## ระบบโปรแกรม OWASP ZAP

OWASP ZAP เป็น Tool ที่เหมาะสำหรับนักพัฒนาเว็บแอพพลิเคชัน ผู้ดูแลระบบ และนักเจาะระบบ ที่ต้องการสแกนและตรวจสอบช่องโหว่ของเว็บแอพพลิเคชัน พัฒนาโดยภาษา Java ส่งผลให้สามารถทำงานได้บนทุกระบบปฏิบัติการไม่เว้นแม้บน Raspberry Pi สำหรับความปลอดภัยด้านเว็บแอพพลิเคชัน เรียกว่า OWASP Zed Attack Proxy (ZAP)

มีคุณสมบัติเด่น ดังนี้

- Intercepting Proxy
- Traditional and AJAX spiders
- Automated scanner
- Passive scanner
- Forced browsing
- Fuzzer
- Dynamic SSL certificates
- Smartcard and Client Digital Certificates support
- Web sockets support
- Support for a wide range of scripting languages
- Plug-n-Hack support
- Authentication and session support
- Powerful REST based API
- Automatic updating option
- Integrated and growing marketplace of add-ons

## ขั้นตอนที่ 1 : การดาวโหลดและการติดตั้งระบบโปรแกรม OWASP ZAP

1.1 ดาวโหลดและติดตั้งโปรแกรม OWASP ZAP ตามขั้นตอน ดังนี้

- โปรแกรม OWASP ZAP สามารถดาวโหลดได้ที่

  https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

➢ ให้กดเลือก Download ZAP แล้วจะพบหน้าต่าง ดังนี้

## Downloads

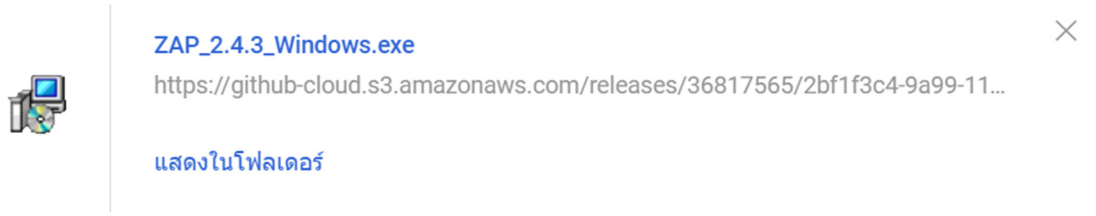
psiinon edited this page 5 days ago · 62 revisions

Not sure how to start using ZAP? Read the Getting Started Guide (pdf).

### ZAP 2.4.3 Standard

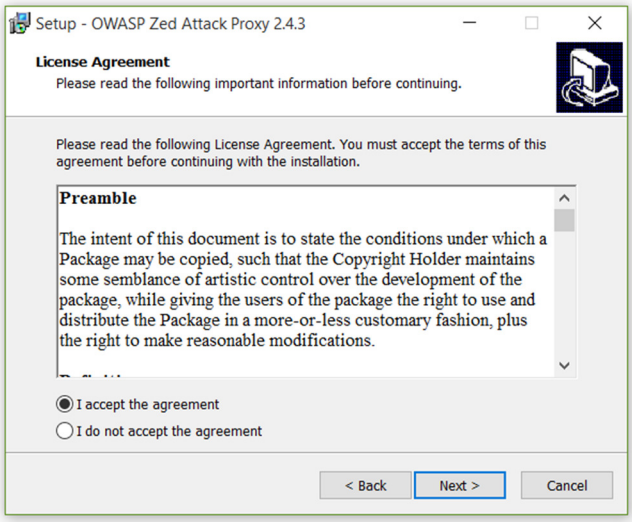
| | | | | |
|---|---|---|---|---|
| | Windows | 2015-12-04 | 72.3 MB | Download now |
| | Linux | 2015-12-04 | 78.1 MB | Download now |
| | Mac OS/X | 2015-12-04 | 114 MB | Download now |
| | Cross platform | 2015-12-04 | 78.2 MB | Download now |

➢ ให้เลือกระบบปฏิบัติการ Windows โดยกดที่ Download now แล้วรอจนโปรแกรมทำการดาวโหลดเสร็จ

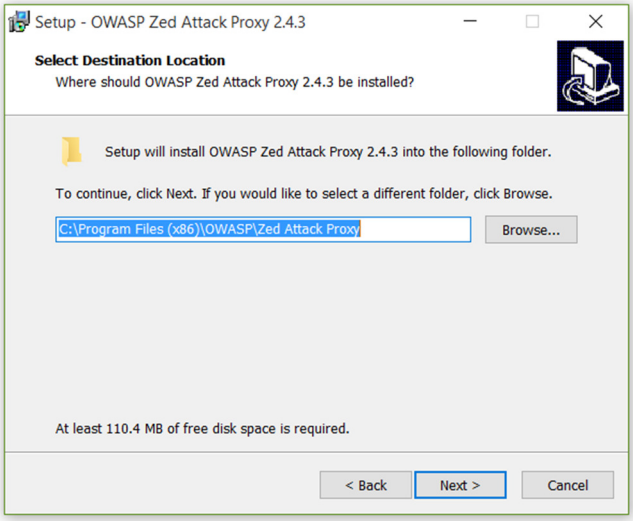



➢ เมื่อ Download สำเร็จ ให้กด Double Click เพื่อทำการ Setup โปรแกรม แล้วกดปุ่ม Next >

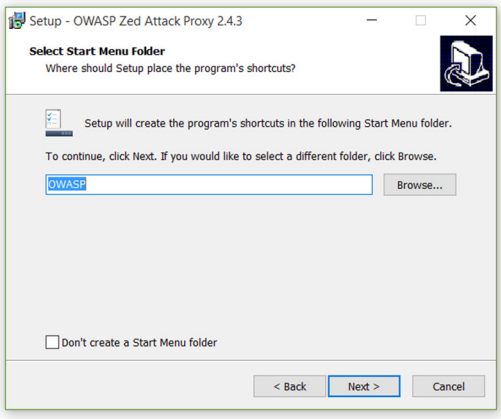
➢ ให้กดเลือก I accept the agreement แล้วกดปุ่ม Next >



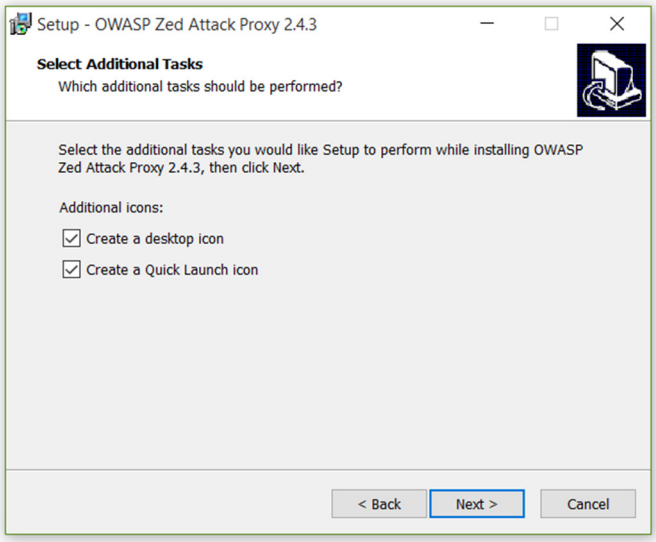

➢ ทำการเลือก C:\Program Files (x86)\OWASP\Zed Attack Proxy ที่จะ Install ใส่โปรแกรม จากนั้นกด Next >



