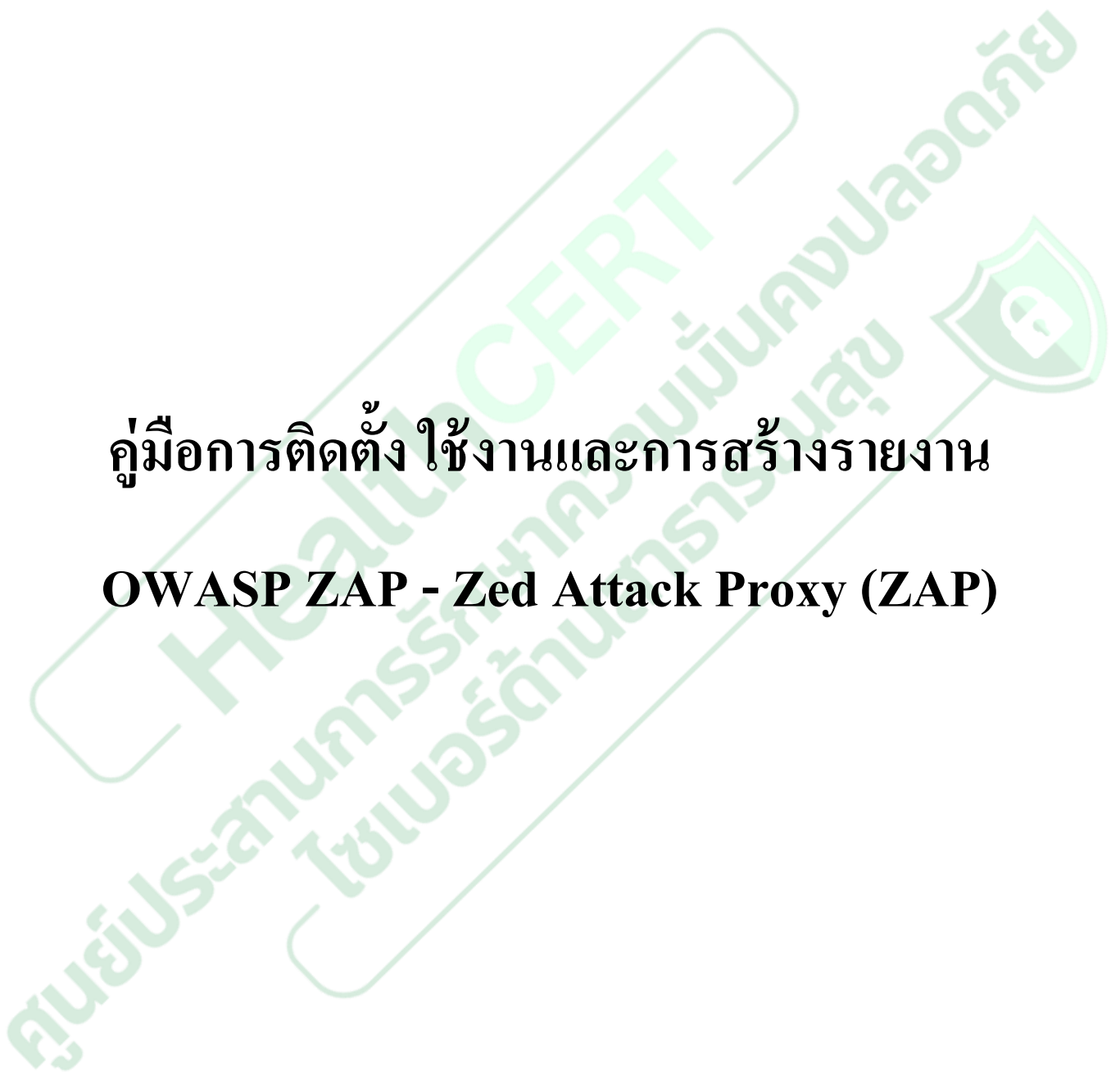
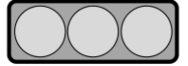


คู่มือการติดตั้ง ใช้งานและการสร้างรายงาน

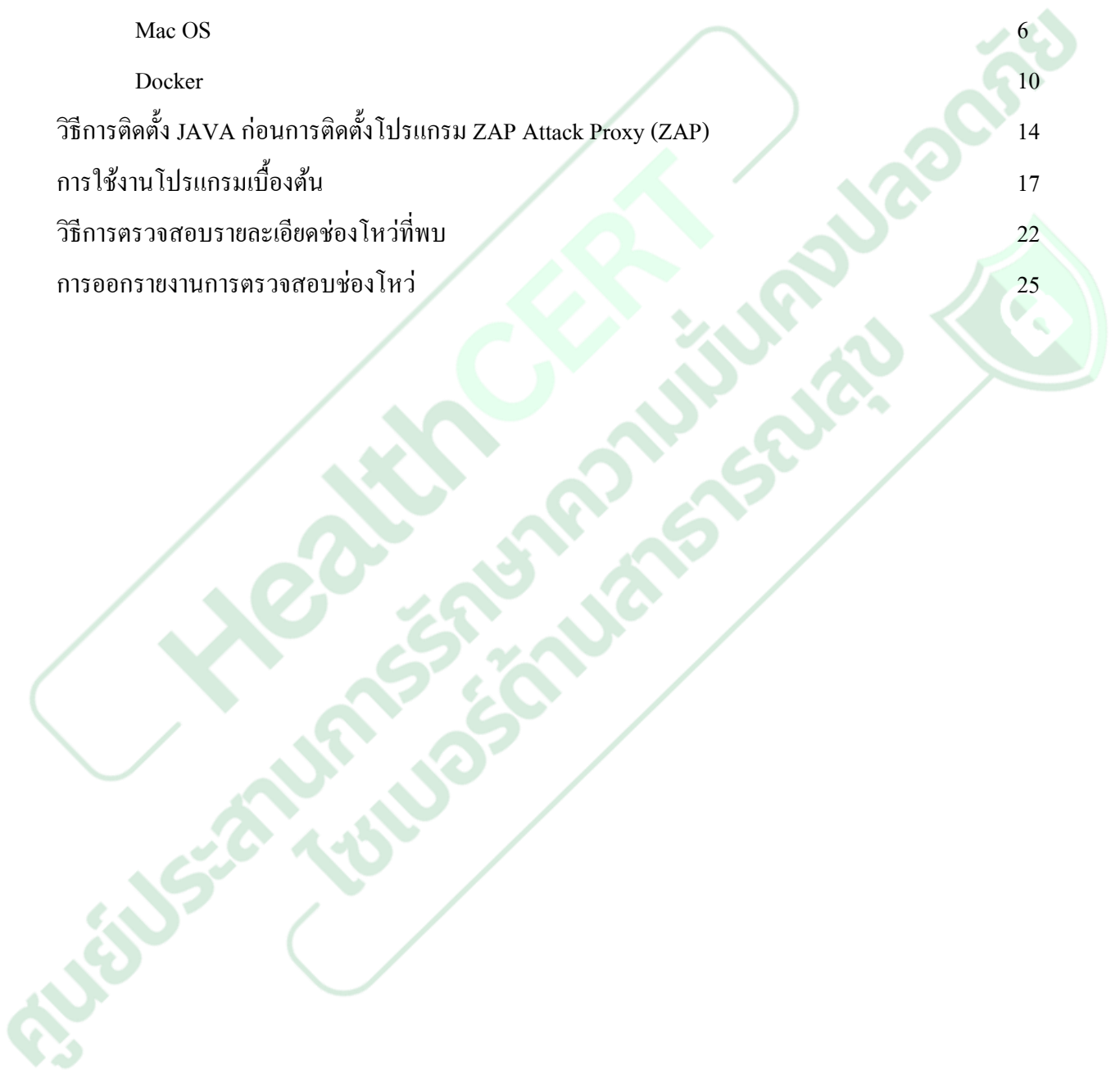
OWASP ZAP - Zed Attack Proxy (ZAP)





สารบัญ

OWASP ZAP Attack Proxy คืออะไร	1
วิธีการติดตั้งโปรแกรม ZAP Attack Proxy (ZAP)	2
Windows OS	2
Mac OS	6
Docker	10
วิธีการติดตั้ง JAVA ก่อนการติดตั้งโปรแกรม ZAP Attack Proxy (ZAP)	14
การใช้งานโปรแกรมเบื้องต้น	17
วิธีการตรวจสอบรายละเอียดช่องโหว่ที่พบ	22
การออกรายงานการตรวจสอบช่องโหว่	25



OWASP ZAP คืออะไร

OWASP ZAP เป็นเครื่องมือที่ใช้สำหรับการทดสอบความปลอดภัยของเว็บแอปพลิเคชัน ซึ่งเป็นกระบวนการที่สำคัญสำหรับการพัฒนาซอฟต์แวร์ที่มีคุณภาพ การทดสอบความปลอดภัยของเว็บแอปพลิเคชันมีวัตถุประสงค์เพื่อค้นหาช่องโหว่หรือจุดอ่อนที่อาจทำให้ผู้ไม่หวังดีสามารถเข้าถึง แก้ไข หรือทำลายข้อมูลที่สำคัญ หรือทำให้เว็บแอปพลิเคชันไม่สามารถทำงานได้

OWASP ZAP เป็นเครื่องมือที่มีความยืดหยุ่นและมีคุณสมบัติที่หลากหลาย เช่น

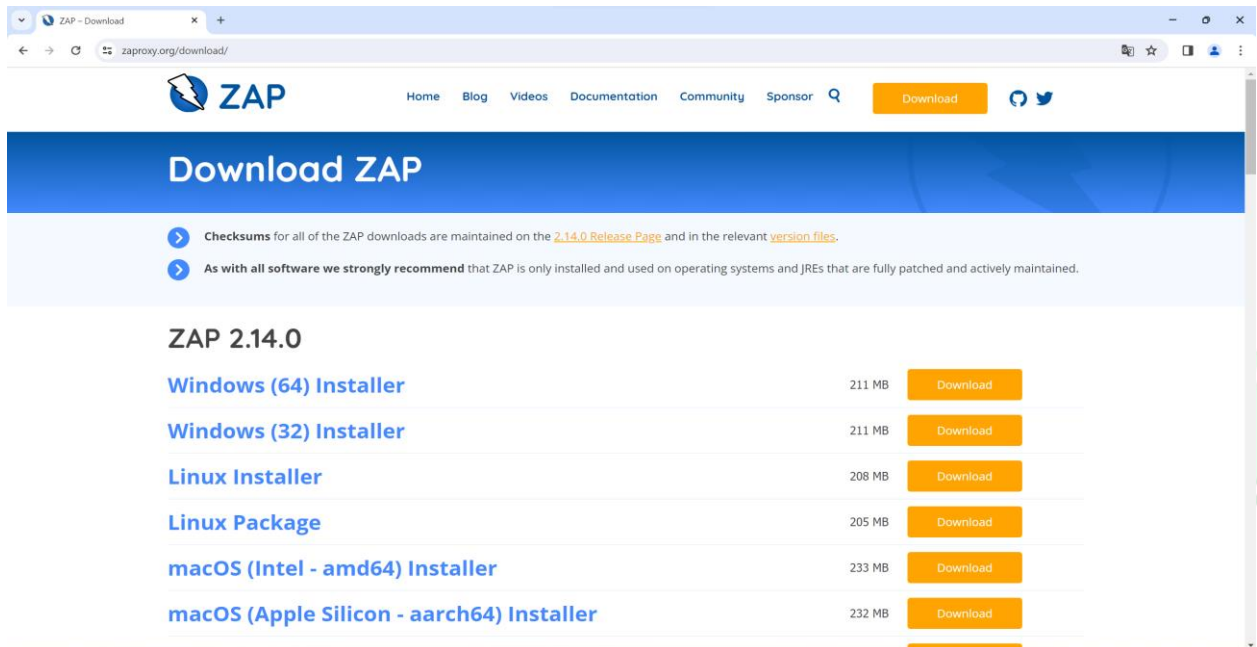
- Proxy interception : เป็นการดักจับการสื่อสารระหว่างเว็บเบราว์เซอร์และเว็บแอปพลิเคชัน เพื่อวิเคราะห์และแก้ไขคำขอและการตอบกลับ ซึ่งช่วยให้ผู้ใช้สามารถเห็นและเปลี่ยนแปลงข้อมูลที่ถูกส่งไปยังเว็บแอปพลิเคชันได้
- Automated scanning : เป็นการส่งคำขอที่มีการเปลี่ยนแปลงค่าต่างๆ เช่น พารามิเตอร์ หัวข้อ หรือโค้ด เพื่อค้นหาช่องโหว่ที่อาจมีอยู่ในเว็บแอปพลิเคชัน โดยการสแกนอัตโนมัติสามารถทำได้ทั้งแบบแอคทีฟ (active) และพาสซีฟ (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

