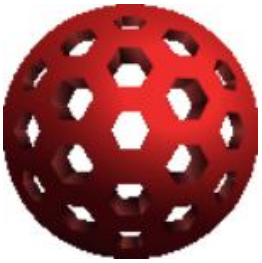


Subgraph Vega

จัดทำโดย

นายกฤษฎา โสมายัง 563020197-5

นางสาวจันทร์จิรา ปู่สูงเนิน 563020202-8

นายธำมรงค์ เวียงอินทร์ 563020765-4

นางสาวพลอย เหลาพิลา 563020771-9

นายพัฒนกฤษณ์ ชาญศิริวัฒน์ 563020773-5

นางสาววรรณวิสา จันทะนป 563020777-7

เสนอ

ผศ.ดร.จักรชัย โสอินทร์

รายงานนี้เป็นส่วนหนึ่งของวิชา 322376 Security

ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

มหาวิทยาลัยขอนแก่น

เครื่องมือป้องกันความปลอดภัย

Subgraph Vega

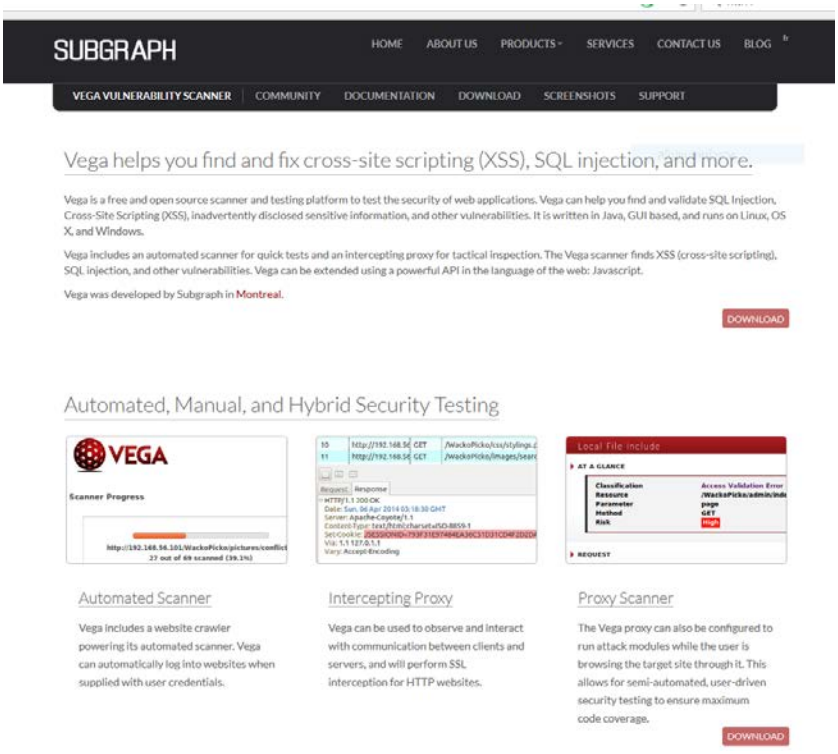
Vega เป็นเครื่องมือในการทดสอบความปลอดภัยของเว็บไซต์ และยังสามารถช่วย ค้นหาและตรวจสอบช่องโหว่เว็บไซต์ที่มีการเชื่อมต่อกับฐานข้อมูล และ Cross-Site Scripting (XSS) ที่อาจเปิดเผยข้อมูลที่สำคัญโดยไม่ได้ตั้งใจและช่องโหว่อื่น ๆ และยังสามารถ ตรวจสอบการโต้ตอบระหว่าง Client และ Server สำหรับเว็บไซต์ HTTP

การตรวจสอบช่องโหว่ของเว็บไซต์จะช่วยให้เราทราบถึงจุดสุ่มเสี่ยงของเว็บไซต์ของเราหรือเว็บไซต์อื่นๆ ซึ่งถ้าเว็บไซต์มีจุดเสี่ยงมากไป อาจจะโดนโจมตีจากผู้ไม่หวังดีต่างๆได้ ตัวอย่างเช่น การแฮกช่องโหว่แบบ XSS ของแฮกเกอร์โดยฝัง Script ลงในเว็บบอร์ด เป็นต้น และยังมี Vega proxy ที่สามารถกำหนดค่าให้เรียกใช้โมดูลโจมตีในขณะที่ผู้ใช้เรียกดูเว็บไซต์เป้าหมาย Vega สามารถใช้ในการ สำรวจ การเชื่อมต่อการสื่อสารกัน ระหว่าง ลูกข่ายกับ เซิฟเวอร์ผู้ให้บริการ และจะดำเนินการสกัดกั้น SSL สำหรับ Website HTTP

