Web Application Security Essentials

ระยะเวลาการฝึกอบรม 5 วัน

หลักการและเหตุผล

หลักสูตรนี้เหมาะสำหรับผู้เชี่ยวชาญที่ต้องรับผิดชอบและทำหน้าที่เกี่ยวข้องกับการปฏิบัติงาน การควบคุมและบริหารจัดการ รวมถึงการป้องกันในส่วนของ Web Application โดยเฉพาะอย่างยิ่งคือผู้ที่อยู่ในสายงานการวิเคราะห์ความปลอดภัยของ Web Application, นักพัฒนา, ผู้ดูแลในการสร้างระบบ (System Architecture), นักทดสอบเจาะระบบ (Pen Tester), ผู้ตรวจสอบ (Auditors) และผู้ที่สนใจในมาตรการด้านการรักษาความปลอดภัยของ Web Application (การพัฒนาระบบงานบนเว็บ) เพื่อลดปัญหาที่อาจเกิดขึ้นในอนาคต รวมถึงผู้เชี่ยวชาญด้านความปลอดภัยในด้านโครงสร้างพื้นฐานต่างๆ ที่ต้องการเรียนรู้เทคนิคและหลักการสำคัญ เพื่อป้องกัน Web Application ของตนเองให้มีความปลอดภัยมากยิ่งขึ้น นอกจากนี้เนื้อหาภายในหลักสูตร ยังครอบคลุมถึงประเด็นเพิ่มเติมเกี่ยวกับแนวทางการพัฒนา Web Application ผ่านการลงมือปฏิบัติจริง ซึ่งประกอบด้วยหัวข้อดังต่อไปนี้ ;

วัตถุประสงค์

1.) มีความรู้พื้นฐานเกี่ยวกับ HTTP and HTTPS ; Protocol (ข้อกำหนด) ซึ่งถือเป็นพื้นฐานในการติดต่อสื่อสารผ่าน Web Application รวมถึงทำความเข้าใจคำขอต่างๆ, การตอบสนอง, Status Codes (Code มาตรฐานที่แสดงขึ้นมาจากการตอบสนองของ Server บนเว็บไซต์ต่างๆที่อยู่บนอินเตอร์เน็ต) โดยผู้เข้าอบรมจะได้เรียนรู้โครงสร้าง Packet (Packet Structure) รวมถึงวิธีการที่ผู้บุกรุก (Attackers) ใช้ในการโจมตีระบบและข้อมูลสำคัญผ่าน Packet

2.) เพราะเหตุใด Web Application จึงถูกโจมตีเพื่อเข้าระบบอยู่บ่อยครั้ง; สาเหตุหลักๆ อาจเป็นเพราะ Website ประกอบด้วยโครงสร้างพื้นฐานขนาดใหญ่ซึ่งจะส่งผลต่อพื้นผิวของการโจมตีมีขนาดเพิ่มมากขึ้น โดยเฉพาะอย่างยิ่งคือเทคโนโลยีต่างๆ ที่ใช้งานอยู่เกิดปัญหา ไม่ว่าจะเป็น SQLI, XSS, LFI และ RFI โดยผู้เข้าอบรมจะได้เรียนรู้แนวทางการโจมตีในลักษณะต่างๆ (Attack Vector) ในรายละเอียดที่มากยิ่งขึ้น

3.) ขั้นตอนการโจมตีระบบของเหล่า Hacker; โดยผู้เข้าอบรมจะได้เรียนรู้ถึงขั้นตอนการติดตาม Hacker (ผู้บุกรุก) ผ่านหลักการต่างๆ ได้แก่ Foot printing (การสำรวจระบบของเป้าหมาย), scanning (การสแกนเพื่อหาจุดอ่อน), enumeration (กระบวนการเพื่อเข้าระบบ), gaining access (การเข้าถึงเป้าหมาย), maintaining access (การสร้างช่องทางเชื่อมต่อ) รวมถึงหลักการ covering one's tracks (การลบร่องรอย) โดยผู้เข้าอบรมจะได้เรียนรู้เครื่องมือและแนวทางสำคัญในแต่ละกระบวนการ

