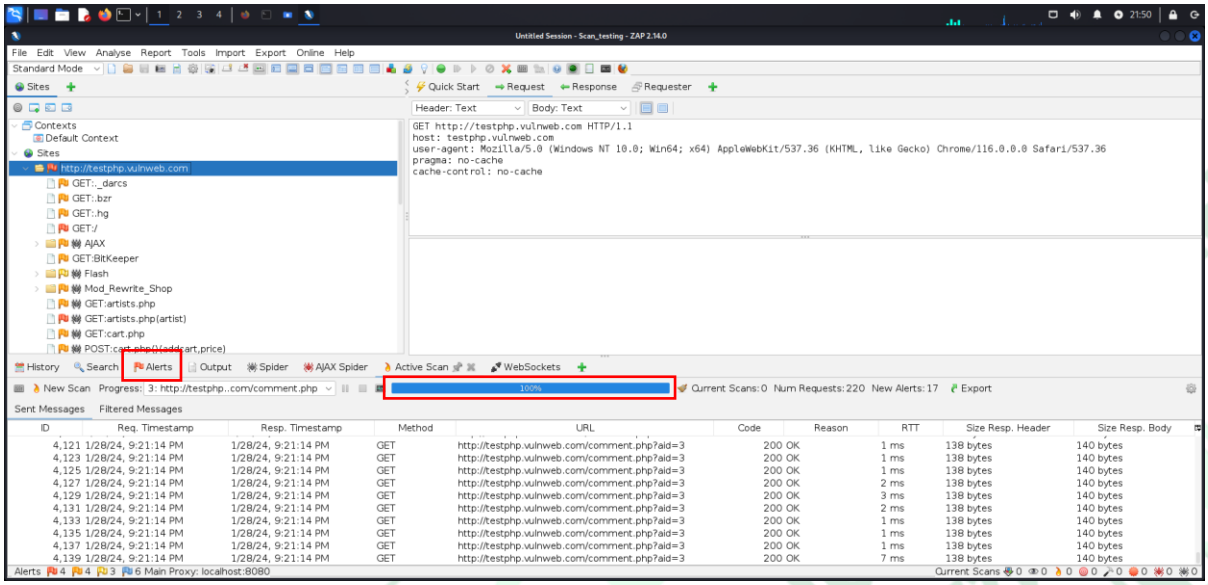
ติ้กเลือกเมนูดังนี้

- Use traditional spider
- Use ajax spider with
- Firefox Headless

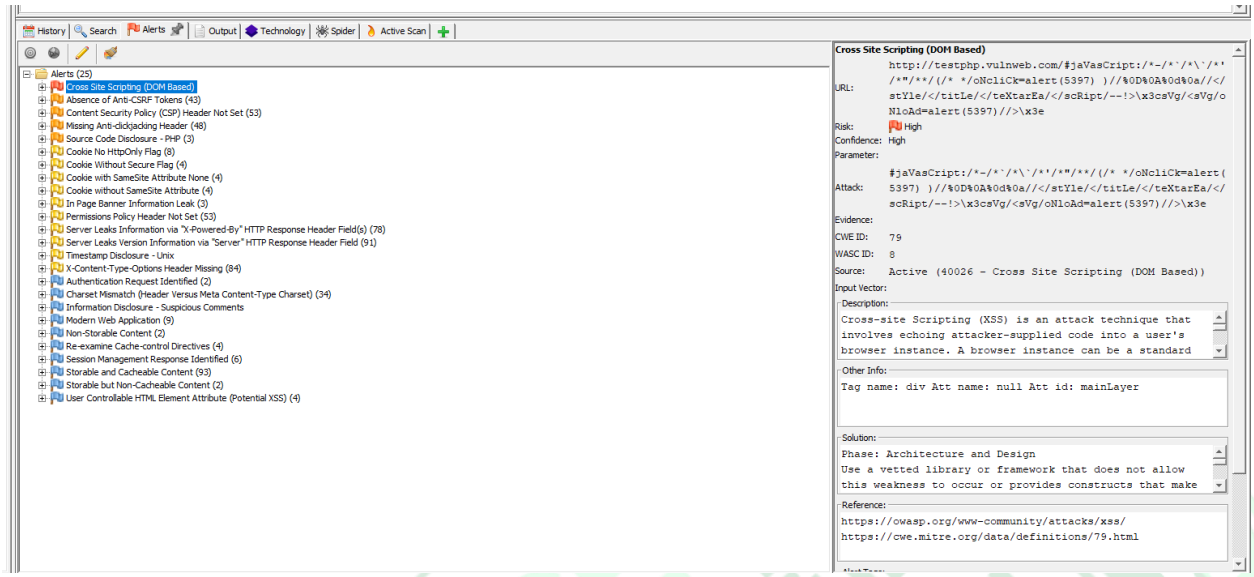