Vega เป็นเครื่องมือแบบ Open Source ซึ่งสามารถดาวน์โหลดมาพัฒนาต่อได้ที่ https://github.com/subgraph/Vega โดยโมดูลการตรวจสอบจะถูกเขียนใน JavaScript

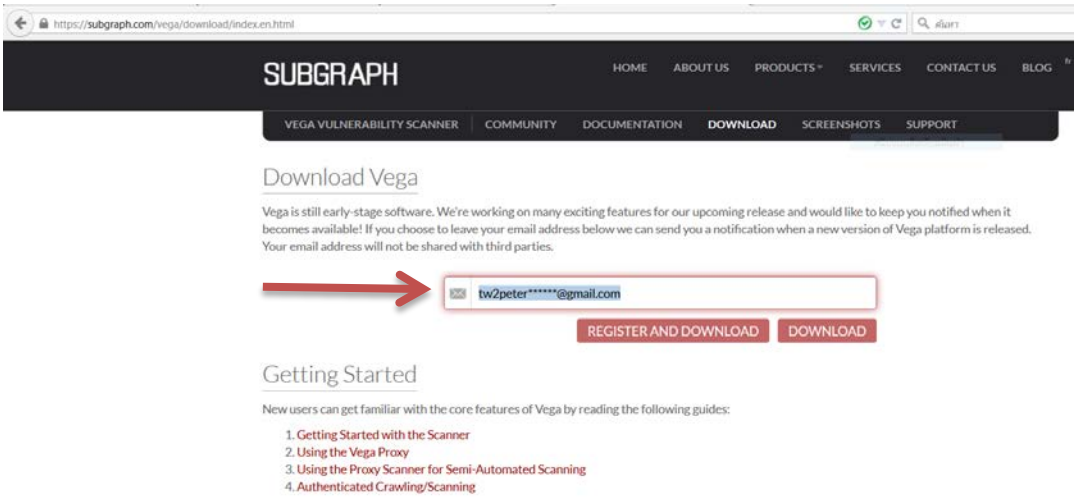
ไฟล์ที่เกี่ยวข้อง

- **VegaSetup32 หรือ VegaSetup64**

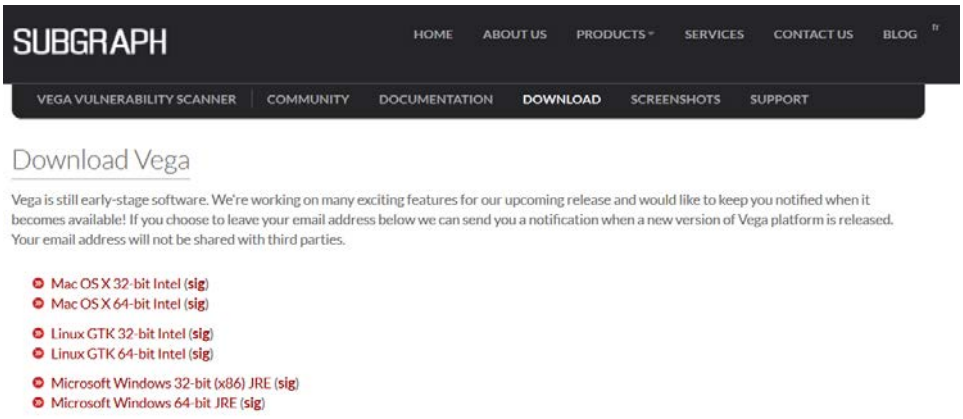


1. ขั้นตอนการติดตั้ง

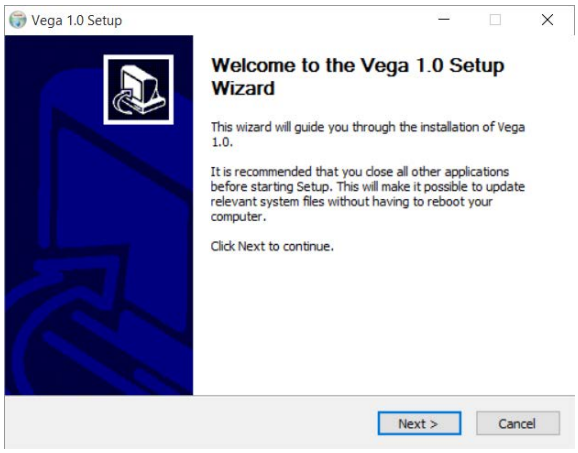
1.1 ให้ผู้ใช้เข้าไปที่เว็บ https://subgraph.com/vega/download/index.en.html เพื่อดาวน์โหลดไฟล์ติดตั้ง โดยผู้ใช้จะต้องกรอก E-mail เพื่อยืนยันตัวตนก่อนดาวน์โหลด ซึ่งทางเว็บจะให้โหลดฟรีไม่มีค่าใช้จ่ายใด ๆ

