

## Subgraph Vega

### จัดทำโดย

นายกฤษฎา	โสมายัง	563020197-5
นางสาวจันทร์จิรา	ปู่สูงเนิน	563020202-8
นายธำรงค์	เวียงอินทร์	563020765-4
นางสาวพลอย	เหล่าพิลา	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

การตรวจสอบช่องโหว่ของเว็บไซต์จะช่วยให้เราทราบถึงจุดอ่อนของเว็บไซต์ของเราหรือเว็บไซต์อื่นๆ ซึ่งถ้าเว็บไซต์มีจุดเสี่ยงมากไป อาจโดนโจมตีจากผู้ไม่หวังดีต่างๆได้ ตัวอย่างเช่น การแทรกช่องโหว่แบบ XSS ของแอสเกตอร์โดยฝัง Script ลงในเว็บบอร์ด เป็นต้น และยังมี Vega proxy ที่สามารถกำหนดค่าให้เรียกใช้โมดูลโจมตีในขณะที่ผู้ใช้เรียกดูเว็บไซต์เป้าหมาย Vega สามารถใช้ในการสำรวจ การเชื่อมต่อการสื่อสารกัน ระหว่าง ลูกข่ายกับ เซิร์ฟเวอร์ผู้ให้บริการ และจะดำเนินการสกรักกัน SSL สำหรับ Website HTTP

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

- VegaSetup32 หรือ VegaSetup64

The screenshot shows the Subgraph Vega website. At the top, there is a navigation menu with links for HOME, ABOUT US, PRODUCTS, SERVICES, CONTACT US, and BLOG. Below this is a secondary menu with links for VEGA VULNERABILITY SCANNER, COMMUNITY, DOCUMENTATION, DOWNLOAD, SCREENSHOTS, and SUPPORT. The main content area features a 'DOWNLOAD' button and three sections:

- Automated Scanner:** Vega includes a website crawler powering its automated scanner. Vega can automatically log into websites when supplied with user credentials.
- Intercepting Proxy:** Vega can be used to observe and interact with communication between clients and servers, and will perform SSL interception for HTTP websites.
- Proxy Scanner:** The Vega proxy can also be configured to run attack modules while the user is browsing the target site through it. This allows for semi-automated, user-driven security testing to ensure maximum code coverage.

### Open Source

Vega is open source software, licensed under the [EPL \(Eclipse Public License\) 1.0](#).

### Getting the Source Code

The source code is hosted on [github](#), and instructions for building it are located here.

### Extending Vega

Vega is more than just a scanner and proxy. Vega is a platform for developing new types of tests for web applications. See the documentation for more information on extending Vega with custom modules and alerts.

### Getting in Touch

Vega users can get involved by visiting the channel [#subgraph](#) on the Freenode IRC server, or by subscribing to the [Vega-Users](#) group hosted at Google Groups.