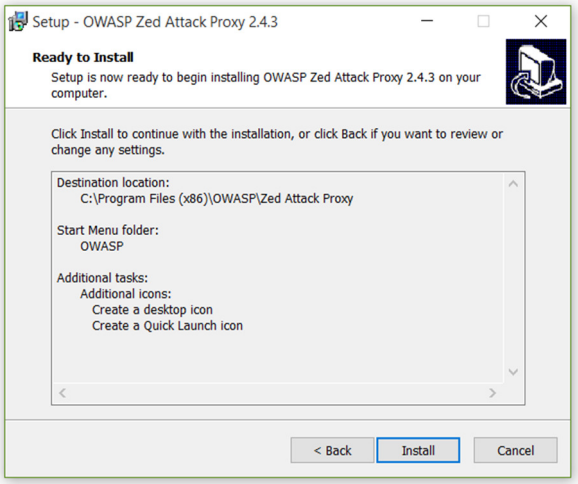

➢ จากนั้นให้เลือก OWASP เป็นตัว Start Menu folder แล้วกด Next >

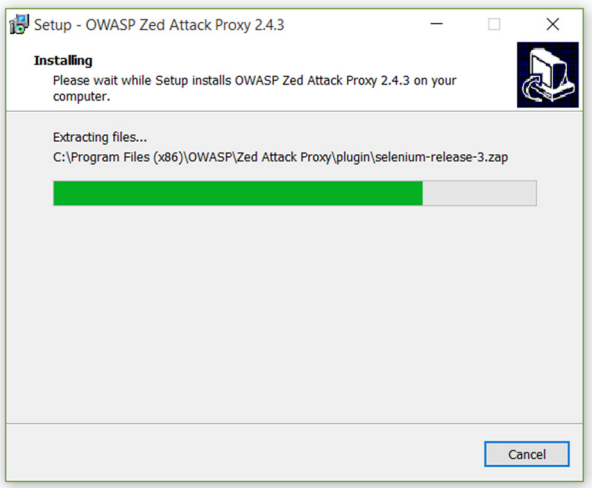


➢ จากนั้น จะขึ้นหน้าต่าง popup ให้เลือกว่าจะติดตั้ง Shortcut กับ Launch แล้วกด Next >




➢ กด Install แล้วจากนั้น popup browser จะขึ้นมา และให้รอจนกว่าจะโหลดเสร็จ

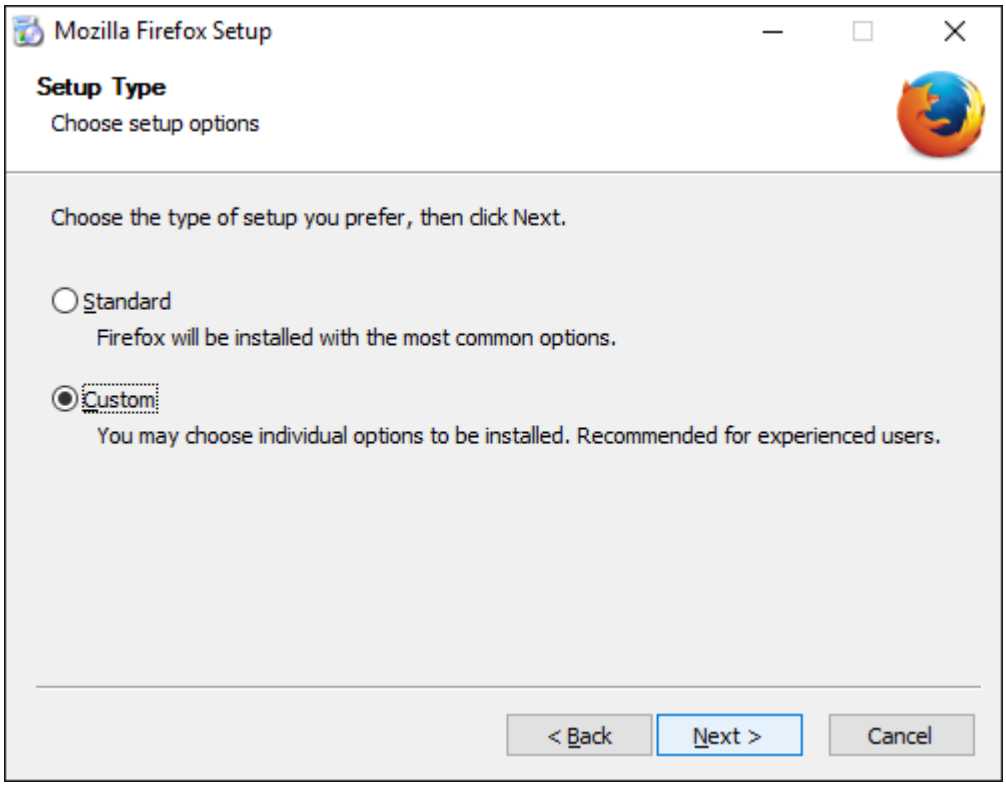


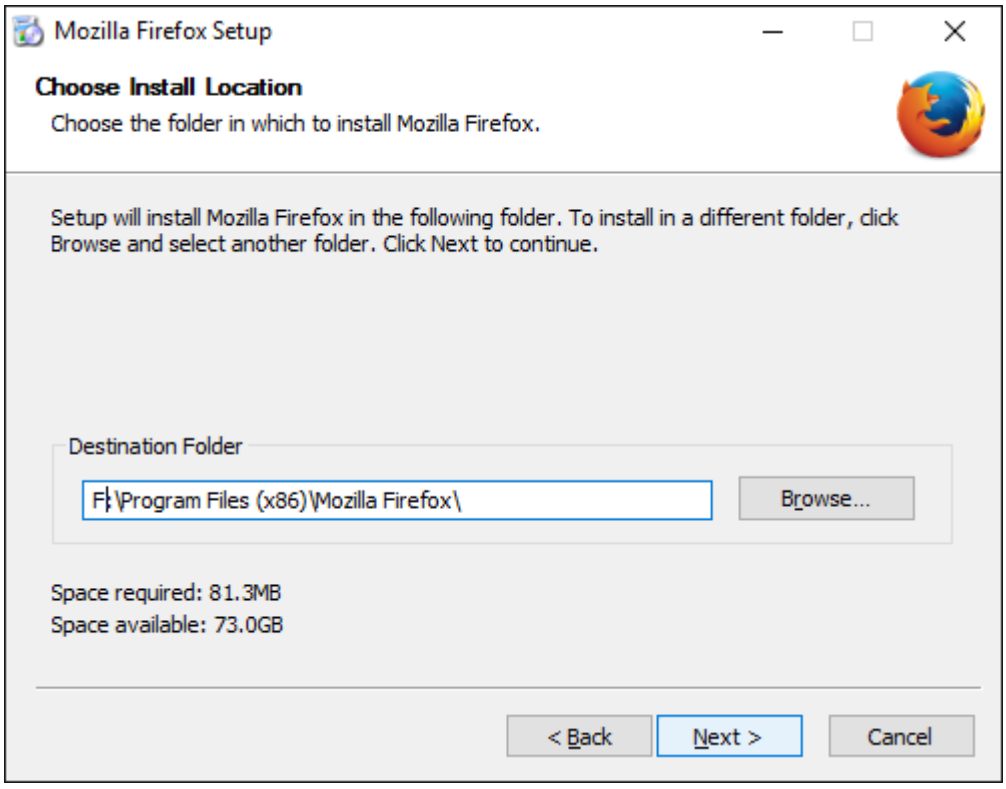
➢ โหลดเสร็จสิ้น กด Finish


➢ ต่อไปจะเป็นการลง FireFox ซึ่งจะต้องเป็นเวอร์ชัน 34 จึงจะสามารถทำงานได้ เพื่อที่จะให้บราวเซอร์เข้าเว็ปแล้วส่งข้อมูลไปยัง Zap