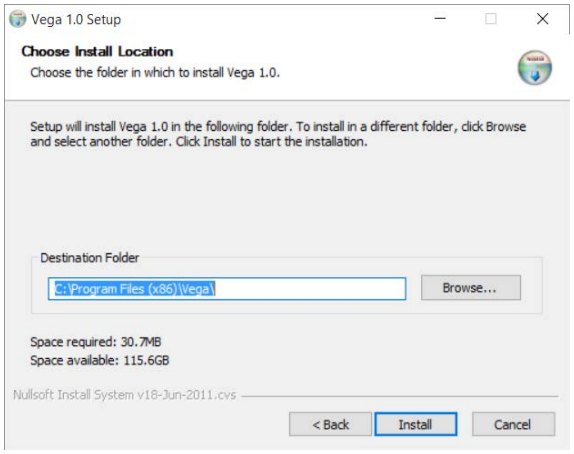


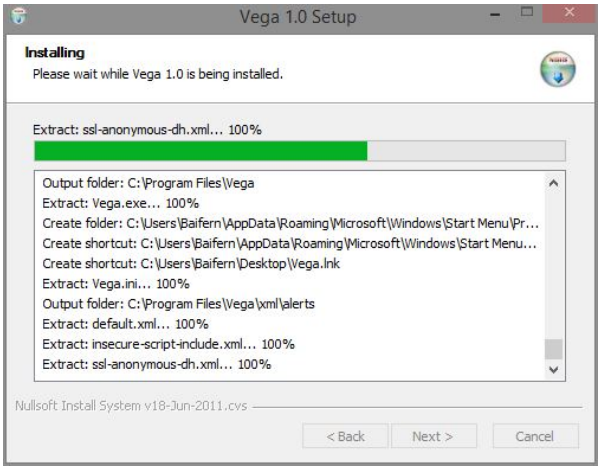
1.2 เลือกตามระบบปฏิบัติการของผู้ใช้

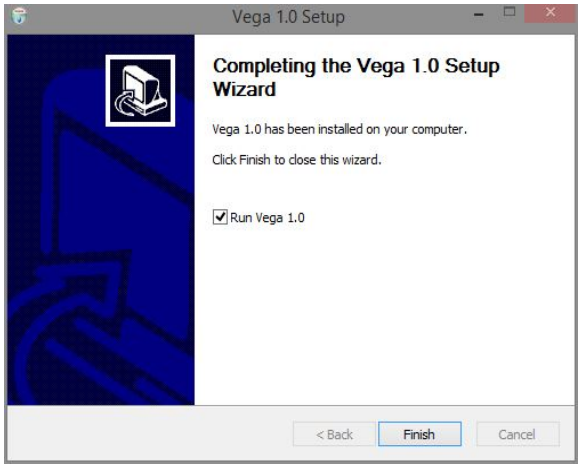


1.3 จะได้ไฟล์ VegaSetup ให้ผู้ใช้ทำการติดตั้ง