หลักสูตร

นักทดสอบการเจาะระบบ Penetration Tester

ภายใต้โครงการพัฒนานักทดสอบการเจาะระบบ เพื่อเสริมสร้างทักษะ และการจ้างงาน สำหรับนักศึกษาจบใหม่

CyberGuardians: Penetration Tester Development Program

สารบัญ

เนื้อหา หน้า

โครงการพัฒนานักทดสอบการเจาะระบบ เพื่อเสริมสร้างทักษะและการจ้างงาน สำหรับนักศึกษาจบใหม่ (CyberGuardians: Penetration Tester Development Program)

รายละเอียดโครงการโดยย่อ

ในบริบทของสังคมดิจิทัลที่มีการขยายตัวอย่างรวดเร็ว ความต้องการบุคลากรที่มีความเชี่ยวชาญเฉพาะด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์มีแนวโน้มเพิ่มสูงขึ้นอย่างมีนัยสำคัญ อันเนื่องมาจากการเพิ่มขึ้นของภัยคุกคามไซเบอร์ที่มีความซับซ้อนและหลากหลายมากขึ้น การทดสอบเจาะระบบ (Penetration Testing) จัดเป็นวิธีการป้องกันภัยคุกคามทางไซเบอร์เชิงรุกที่มีประสิทธิภาพ เนื่องจากเป็นการค้นหาช่องโหว่ของระบบให้พบเสียก่อนที่จะเกิดการโจมตีจากผู้ไม่ประสงค์ดี เพื่อเป็นการพัฒนากำลังคนให้สอดคล้องกับความต้องการในภาคอุตสาหกรรม จึงมีความจำเป็นในการพัฒนาหลักสูตรนักทดสอบการเจาะระบบ (Penetration Tester) โดยมุ่งเน้นการบูรณาการหลักการพื้นฐานทางด้านการเขียนโปรแกรม ความปลอดภัยของระบบเครือข่าย และการจัดการช่องโหว่ในระบบสารสนเทศ ตลอดจนการประยุกต์ใช้เครื่องมือด้านความมั่นคงปลอดภัยที่เป็นมาตรฐานสากลในอุตสาหกรรม

หลักสูตรนี้มุ่งเน้นกลุ่มเป้าหมายเป็นนักศึกษาที่กำลังสำเร็จการศึกษา และนักศึกษาที่สำเร็จการศึกษาแล้วไม่เกิน 2 ปี แต่ยังไม่มีงานทำ โดยมีเป้าหมายเพื่อพัฒนาทักษะเชิงเทคนิคและเตรียมความพร้อมสำหรับการทำงานจริงในสายงานการทดสอบการเจาะระบบ รวมถึงการส่งเสริมการจ้างงานผ่านกระบวนการจับคู่กับนายจ้าง เพื่อให้นักศึกษาที่ผ่านการอบรมสามารถเข้าสู่การทำงานในภาคอุตสาหกรรมได้

ผู้ที่จบหลักสูตรนี้จะสามารถทำงานในตำแหน่งต่าง ๆ เช่น นักทดสอบการเจาะระบบ (Penetration Tester), นักวิเคราะห์ความปลอดภัย (Security Analyst), ผู้เชี่ยวชาญด้านการตอบสนองต่อเหตุการณ์ (Incident Response Specialist), ผู้เชี่ยวชาญด้านการไล่ล่าภัยคุกคาม (Threat Hunter), และวิศวกรความปลอดภัยทางไซเบอร์ (Cybersecurity Engineer)

วัตถุประสงค์โครงการ

1. พัฒนาทักษะนักศึกษาที่กำลังสำเร็จการศึกษา เพื่อยกระดับทักษะด้านความปลอดภัยทางไซเบอร์ให้สูงขึ้น โดยเน้นการทดสอบการเจาะระบบ เพื่อเตรียมความพร้อมสู่การประกอบอาชีพในอนาคต
2. สร้างโอกาสในการจ้างงาน เปิดโอกาสให้นักศึกษาได้พบกับบริษัทที่กำลังมองหาบุคลากรที่มีความสามารถ เพื่อเพิ่มโอกาสในการจ้างงานและสร้างเครือข่ายทางอาชีพ
3. เสริมสร้างความรู้และทักษะเชิงเทคนิค เพื่อให้นักศึกษามีความรู้และทักษะในการใช้เครื่องมือและเทคนิคที่เป็นมาตรฐานสากลในการทดสอบการเจาะระบบ
4. สนับสนุนการพัฒนาภูมิคุ้มกันทางไซเบอร์ เพื่อเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรและประเทศชาติอย่างยั่งยืน