คลิก Attack



รอเมนู Active Scan ของโปรแกรมดำเนินการสแกนจนครบ 100 %



วิธีการตรวจสอบรายละเอียดช่องโหว่ที่พบ

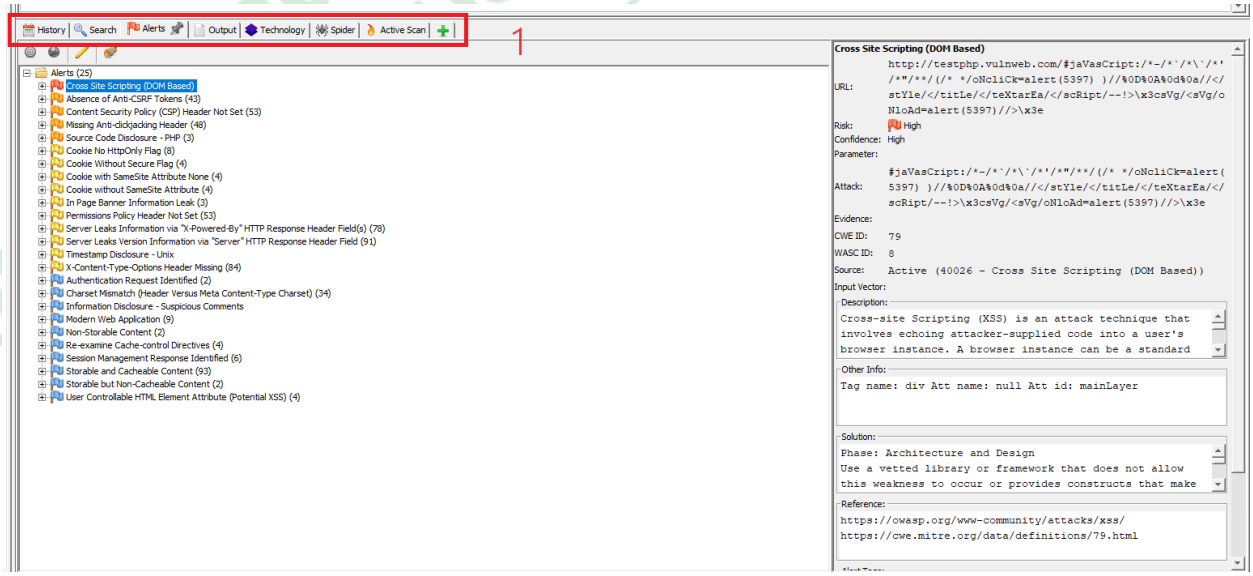