Vega ลงบนคอมพิวเตอร์





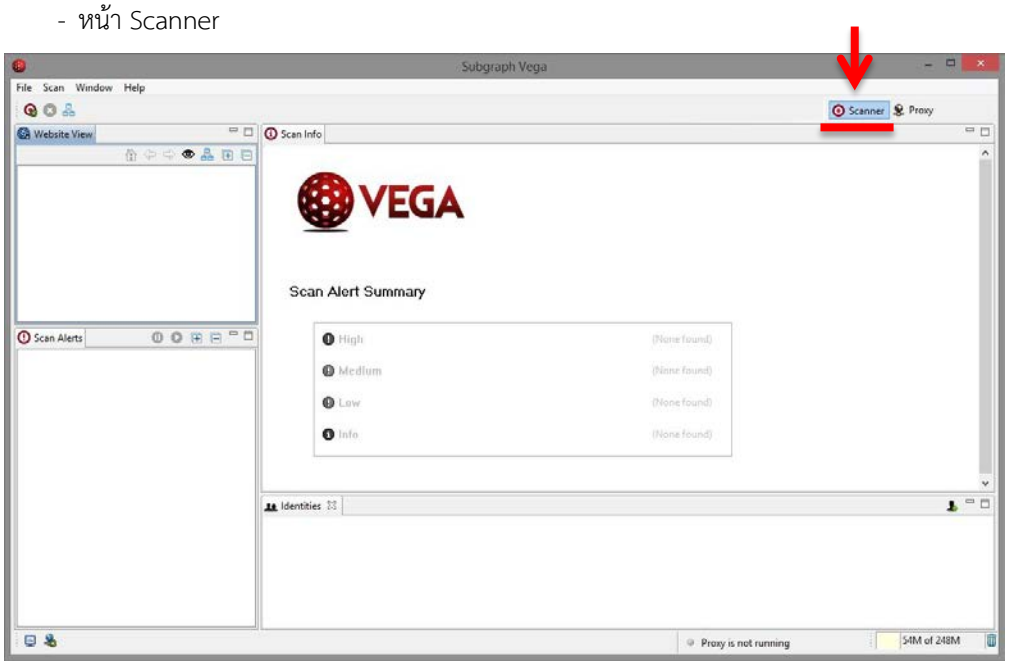




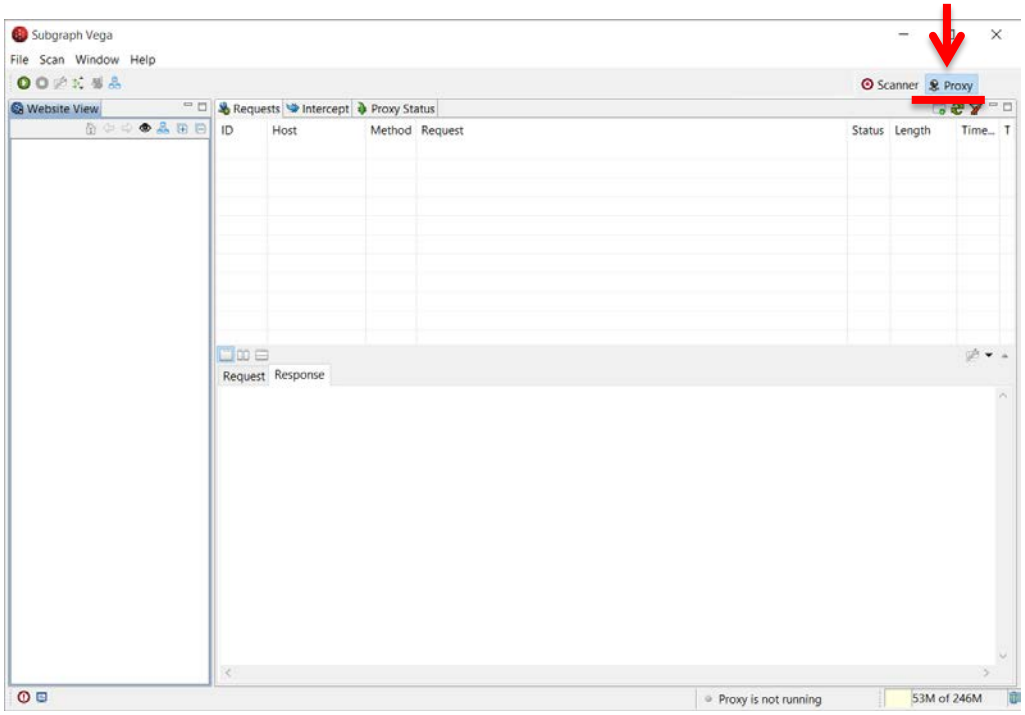
2. การใช้งาน Vega

2.1 หน้าแรกของโปรแกรม

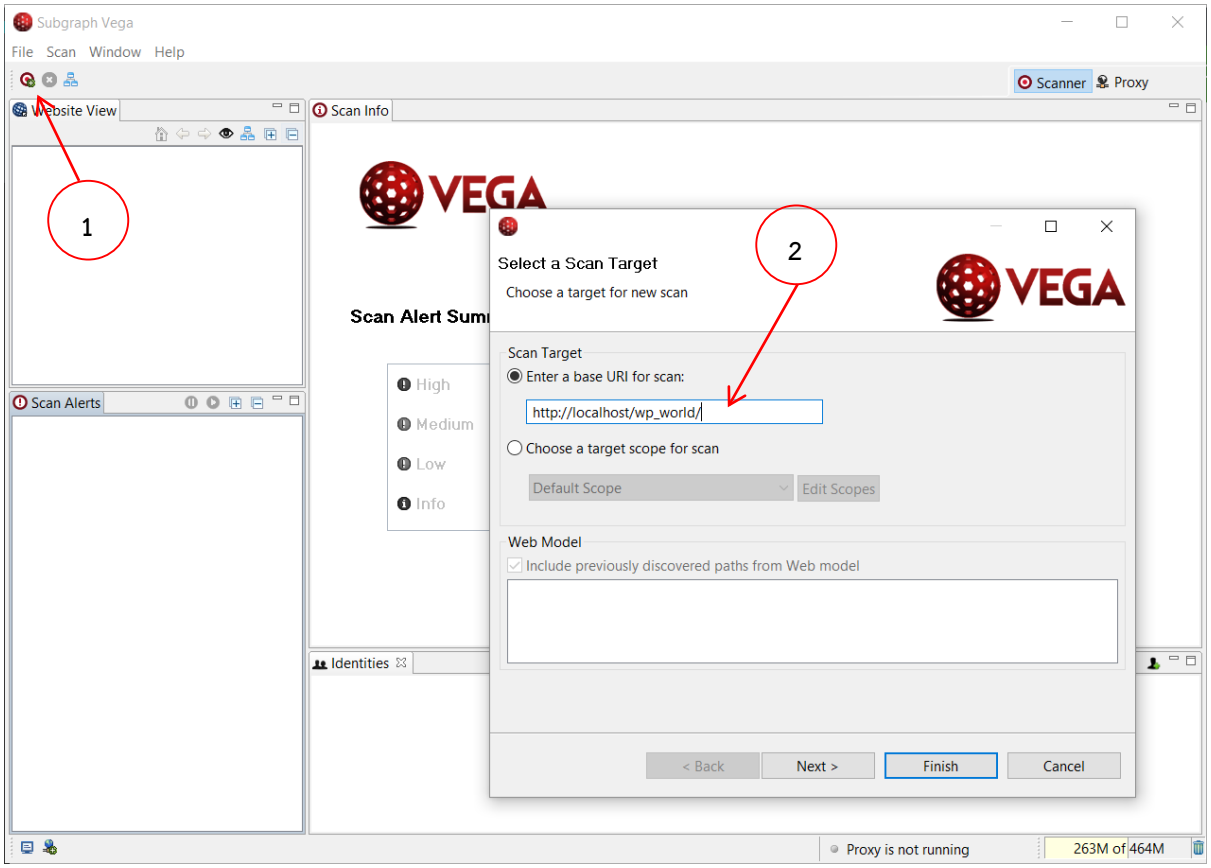