5. ส่งเสริมการเรียนรู้และการพัฒนาตนเอง เพื่อให้นักศึกษาได้เรียนรู้และพัฒนาทักษะใหม่ๆ ที่จำเป็นในสายงานการทดสอบการเจาะระบบ

กลุ่มเป้าหมาย จำนวน 70 คน/โครงการฯ

1. นักศึกษาชั้นปีสุดท้าย
2. บัณฑิตจบใหม่ (ไม่เกิน 2 ปีหลังสำเร็จการศึกษา) ที่ยังไม่มีงานทำ
3. ผู้สมัครต้องมี เกรดเฉลี่ยสะสม (GPA) ไม่น้อยกว่า 2.90
4. ศึกษาในสาขาวิชาที่เกี่ยวข้อง กับหลักสูตรอบรมและตำแหน่งงานที่ต้องการ

คุณสมบัติผู้เข้ารับการอบรม

1. นักศึกษาชั้นปีสุดท้าย (เกรดเฉลี่ยไม่ต่ำกว่า 2.90) หรือผู้สำเร็จการศึกษาไม่เกิน 2 ปี
2. มีพื้นฐานด้าน Cybersecurity / Information Security
3. ผ่านการทดสอบ Screen Test จากโครงการ
4. สามารถเข้าร่วมโครงการได้ครบทุกช่วง ตั้งแต่เริ่มต้นจนจบโครงการ

สิ่งที่ผู้เข้ารับการอบรมจะได้รับ

1. อบรมฟรี มูลค่า 50,000 บาท (ไม่มีค่าใช้จ่าย)
2. อัพสกิล Penetration Tester ครบวงจร
3. อบรมออนไลน์ 10 วัน (60 ชั่วโมง) พร้อม Workshop ฝึกปฏิบัติจริง
4. รับ 2 ใบประกาศ
   - ใบรับรองสากล IT Specialist: Cyber Security Certification
   - ใบประกาศนียบัตรจาก depa
5. เตรียมพร้อมสู่การทำงานจริง
6. มีโอกาสได้งานทันที ในตำแหน่ง นักทดสอบการเจาะระบบ (Penetration Tester), นักวิเคราะห์ความปลอดภัย (Security Analyst), ผู้เชี่ยวชาญด้านการตอบสนองต่อเหตุการณ์ (Incident Response Specialist), ผู้เชี่ยวชาญด้านการไล่ล่าภัยคุกคาม (Threat Hunter), และวิศวกรความปลอดภัยทางไซเบอร์ (Cybersecurity Engineer)

ขั้นตอนการเข้าร่วมโครงการ

1. ลงทะเบียนผ่านเว็บไซต์โครงการ
2. โครงการคัดเลือกผู้สมัคร และประกาศผล
3. อบรมออนไลน์
4. สอบใบรับรองมาตรฐานสากล IT Specialist: Cyber Security Certification
5. ผู้อบรมจัดทำและส่ง Resume
6. กิจกรรม Job Matching (ออนไลน์)
7. บริษัทพันธมิตรนัดสัมภาษณ์
8. บริษัทคัดเลือกและตกลงจ้างงาน
9. โครงการติดตามและรายงานผล
10. สิ้นสุดโครงการ

กำหนดการฝึกอบรม (ออนไลน์) เดือนพฤศจิกายน - เดือนธันวาคม 2568
เวลา: 09.00 – 16.00 น.