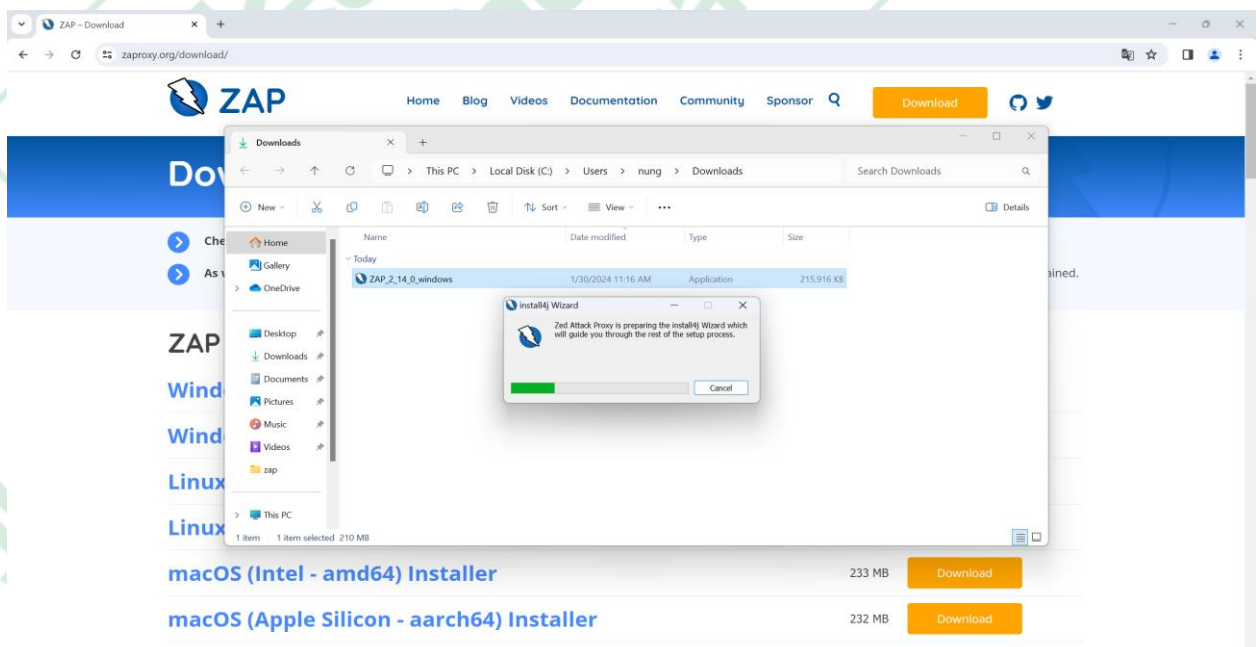
วิธีการติดตั้งโปรแกรม ZAP Attack Proxy (ZAP) สำหรับผู้ใช้ Windows

เข้าที่ Website : zapproxy.org และเข้าสู่หน้าของการ Download และ เลือกดาวน์โหลดไฟล์ Windows (64)

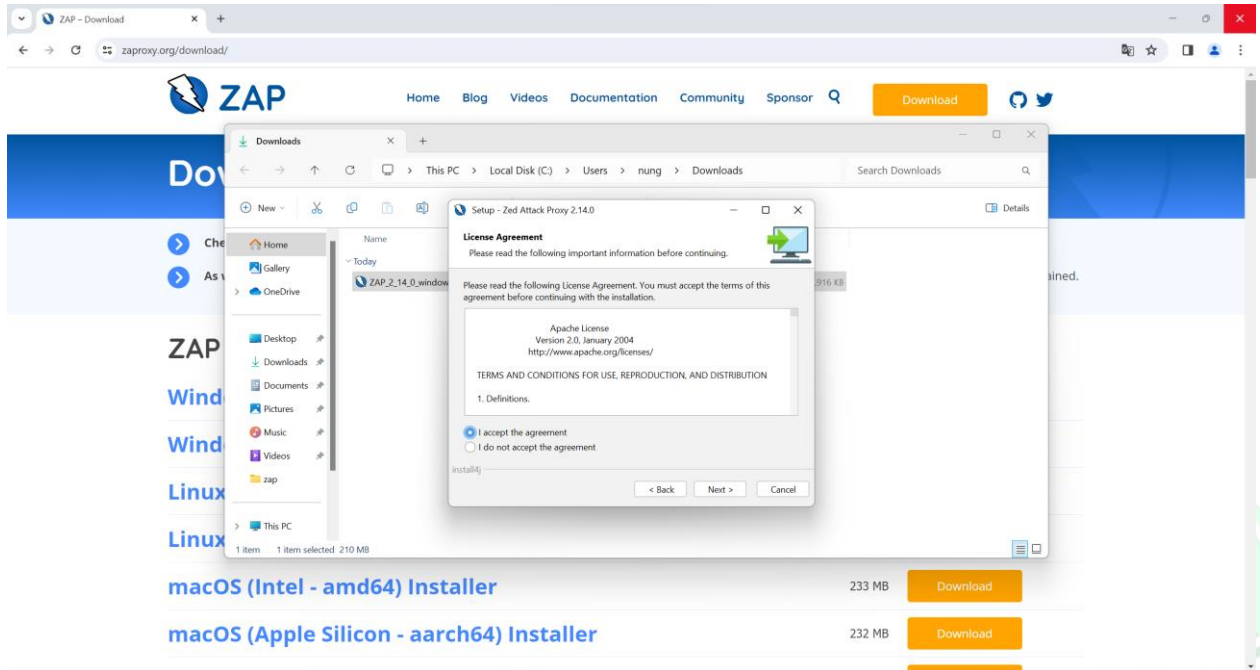
Installer



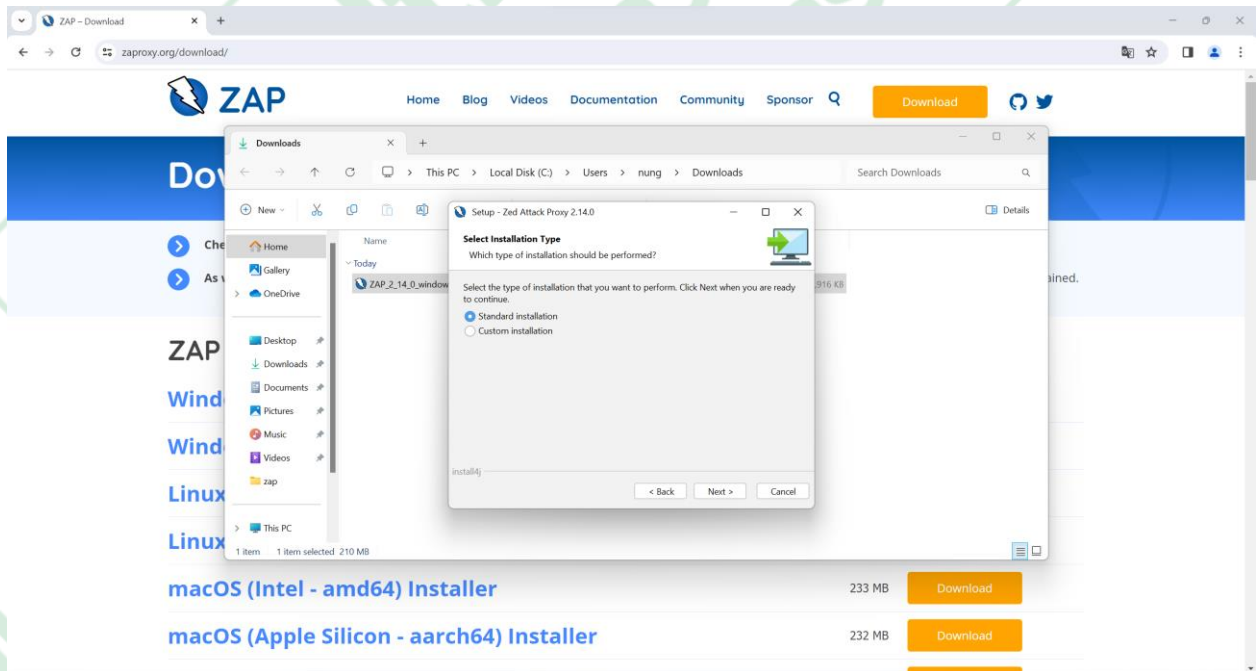
ทำการตรวจสอบไฟล์ที่ดาวน์โหลดและ Double Click เพื่อติดตั้งโปรแกรม



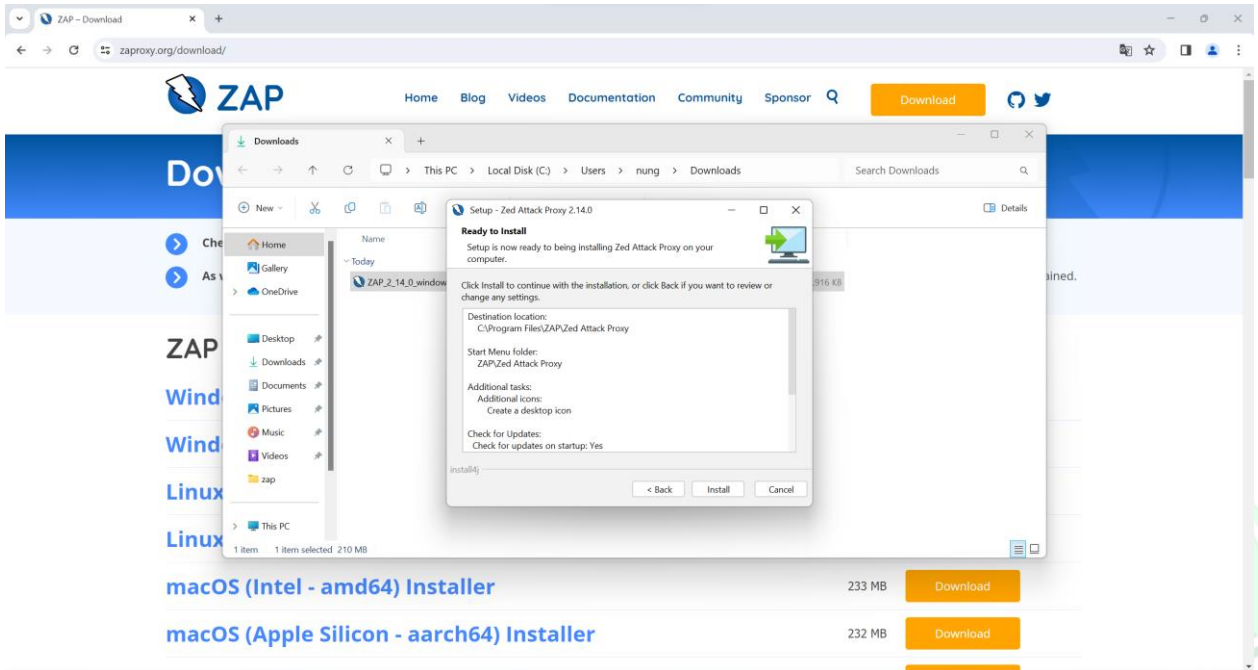
กด Next ไปจนกระทั่งแสดงหน้า License Agreement ให้เลือก Accept และกด Next



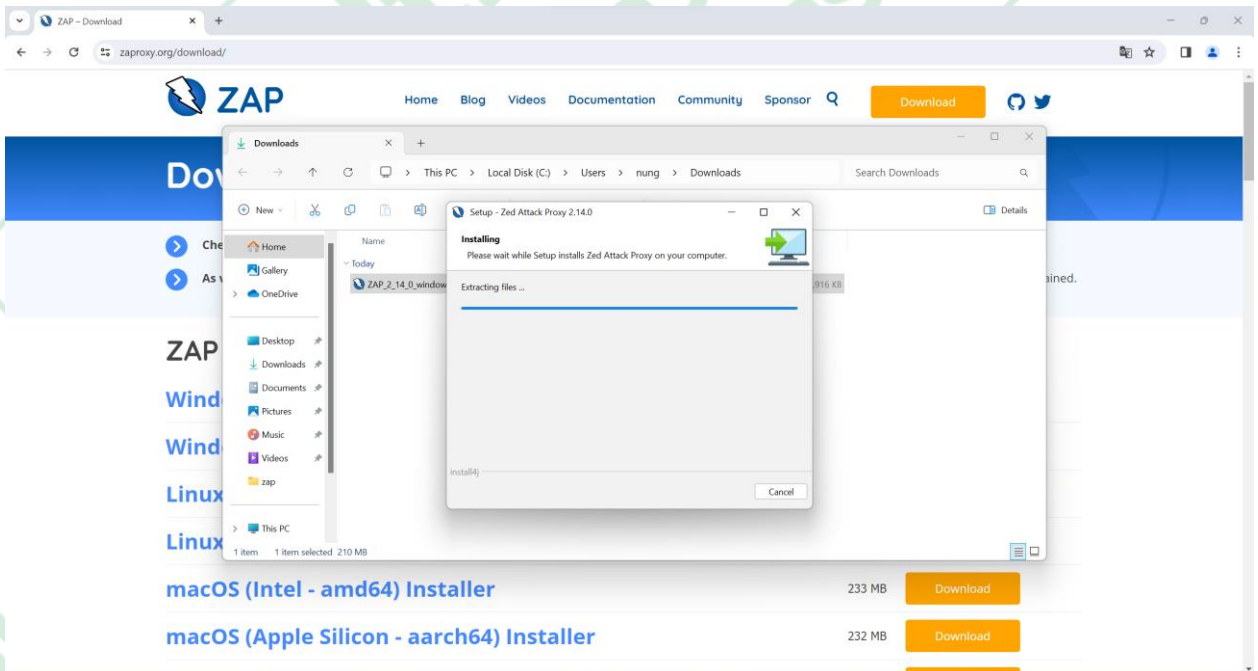
เลือก Standard Installation และไปสู่อันดับต่อไปโดยการเลือก Next