- หน้า Scanner



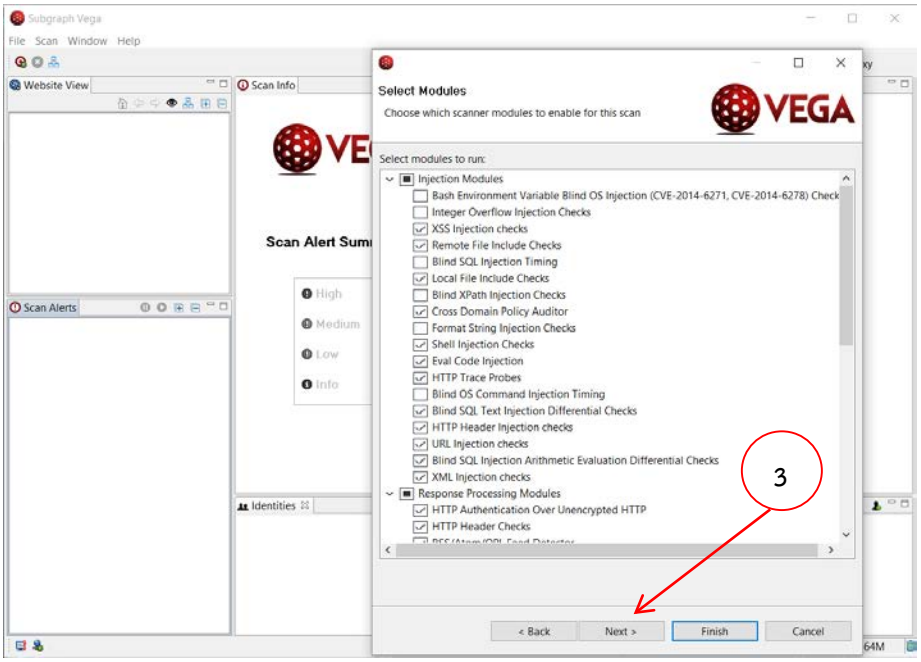
- หน้า Proxy



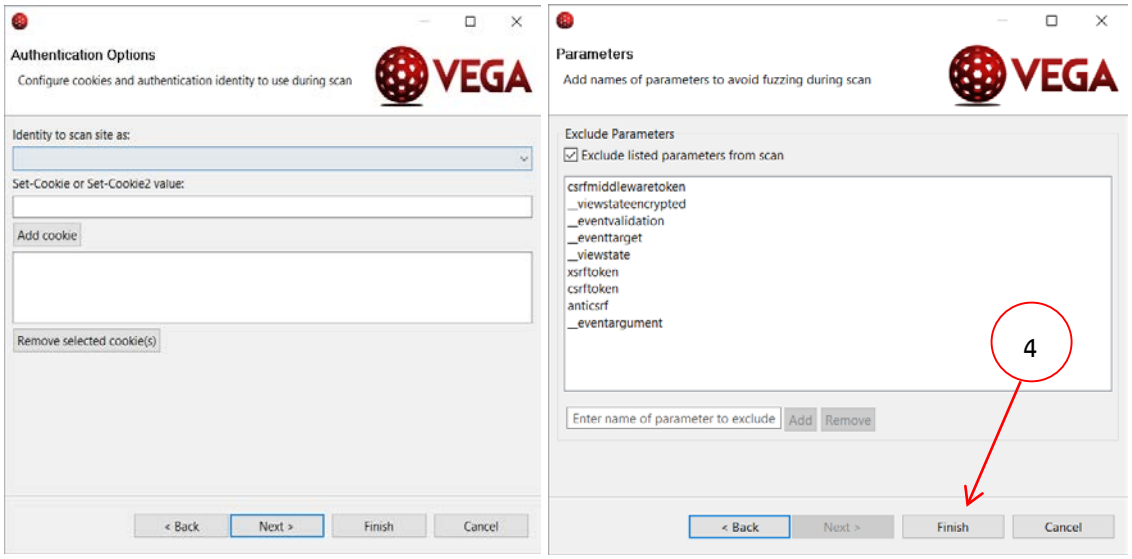
2.2 ให้ผู้ใช้คลิกที่ (1)Start New Scan แล้วกรอก (2)URL ของเว็บไซต์ที่ต้องการจะสแกน