เดือนพฤศจิกายน 2568						
อาทิตย์	จันทร์	อังคาร	พุธ	พฤหัสบดี	ศุกร์	เสาร์
16	17	18	19	20	21	22
23	24	25	26	27	28	29
เดือนธันวาคม 2568						
อาทิตย์	จันทร์	อังคาร	พุธ	พฤหัสบดี	ศุกร์	เสาร์
30	1	2	3	4	5	6
7	8	9	10	11	12	13

สรุปวันอบรม เดือนพฤศจิกายน 2568 รวม 4 วัน ดังนี้
สัปดาห์ที่ 1 → 17
สัปดาห์ที่ 1 → 24, 25, 26, 27, 28
เดือนธันวาคม 2568 รวม 5 วัน ดังนี้
สัปดาห์ที่ 2 → 1, 2
สัปดาห์ที่ 3 → 8, 9

ตารางแผนงานและช่วงเวลาดำเนินโครงการ

ขอบเขตและแผนการดำเนินงาน	พ.ศ. 2568				พ.ศ. 2569							
	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	มิ.ย.
1. วางแผนและการประชาสัมพันธ์	➢											
2. รับสมัครผู้เข้าร่วมโครงการ	➢											
3. กิจกรรมฝึกอบรม		➢	➢	➢								
4. กิจกรรม Job Matching ออนไลน์					➢	➢	➢					
5. การติดตามผู้อบรมหลังการสัมภาษณ์							➢	➢				
6. การจัดทำรายงานส่งมอบงานให้กับ									➢	➢	➢	➢

รูปแบบและระยะเวลาการอบรม

1. อบรมรูปแบบออนไลน์ 2. ระยะเวลา 10 วัน (60 ชั่วโมง)

หลักสูตร นักทดสอบการเจาะระบบ (Penetration Tester)

ครอบคลุมเนื้อหา ดังนี้

- ☑ Programming/Coding
- ☑ Network Security
- ☑ Security Frameworks
- ☑ Threat Hunting
- ☑ Incident Response
- ☑ Core Security Principles
- ☑ Security Tools
- ☑ Linux Administration
- ☑ Cloud Security
- ☑ Vulnerability Assessment and Penetration Testing (VAPT)

ช่องทางการรับสมัคร
สมัครผ่านเว็บไซต์โครงการ https://nextpentest.com
ภายในวันที่ 17 ตุลาคม 2568
ประกาศผลผู้ผ่านการคัดเลือกเข้ารับอบรม วันที่ 24 ตุลาคม 2568

ผู้บริหารโครงการ
บริษัท เออาร์ไอที จำกัด
1023 อาคารเอ็มเอสสยาม ชั้น 8 ถ.พระราม 3 ช่องนนทรี ยานนาวา กรุงเทพฯ 10120

ฝ่ายประสานงานโครงการ
คุณวิภู โอภาสพินิจ
084-581-7497
Primedigital.nextpentest@gmail.com

รายละเอียดหลักสูตรและกำหนดการอบรม
หลักสูตร นักทดสอบการเจาะระบบ (Penetration Tester)

ในบริบทของสังคมดิจิทัลที่มีการขยายตัวอย่างรวดเร็ว ความต้องการบุคลากรที่มีความเชี่ยวชาญเฉพาะด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์มีแนวโน้มเพิ่มสูงขึ้นอย่างมีนัยสำคัญ อันเนื่องมาจากการเพิ่มขึ้นของภัยคุกคามไซเบอร์ที่มีความซับซ้อนและหลากหลายมากขึ้น การทดสอบเจาะระบบ (Penetration Testing) จัดเป็นวิธีการป้องกันภัยคุกคามทางไซเบอร์เชิงรุกที่มีประสิทธิภาพ เนื่องจากเป็นการค้นหาช่องโหว่ของระบบให้พบเสียก่อนที่จะเกิดการโจมตีจากผู้ไม่ประสงค์ดี ดังนั้นเพื่อเป็นการพัฒนากำลังคนให้สอดคล้องกับความต้องการในภาคอุตสาหกรรม จึงมีความจำเป็นในการพัฒนาหลักสูตรนักทดสอบการเจาะระบบ (Penetration Tester) โดยมุ่งเน้นการบูรณาการหลักการพื้นฐานทางด้านการเขียนโปรแกรม ความปลอดภัยของระบบเครือข่าย และการจัดการช่องโหว่ในระบบสารสนเทศ ตลอดจนการประยุกต์ใช้เครื่องมือด้านความมั่นคงปลอดภัยที่เป็นมาตรฐานสากลในอุตสาหกรรม หลักสูตรนี้จึงมีบทบาทสำคัญในการผลิตกำลังคนที่มีสมรรถนะเชิงเทคนิคและความสามารถในการปฏิบัติงานจริง เพื่อตอบสนองต่อความท้าทายดังกล่าว และสนับสนุนการเสริมสร้างภูมิคุ้มกันทางไซเบอร์ขององค์กรและประเทศชาติอย่างยั่งยืน