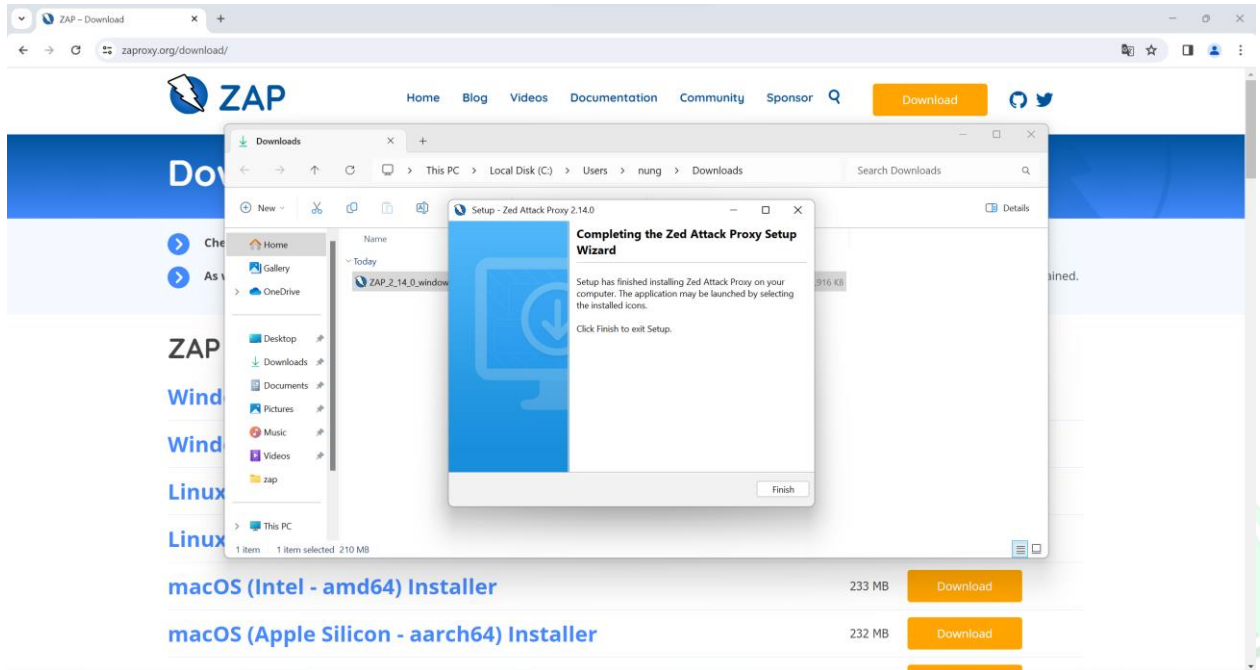
ทำการเลือก Install เพื่อติดตั้งโปรแกรม



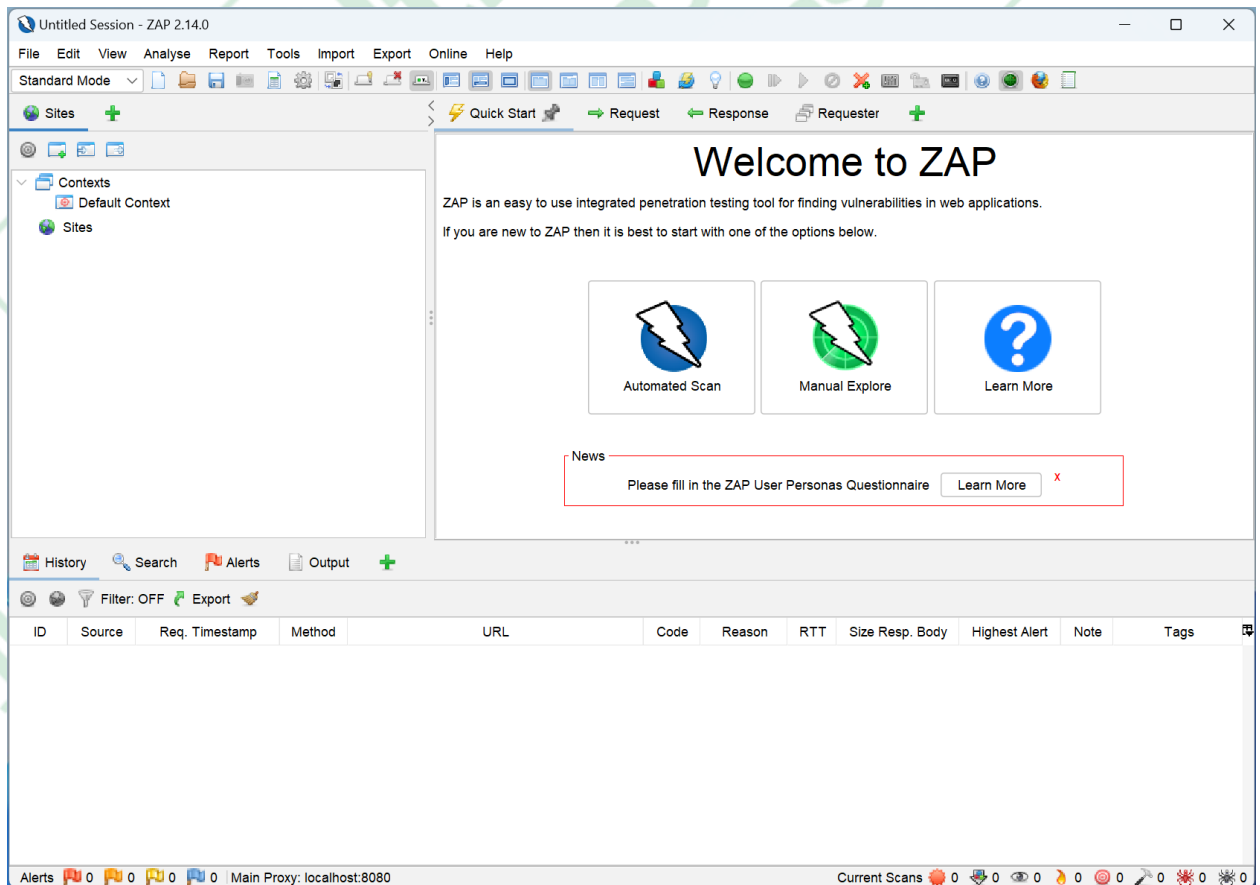
รอนจนกว่าจะติดตั้งโปรแกรมสำเร็จ



แสดงหน้าเสร็จสิ้นขั้นตอนการติดตั้งโปรแกรมให้คลิกปุ่ม Finish

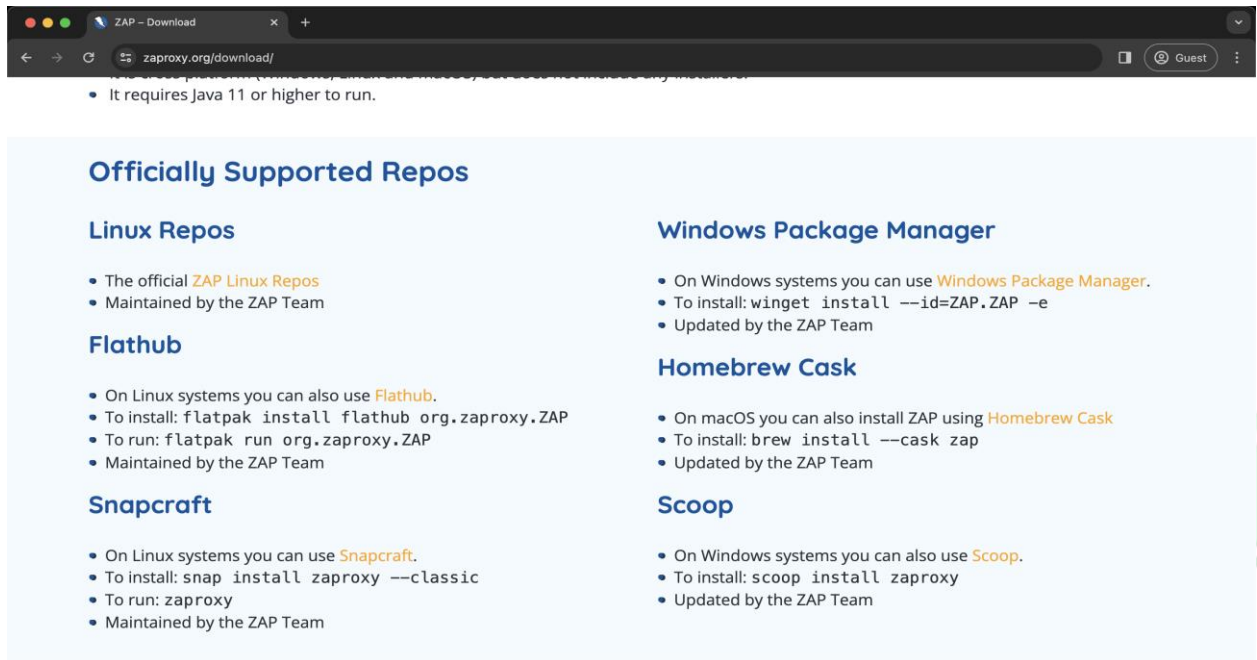


เปิดโปรแกรมเพื่อใช้งาน



วิธีการติดตั้งโปรแกรม Zed Attack Proxy (ZAP) สำหรับผู้ใช้ Mac

เข้าที่ Website : zapproxy.org และเข้าสู่หน้าของการ Download และค้นหาที่มีคำว่า Homebrew Cask



It requires Java 11 or higher to run.

Officially Supported Repos

Linux Repos

- The official [ZAP Linux Repos](#)
- Maintained by the ZAP Team

Flathub

- On Linux systems you can also use [Flathub](#).
- To install: `flatpak install flathub org.zaproxy.ZAP`
- To run: `flatpak run org.zaproxy.ZAP`
- Maintained by the ZAP Team

Snapcraft

- On Linux systems you can use [Snapcraft](#).
- To install: `snap install zaproxy --classic`
- To run: `zaproxy`
- Maintained by the ZAP Team

Windows Package Manager

- On Windows systems you can use [Windows Package Manager](#).
- To install: `winget install --id=ZAP.ZAP -e`
- Updated by the ZAP Team

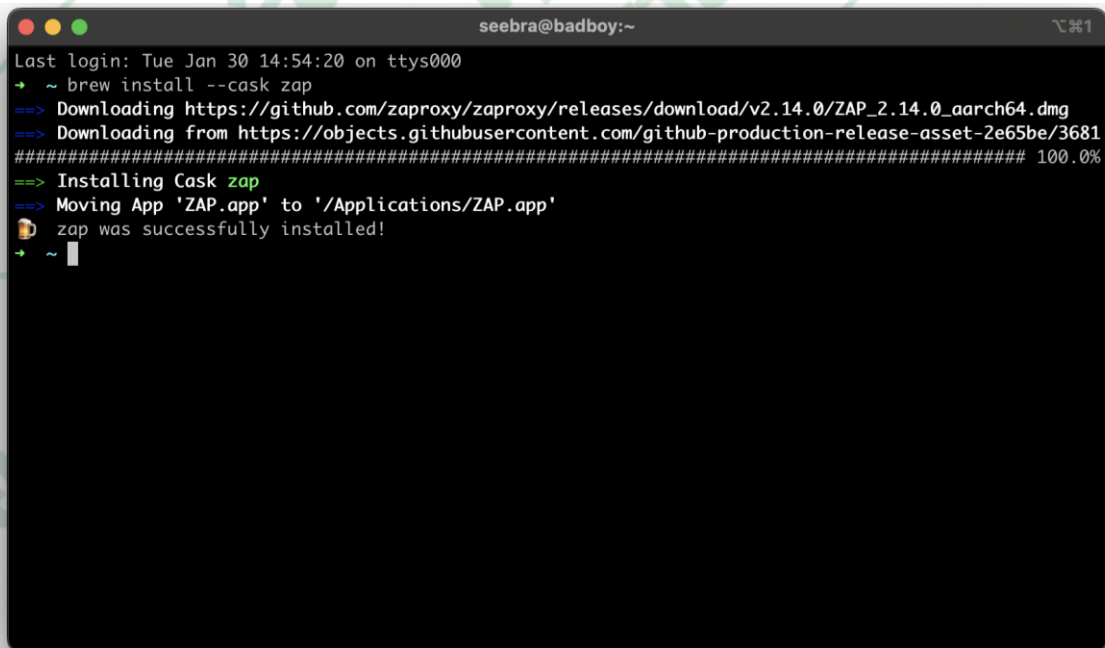
Homebrew Cask

- On macOS you can also install ZAP using [Homebrew Cask](#)
- To install: `brew install --cask zap`
- Updated by the ZAP Team