## 1. ขั้นตอนการติดตั้ง

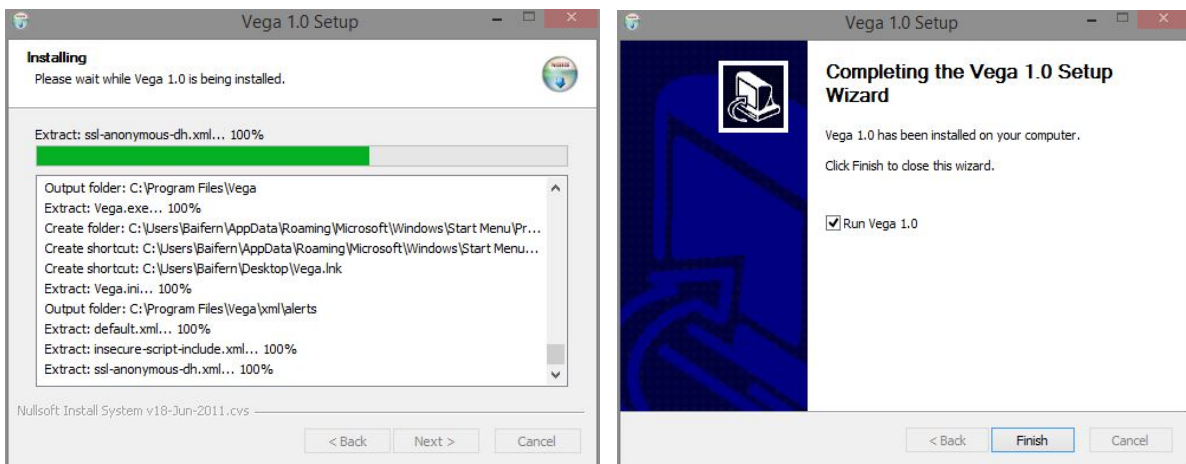
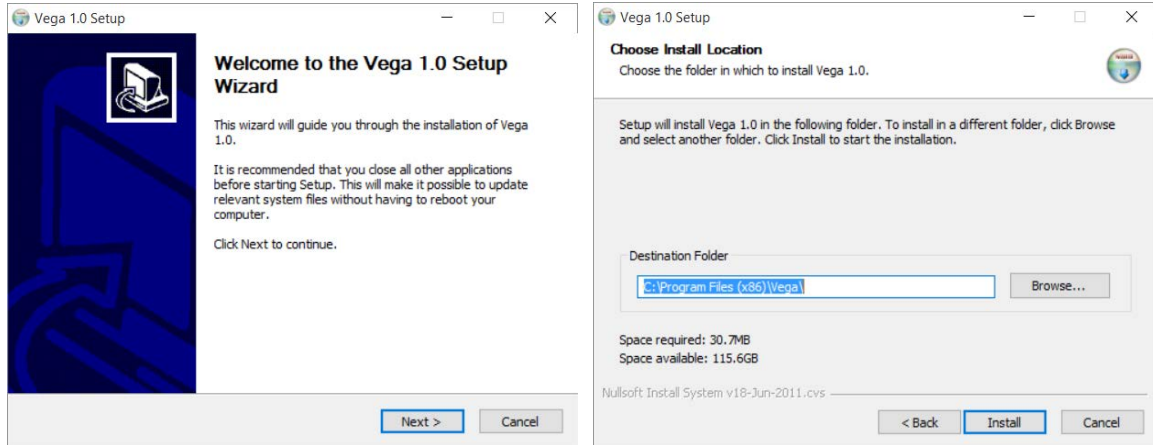
1.1 ให้ผู้ใช้เข้าไปที่เว็บ <https://subgraph.com/vega/download/index.en.html> เพื่อดาวน์โหลดไฟล์ติดตั้ง โดยผู้ใช้จะต้องกรอก E-mail เพื่อยืนยันตัวตนก่อนดาวน์โหลด ซึ่งทางเว็บจะให้โหลดฟรีไม่มีค่าใช้จ่ายใด ๆ

The screenshot shows the Vega download page. The navigation menu includes: HOME, ABOUT US, PRODUCTS, SERVICES, CONTACT US, BLOG. The main menu includes: VEGA VULNERABILITY SCANNER, COMMUNITY, DOCUMENTATION, DOWNLOAD, SCREENSHOTS, SUPPORT. The 'Download Vega' section contains the text: "Vega is still early-stage software. We're working on many exciting features for our upcoming release and would like to keep you notified when it becomes available! If you choose to leave your email address below we can send you a notification when a new version of Vega platform is released. Your email address will not be shared with third parties." Below this is an email input field with the value "tw2peter\*\*\*\*\*@gmail.com" and two buttons: "REGISTER AND DOWNLOAD" and "DOWNLOAD". A red arrow points to the email input field. Below this is the "Getting Started" section with the text: "New users can get familiar with the core features of Vega by reading the following guides:" followed by a list of four guides: 1. Getting Started with the Scanner, 2. Using the Vega Proxy, 3. Using the Proxy Scanner for Semi-Automated Scanning, 4. Authenticated Crawling/Scanning.