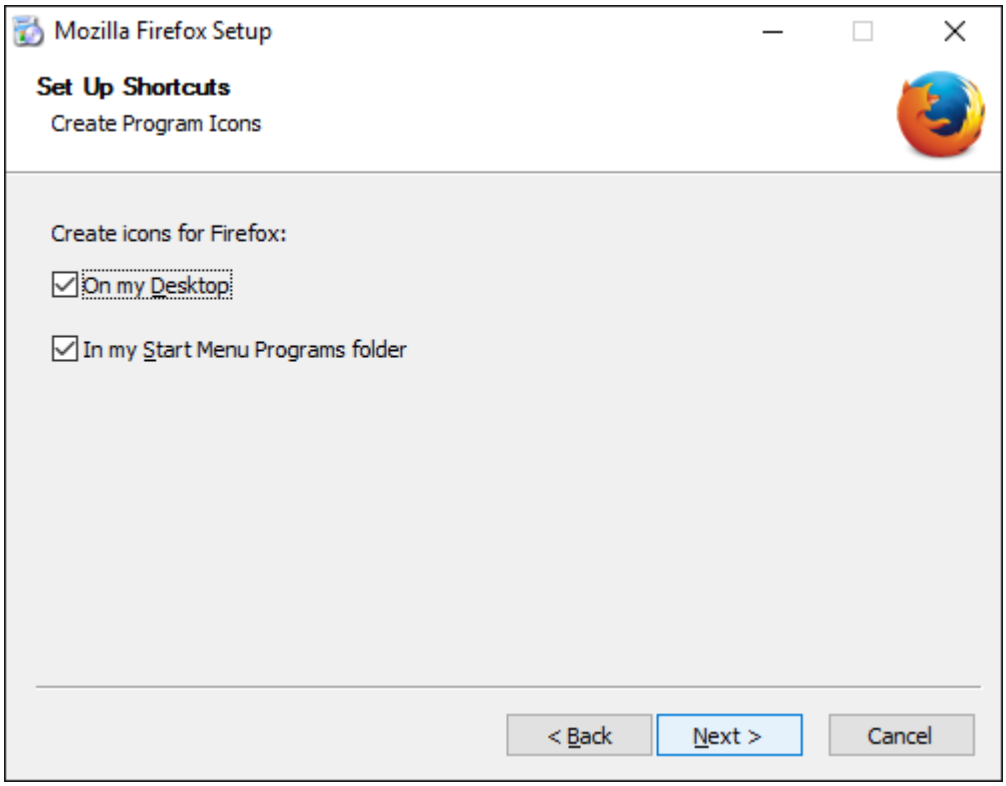
➢ ในส่วนนี้ให้เลือกแบบ Custom เพื่อเลือกพาทที่จะลง