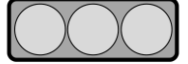
Scoop

- On Windows systems you can also use [Scoop](#).
- To install: `scoop install zaproxy`
- Updated by the ZAP Team

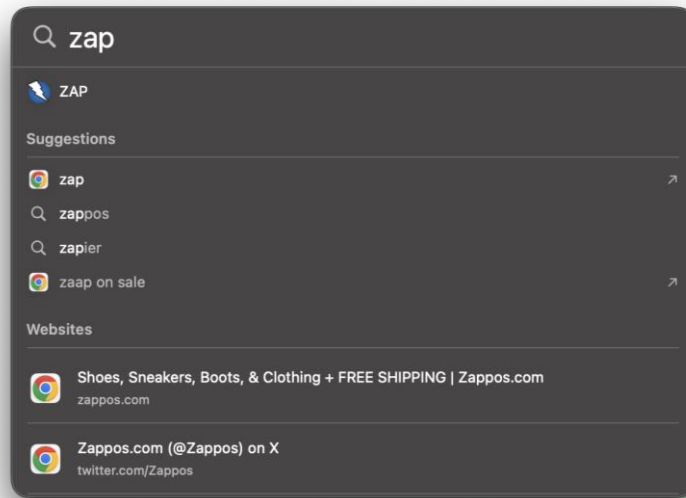
เปิด Terminal และใช้คำสั่ง `brew install --cask zap` และรอนจนกว่าจะติดตั้งโปรแกรมเสร็จ



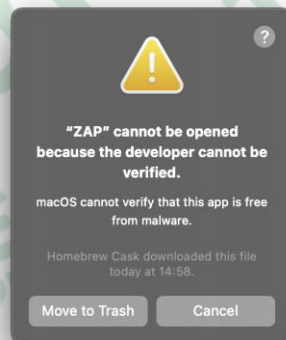
```
seebra@badboy:~
Last login: Tue Jan 30 14:54:20 on ttys000
~ brew install --cask zap
=> Downloading https://github.com/zaproxy/zaproxy/releases/download/v2.14.0/ZAP_2.14.0_aarch64.dmg
=> Downloading from https://objects.githubusercontent.com/github-production-release-asset-2e65be/3681
##### 100.0%
=> Installing Cask zap
=> Moving App 'ZAP.app' to '/Applications/ZAP.app'
📦 zap was successfully installed!
~
```

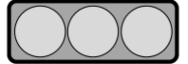



ทำการเปิดโปรแกรม ZAP

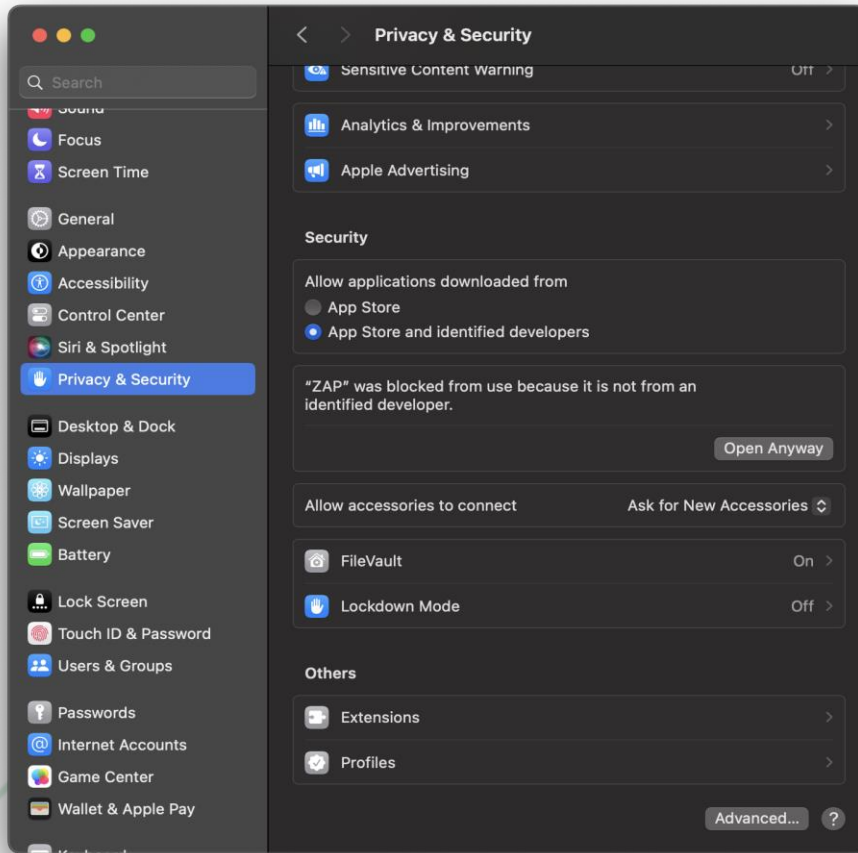


กรณีที่มีข้อความแจ้งเตือนเกี่ยวกับเรื่องความปลอดภัย ให้เลือก Cancel

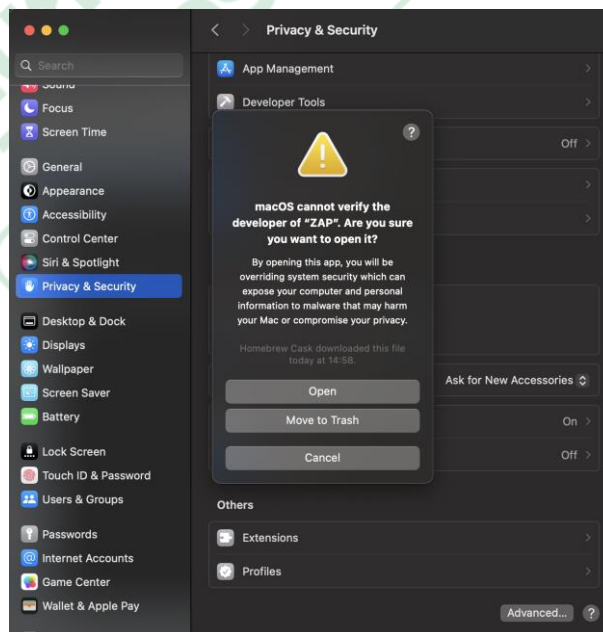




เข้าที่ setting -> Privacy & Security ดูที่ส่วนของ “ZAP” was blocked และเลือก Open Anyway

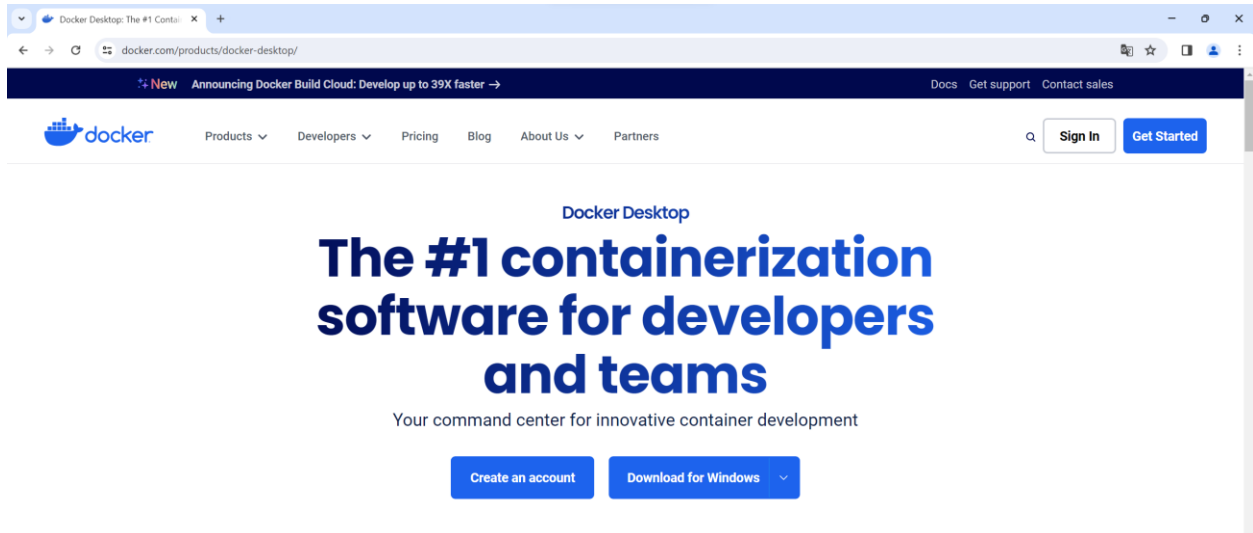


แสดงหน้าต่างการยืนยันการเปิดโปรแกรม zap ให้เลือก Open

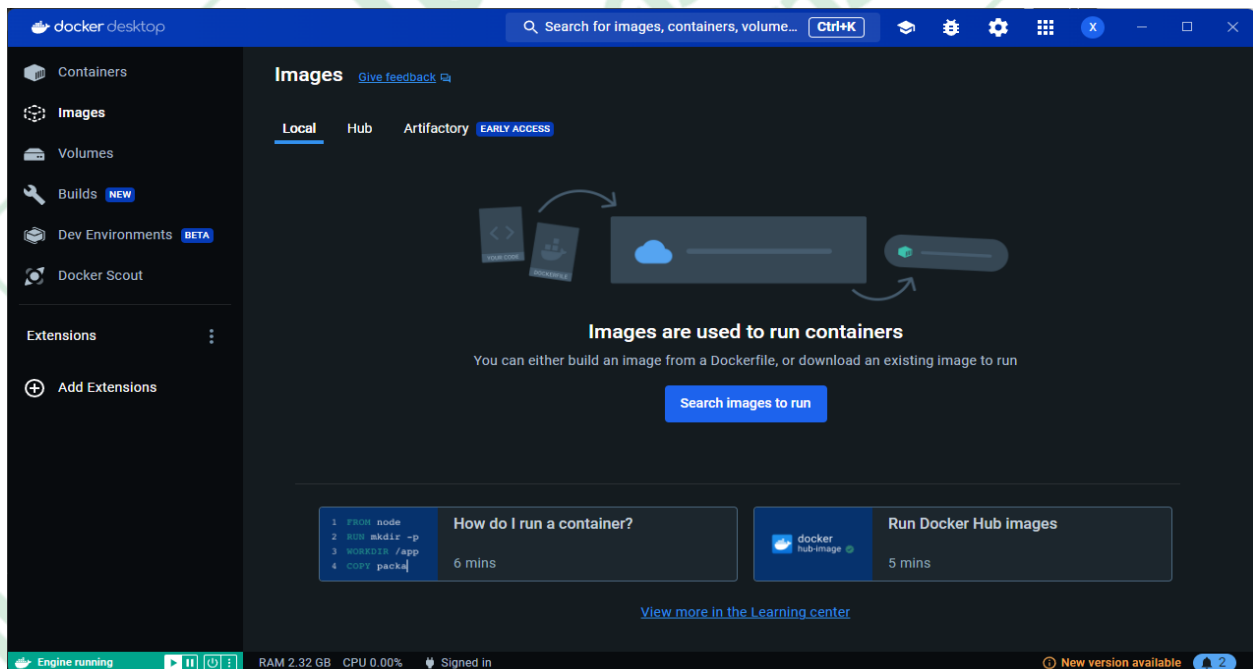


วิธีการติดตั้งโปรแกรม Zed Attack Proxy (ZAP) สำหรับผู้ใช้ Docker

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`

```

Command Prompt
C:\project\zap>docker --version
Docker version 24.0.7, build afdd53b
C:\project\zap>

```

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

The screenshot shows the download page for zapproxy.org. It features a four-step installation wizard and a table of Docker images.