1.2 เลือกตามระบบปฏิบัติการของผู้ใช้

The screenshot shows the Vega download page. The navigation menu includes: HOME, ABOUT US, PRODUCTS, SERVICES, CONTACT US, BLOG. The main menu includes: VEGA VULNERABILITY SCANNER, COMMUNITY, DOCUMENTATION, DOWNLOAD, SCREENSHOTS, SUPPORT. The 'Download Vega' section contains the text: "Vega is still early-stage software. We're working on many exciting features for our upcoming release and would like to keep you notified when it becomes available! If you choose to leave your email address below we can send you a notification when a new version of Vega platform is released. Your email address will not be shared with third parties." Below this is a list of download links: Mac OS X 32-bit Intel (sig), Mac OS X 64-bit Intel (sig), Linux GTK 32-bit Intel (sig), Linux GTK 64-bit Intel (sig), Microsoft Windows 32-bit (x86) JRE (sig), Microsoft Windows 64-bit JRE (sig).

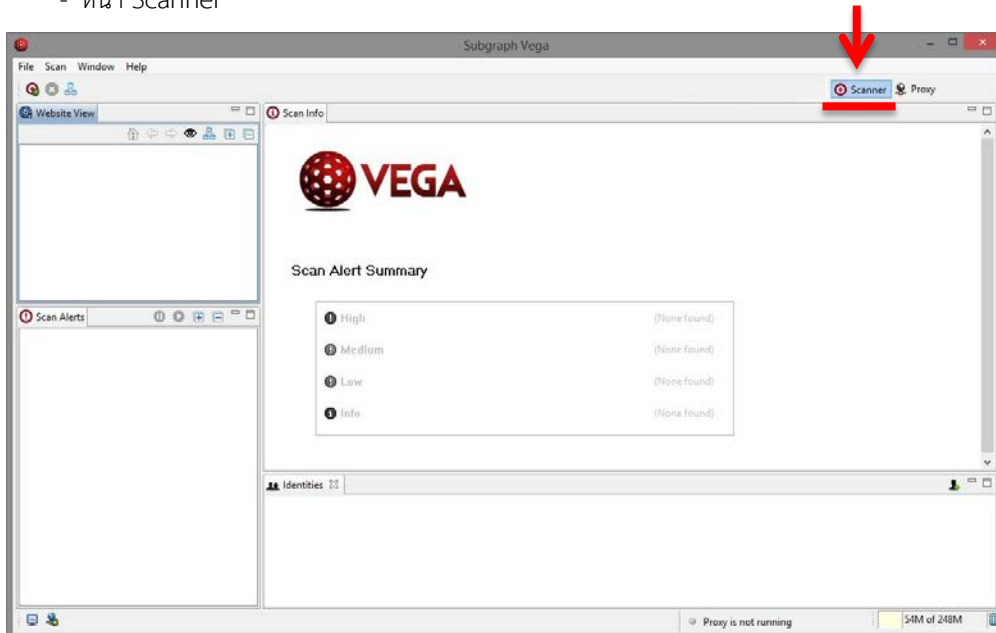
### 1.3 จะได้ไฟล์ VegaSetup ให้ผู้ใช้ทำการติดตั้ง Vega ลงบนคอมพิวเตอร์