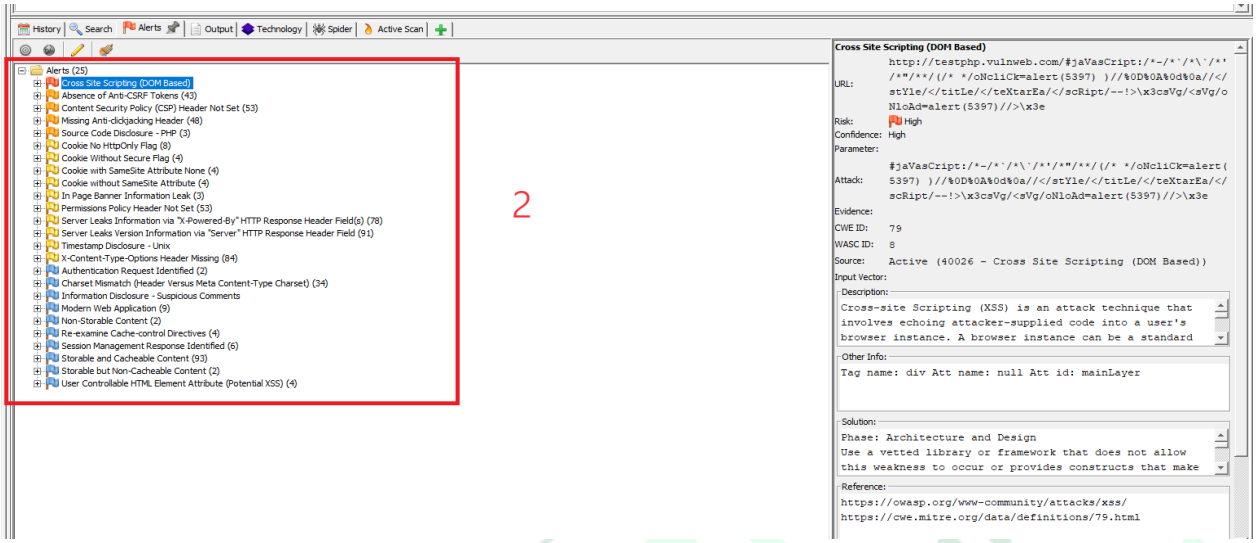
การอ่านรายละเอียดที่จำเป็น

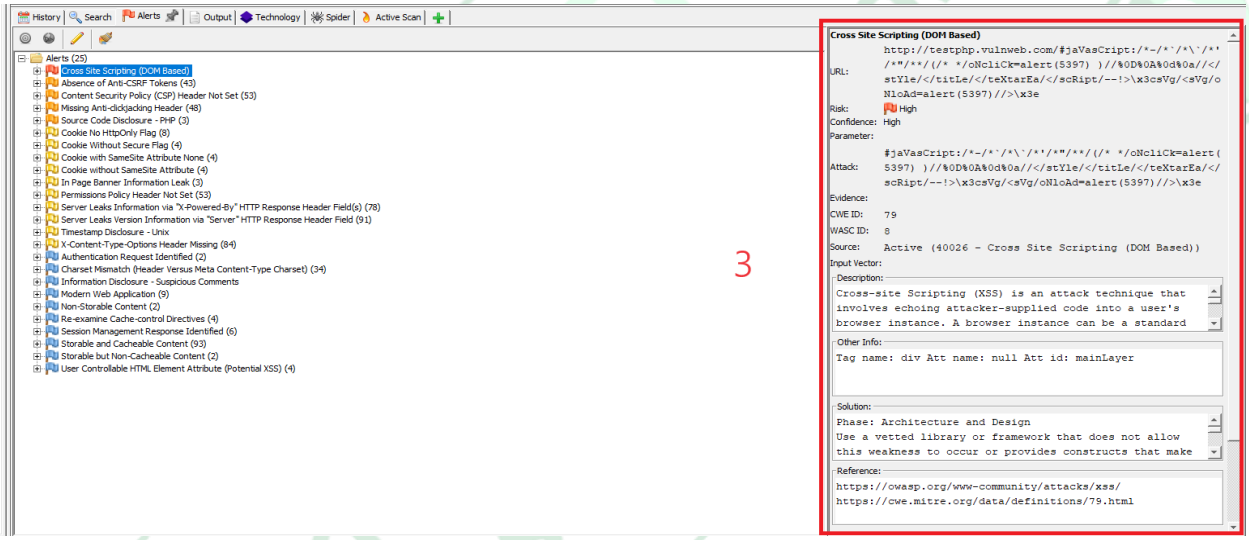
เมื่อทำการ Attack แล้ว จะมีส่วนที่จำเป็นต้องตรวจสอบอยู่ 3 ส่วน