วัตถุประสงค์

1. เพื่อให้ผู้เข้าอบรมสามารถเขียนโปรแกรมเบื้องต้นได้
2. เพื่อให้ผู้เข้าอบรมสามารถจัดการระบบสารสนเทศให้มีมาตรฐานด้านความปลอดภัยทางไซเบอร์
3. เพื่อให้ผู้เข้าอบรมสามารถใช้เครื่องมือด้านความมั่นคงปลอดภัยทางไซเบอร์ได้
4. เพื่อให้ผู้เข้าอบรมสามารถทดสอบการเจาะระบบได้
5. เพื่อให้ผู้เข้าอบรมสามารถใช้งานระบบปฏิบัติการ Linux ได้

เนื้อหาการอบรม วันที่ 1

- Introduction to Programming
  - What is Programming?
  - Overview of Programming Languages & Their Uses (Python, JavaScript, Java, C, etc.)
  - Understanding Syntax, Variables, Data Types
  - Setting Up the Development Environment (IDE, Code Editors, Terminals)
  - Hands-on: Writing & Executing Your First Program
- Control Structures & Logic Building
  - Conditional Statements (if-else, switch-case)
  - Loops (for, while)
  - Logical & Comparison Operators
  - Hands-on: Building a Simple Decision-Making Program

- Functions & Code Reusability
  - What Are Functions & Why Are They Important?
  - Defining & Calling Functions
  - Function Parameters & Return Values
  - Hands-on: Creating Functions for Code Modularity
- Data Structures & Working with Collections
  - Lists, Arrays, Tuples, and Dictionaries
  - Basic Operations on Data Structures (Adding, Removing, Modifying)
  - Hands-on: Implementing a Simple Data Processing Program
- File Handling & Basic Debugging
  - Reading & Writing to Files
  - Handling Errors & Debugging Techniques
  - Hands-on: Creating a Simple File-Based Data Storage Program
- Mini Project & Course Wrap-Up
  - Mini Project: Build a Basic CLI Tool or Simple Web Script
  - Best Practices in Programming (Code Readability, Comments, DRY Principle)
  - Next Steps: Learning Paths in Web Development, Data Science, Automation

เนื้อหาการอบรม วันที่ 2

Introduction to Security Principles

- Understanding Cybersecurity & Its Importance
- The CIA Triad (Confidentiality, Integrity, Availability)
- Common Cyber Threats (Malware, Phishing, Ransomware, Insider Threats)
- Security Frameworks & Standards (NIST, ISO 27001, CIS Controls)

- Risk Management & Security Controls
  - Identifying & Assessing Security Risks
  - Security Control Types: Preventive, Detective, Corrective
  - Defense in Depth (Layered Security) & Zero Trust Model
- Identity & Access Management (IAM)
  - Authentication vs. Authorization
  - Role-Based Access Control (RBAC) & Least Privilege Principle
  - Multi-Factor Authentication (MFA) & Identity Federation
- Network & Endpoint Security
  - Secure Network Architecture (Firewalls, IDS/IPS, VPN)

        - Endpoint Security & Hardening (Antivirus, Patching, EDR)
        - Secure Configurations & Hardening Best Practices
    - Security Awareness & Incident Response
        - Understanding Social Engineering Attacks (Phishing, Pretexting, Baiting)
        - Best Practices for Security Awareness Training
        - Incident Response Lifecycle (Detection, Containment, Eradication, Recovery)
    - Security Best Practices
        - Implementing Security Policies & Governance
        - Cyber Hygiene & Secure Coding Practices
        - The Future of Cybersecurity: AI & Cloud Security Trends