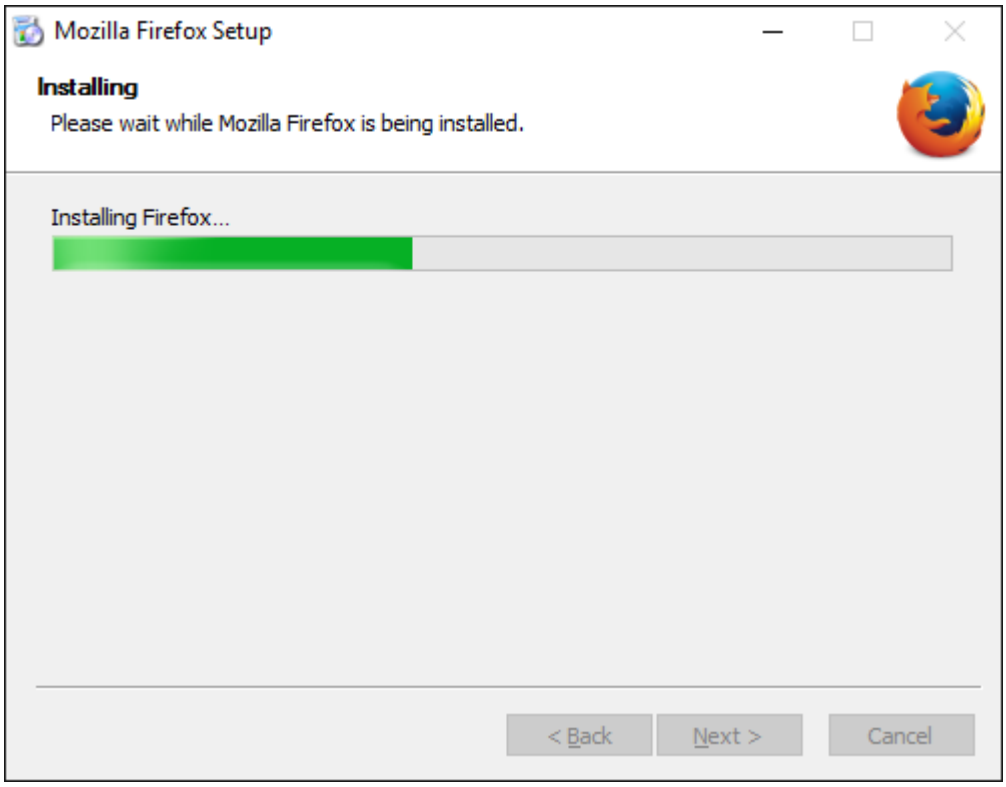

➢ เมื่อเลือกพาทได้แล้วให้กด Next



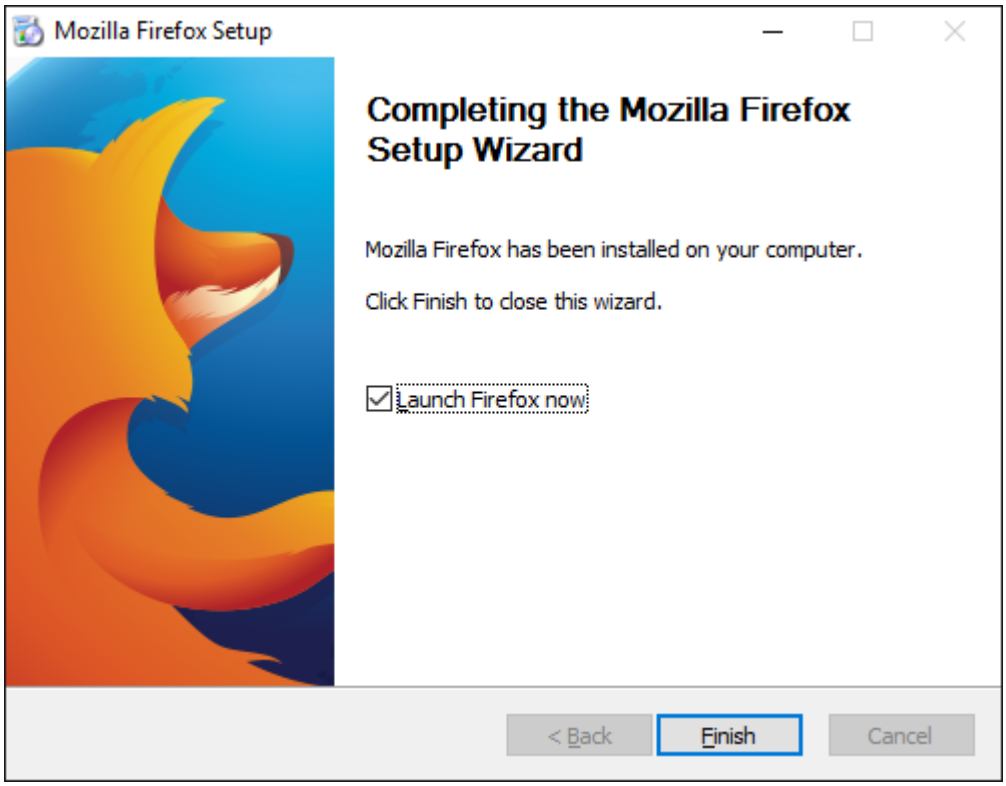
➢ กด Next



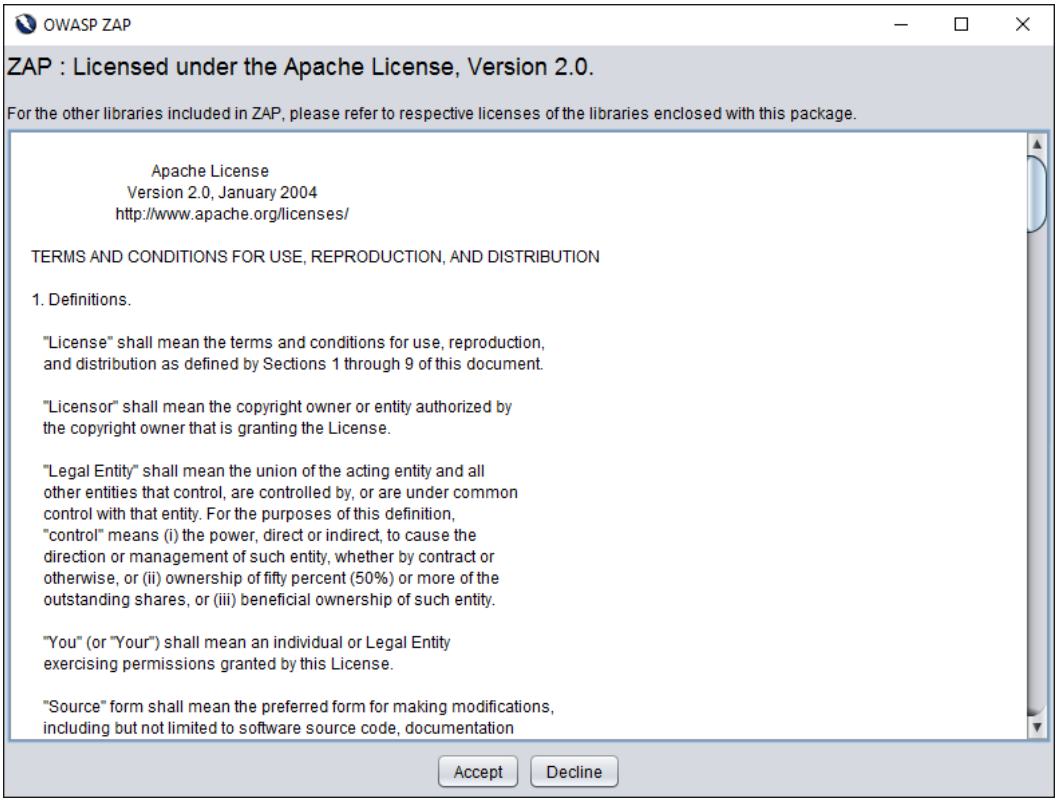

รอจนกว่าจะโหลดเสร็จสิ้น



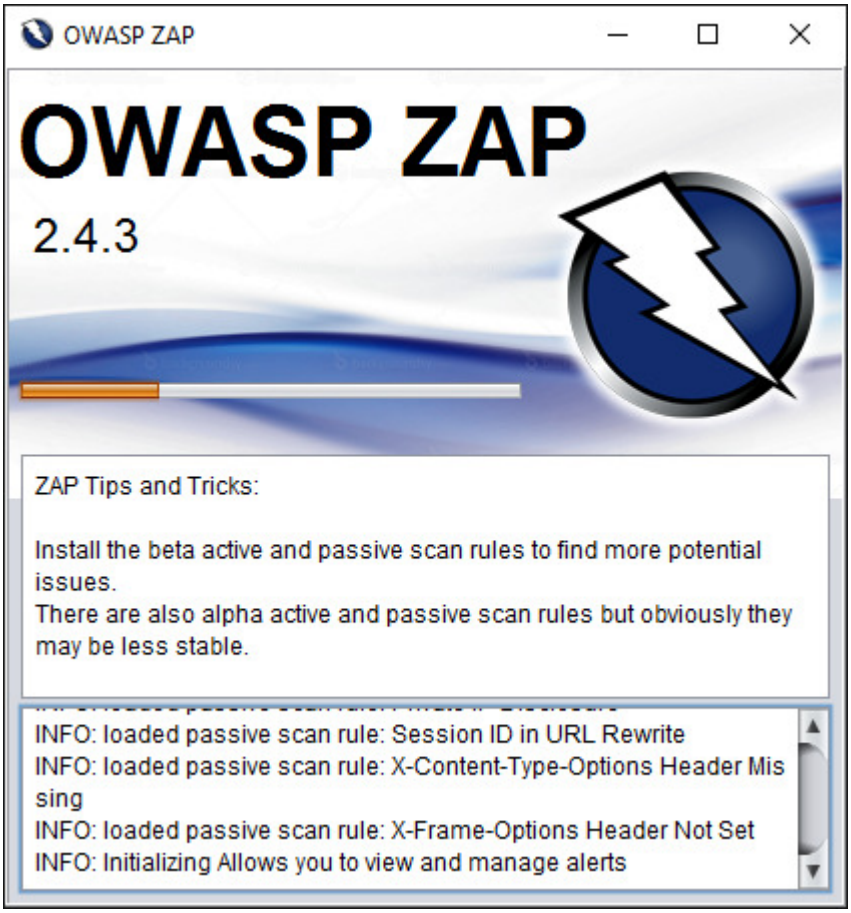
➢ เมื่อลงสำเร็จแล้วให้กดที่ Finish



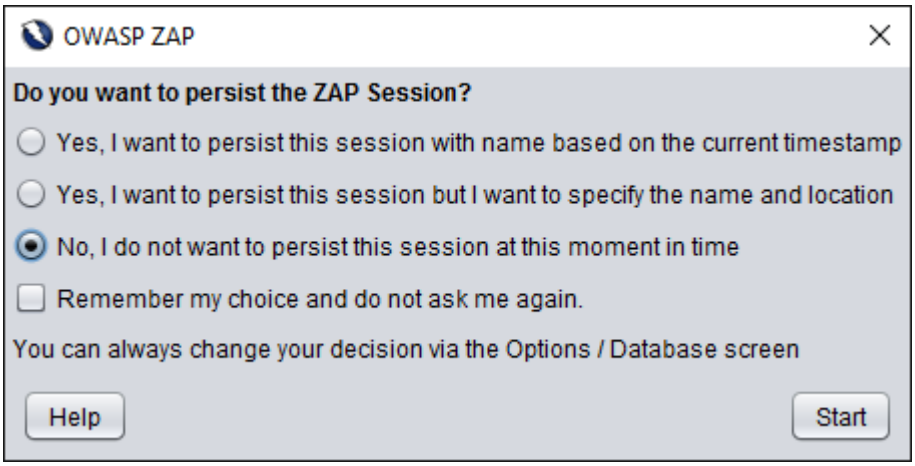

➢ ต่อไปให้ทำการเปิดโปรแกรม OWASP ZAP ขึ้นมา ก็จะมีข้อตกลงก่อนใช้โปรแกรม โดยให้คลิกที่ Accept



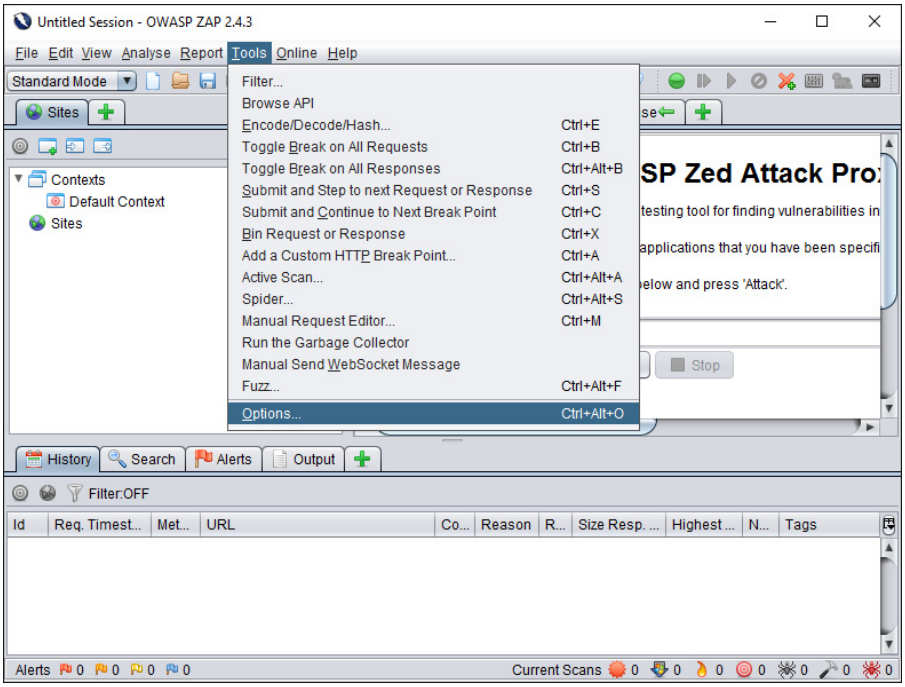
- เมื่อถึงหน้านี้ให้รอจนกว่าโปรแกรมจะโหลดเสร็จสิ้น