4.) หลักการเจาะเข้าระบบด้วย SQL Injection โดยอาศัยช่องโหว่ของการใส่ข้อมูล input ของผู้ใช้งาน ซึ่งถือเป็นเทคนิคที่ใช้ประโยชน์จากการส่งคำสั่ง SQL ผ่านทาง Web Application เพื่อไปโจมตีระบบฐานข้อมูลหลังบ้าน (Database)

5.) หลักการ XSS Cross site scripting; ซึ่งเป็นภัยจากการเล่นเว็บและใช้ข้อมูลส่วนตัวในการเข้าถึงข้อมูลต่างๆ, ภัยการคลิกลิงค์, การได้รับลิงค์แปลกหรือการได้รับแบบฟอร์ม ซึ่งเมื่อมีการคลิกก็จะมีการรัน Script หรือคำสั่งบางอย่าง ทำให้ Hacker สามารถรันคำสั่งที่ต้องการบนเว็บเป้าหมาย รวมถึงควบคุมการทำงานของเราได้ในระดับหนึ่ง และอาจส่งผลให้ค่าของ Cookie, Username, Password ของผู้ใช้งานอาจจะถูกขโมยไปได้

6.) LFI and RFI; ซึ่งถือเป็นการ Hack ข้อมูลโดยใช้ช่องโหว่ RFI (Remote File Inclusion) คือ ช่องโหว่ชนิดหนึ่งที่เปิดทางให้ Hacker โจมตี Website ได้ ด้วยการดึงไฟล์จากข้างนอกเข้ามารันในเว็บของคุณ หรือ หลักการ LFI (Local File Inclusion) คือ ช่องโหว่ที่เปิดทางให้ Hacker ดึงไฟล์อื่นๆ ที่อยู่ใน Website มา Run หรือดูข้อมูล (อาทิเช่น ไฟล์ Config หรือไฟล์เก็บ Password ต่างๆ) โดยการกระทำในลักษณะนี้ ได้แก่ การสร้าง Backdoor (การเข้าถึงระบบหรือเครื่องคอมพิวเตอร์โดยเส้นทางพิเศษที่สร้างไว้), Key loggers (การบันทึกการกดจากแป้นพิมพ์ของเหยื่อบนคอมพิวเตอร์ เพื่อเจาะเข้าระบบมาโจรกรรมข้อมูลต่างๆ), Malware Distribution (การแพร่กระจายของมัลแวร์) และ Bots ซึ่งถือเป็นภัยคุกคามที่ระบาดในกลุ่มผู้ใช้คอมพิวเตอร์

7.) แนวทางปฏิบัติที่ดีที่สุด (Best Practices) เพื่อป้องกันอันตรายจากภัยคุกคามทุกประเภท, การจัดทำรายงานการทดสอบ (Test Plan) เพื่อเสนอแก่ลูกค้าให้เกิดความเข้าใจที่ตรงกัน รวมถึงรายงานขั้นสุดท้ายเมื่อเสร็จสิ้นการทดสอบระบบ โดยการระบุรายละเอียดเกี่ยวกับการทดสอบ, ช่องโหว่ถูกค้นพบ, คำแนะนำสำหรับวิธีการแก้ไขปัญหาเกี่ยวกับช่องโหว่ที่ถูกค้นพบในระหว่างการทดสอบ

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

รายละเอียดหลักสูตร

วันที่ 1

- พื้นฐานหลักสูตร "Web Application Security Essentials"
- ความรู้พื้นฐานเกี่ยวกับ HTTP
- การใช้โปรแกรม Netcat เพื่อใช้ใน HTTP 1.1 และ 1.0
- ส่วนประกอบสำคัญของ HTTP และหลักการ HTTP Verb Tampering
- หลักการสำคัญเพื่อทดสอบความปลอดภัยของ HTTP โดยใช้ Nmap (โปรแกรมที่ใช้ในการ Scan ตรวจสอบเครื่อง) และ Metasploit (เครื่องมือในการช่วย Hack ระบบของเป้าหมาย)
- ยกตัวอย่างการทำ HTTP Verb Tampering
- แบบฝึกหัด (Lab) เกี่ยวกับหลักการ HTTP Verb Tampering
- การตรวจสอบสิทธิ ความถูกต้องและการพิสูจน์ตัวตนของ HTTP
- การโจมตีผ่าน Web Browser ด้วย Nmap และ Metasploit
- ทำความรู้จักกับ Metasploit
- HTTP Digest Authentication RFC 2069
- HTTP Digest Auth Hashing (RFC 2069)
- HTTP Digest Authentication (RFC 2617)
- HTTP Statelessness and Cookies
- Session ID (หมายเลขประจำตัว ที่ Web Server ส่งมายัง Client)
- การลงมือปฏิบัติจริงผ่าน Lab
- สรุปรายละเอียดเนื้อหาที่สำคัญ