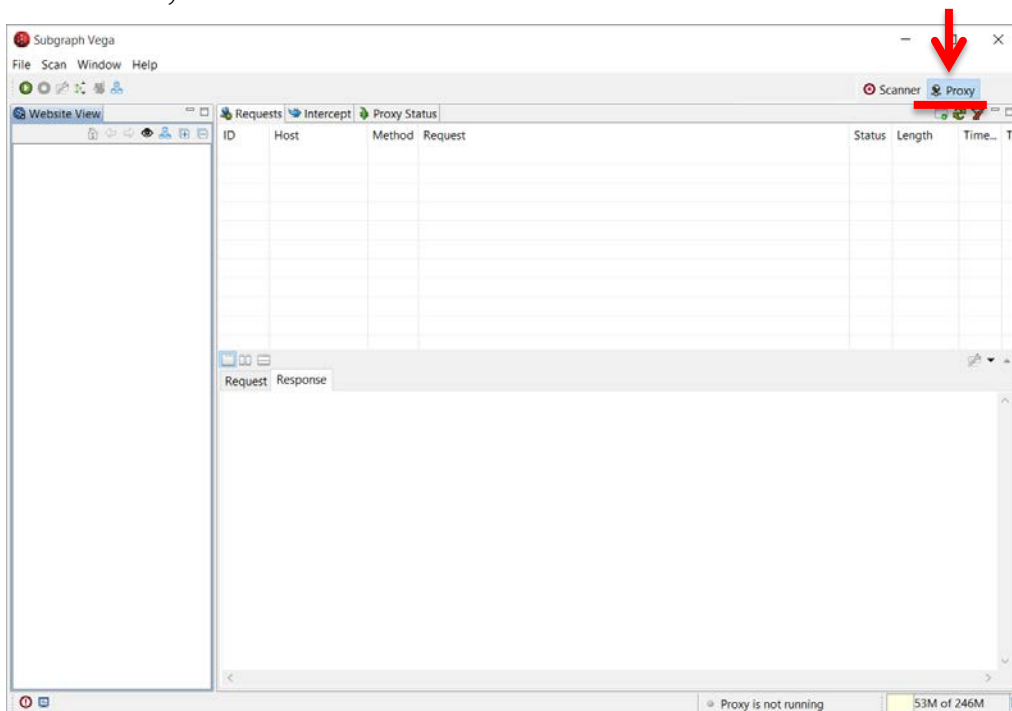
## 2. การใช้งาน Vega

### 2.1 หน้าแรกของโปรแกรม

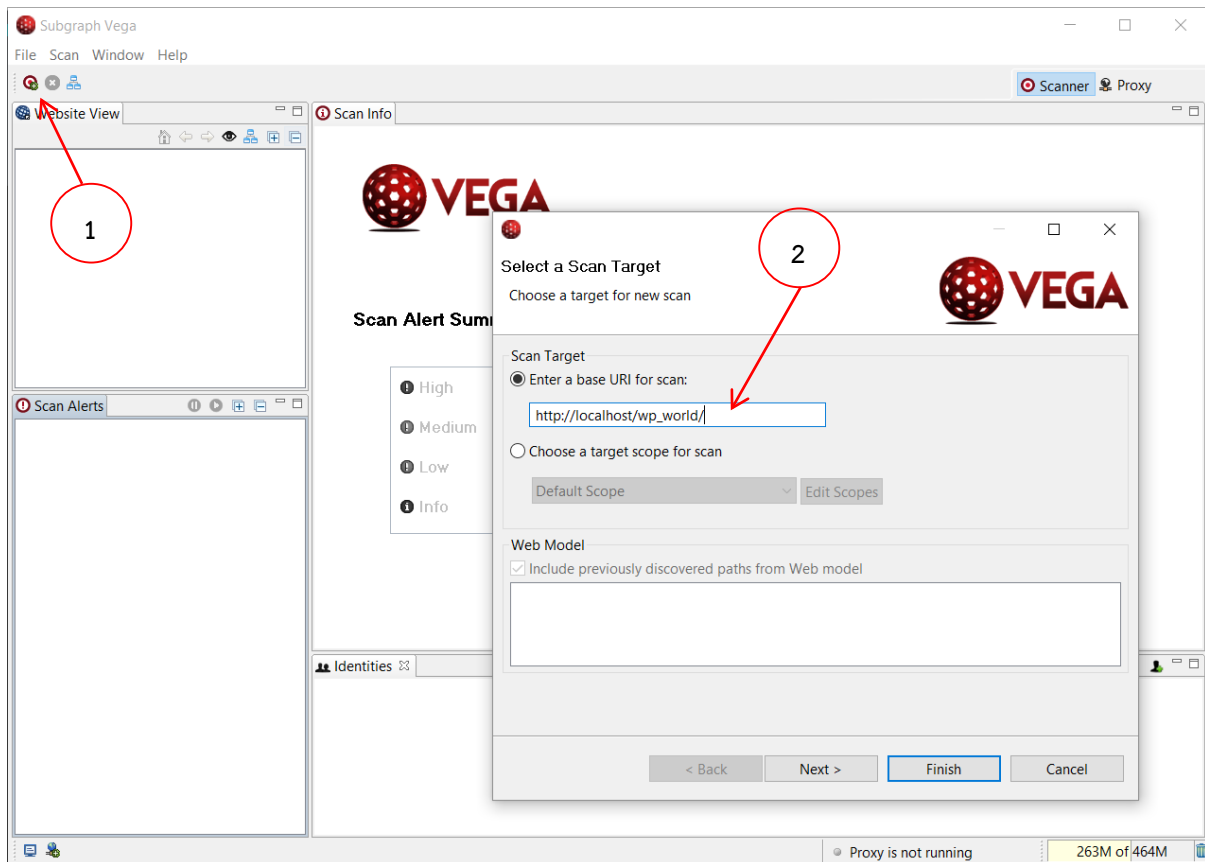
- หน้า Scanner