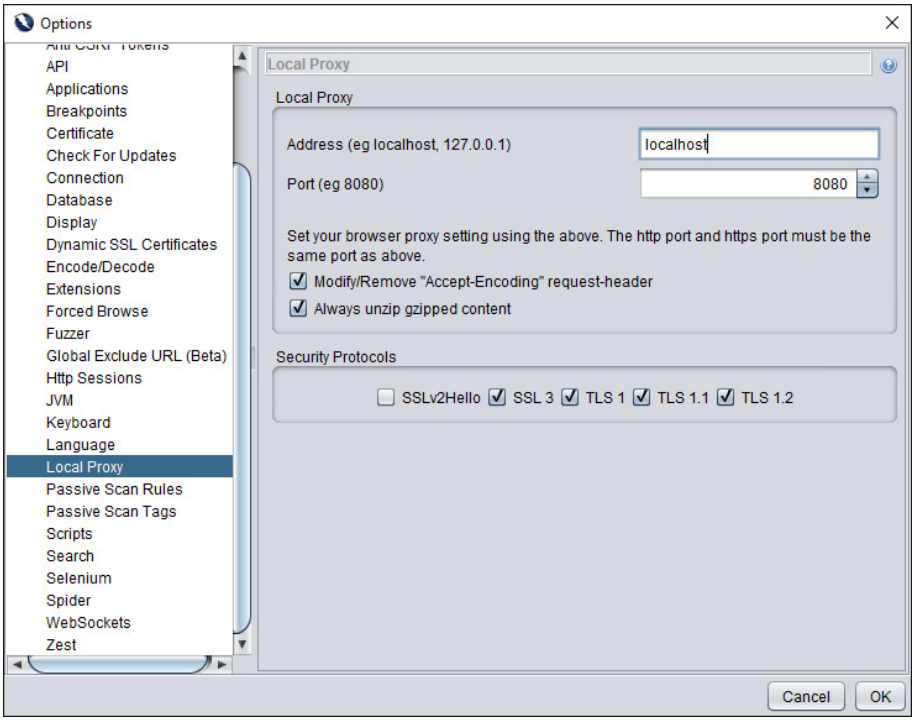

- ต่อไปจะมีหน้าต่างขึ้นว่า เราจะเก็บข้อมูลแบบไหน โดยในที่นี้ให้เลือก No (ไม่เก็บ)



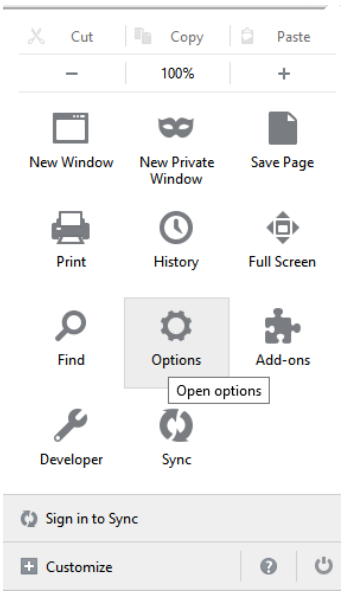
- ขั้นตอนต่อไปจะเป็นการดูที่อยู่ของ proxy ของโปรแกรมเพื่อใช้งานได้อย่างมีประสิทธิภาพมากขึ้น โดยกดที่ Tools>>Options



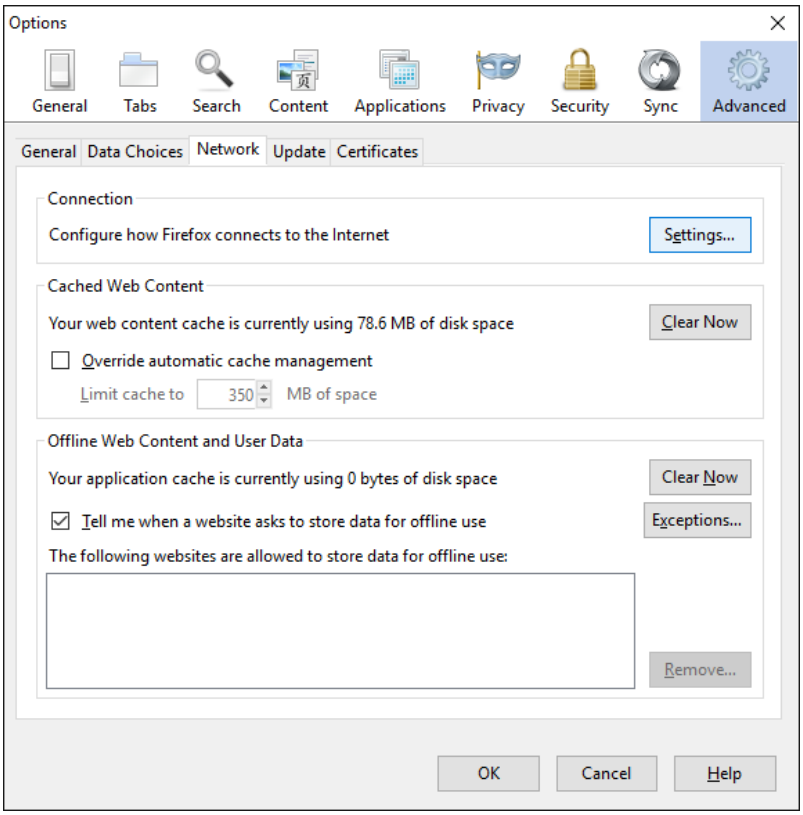

- จากนั้นเลือกในส่วนของ Local Proxy จะเห็นได้ว่า มีแอดเดรซคือ localhost และ Port คือ 8080



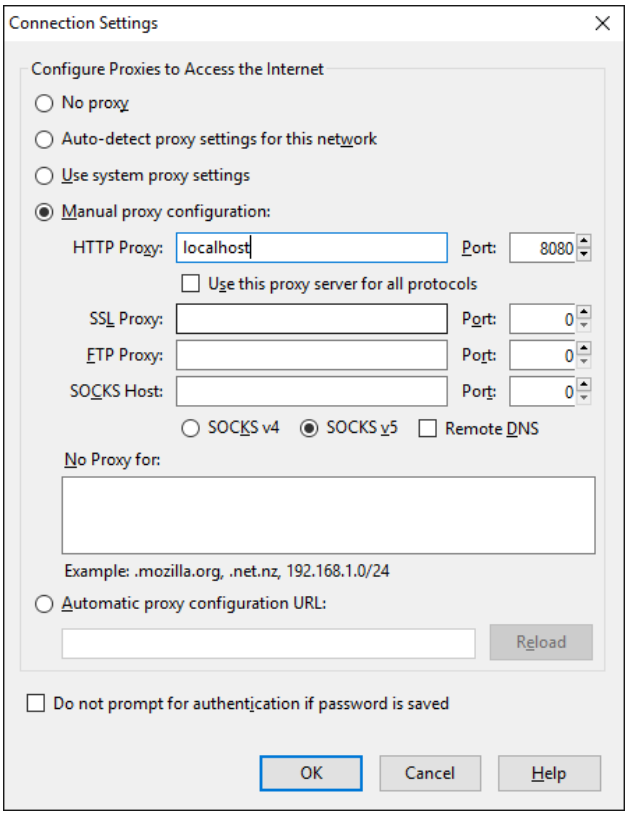
➢ จากนั้นให้เข้า FireFox แล้วไปที่Menu Options