วันที่ 2

- SSL - Transport Layer Protection : ชั้นสื่อสารการนำส่งข้อมูล
- SSL MITM using Proxies : การโจมตีด้วยเทคนิค MITP (man-in-the-middle attack)
- File Extraction from HTTP Traffic : การสกัดกั้น file ที่มาจากการเข้าดู Web ประเภท HTTP
- HTML Injection Basics : พื้นฐานด้านการปรับแก้ไข HTML เพื่อให้ทำงานผิดพลาดหรือทำงานในสิ่งที่ต้องการได้
- HTML Injection in Tag Parameters
- HTML Injection using 3rd Party Data Source
- HTML Injection - Bypass Filters Cgi.Escape
- Command Injection : การโจมตีเพื่อเข้าถึงระบบปฏิบัติการโดยตรงผ่าน Command Line
- Command Injection – Filters
- Web to Shell on the Server
- Web Shell: PHP Meterpreter
- Web Shell: Netcat Reverse Connects
- Web Shell: Using Python, PHP etc.
- Getting Beyond Alert (XSS) : เทคนิคการฝัง Code เข้าไปกับหน้า Webpage ที่มีช่องโหว่
- การลงมือปฏิบัติจริงผ่าน Lab
- สรุปรายละเอียดเนื้อหาที่สำคัญ

วันที่ 3

- XSS: Cross Site Scripting : การส่ง Script ข้าม Website เพื่อโจมตีเหยื่อที่เปิดเข้าไปหรือโจมตีหน้า Webpage
- Javascript Variables : ตัวแปรใน Javascript
- Types of XSS : ลักษณะของ XSS แต่ละประเภท
- Javascript Operators : ชนิดของ Operator ใน Javascript
- XSS via Event Handler Attributes
- Javascript for Pentesters: Conditionals
- DOM XSS
- Javascript Loops : เงื่อนไขการทำงานแบบซ้ำ
- Javascript Functions : ชุดคำสั่งที่ใช้ในการทำงาน

- Javascript Data Types : การกำหนดประเภทของค่าข้อมูลให้ตัวแปร
- Javascript Enumerating Object Properties : การเข้าดูข้อมูลใน Javascript Object
- Javascript HTML DOM : รูปแบบวัตถุและ Interface การเขียนโปรแกรมมาตรฐาน HTML
- Javascript Cookies : ข้อมูลการเข้า Website ต่างๆ ซึ่งจะถูกบันทึกไว้ที่ Web Browser
- กรณีศึกษาจากเหตุการณ์จริง (Real World Example)
- การลงมือปฏิบัติจริงผ่าน Lab
- สรุปรายละเอียดเนื้อหาที่สำคัญ