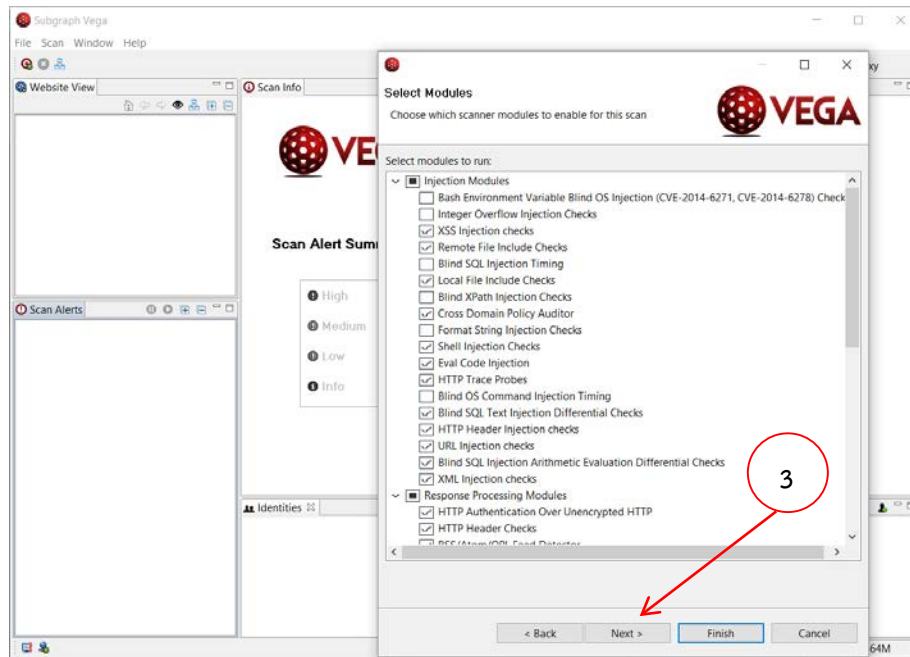
- หน้า Proxy



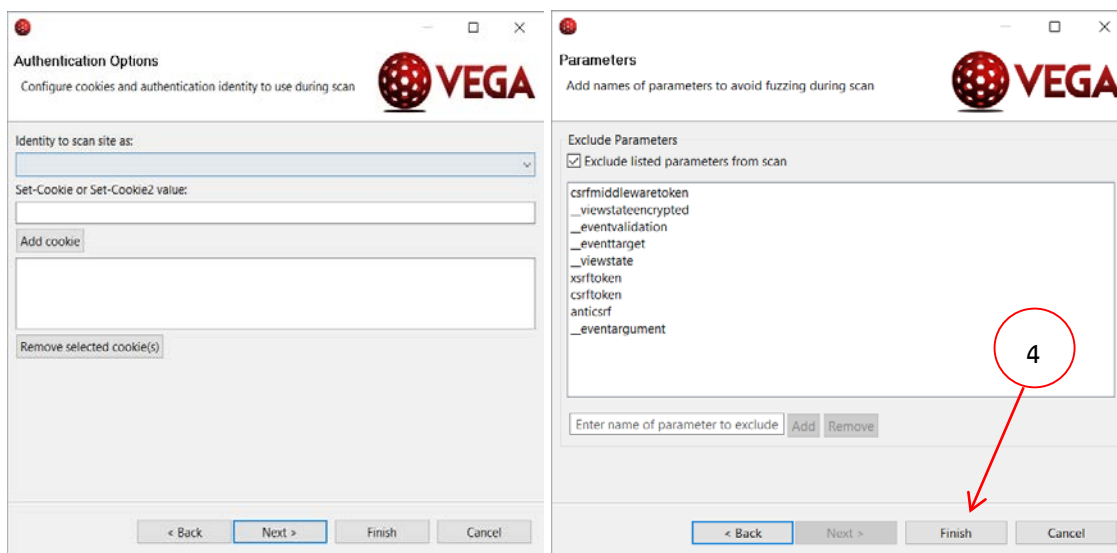
2.2 ให้ผู้ใช้คลิกที่ (1)Start New Scan แล้วกรอก (2)URL