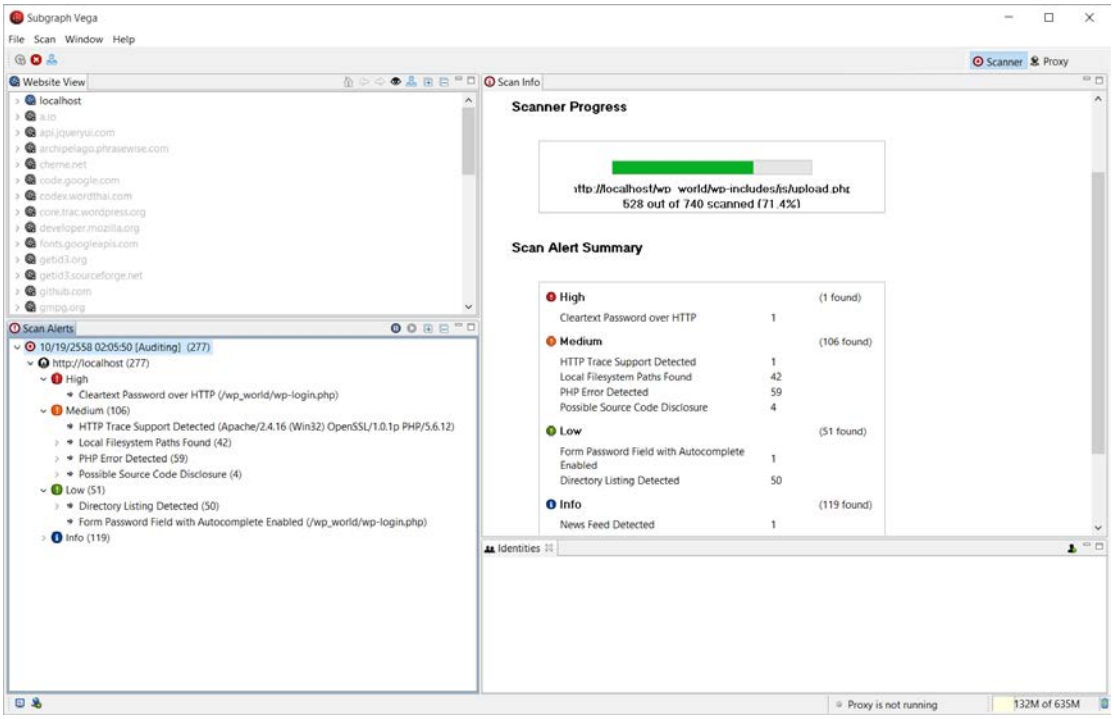
2.3 เลือกขอบเขตในการสแกน ว่าต้องการสแกนหาช่องโหว่แบบใดบ้าง แล้วกด (3)Next