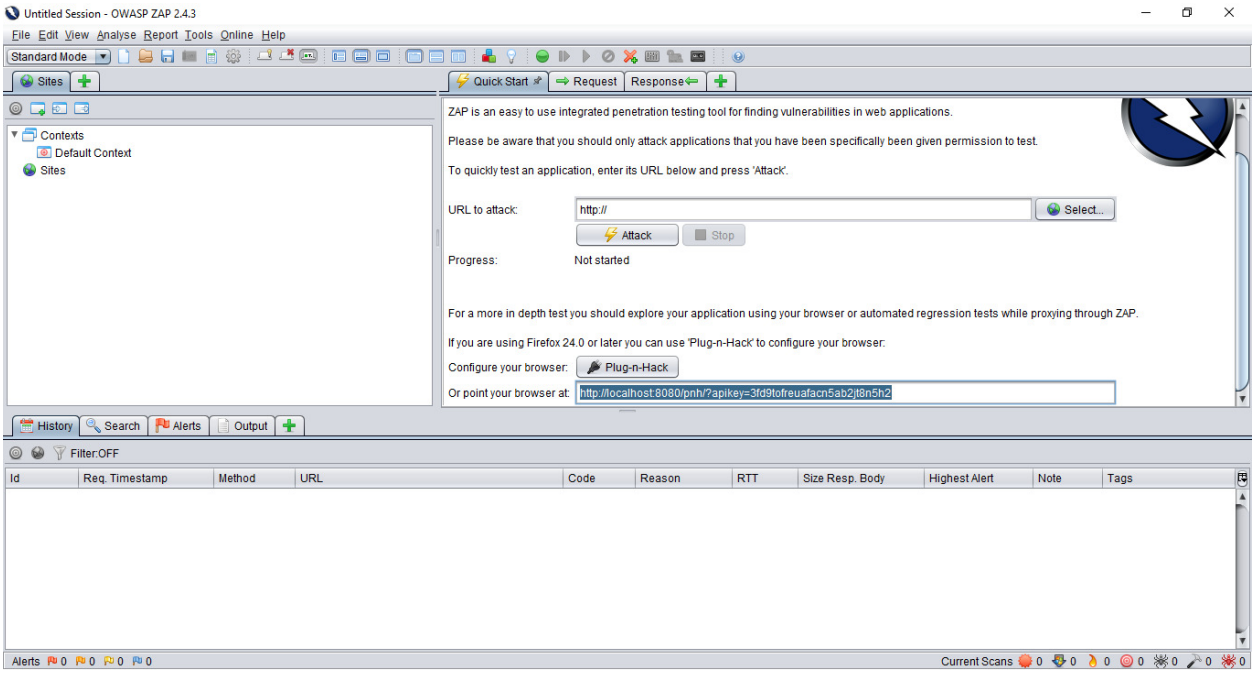

➢ ให้เลือกในส่วน Advanced แล้วไปที่ Tab 'Network' จากนั้น คลิกที่ Setting ในส่วนของ Connection



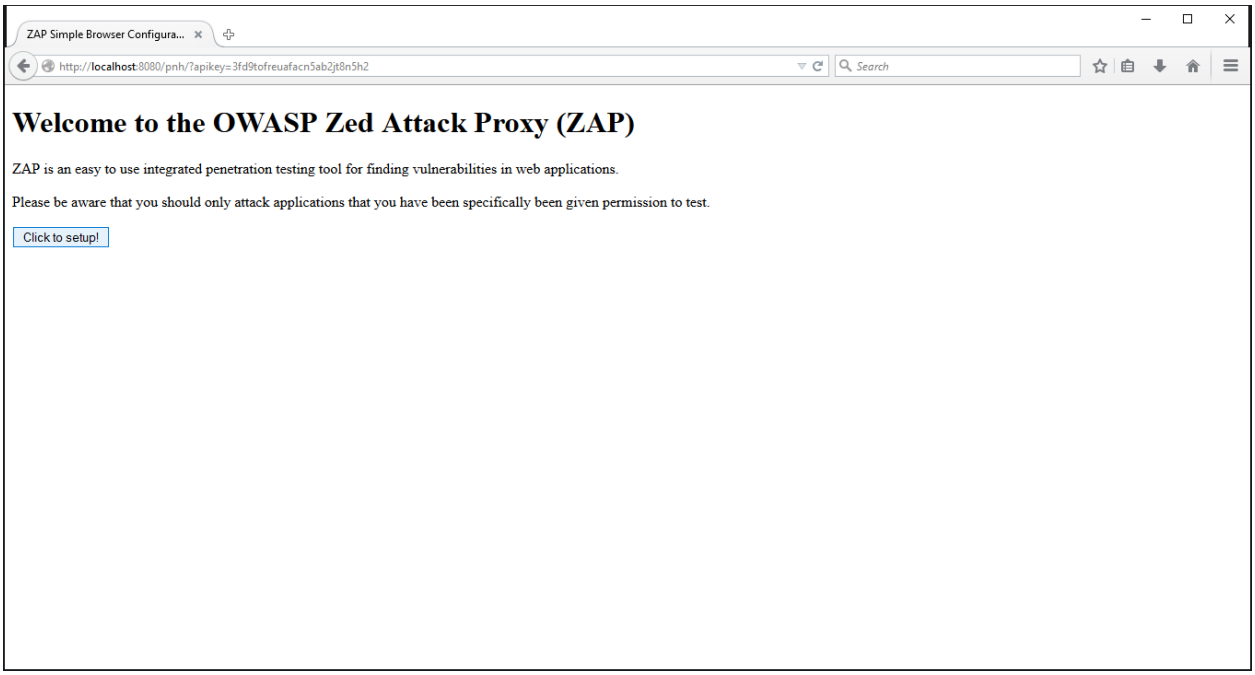
- ให้ผู้ใช้ทำการเลือก Radio Buttion ของ Manual proxy configuration แล้วทำการกรอกค่า Proxy ที่ได้จากโปรแกรม OWASP ZAP แล้วกด OK



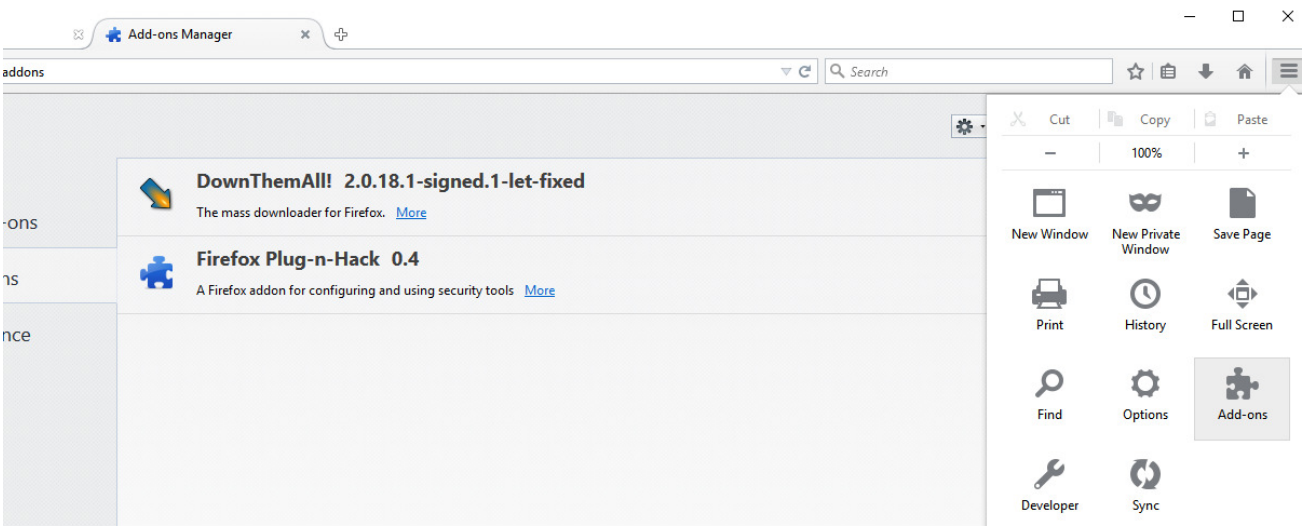

- พอเสร็จแล้วให้กลับมายังโปรแกรม OWASP ZAP แล้วทำการลงส่วนเสริมของโปรแกรมเพื่อที่เวลาเข้าเว็บผ่านบราวเซอร์ FireFox จะมีการส่งข้อมูลมาที่ตัวโปรแกรม โดยทำการก๊อปปี้ ลิงท์ใต้ปุ่ม Plug-n-Hack