ของเว็บไซต์ที่ต้องการจะสแกน



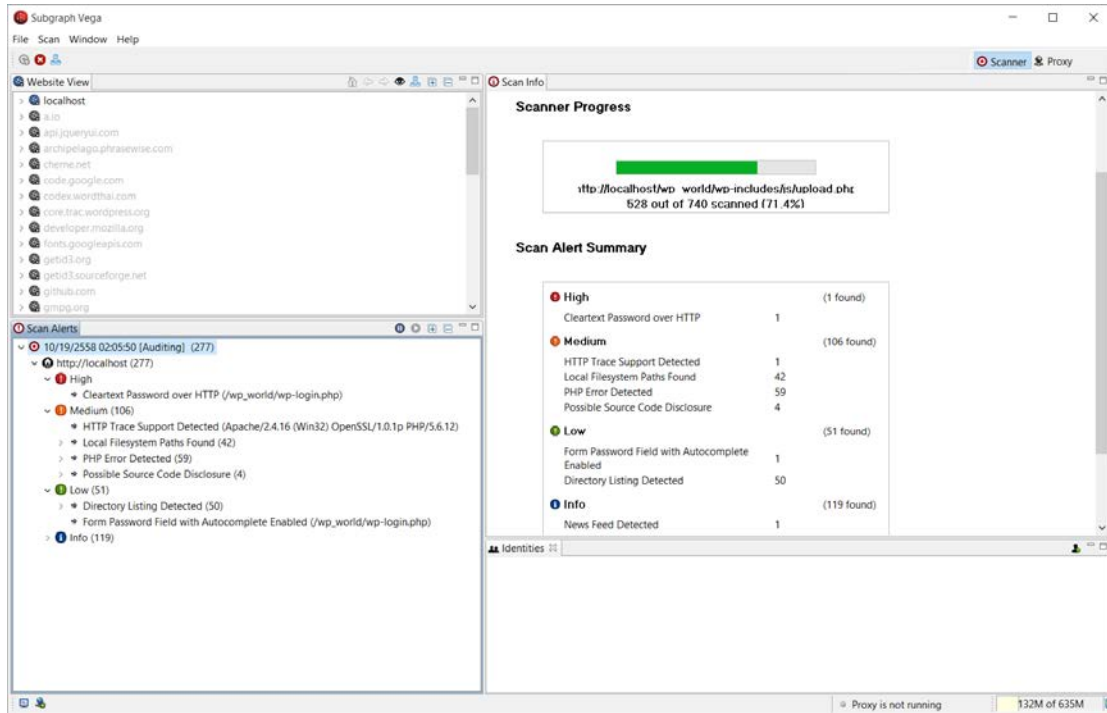
## 2.3 เลือกขอบเขตในการสแกน ว่าต้องการสแกนหาช่องโหว่แบบใดบ้าง แล้วกด (3)Next