วันที่ 4

- Javascript Exceptions : คำสั่งสำหรับดักจับข้อผิดพลาดต่างๆ
- Javascript สำหรับผู้ทดสอบความปลอดภัยระบบงานสารสนเทศ
  - Javascript for Pentesters: Advanced Forms Manipulation
  - Javascript for Pentesters: XMLHttpRequest Basics (XHR)
    พื้นฐาน API ที่สามารถเรียกใช้ได้จาก Javascript ทำหน้าที่ในการแลกเปลี่ยนข้อมูลระหว่าง Web Server & Web Browser
  - Javascript for Pentesters: XHR and HTML Parsing
    หลักการ XHR และการแยกวิเคราะห์ข้อมูลรวมถึงหลักการทำงานของ Parsing ใน HTML
  - Javascript for Pentesters: XHR and JSON Parsing
    หลักการ XHR และวิธีการ Parse JSON
  - Javascript for Pentesters: XHR and XML Parsing
    หลักการ XHR และวิธีการ XML Parsing (ตัวกลางในการดึงข้อมูลจากเอกสาร XML & Application)
- File Upload Vulnerability Basics : พื้นฐานและช่องโหว่ที่อาจเกิดขึ้นจากการ Upload ไฟล์
- Beating Content-Type Check in File Uploads
- Bypassing Blacklists in File Upload
- Bypassing Blacklists using PHPx
- Bypassing Whitelists using Double Extensions in File Uploads
- Defeating Getimagesize() Checks in File Uploads
- Null Byte Injection in File Uploads
- Exploiting File Uploads to get Meterpreter
- Remote File Inclusion Vulnerability Basics : พื้นฐานเกี่ยวกับช่องโหว่ชนิด RFI (Remote File Inclusion) ซึ่งเป็นช่องโหว่ชนิดหนึ่งที่เปิดทางให้ Hacker โจมตี Website ได้ ด้วยการดึงไฟล์จากข้างนอก Web เข้ามารันใน Web ของตนเอง
- สรุปรายละเอียดเนื้อหาที่สำคัญ

วันที่ 5

- Exploiting RFI with Forced Extensions
- RFI to Meterprete
- LFI Basics :พื้นฐานเกี่ยวกับช่องโหว่ชนิด LFI (Local File Inclusion)
- LFI with Directory Prepends
- Remote Code Execution with LFI and File Upload Vulnerability
  ช่องโหว่ Remote Code Execution ด้วย LFI รวมถึงช่องโหว่ที่เกิดจากการ Upload File
- LFI with File Extension Appended - Null Byte Injection
- Remote Code Execution with LFI and Apache Log Poisoning
  การสั่งประมวลผลคำสั่งอันตรายจากระยะไกลด้วย LFI และ Apache Log Poisoning
- Remote Code Execution with LFI and SSH Log Poisoning
  การสั่งประมวลผลคำสั่งอันตรายจากระยะไกลด้วย LFI และ SSH Log Poisoning
- Unvalidated Redirects : ช่องโหว่ที่เกิดขึ้นจากการที่ระบบขาดการป้องกันการรับค่า Input อย่างเหมาะสม
- Encoding Redirect Params : กระบวนการที่ผู้ให้ข้อมูลทำการแปลงสารสนเทศให้กลายเป็นข้อมูลที่จะถูกส่งไปยังผู้รับ
- Open Redirects: Base64 Encoded Params : ช่องโหว่ที่ใช้วิธีการเข้ารหัสข้อมูลรูปแบบหนึ่งที่จะเปลี่ยนข้อความหรือข้อมูลต้นฉบับเป็นข้อมูลใหม่ที่ไม่สามารถอ่านได้ โดยใช้ตัวอักษรทั้งหมด 64 ตัว
- Open Redirects: Beating Hash Checking : ระบบในการตรวจสอบความสมบูรณ์ของไฟล์

- CSRF and XSS
  การโจมตีแบบ Cross-site Request Forgery (CSRF) และ Cross-site Scripting (XSS)
- CSRF Token Bypass with Hidden Frames
- Insecure Direct Object Reference
  ความเสี่ยงที่เกิดจาก "นักพัฒนาซอฟต์แวร์" ในการอ้างอิงวัตถุต่างๆ ลงใน Code
- สรุปรายละเอียดเนื้อหาที่สำคัญ

สิ่งที่จำเป็นต้องมีก่อนเข้ารับการอบรม

ผู้เข้าอบรมควรมีพื้นฐานความรู้และประสบการณ์ทำงานด้าน Linux Command Line

หลักสูตรนี้เหมาะสำหรับ

- ผู้ปฏิบัติงานด้านความปลอดภัยทั่วไป
- นักทดสอบเพื่อการเจาะระบบ
- Hacker
- นักพัฒนา Web Application
- ผู้ออกแบบและพัฒนา Website