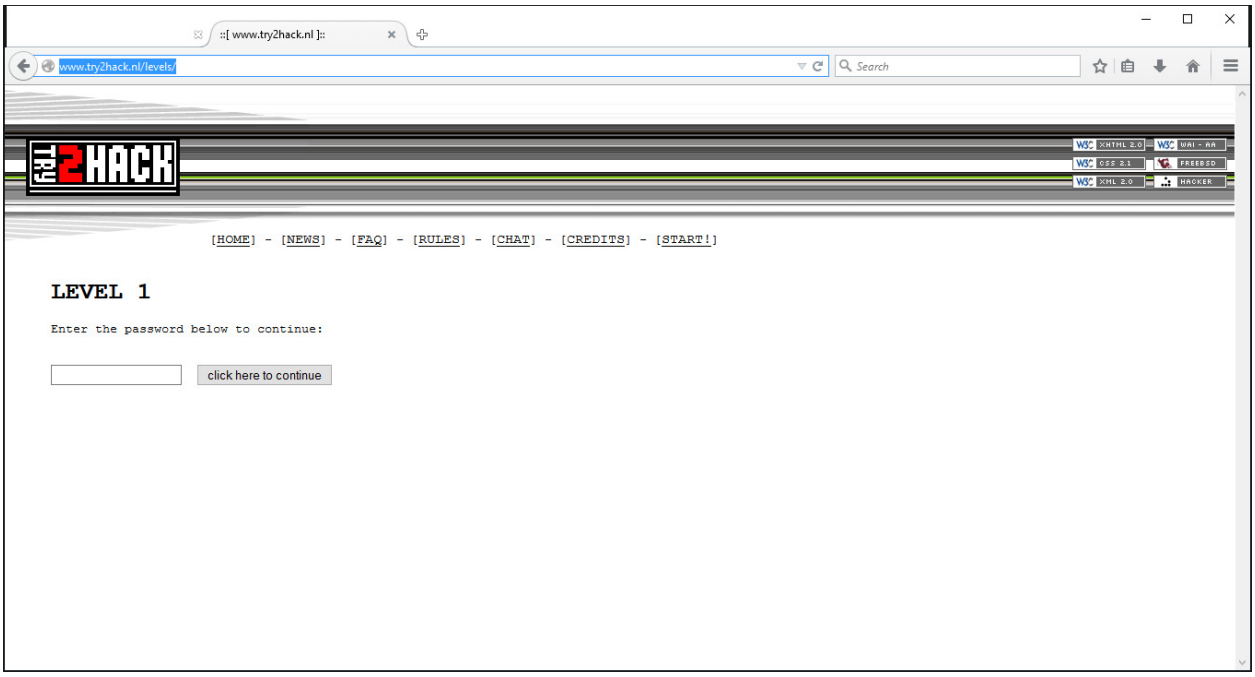
- นำลิงก์ที่ได้มาเข้าในบราวเซอร์ FireFox ที่ได้ทำการลงไว้ จากนั้นกดปุ่ม Click to setup! เพื่อติดตั้ง จะเป็นอันเสร็จเรียบร้อย



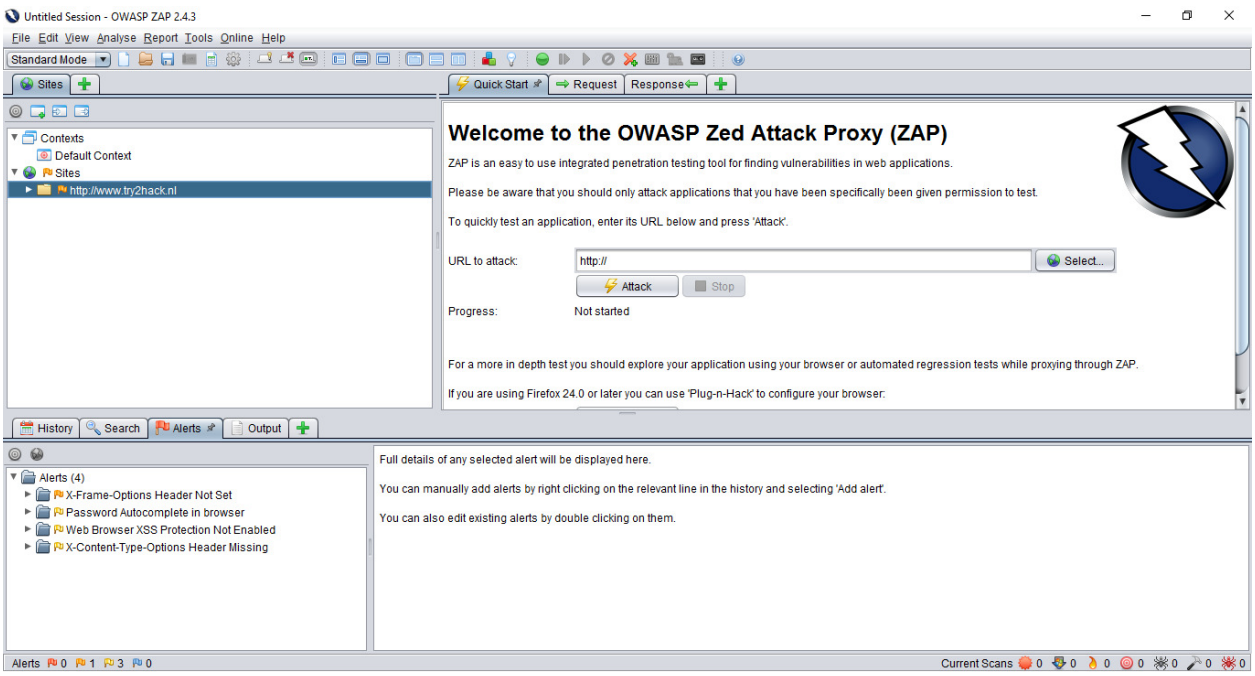

- สามารถตรวจสอบได้ว่า ติดตั้งสำเร็จจริงหรือไม่โดยการเข้าไปที่ Menu Add-ons โดยให้สังเกตดูว่ามีตัวเสริมที่ชื่อ Firefox Plug-n-Hack 0.4 หรือไม่ ถ้ามีแสดงว่าผ่าน



