SEC542: Web App Penetration Testing and Ethical Hacking

Course Overview

If your organization does not properly test and secure its web applications, adversaries can compromise these apps, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, so major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets, either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

SEC542 enables students to assess a web application's security posture and convincingly demonstrate the business impact should attackers exploit the discovered vulnerabilities. You will practice the art of exploiting web applications to find flaws in your enterprise's web apps. You'll learn about the attacker's tools and methods and, through detailed hands-on exercises, you will learn a best practice process for web application penetration testing, inject SQL into back-end databases to learn how attackers exfiltrate sensitive data, and utilize cross-site scripting attacks to dominate a target infrastructure.

Job Roles

- Senior Web Application Penetration Tester
- Penetration Tester
- Cyber Security Analyst
- Ethical Hacker
- Vulnerability Assessment Analyst
- Senior Application Security Engineer

Intended Audience

- General security practitioners
- Penetration testers
- Ethical hackers
- Web application developers
- Website designers, architects, and developers

Prerequisites

SEC542 assumes students have a basic working knowledge of the Linux command line.

Duration

6 Days

Certifications

GIAC Web Application Penetration Tester (GWAPT)

Contact Us

800.674.3550

2151 W. Hillsboro Blvd.
Suite 210
Deerfield Beach, FL 33442

Connect with us

APPLIED TECHNOLOGY ACADEMY

Sign Up Today!

AppliedTechnologyAcademy.com

SEC542: Web App Penetration Testing and Ethical Hacking

APPLIED TECHNOLOGY ACADEMY

Course Outline

SECTION 1: Introduction and Information Gathering

TOPICS: Overview of the web from a penetration tester's perspective; Web application assessment methodologies; The penetration tester's toolkit; Interception proxies; Proxying SSL through BurpSuite Pro and Zed Attack Proxy; DNS reconnaissance; Virtual host discovery; The HTTP protocol; Secure Sockets Layer (SSL) configurations and weaknesses; Target discovery and profiling; Content Discovery: Spidering/Crawling

SECTION 2: Fuzzing, Scanning, Authentication, and Session Testing

TOPICS: Fuzzing; Information Leakage; Burp Professional's Vulnerability Scanning; Content Discovery: Forced Browsing; Finding unlinked content with ZAP and ffuf; Web authentication mechanisms; Federated Identity and Access Protocols (SAML and OAuth); JWTs and Flask Session Cookies; Username harvesting and password guessing; Session management and attacks; Burp sequencer

SECTION 3: Injection

TOPICS: Authentication and authorization bypass; Command injection: Blind and Non-Blind; Directory traversal; Local File Inclusion (LFI); Remote File Inclusion (RFI); Insecure Deserialization; SQL injection; Blind SQL; injection; Error-based SQL injection; Exploiting SQL injection; SQL injection tools: sqlmap

SECTION 4: XSS, SSRF, and XXE

TOPICS: Cross-Site Scripting (XSS); Browser Exploitation Framework (BeEF); AJAX; XML and JSON; Document Object Model (DOM); API attacks; Data attacks; REST and SOAP; Prototype Pollution; Server-Side Request Forgery (SSRF); XML External Entity (XXE)

SECTION 5: CSRF, Logic Flaws and Advanced Tools

TOPICS: Cross-Site Request Forgery (CSRF); Logic Flaws; Logging and monitoring; Python for web app penetration testing; WPScan; ExploitDB; BurpSuite Pro scanner; Nuclei; Metasploit; When tools fail; Business of Penetration Testing

SECTION 6: Capture the Flag

During section six, students form teams and compete in a web application penetration testing tournament. This Netwars-powered Capture-the-Flag exercise provides students an opportunity to wield their newly developed or further-honed skills to answer questions, complete missions, and exfiltrate data, applying skills gained throughout the course. The style of challenge and integrated hint system allows students of various skill levels to both enjoy a game environment and solidify the skills learned in class.

Course Objectives

- Apply OWASP's methodology to your web application penetration tests to ensure they are consistent, reproducible, rigorous, and under quality control.
- Assess both traditional server-based web applications, as well as modern AJAX-heavy applications that interact with APIs.
- Analyze the results from automated web testing tools to validate findings, determine their business impact, and eliminate false positives.
- Manually discover key web application flaws.
- Use Python to create testing and exploitation scripts during a penetration test.
- Discover and exploit SQL Injection flaws to determine true risk to the victim organization.
- Understand and exploit insecure deserialization vulnerabilities with ysoserial and similar tools.
- Create configurations and test payloads within other web attacks.
- Fuzz potential inputs for injection attacks with ZAP, Burp's Intruder and ffuf.
- Explain the impact of exploitation of web application flaws.
- Analyze traffic between the client and the server application using tools such as the Zed Attack Proxy and BurpSuite Pro to find security issues.
- Leverage resources, such as the browser's developer tools, to assess findings within the client-side application code.
- Manually discover and exploit vulnerabilities such as Command Injection, Cross-Site Request Forgery (CSRF), Server-Side Request Forgery (SSRF), and more.
- Learn strategies and techniques to discover and exploit blind injection flaws.
- Use the Browser Exploitation Framework (BeEF) to hook victim browsers, attack client software and the network, and evaluate the potential impact that XSS flaws have within an application.
- Use the Nuclei tool to perform scans of target web sites/servers.
- Perform two complete web penetration tests, one during the first five sections of course instruction, and the other during the Capture the Flag exercise.

GIAC Web Application Penetration Tester (GWAPT)

The GIAC Web Application Penetration Tester (GWAPT) certification validates a practitioner's ability to better secure organizations through penetration testing and a thorough understanding of web application security issues. GWAPT certification holders have demonstrated knowledge of web application exploits and penetration testing methodology.

- Web application overview, authentication attacks, and configuration testing
- Web application session management, SQL injection attacks, and testing tools
- Cross site request forgery and scripting, client injection attack, reconnaissance and mapping