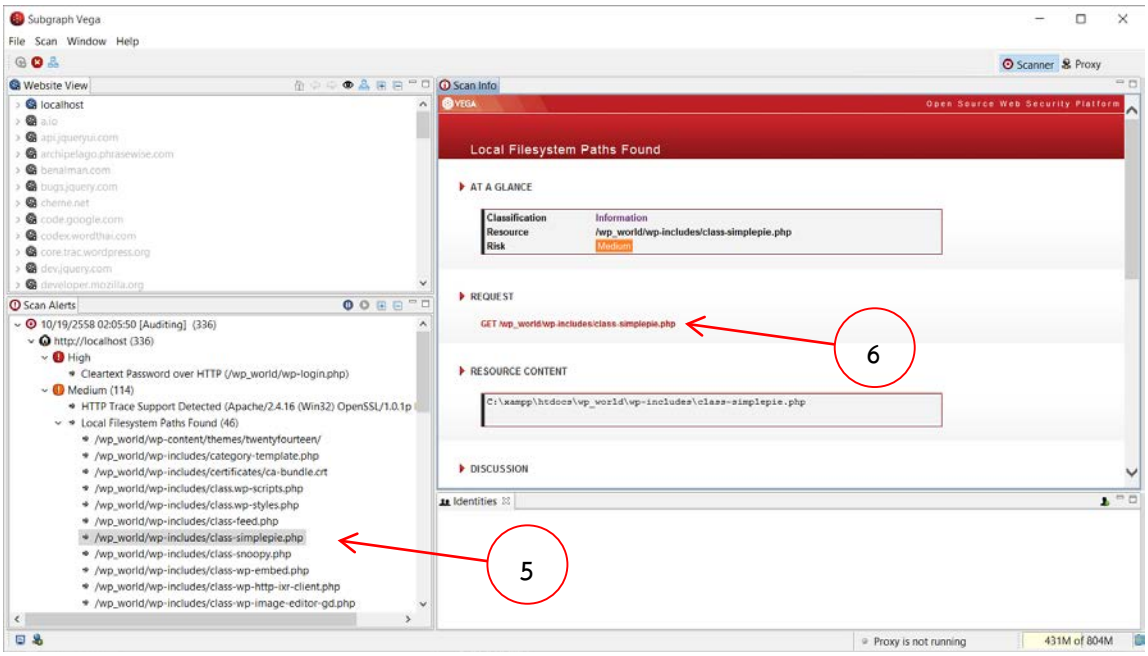
2.4 ส่วนนี้จะเป็นการเลือกคุกกี้ที่เราได้ตั้งค่าไว้ ในส่วนนี้ถ้าผู้ใช้ไม่ได้เจาะจงไปที่ส่วนใดส่วนหนึ่งให้กด Next อีกครั้ง แล้วกด (4)Finish



2.5 โปรแกรมจะแสดงผลการสแกน และบอกจุดที่เสี่ยงของเว็บไซต์เรา โดยแบ่งเป็น 4 ระดับ คือ High (ความเสี่ยงสูง) ,Medium (ความเสี่ยงปานกลาง) ,Low (ความเสี่ยงต่ำ) และ Info (ข้อมูล)

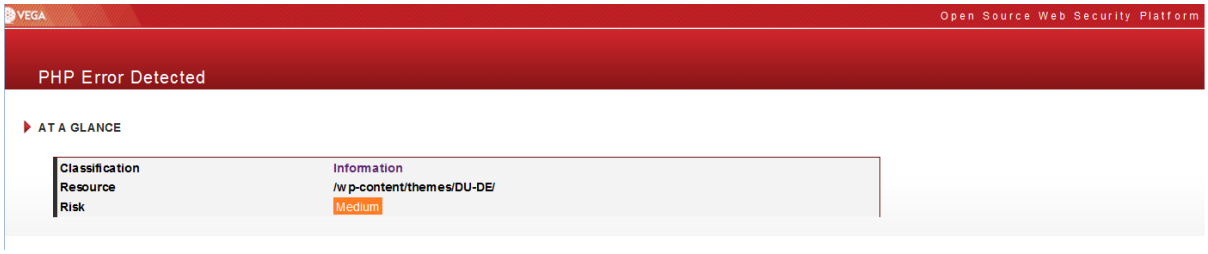


2.6 (5)แสดงรายละเอียดข้อผิดพลาดของแต่ละจุด



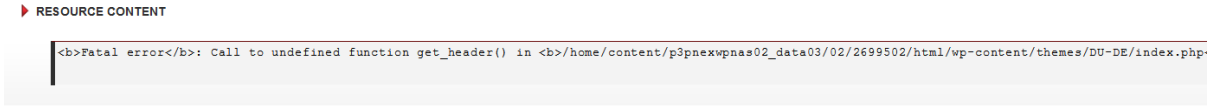
ในส่วนของรายละเอียดก็จะบอกรายละเอียดต่างๆ เช่น

1. At a Glance จะบอกถึงรายระเอียดคร่าวๆ ว่าจุดที่พบนั้นอยู่ที่ใด มีความเสี่ยงมากแค่ไหน

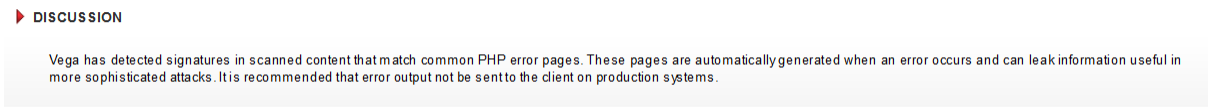


2. Request บอกถึงจุดที่เว็บร้องขอไป

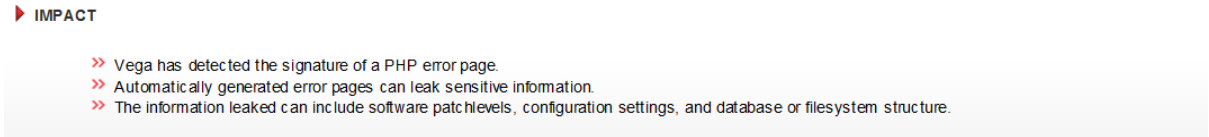
3. Resource Content แสดงเนื้อหา Script ที่เป็นจุดบกพร่องต่อความปลอดภัย