เนื้อหาการอบรม วันที่ 3

- Introduction to Network Security
    - Importance of Network Security
    - Threat Landscape & Common Attacks
    - Cybersecurity Frameworks & Best Practices
    - Role of Security Policies
- Network Security Fundamentals
    - OSI & TCP/IP Models – Security Considerations
    - Firewalls: Types & Configurations
    - IDS/IPS (Intrusion Detection & Prevention Systems)
    - VPNs & Secure Communication Channels
- Threats and Vulnerabilities
    - Common Network Attacks (DDoS, Man-in-the-Middle, Phishing, etc.)
    - Malware & Ransomware in Networks
    - Vulnerability Assessment vs. Penetration Testing
- Secure Network Design
    - Network Segmentation & VLANs
    - Zero Trust Security Model
    - Secure Network Architecture
    - Cloud Security Considerations

เนื้อหาการอบรม วันที่ 4

- Cryptography & Authentication
  - Symmetric vs. Asymmetric Encryption
  - SSL/TLS in Network Security
  - Authentication Protocols (LDAP, RADIUS, Kerberos)
  - Multi-Factor Authentication (MFA)
- Wireless & Cloud Security
  - Wireless Network Security (WPA3, WEP, WPA2)
  - Cloud Security Best Practices
  - Securing Hybrid Environments
  - Secure SD-WAN Implementation
- Security Operations & Incident Response
  - Security Operations Center (SOC) Overview
  - Network Monitoring & Logging (SIEM, Syslog, NetFlow)
  - Incident Response & Forensics
  - Handling a Network Security Breach
- Hands-on & Final Assessment
  - Firewall & IDS/IPS Lab Exercise
  - Simulated Attack & Defense Scenarios
  - Security Best Practices Checklist

เนื้อหาการอบรม วันที่ 5

- Overview of Cybersecurity Tools
- Categories of Security Tools:
  - Network Security
  - Endpoint Security
  - Threat Detection & Monitoring
  - Forensics & Incident Response
- Network Security Tools
  - Firewalls: Configuration & Management (pfSense, Cisco ASA, iptables)
  - Intrusion Detection/Prevention Systems (IDS/IPS): Snort & Suricata
  - Wireshark: Packet Analysis & Network Traffic Monitoring
  - Demo: Capturing & Analyzing Network Traffic with Wireshark
- Vulnerability Assessment & Penetration Testing Tools
  - Nmap: Network Scanning & Discovery
  - Metasploit Framework: Exploitation Techniques
  - Nessus/OpenVAS: Vulnerability Scanning

- Demo:Scanning & Identifying Vulnerabilities with Nmap & Nessus
- Web Security & Application Testing Tools
  - Burp Suite: Web Application Security Testing
  - OWASP ZAP: Web Security Scanning
  - SQLmap: Database Exploitation Testing
  - Demo: Identifying Web Security Vulnerabilities

เนื้อหาการอบรม วันที่ 6

- Threat Detection & SIEM Tools
  - Security Information & Event Management (SIEM): Overview
  - Splunk & ELK Stack: Log Analysis & Threat Hunting
  - Demo: Detecting Malicious Activities Using Splunk
- Digital Forensics & Incident Response Tools
  - Autopsy & FTK Imager: Digital Forensics & Data Recovery
  - Volatility: Memory Forensics for Incident Response
  - Demo: Conducting Basic Digital Forensics Investigation
- Endpoint Security & Malware Analysis
  - EDR Solutions (CrowdStrike, SentinelOne, Windows Defender ATP)
  - YARA & PEStudio: Malware Detection & Reverse Engineering
  - Demo: Analyzing Malware with YARA Rules
- Security Automation & Final Assessment
  - Automating Security Tasks with Python & PowerShell
  - SOAR (Security Orchestration, Automation, and Response) Overview
  - Demo: Simulating a Cyber Attack & Implementing Defense Mechanisms

เนื้อหาการอบรม วันที่ 7

- Introduction to Linux
  - History & Evolution of Linux
  - Linux Distributions (Ubuntu, CentOS, RHEL, Debian)
  - Linux File System Hierarchy
  - User & Group Management
- Linux Command Line & Shell Scripting
  - Basic Linux Commands (ls, cd, mv, cp, rm, cat, etc.)
  - File Permissions & Ownership (chmod, chown, chgrp)
  - Process Management (ps, top, kill, nice, nohup)
  - Introduction to Bash Scripting

- Demo: Writing Basic Shell Scripts
- Package Management & Software Installation
  - Package Managers (APT, YUM, DNF, Zypper)
  - Installing & Removing Software
  - Managing Repositories & Dependencies
  - Demo: Installing & Configuring Applications
- User & Permission Management
  - Creating & Managing Users & Groups
  - Setting Password Policies
  - sudo & Privilege Escalation
  - Demo: Configuring User Access & Permissions