ส่วนที่ 1 และ 2

เราจะทำการตรวจสอบ Alerts Tab เป็นหลักว่าการโจมตีที่ได้ดำเนินการไปแล้วนั้น โปรแกรมตรวจพบอะไรบ้าง แบ่งลำดับความสำคัญคือ High, Medium และ Low โดยในตัวอย่างจะพบว่า สามารถทำ Cross-site Scripting ได้







ส่วนที่ 3

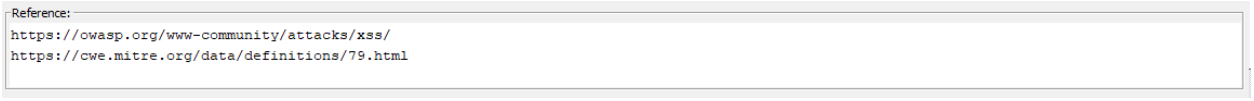
รายละเอียดการโจมตีที่โจมตีสำเร็จ โปรแกรมจะอธิบายถึง Payload ที่ใช้โจมตี รวมถึงรายละเอียดต่างๆ ของประเภทการโจมตีนั้นๆ ภายในส่วนของ Description

Description:
Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash,

และวิธีการแก้ไขปัญหาเพื่อป้องกันหรือลดผลกระทบของการโจมตีจะอยู่ในส่วนของ Solution

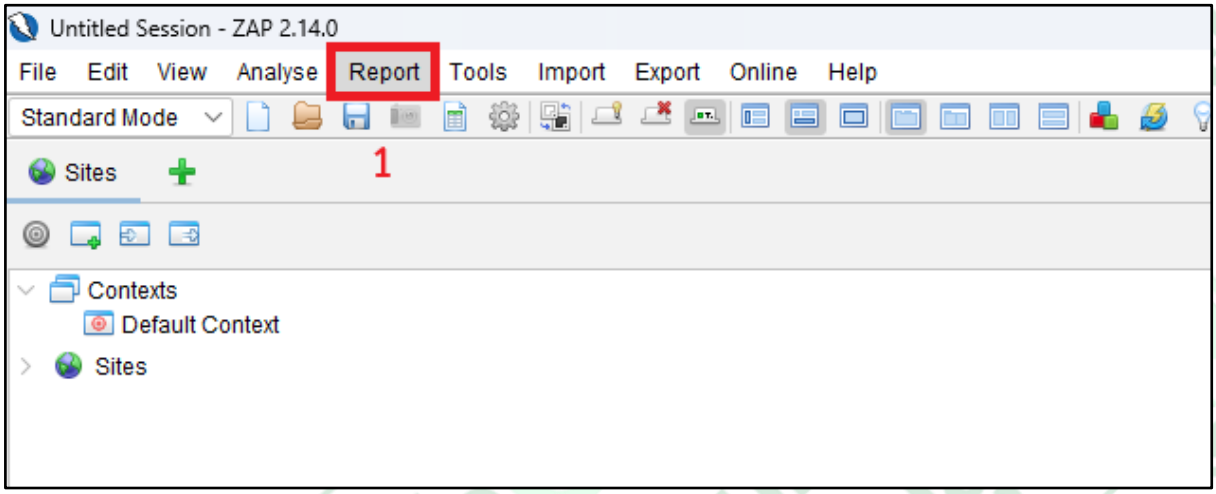
Solution:
Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