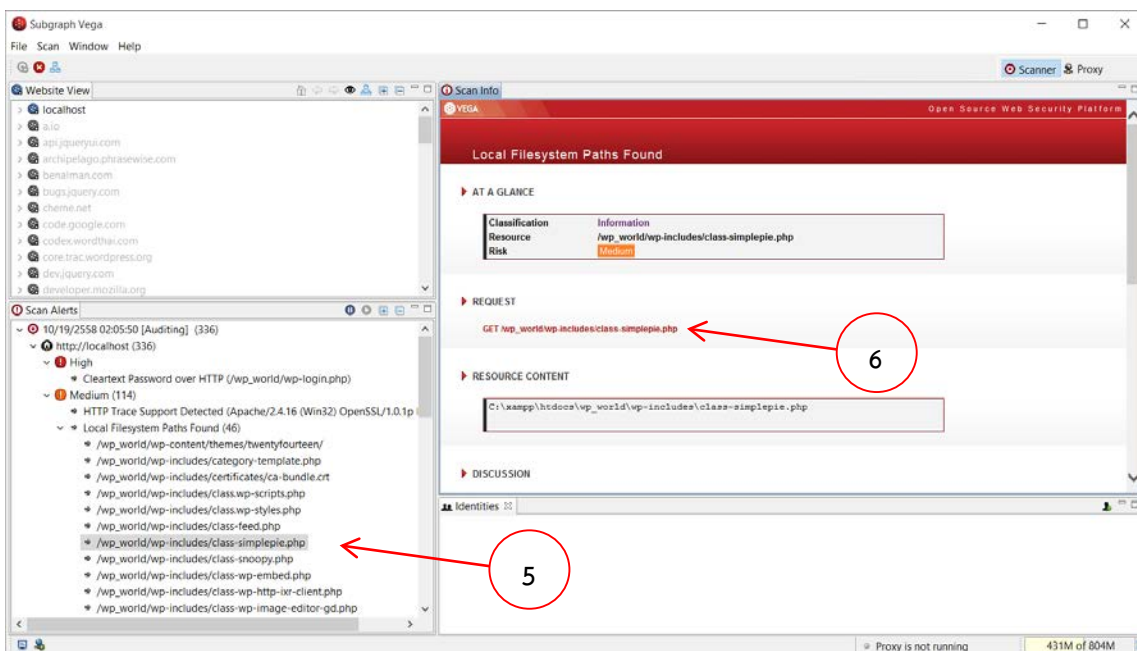
2.4 ส่วนนี้จะเป็นการเลือกคูกี้ที่เราได้ตั้งค่าไว้ ในส่วนนี้ถ้าผู้ใช้ไม่ได้เจาะจงไปที่ส่วนใดส่วนหนึ่งให้กด Next อีกครั้ง แล้วกด (4)Finish



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 จะบอกถึงรายละเอียดคร่าวๆ ว่าจุดที่พบนี้อยู่ที่ใด มีความเสี่ยงมากแค่ไหน

The screenshot shows the 'AT A GLANCE' section of the Vega Scanner report. It features a table with the following information:

Classification	Information
Resource	/wp-content/themes/DU-DE/
Risk	Medium

2. Request บอกถึงจุดที่เว็บร้องขอไป

The screenshot shows the 'REQUEST' section of the Vega Scanner report. It displays the request URL: GET /wp-content/themes/DU-DE/

3. Resource Content แสดงเนื้อหา Script ที่เป็นจุดบกพร่องต่อความปลอดภัย

The screenshot shows the 'RESOURCE CONTENT' section of the Vega Scanner report. It displays the content of the resource, which is a PHP error message: <b>Fatal error</b>: Call to undefined function get\_header() in <b>/home/content/p3pnexwpnas02\_data03/02/2699502/html/wp-content/themes/DU-DE/index.php

4. Discussion เป็นการอภิปรายในเนื้อหาที่ผิดพลาดที่สแกนพบ และอธิบายถึงแนวโน้มที่อาจจะเกิดขึ้นกับเว็บไซต์ได้

The screenshot shows the 'DISCUSSION' section of the Vega Scanner report. It contains the following text: Vega has detected signatures in scanned content that match common PHP error pages. These pages are automatically generated when an error occurs and can leak information useful in more sophisticated attacks. It is recommended that error output not be sent to the client on production systems.