Step	Description
1	Launch the installation wizard by double clicking on the downloaded executable file
2	Read the License agreement and click 'Accept' to continue the installation
3	Select 'Standard' or 'Custom' installation
4	Click 'Finish' to exit set up

Release Type	Description	Commands	Links
Stable	The standard release	docker pull ghcr.io/zaproxy/zaproxy:stable docker pull softwaresecurityproject/zap-stable	GHCR Page Docker Hub Page
Bare	Minimal release, ideal for CI	docker pull ghcr.io/zaproxy/zaproxy:bare docker pull softwaresecurityproject/zap-bare	GHCR Page Docker Hub Page
Weekly	Updated every week	docker pull ghcr.io/zaproxy/zaproxy:weekly docker pull softwaresecurityproject/zap-weekly	GHCR Page Docker Hub Page
Nightly	The very latest source code	docker pull ghcr.io/zaproxy/zaproxy:nightly docker pull softwaresecurityproject/zap-nightly	GHCR Page Docker Hub Page

• See [Docker](#) for more information.

ZAP Weekly

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

```

Command Prompt
C:\project\zap>docker pull ghcr.io/zaproxy/zaproxy:stable
stable: Pulling from zaproxy/zaproxy
b5a0d5c14ba9: Pull complete
a1381635860e: Pull complete
c3ccdab28863: Pull complete
5d52b39665a1: Pull complete
25de882cee95: Pull complete
525cb83b48c5: Pull complete
4f4fb700ef54: Pull complete
6c24b5d71c3f: Pull complete
a9792d831c31: Pull complete
21a8cac5b136: Pull complete
7e220b117dd8: Pull complete
dd2e9b4152b9: Pull complete
a59ebfb99464: Pull complete
c2747c5235b1: Pull complete
a821dd6d684f: Pull complete
fa5542dbfc22: Pull complete
3cf7759d13fb: Pull complete
314a804b40d7: Pull complete
788fe2e1e278: Pull complete
Digest: sha256:3bab2978aaf980abffbb7c4382fc87073ca01cd3880662afcc4a3bde9e7b2d84
Status: Downloaded newer image for ghcr.io/zaproxy/zaproxy:stable
ghcr.io/zaproxy/zaproxy:stable

What's Next?
View a summary of image vulnerabilities and recommendations → docker scout quickview ghcr.io/zaproxy/zaproxy:stable

C:\project\zap>

```

เข้าที่หน้า Document ในส่วน ZAP – Webswing Usage

ZAP - Webswing Usage

DOCKER > ZAP - WEBSWING USAGE

ZAP - Webswing Usage

Starting with version 2.5.0 you can run the ZAP Desktop UI in your browser without having to install Java, thanks to the magic of [Docker](#) and [Webswing](#)

To do this you will just need Docker installed. Start the container with webswing support:

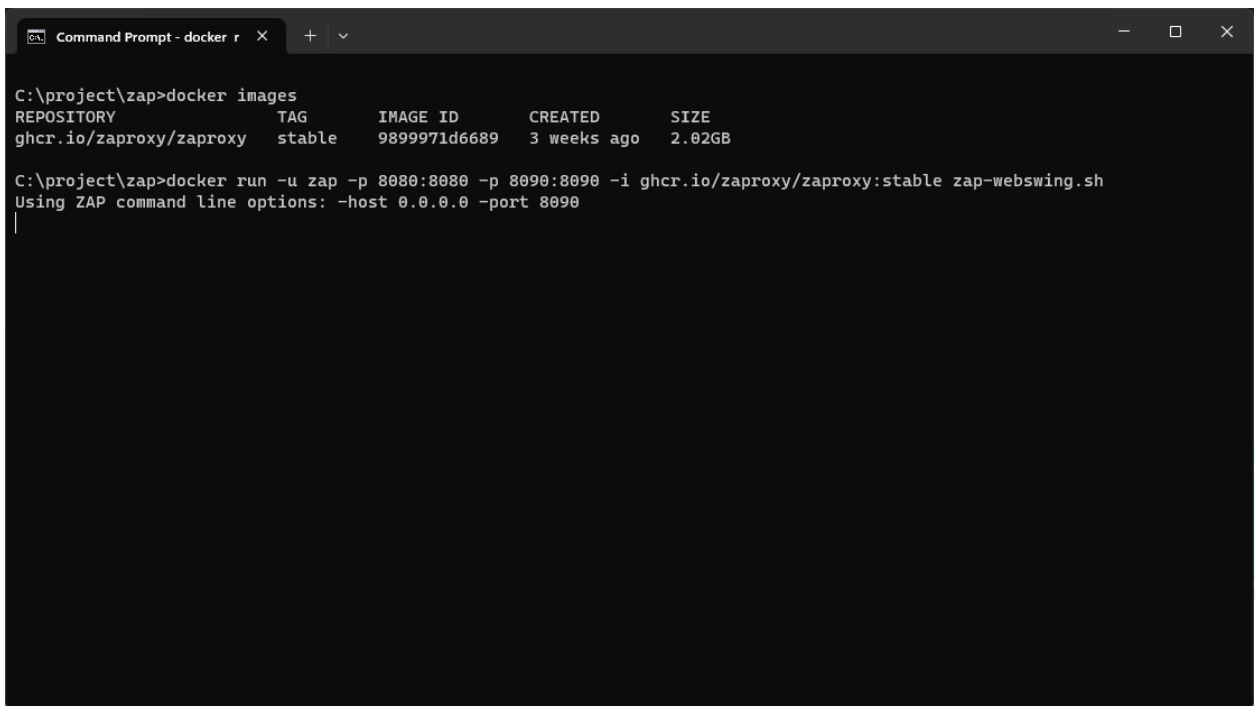
- Stable:
 - `docker run -u zap -p 8080:8080 -p 8090:8090 -i ghcr.io/zaproxy/zaproxy:stable zap-webswing.sh`
- Weekly:
 - `docker run -u zap -p 8080:8080 -p 8090:8090 -i ghcr.io/zaproxy/zaproxy:weekly zap-webswing.sh`

Then point your browser at:

- `http://localhost:8080/zap`

You will then see the familiar ZAP splash screen while ZAP starts up.

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

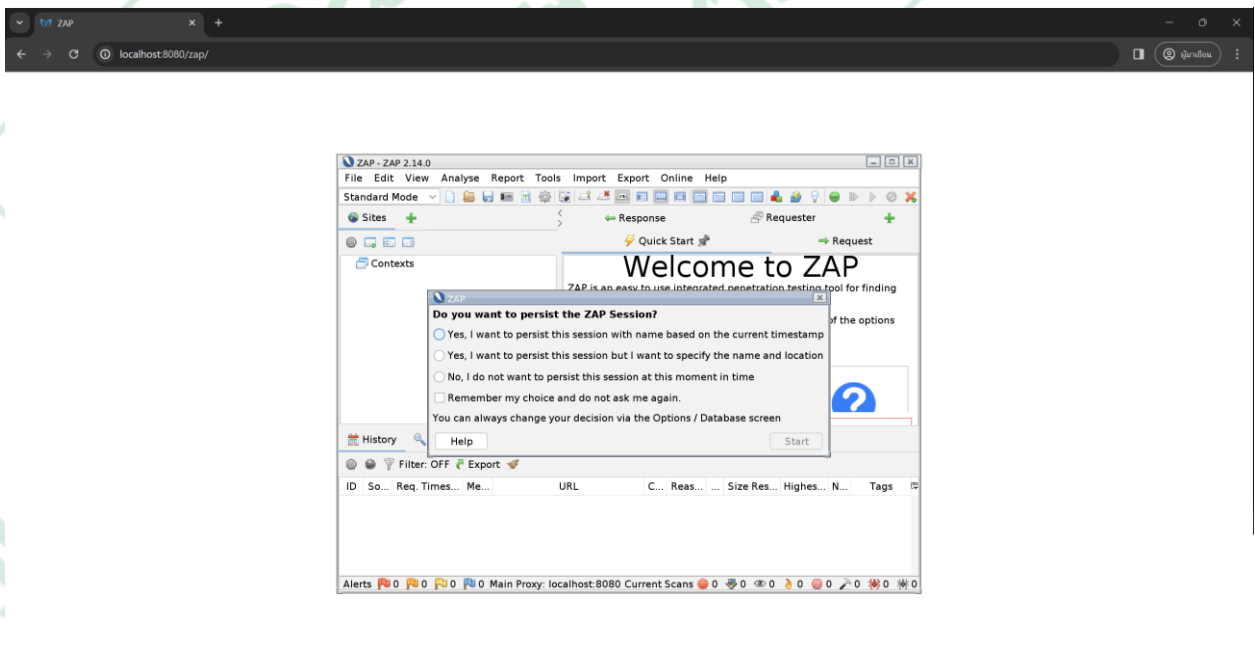


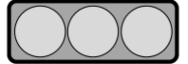
```

C:\project\zap>docker images
REPOSITORY          TAG         IMAGE ID      CREATED        SIZE
ghcr.io/zaproxy/zaproxy  stable     9899971d6689  3 weeks ago   2.02GB

C:\project\zap>docker run -u zap -p 8080:8080 -p 8090:8090 -i ghcr.io/zaproxy/zaproxy:stable zap-webswing.sh
Using ZAP command line options: -host 0.0.0.0 -port 8090
  
```

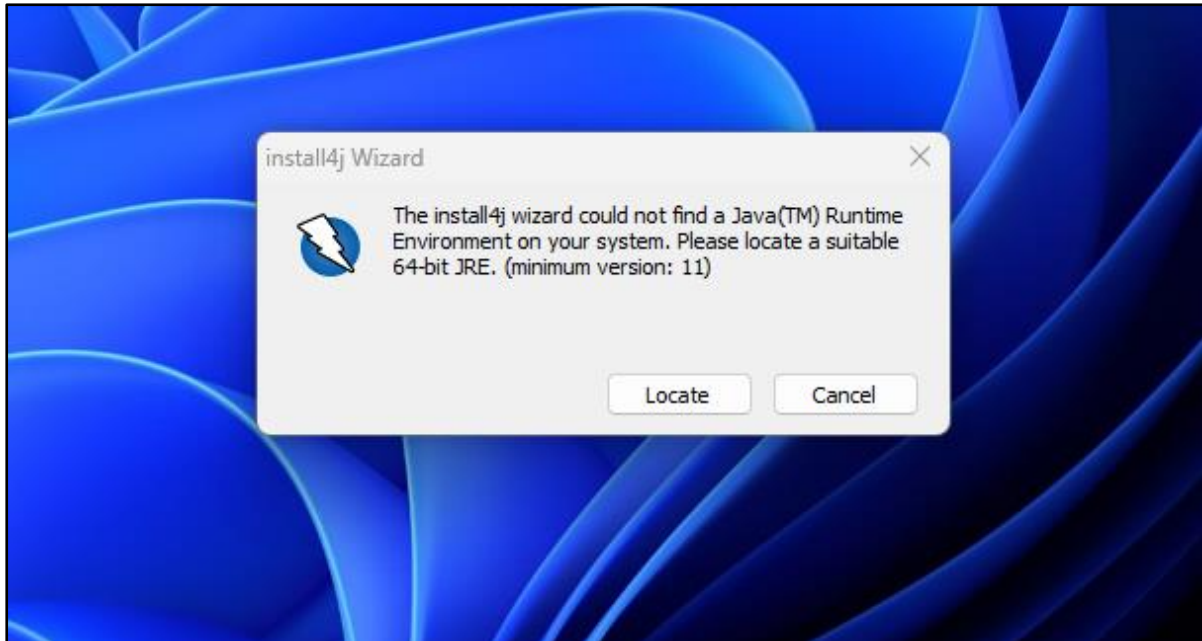
เปิด Browser และเข้า url : <http://localhost:8080/zap>