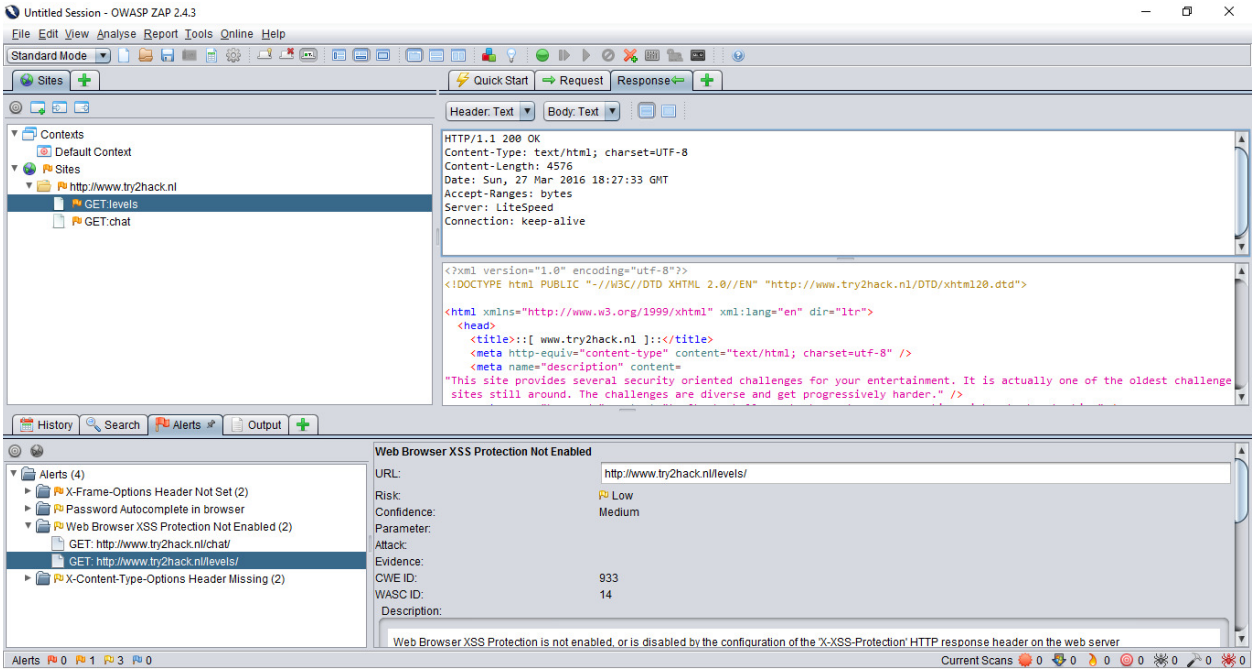
- ลองทำการเข้าเว็ปไซต์ www.try2hack.nl/levels/ เพื่อทดลองการส่งข้อมูล



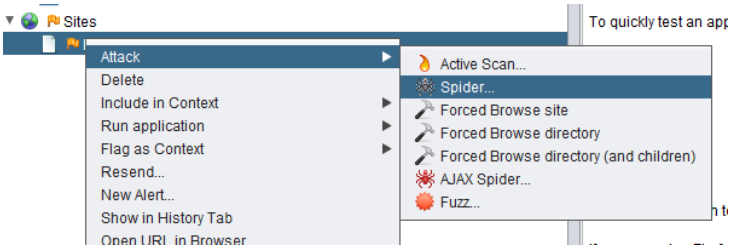

- กลับไปที่โปรแกรม OWASP ZAP จะเห็นได้ว่า มีข้อมูลของเว็ป http://www.try2hack.nl/ อยู่ในโปรแกรม



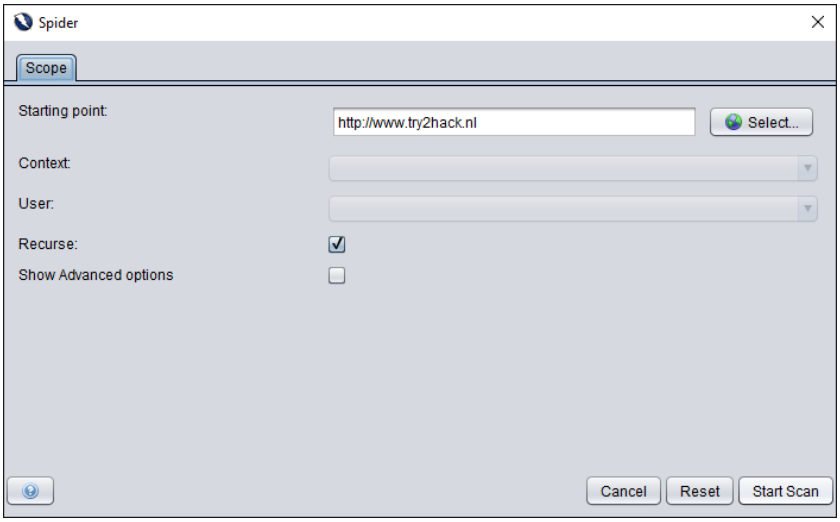
- ซึ่งข้อมูลประกอบคร่าวๆก็จะมีบอกว่า เว็ปไซต์นี้ มีส่วนประกอบอะไรบ้าง ใช้เซิฟเวอร์รุ่นไหน php เวอร์ชั่นอะไร



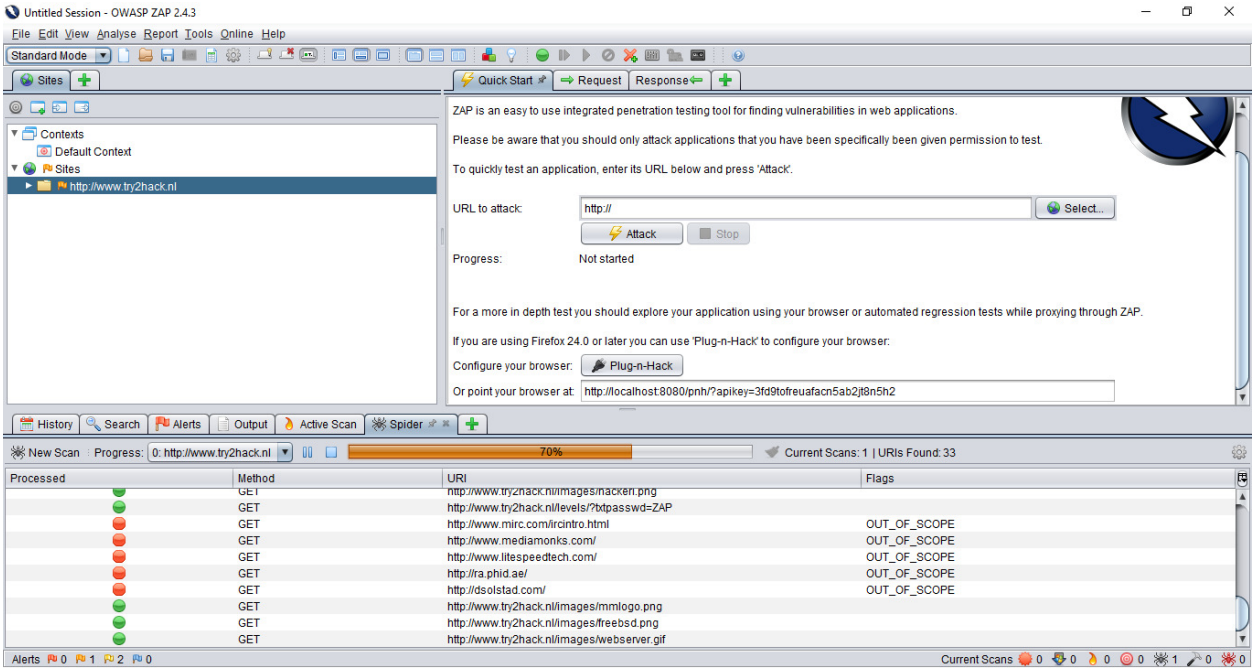

- ต่อไปจะทำการทดลองแสกน โดยคลิกขวาที่เว็ปไซต์เป้าหมาย จากนั้นกด Attack แล้วคลิกที่ Spider...




- กด Start Scan เพื่อเริ่ม




- จะเห็นได้ว่า ตัวโปรแกรมเริ่มทำการค้นหา เพื่อเช็คว่าเว็ปไซต์เป้าหมายมีช่องโหว่อะไรบ้าง



- โดยสามารถดูรายละเอียดได้ที่ tab Alerts