4. Discussion เป็นการอภิปรายในเนื้อหาที่ผิดพลาดที่สแกนพบ และอธิบายถึงแนวโน้มที่อาจจะเกิดกับเว็บไซต์ได้



5. Impact จะเป็นการบอกถึงผลกระทบที่จะเกิดขึ้นหากไม่แก้ไข



6. Remediation เป็นส่วนที่จะบอกถึงแนวทางแก้ไข เป็นคำแนะนำ

REMEDIATION

» The PHP manual recommends disabling "display_errors" on servers exposed to the Internet. For PHP 5.2.4 and greater, the "display_errors" setting in the "php.ini" configuration file should be set to "stderr" (error output stream), rather than "stdout" (output stream sent to clients). For earlier versions, "display_errors" is a boolean type, and can be set to "False" for disabling. The setting can also be disabled at runtime using ini_set() from within a PHP script.

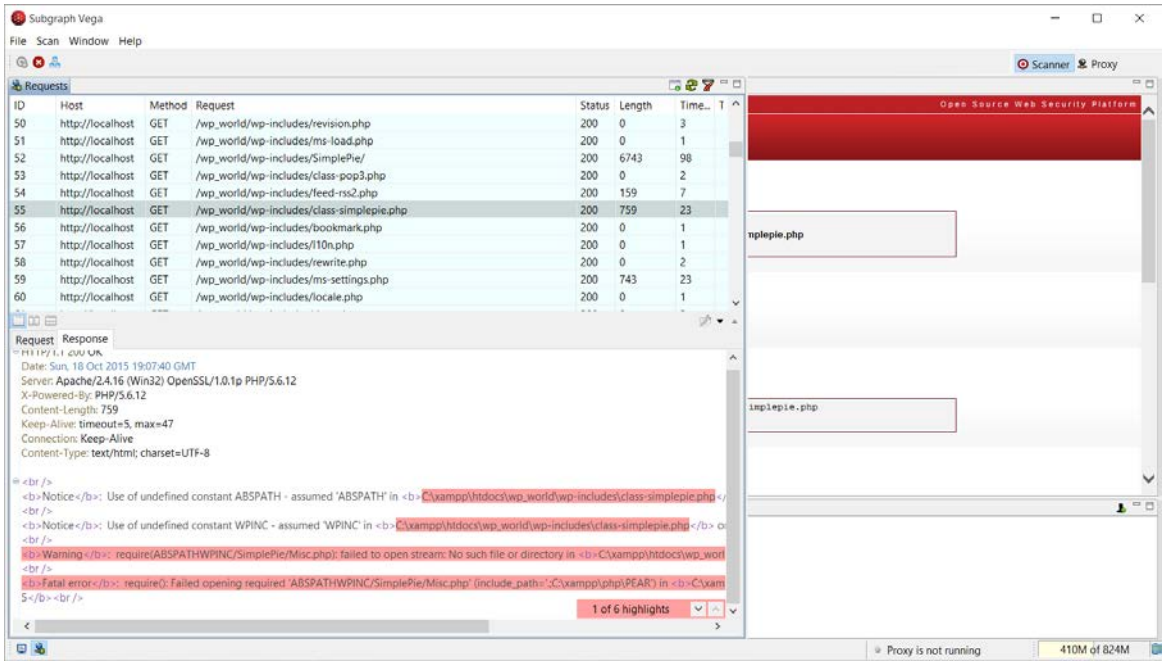
7. References เป็นส่วนที่จะเชื่อมโมงไปยังอ้างอิงที่โปรแกรมได้ ให้ข้อมูลกับเรามา หรือคู่มือในการแก้ไขจากผู้พัฒนาภาษา Script นั้นๆ

REFERENCES

Some additional links with relevant information published by third-parties:

→ Turning off display-errors (php Manual)

2.7 (6)แสดงรายละเอียดจุดที่มีความเสี่ยงในระดับ script ซึ่งจุดมาร์คสีแดงคือจุดที่มีความเสี่ยงที่ผู้ไม่หวังดีอาจนำช่องโหว่นี้ ไปทำอันตรายกับเว็บไซต์นั้น ๆ ได้



2.8 ถ้าผู้ใช้อยากทราบรายละเอียดทั้งหมดของข้อผิดพลาด ให้คลิกที่ (7)Proxy