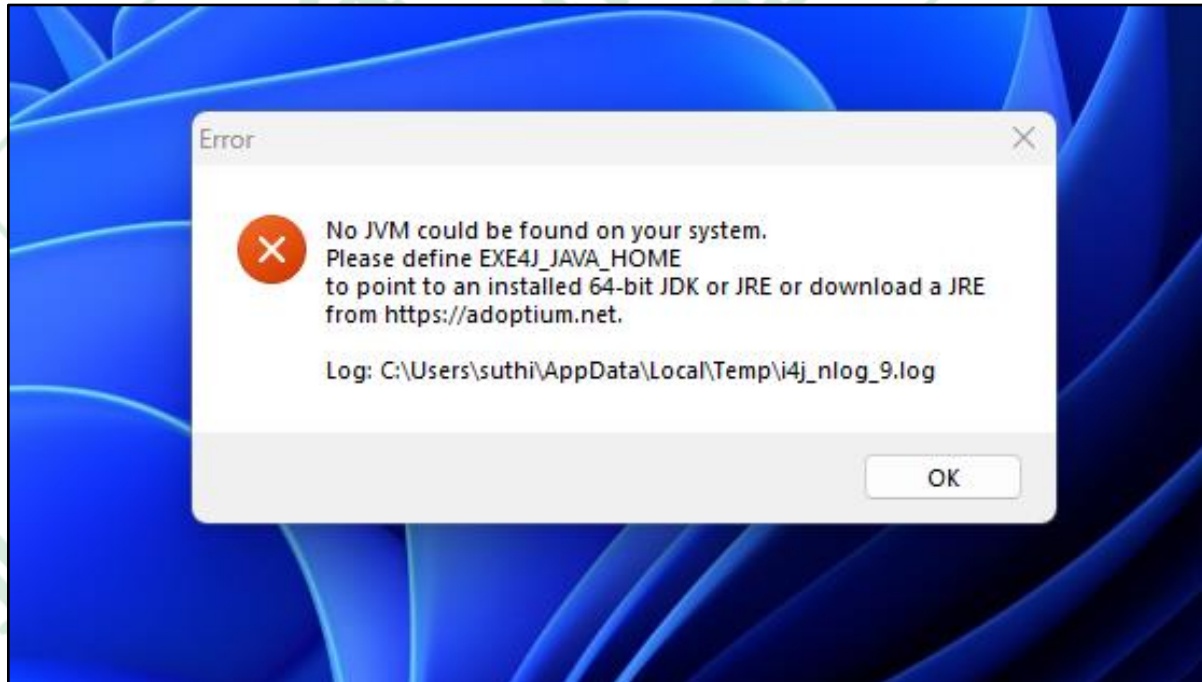


วิธีการติดตั้ง JAVA ก่อนการติดตั้งโปรแกรม ZAP

ภาพแสดง Error การติดตั้งโปรแกรม ZAP

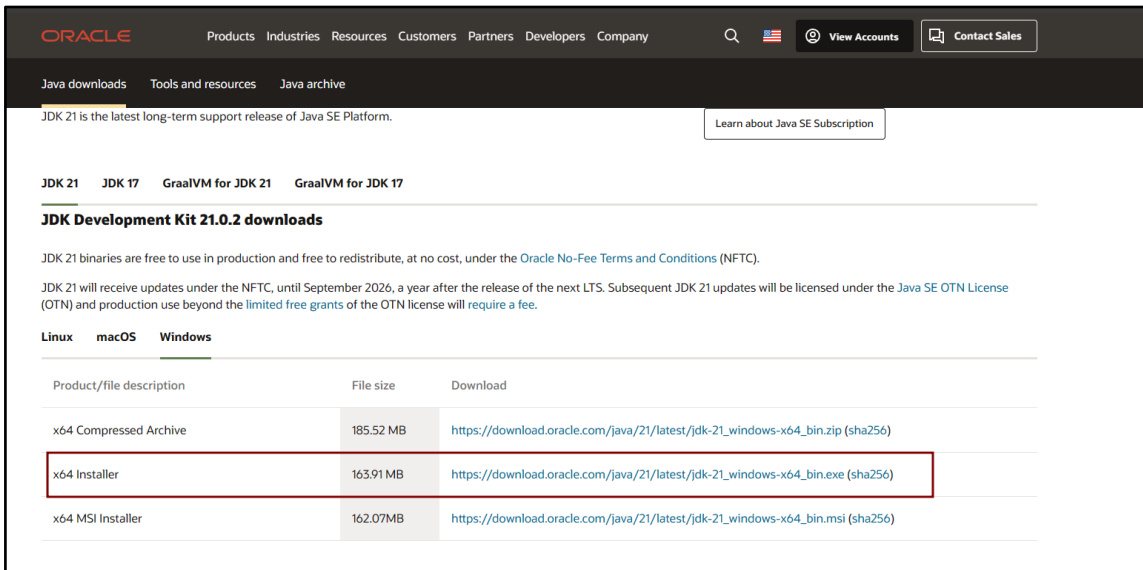


ภาพแสดง Error การติดตั้งโปรแกรม ZAP



ให้หน่วยงานทำการดาวน์โหลด JDK ตาม OS ของตนเองที่ใช้งาน ที่ลิงก์

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



JDK 21 is the latest long-term support release of Java SE Platform. [Learn about Java SE Subscription](#)

JDK 21 **JDK 17** **GraalVM for JDK 21** **GraalVM for JDK 17**

JDK Development Kit 21.0.2 downloads

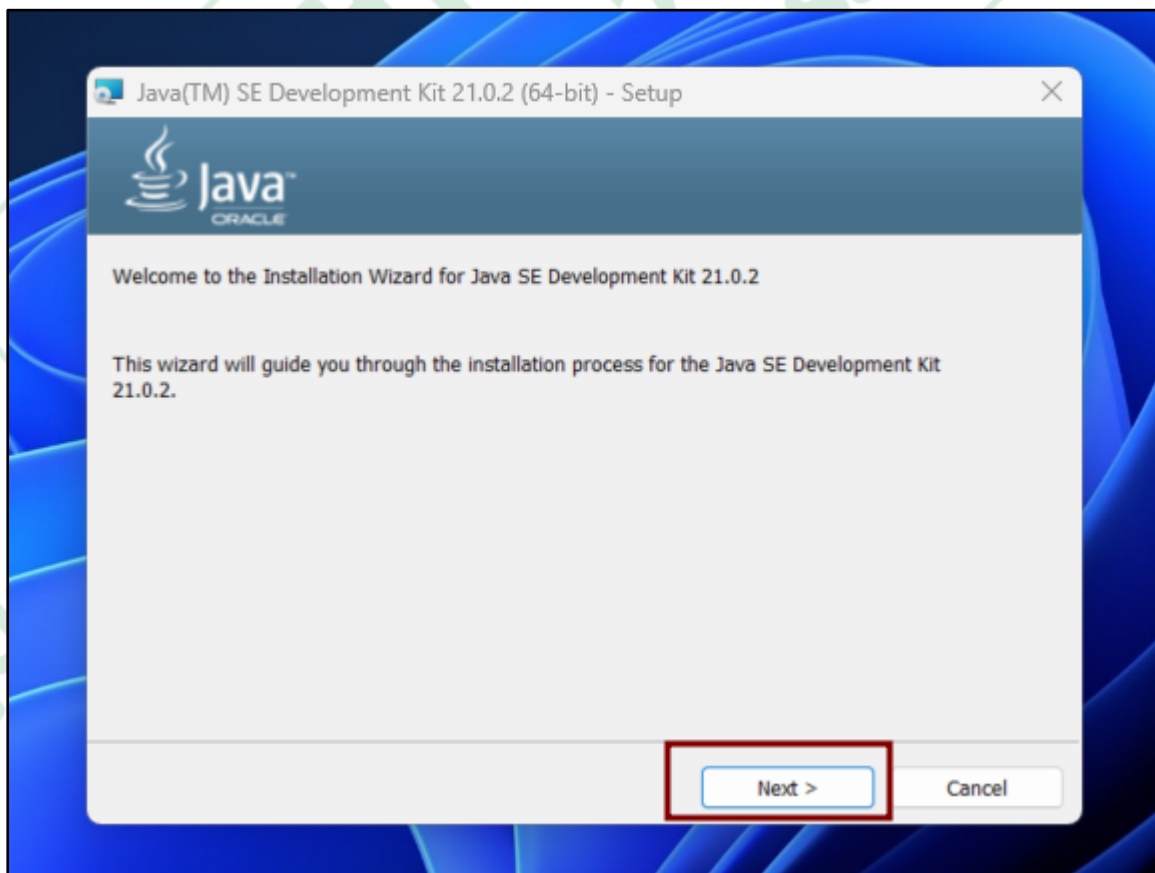
JDK 21 binaries are free to use in production and free to redistribute, at no cost, under the [Oracle No-Fee Terms and Conditions \(NFTC\)](#).

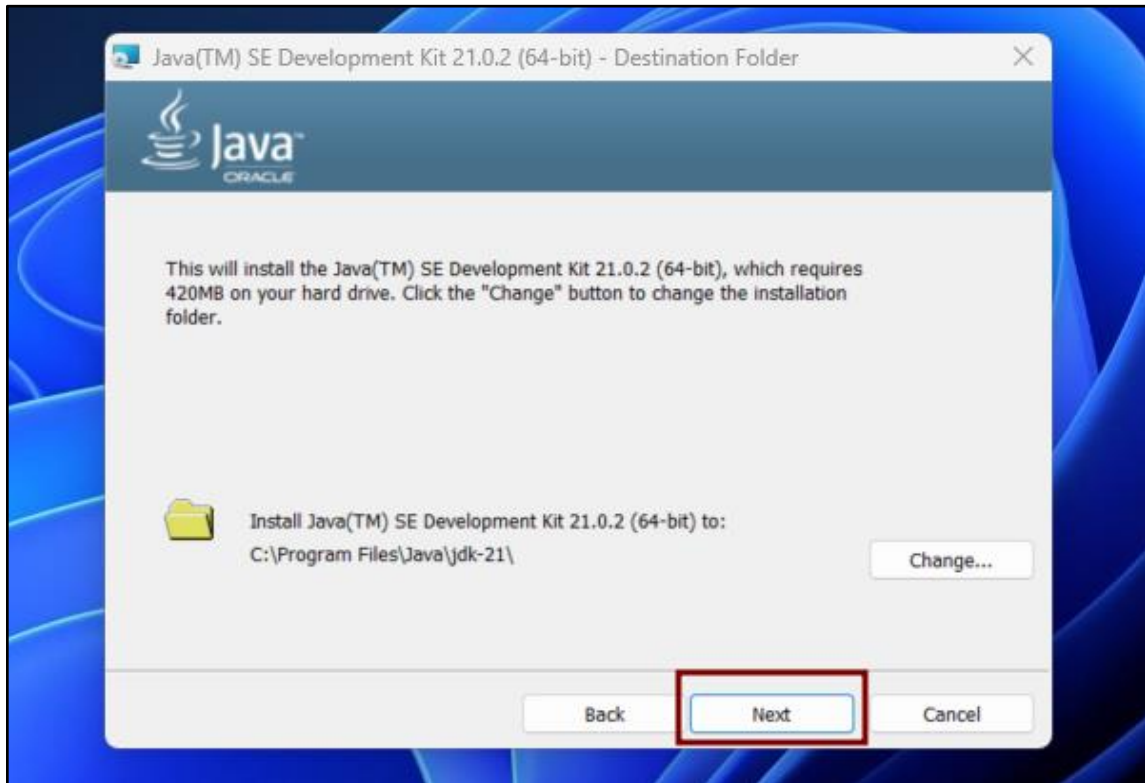
JDK 21 will receive updates under the NFTC, until September 2026, a year after the release of the next LTS. Subsequent JDK 21 updates will be licensed under the Java SE OTN License (OTN) and production use beyond the [limited free grants](#) of the OTN license will require a fee.

Linux **macOS** **Windows**

Product/file description	File size	Download
x64 Compressed Archive	185.52 MB	https://download.oracle.com/java/21/latest/jdk-21_windows-x64_bin.zip (sha256)
x64 Installer	163.91 MB	https://download.oracle.com/java/21/latest/jdk-21_windows-x64_bin.exe (sha256)
x64 MSI Installer	162.07MB	https://download.oracle.com/java/21/latest/jdk-21_windows-x64_bin.msi (sha256)