โดยผู้ใช้งาน สามารถตรวจสอบรายละเอียดเพิ่มเติมของการโจมตีนี้ได้จากส่วน Reference

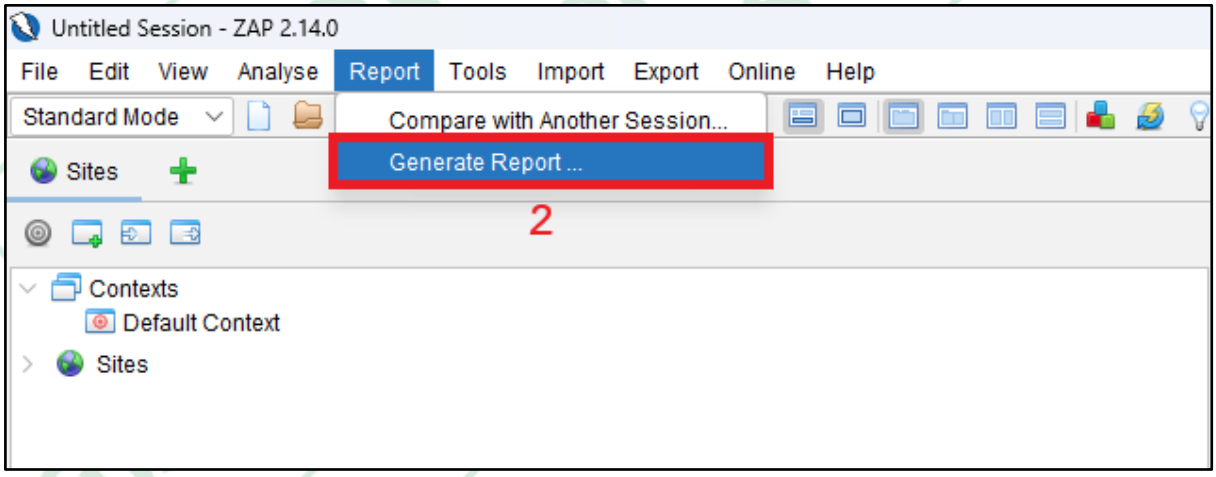


การออกรายงานการตรวจสอบช่องโหว่

ขั้นตอนที่ 1 หลักจากการสแกนหาช่องโหว่ให้ไปเลือกเมนู Report เพื่อทำการออกรายงาน



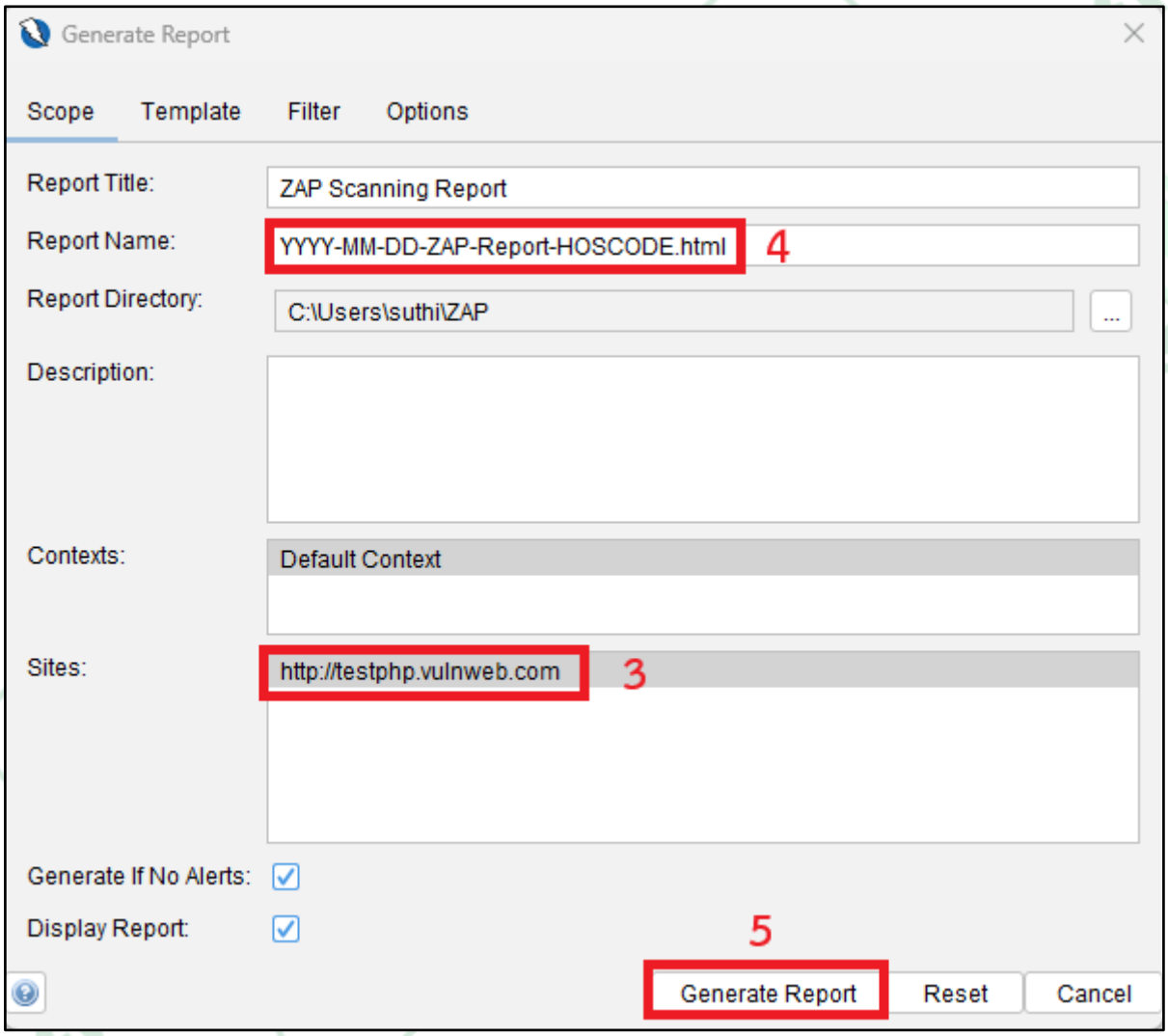
ขั้นตอนที่ 2 ให้คลิก Generate Report จะปรากฏหน้าการตั้งค่าการออกรายงาน



ขั้นตอนที่ 3 เลือก sites ที่ต้องการออกรายงาน

ขั้นตอนที่ 4 ให้ตั้งชื่อไฟล์ YYYY-MM-DD-ZAP-Report-รหัสสถานพยาบาล5หลัก.html

ขั้นตอนที่ 5 คลิก Generate Report เพื่อออกรายงาน



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)

ภาพแสดงตัวอย่างแบบรายงานที่ได้รับ

Contents

ภาพแสดงตัวอย่างแบบรายงานที่ได้รับ

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

ภาพแสดงตัวอย่างแบบรายงานที่ได้รับ

Alerts

Risk=Medium, **Confidence**=High (1)

http://testphp.vulnweb.com (1)

Content Security Policy (CSP) Header Not Set (1)

▶ GET http://testphp.vulnweb.com/robots.txt

Risk=Medium, **Confidence**=Medium (1)

http://testphp.vulnweb.com (1)

Missing Anti-clickjacking Header (1)

▶ GET http://testphp.vulnweb.com/

Risk=Medium, **Confidence**=Low (1)

http://testphp.vulnweb.com (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://testphp.vulnweb.com/

Risk=Low, **Confidence**=High (1)

ภาพแสดงตัวอย่างแบบรายงานที่ได้รับ