5. Impact จะเป็นการบอกถึงผลกระทบที่จะเกิดขึ้นหากไม่แก้ไข

The screenshot shows the 'IMPACT' section of the Vega Scanner report. It lists the following impacts:

- >> Vega has detected the signature of a PHP error page.
- >> Automatically generated error pages can leak sensitive information.
- >> The information leaked can include software patchlevels, configuration settings, and database or filesystem structure.

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.

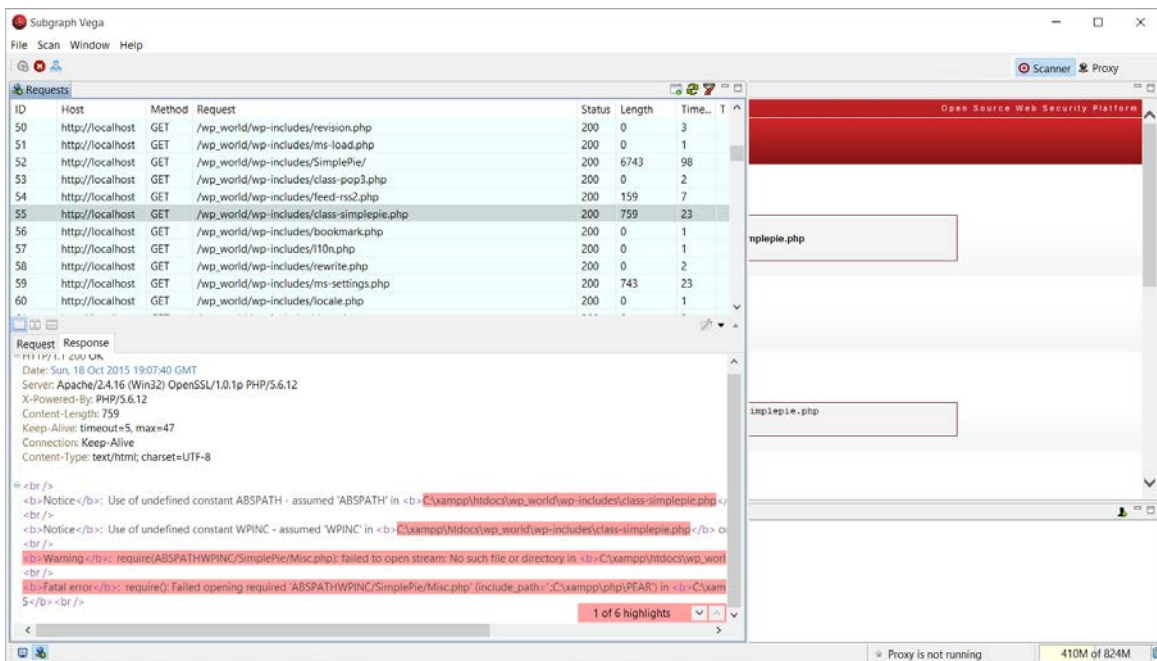
7. References เป็นส่วนที่จะเชื่อมโยงไปยังอ้างอิงที่โปรแกรมได้ ให้ข้อมูลกับเรามา หรือคู่มือในการแก้ไขจากผู้พัฒนาภาษา Script นั้นๆ

► 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 ถ้าผู้ใช้ขอยกทราบรายละเอียดทั้งหมดของข้อผิดพลาด ให้คลิกที่ (7)Proxy