กดติดตั้งไฟล์ที่ได้รับมา คลิก **Next**



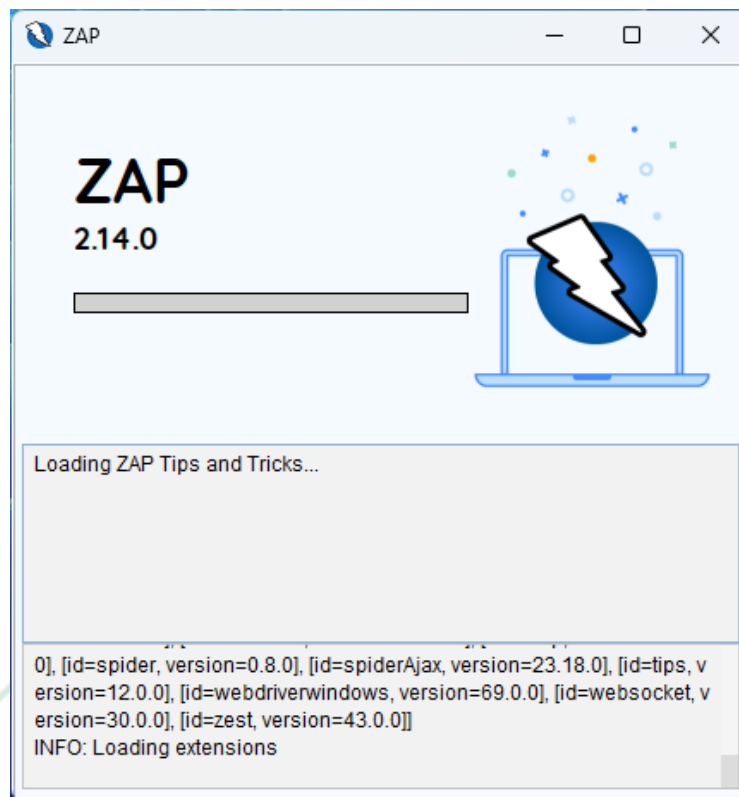
คลิกปุ่ม **Next**

การติดตั้ง JAVA เสร็จเรียบร้อย ทดสอบเปิด โปรแกรม ZAP

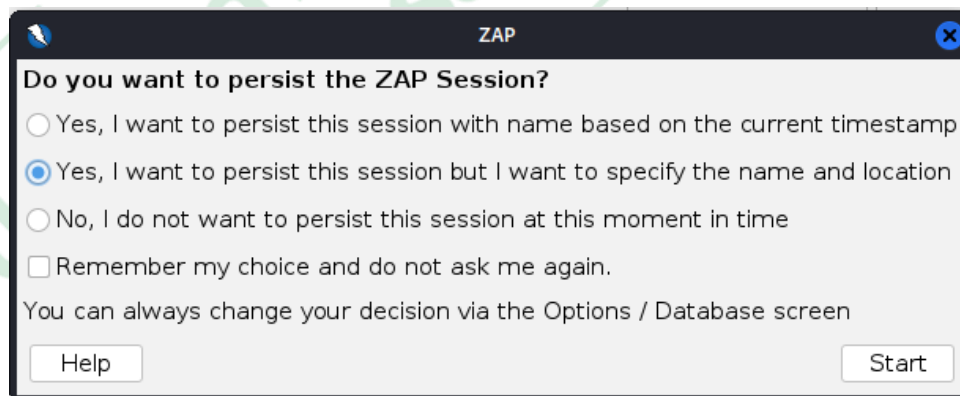


การใช้งานโปรแกรมเบื้องต้น

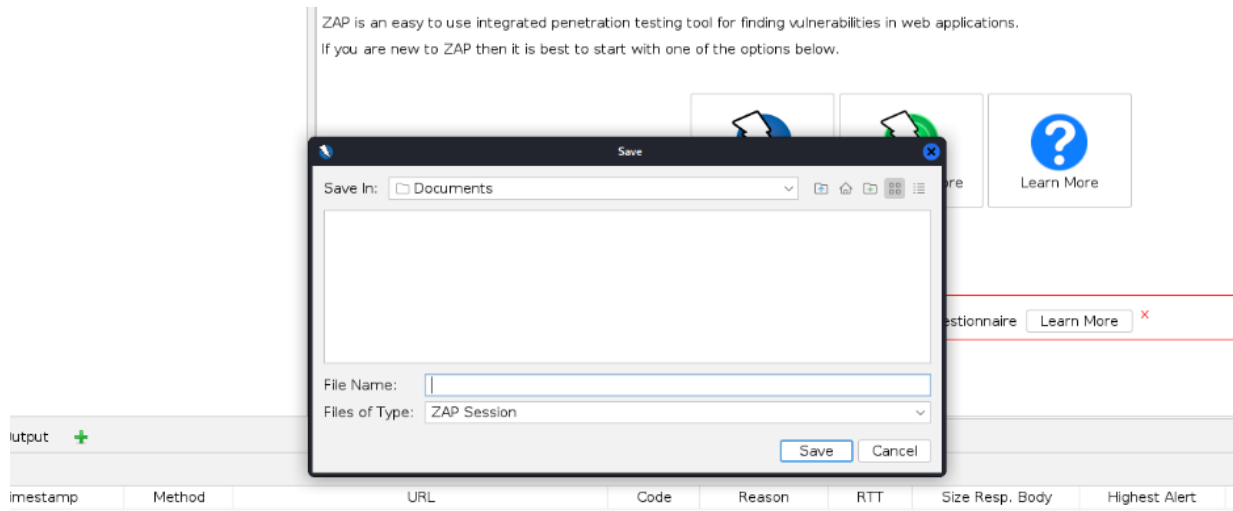
เปิดโปรแกรม ZAP ที่ทำการติดตั้งสำเร็จเรียบร้อยแล้ว



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

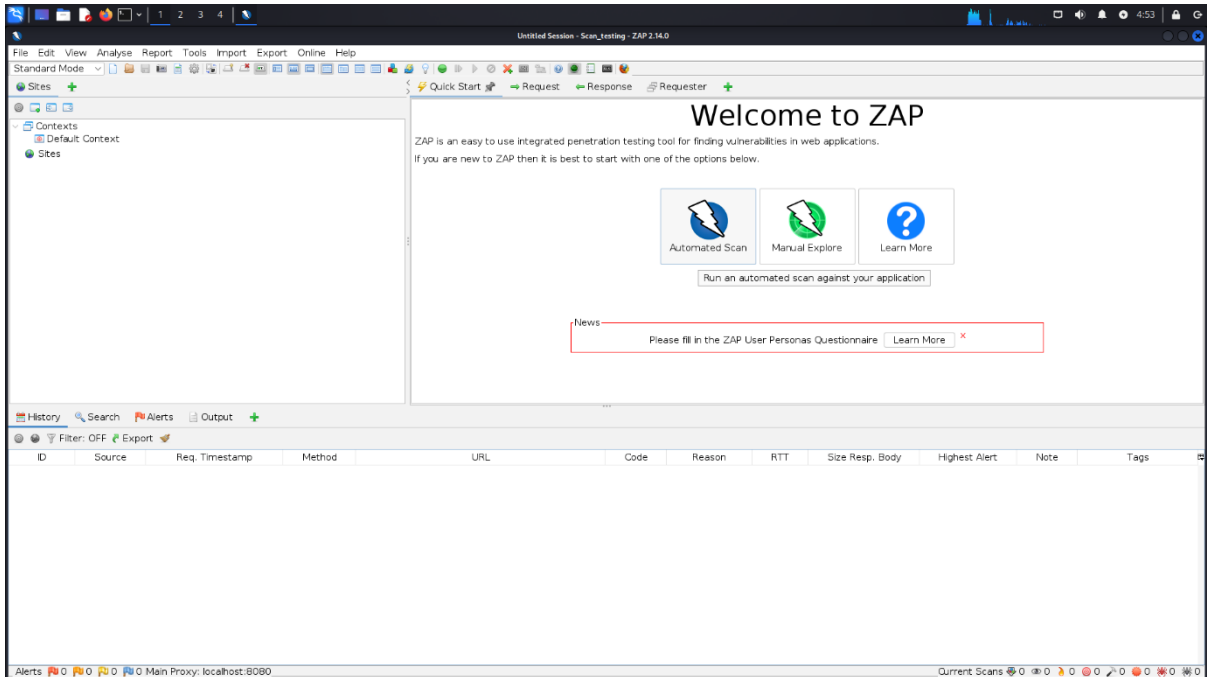


เลือก Folder และตั้งชื่อไฟล์ที่ต้องการ Save

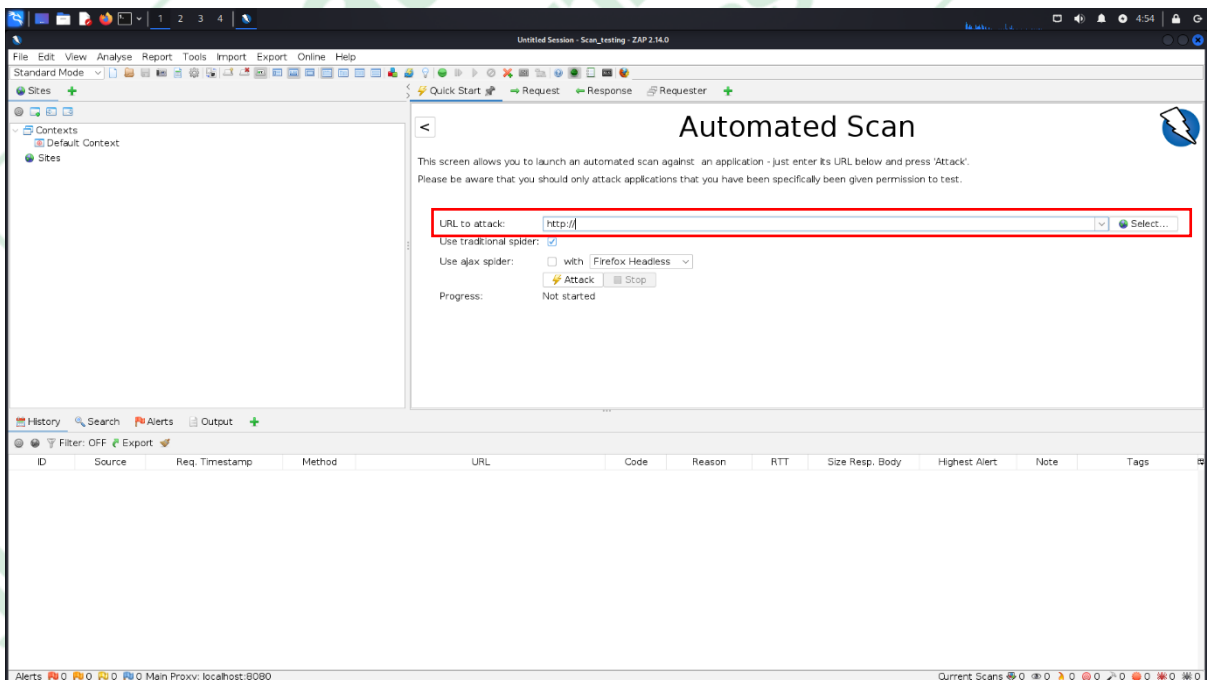


Health
ศูนย์ประสานการรักษาความ
ไซเบอร์ต้านสาธารณ...

เข้าสู่หน้าต่าง โปรแกรมคลิกเลือก Automated Scan



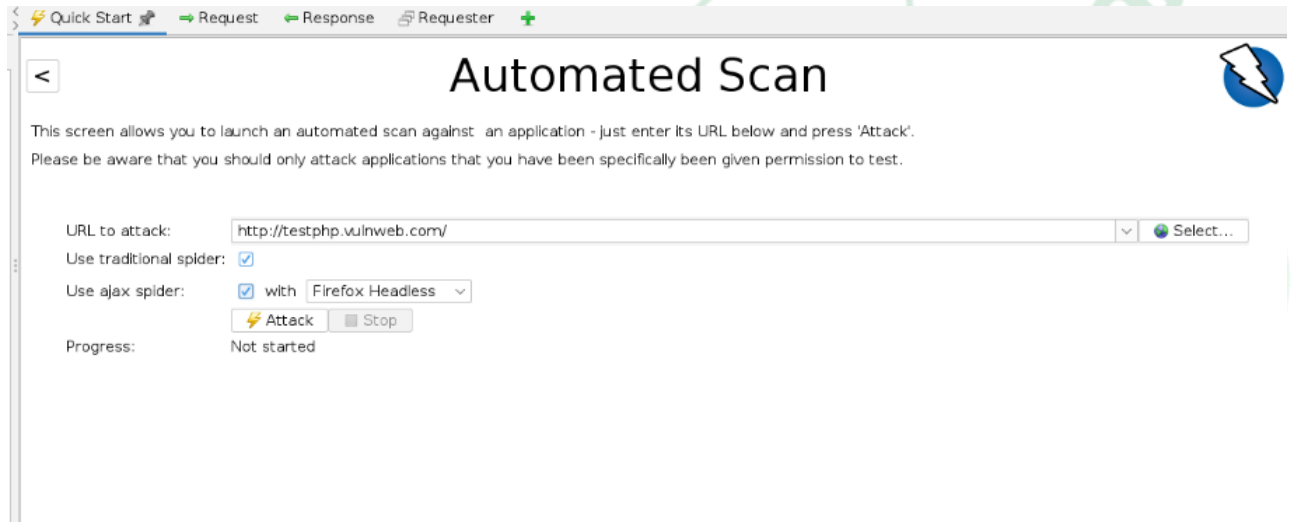
ใส่ URL Website ที่ต้องการตรวจสอบช่องโหว่ลงในช่อง URL to attack เช่น <https://xxxx.moph.go.th>



ติ๊กเลือกเมนูดังนี้

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

คลิก Attack



Quick Start Request Response Requester +

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack: Select...

Use traditional spider:

Use ajax spider: with Firefox Headless

Progress: Not started

รอมenu Active Scan ของโปรแกรมดำเนินการสแกนจนครบ 100 %

The screenshot displays the Burp Suite interface during an Active Scan. The 'Active Scan' tab is selected, and the progress bar indicates 100% completion. The 'Alerts' tab is also visible, showing 4 alerts. The 'Sent Messages' table below lists the scan results.