เนื้อหาการอบรม วันที่ 8

- Introduction to Threat Hunting
  - What is Threat Hunting?
  - Proactive vs. Reactive Security
  - Threat Hunting vs. Threat Intelligence vs. Incident Response
  - The Cyber Kill Chain & MITRE ATT&CK Framework
- Understanding Adversary Tactics & Techniques
  - Common Attack Vectors (Phishing, Ransomware, Insider Threats)
  - Advanced Persistent Threats (APTs) & Their Methodologies
  - Understanding Indicators of Compromise (IoCs) & Indicators of Attack (IoAs)
  - Demo: Mapping Attacks to MITRE ATT&CK Framework
- Threat Hunting Methodologies & Techniques
  - Hypothesis-Driven vs. Data-Driven Threat Hunting
  - TTP-Based Hunting (Tactics, Techniques, and Procedures)
  - Threat Hunting with Logs & Network Data
  - Demo: Building a Threat Hunting Hypothesis
- Tools & Data Sources for Threat Hunting
  - SIEM Solutions (Splunk, ELK, Graylog)
  - EDR & XDR Platforms (CrowdStrike, SentinelOne, Microsoft Defender)
  - Network Traffic Analysis (Wireshark, Zeek, Suricata)
  - Demo: Collecting & Analyzing Threat Intelligence

เนื้อหาการอบรม วันที่ 9

- Introduction to Vulnerability Assessment (VA)

- Overview of Cybersecurity & Threat Landscape
- Difference Between Vulnerability Assessment (VA) and Penetration Testing (PT)
- Importance of Regular Vulnerability Assessments
- Common Types of Vulnerabilities (OWASP, CVEs, Misconfigurations)
- Regulatory Compliance (PCI-DSS, NIST, ISO 27001, GDPR)

- Understanding Vulnerability Scanning Tools
  - Scanning Methodologies
  - Interpreting CVSS (Common Vulnerability Scoring System)
  - Types of vulnerability scanners
  - Setting Up a Lab Environment for Scanning
- Vulnerability Scan (Hands-On)
  - Nmap
  - Nessus
  - OWASP ZAP
- Reporting & Remediation Strategies
  - Best Practices for Documenting Vulnerabilities
  - Creating a Detailed VA Report (Executive vs. Technical Report)
  - Risk-Based Prioritization (Critical, High, Medium, Low)
  - Remediation Strategies:
  - Patching & Updates
  - Configuration Changes
  - Network Segmentation
  - Continuous Monitoring & Integrating VA into Security Framework

เนื้อหาการอบรม วันที่ 10

- Introduction to Penetration Testing
  - Understanding Cybersecurity Threats
  - Difference Between Penetration Testing & Vulnerability Assessment
  - Penetration Testing Methodologies (OWASP, PTES, NIST)
  - Ethical Hacking & Legal Considerations (Laws & Compliance)
  - Types of Penetration Tests
- Setting Up the Penetration Testing Environment
  - Introduction to Kali Linux & Other Pentesting Tools
  - Installing & Configuring Virtual Labs (Metasploitable, DVWA)
  - Understanding Attack Surfaces & Scoping a Test
  - Reconnaissance & Information Gathering

- Passive vs. Active Reconnaissance
- OSINT (Open-Source Intelligence)
- Tools: Nmap, Shodan, Whois, Google Dorking

- Scanning & Enumeration (Hands-On)
  - Network Scanning Using Nmap
  - Identifying Open Ports & Services
  - Enumerating Users & Services
  - Banner Grabbing & Fingerprinting
  - Web Application Reconnaissance (Dirb, Nikto, Gobuster)
- Exploitation & Gaining Access (Hands-On)
  - Exploiting Vulnerabilities with Metasploit Framework
  - Manual Exploitation Techniques
  - Brute Force Attacks & Credential Exploitation
  - Privilege Escalation Techniques
  - Web Application Attacks:
  - SQL Injection
  - Cross-Site Scripting (XSS)
  - File Inclusion Attacks
  - Post-Exploitation: Maintaining Access & Pivoting