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
4,121	1/28/24, 9:21:14 PM	1/28/24, 9:21:14 PM	GET	http://testphp.vulnweb.com/comment.php?aid=3	200	OK	1 ms	138 bytes	140 bytes
4,123	1/28/24, 9:21:14 PM	1/28/24, 9:21:14 PM	GET	http://testphp.vulnweb.com/comment.php?aid=3	200	OK	1 ms	138 bytes	140 bytes
4,125	1/28/24, 9:21:14 PM	1/28/24, 9:21:14 PM	GET	http://testphp.vulnweb.com/comment.php?aid=3	200	OK	1 ms	138 bytes	140 bytes
4,127	1/28/24, 9:21:14 PM	1/28/24, 9:21:14 PM	GET	http://testphp.vulnweb.com/comment.php?aid=3	200	OK	2 ms	138 bytes	140 bytes
4,129	1/28/24, 9:21:14 PM	1/28/24, 9:21:14 PM	GET	http://testphp.vulnweb.com/comment.php?aid=3	200	OK	3 ms	138 bytes	140 bytes
4,131	1/28/24, 9:21:14 PM	1/28/24, 9:21:14 PM	GET	http://testphp.vulnweb.com/comment.php?aid=3	200	OK	2 ms	138 bytes	140 bytes
4,133	1/28/24, 9:21:14 PM	1/28/24, 9:21:14 PM	GET	http://testphp.vulnweb.com/comment.php?aid=3	200	OK	1 ms	138 bytes	140 bytes
4,135	1/28/24, 9:21:14 PM	1/28/24, 9:21:14 PM	GET	http://testphp.vulnweb.com/comment.php?aid=3	200	OK	1 ms	138 bytes	140 bytes
4,137	1/28/24, 9:21:14 PM	1/28/24, 9:21:14 PM	GET	http://testphp.vulnweb.com/comment.php?aid=3	200	OK	1 ms	138 bytes	140 bytes
4,139	1/28/24, 9:21:14 PM	1/28/24, 9:21:14 PM	GET	http://testphp.vulnweb.com/comment.php?aid=3	200	OK	7 ms	138 bytes	140 bytes

วิธีการตรวจสอบรายละเอียดช่องโหว่ที่พบ

การอ่านรายละเอียดที่จำเป็น

เมื่อทำการ Attack แล้ว จะมีส่วนที่จำเป็นต้องตรวจสอบอยู่ 3 ส่วน

ส่วนที่ 1 และ 2

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

Alerts (25)

- Cross Site Scripting (DOM Based)
- Absence of Anti-CSRF Tokens (43)
- Content Security Policy (CSP) Header Not Set (53)
- Missing Anti-clickjacking Header (48)
- Source Code Disclosure - PHP (3)
- Cookie No HttpOnly Flag (8)
- Cookie Without Secure Flag (4)
- Cookie with SameSite Attribute None (4)
- Cookie without SameSite Attribute (4)
- In Page Banner Information Leak (3)
- Permissions Policy Header Not Set (53)
- Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (78)
- Server Leaks Version Information via "Server" HTTP Response Header Field (91)
- Timestamp Disclosure - Unix
- X-Content-Type-Options Header Missing (84)
- Authentication Request Identified (2)
- Charset Mismatch (Header Versus Meta Content-Type Charset) (34)
- Information Disclosure - Suspicious Comments
- Modern Web Application (9)
- Non-Storable Content (2)
- Re-examine Cache-control Directives (4)
- Session Management Response Identified (6)
- Storable and Cacheable Content (93)
- Storable but Non-Cacheable Content (2)
- User Controllable HTML Element Attribute (Potential XSS) (4)

Cross Site Scripting (DOM Based)

URL: http://testphp.vulnweb.com/#j\$VasCript:/*-/*\`/*!/*
 /***/ (/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</tItLe/</tEXtarEa/</scRipt/--!>\x3csVg/<svG/oNlOAd=alert(5397) //>\x3e

Risk: High
 Confidence: High

Parameter: #j\$VasCript:/*-/*\`/*!/*
 /***/ (/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</tItLe/</tEXtarEa/</scRipt/--!>\x3csVg/<svG/oNlOAd=alert(5397) //>\x3e

Attack: 5397))//%0D%0A%0d%0a//</stYle/</tItLe/</tEXtarEa/</scRipt/--!>\x3csVg/<svG/oNlOAd=alert(5397) //>\x3e

Evidence:
 CWE ID: 79
 WASC ID: 8

Source: Active (40026 - Cross Site Scripting (DOM Based))

Input Vector:
 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

Other Info:
 Tag name: div Att name: null Att id: mainLayer

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

Reference:
<https://owasp.org/www-community/attacks/xss/>
<https://cwe.mitre.org/data/definitions/79.html>

Alerts (25)

- Cross Site Scripting (DOM Based)
- Absence of Anti-CSRF Tokens (43)
- Content Security Policy (CSP) Header Not Set (53)
- Missing Anti-clickjacking Header (48)
- Source Code Disclosure - PHP (3)
- Cookie No HttpOnly Flag (8)
- Cookie Without Secure Flag (4)
- Cookie with SameSite Attribute None (4)
- Cookie without SameSite Attribute (4)
- In Page Banner Information Leak (3)
- Permissions Policy Header Not Set (53)
- Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (78)
- Server Leaks Version Information via "Server" HTTP Response Header Field (91)
- Timestamp Disclosure - Unix
- X-Content-Type-Options Header Missing (84)
- Authentication Request Identified (2)
- Charset Mismatch (Header Versus Meta Content-Type Charset) (34)
- Information Disclosure - Suspicious Comments
- Modern Web Application (9)
- Non-Storable Content (2)
- Re-examine Cache-control Directives (4)
- Session Management Response Identified (6)
- Storable and Cacheable Content (93)
- Storable but Non-Cacheable Content (2)
- User Controllable HTML Element Attribute (Potential XSS) (4)

Cross Site Scripting (DOM Based)

URL: http://testphp.vulnweb.com/#j\$VasCript:/*-/*\`/*!/*
 /***/ (/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</tItLe/</tEXtarEa/</scRipt/--!>\x3csVg/<svG/oNlOAd=alert(5397) //>\x3e

Risk: High
 Confidence: High

Parameter: #j\$VasCript:/*-/*\`/*!/*
 /***/ (/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</tItLe/</tEXtarEa/</scRipt/--!>\x3csVg/<svG/oNlOAd=alert(5397) //>\x3e

Attack: 5397))//%0D%0A%0d%0a//</stYle/</tItLe/</tEXtarEa/</scRipt/--!>\x3csVg/<svG/oNlOAd=alert(5397) //>\x3e

Evidence:
 CWE ID: 79
 WASC ID: 8

Source: Active (40026 - Cross Site Scripting (DOM Based))

Input Vector:
 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

Other Info:
 Tag name: div Att name: null Att id: mainLayer

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

Reference:
<https://owasp.org/www-community/attacks/xss/>
<https://cwe.mitre.org/data/definitions/79.html>

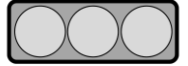
ส่วนที่ 3

รายละเอียดการ โจมตีที่ โจมตีสำเร็จ โปรแกรมจะอธิบายถึง Payload ที่ใช้โจมตี รวมถึงรายละเอียดต่างๆ ของประเภทการ โจมตีนั้นๆ 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,

และวิธีการแก้ไขปัญหาเพื่อป้องกันหรือลดผลกระทบของการ โจมตีจะอยู่ในส่วนของ 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

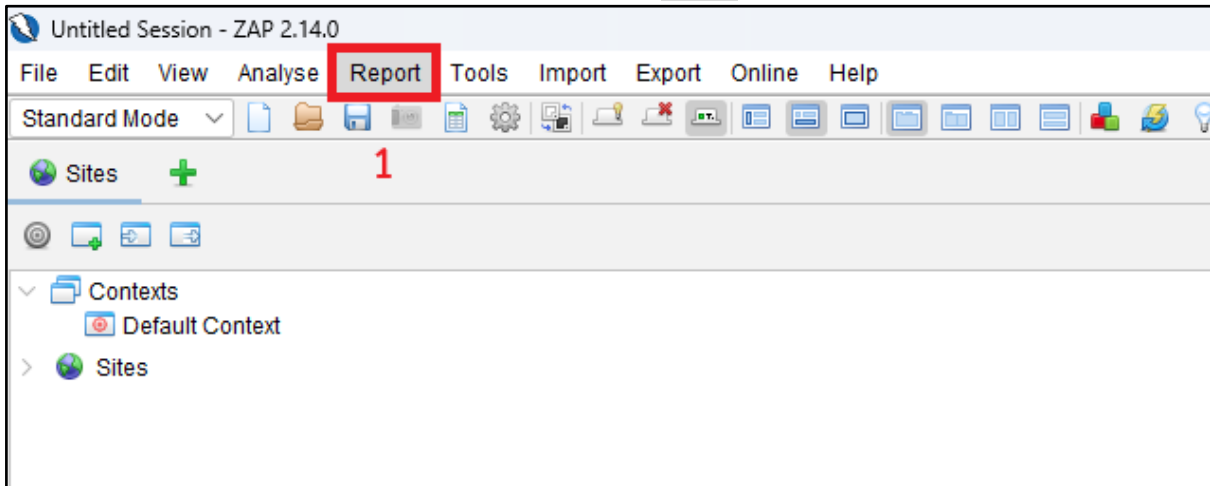
Reference:

<https://owasp.org/www-community/attacks/xss/>
<https://cwe.mitre.org/data/definitions/79.html>

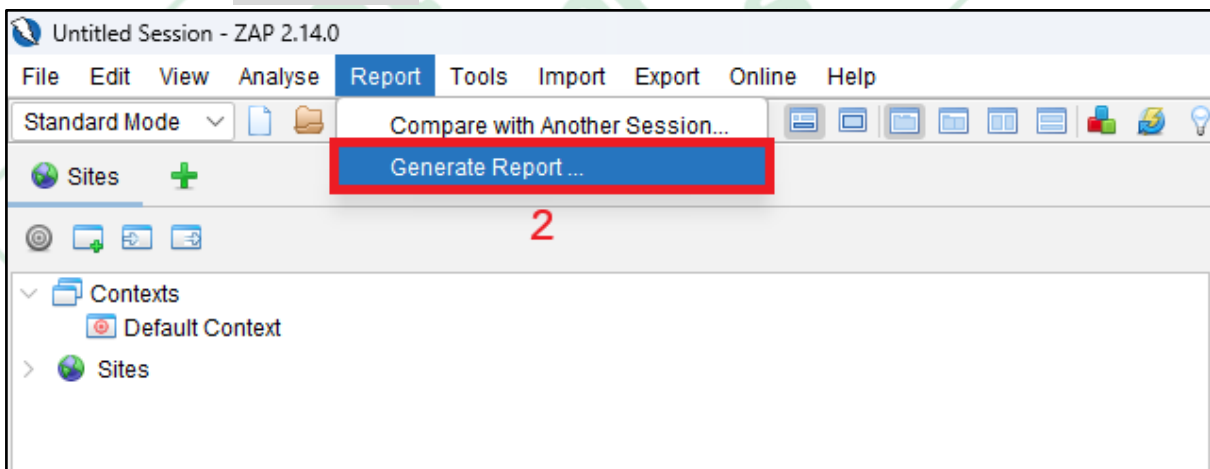


การออกรายงานการตรวจสอบช่องโหว่

ขั้นตอนที่ 1 หลังจากการสแกนหาช่องโหว่ให้ไปเลือกเมนู **Report** เพื่อทำการออกรายงาน



ขั้นตอนที่ 2 ให้คลิก **Generate Report** จะปรากฏหน้าต่างการตั้งค่าการออกรายงาน



ขั้นตอนที่ 3 เลือก sites ที่ต้องการออกรายงาน

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

ขั้นตอนที่ 5 คลิก **Generate Report** เพื่อออกรายงาน

Generate Report

Scope Template Filter Options

Report Title: ZAP Scanning Report

Report Name: YYYY-MM-DD-ZAP-Report-HOSCODE.html 4

Report Directory: C:\Users\suthi\ZAP

Description:

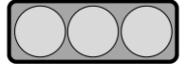
Contexts: Default Context

Sites: http://testphp.vulnweb.com 3


Generate If No Alerts:

Display Report:

Generate Report 5 Reset Cancel



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 \(1\)](#)

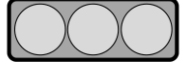
ภาพแสดงตัวอย่างแบบรายงานที่ได้รับ



Contents

- [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=Medium, Confidence=High \(1\)](#)
 - [Risk=Medium, Confidence=Medium \(1\)](#)
 - [Risk=Medium, Confidence=Low \(1\)](#)
 - [Risk=Low, Confidence=High \(1\)](#)
 - [Risk=Low, Confidence=Medium \(2\)](#)
 - [Risk=Informational, Confidence=Medium \(1\)](#)
 - [Risk=Informational, Confidence=Low \(4\)](#)
- [Appendix](#)
 - [Alert types](#)

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`

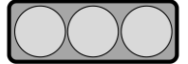
Excluded: `None`

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