SEC542: Web App Penetration Testing and Ethical Hacking

GWAPT
Web Application Penetration Tester
giac.org/gwapt

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Apply a detailed, four-step methodology to your web application penetration tests: reconnaissance, mapping, discovery, and exploitation
- 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
- Create configurations and test payloads within other web attacks
- Fuzz potential inputs for injection attacks
- 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 Burp Suite to find security issues within the client-side application code
- Manually discover and exploit Cross-Site Request Forgery (CSRF) attacks
- 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
- Perform a complete web penetration test during the Capture-the-Flag exercise to bring techniques and tools together into a comprehensive test

"This course taught me to truly focus on the methodology while performing a pen test. During the Capture-the-Flag event, I realized how much time can be wasted if you fail to respect your methodology."

— Sean Rosado, **RavenEye**

Web applications play a vital role in every modern organization. However, if your organization doesn't properly test and secure its web apps, adversaries can compromise these applications, 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.

SEC542 helps students move beyond push-button scanning to professional, thorough, and high-value web application penetration testing.

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, and 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.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

SEC542 enables students to assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations.

In this course, students will come to understand major web application flaws and their exploitation. Most importantly, they'll learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations. Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. This course will help you demonstrate the true impact of web application flaws through exploitation.

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn.

In addition to having more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way that hammers home lessons learned.

SEC542 will you:

- To apply a repeatable methodology to deliver high-value penetration tests
- How to discover and exploit key web application flaws
- How to explain the potential impact of web application vulnerabilities
- The importance of web application security to an overall security posture
- How to wield key web application attack tools more efficiently
- How to write web application penetration test reports

Section Descriptions

SECTION 1: Introduction and Information Gathering

Understanding the attacker's perspective is key to successful web application penetration testing. The course begins by thoroughly examining web technology, including protocols, languages, clients, and server architectures, from the attacker's perspective. We look at collecting open source intelligence (OSINT) specific to data points likely to help exploitation be more successful. We analyze the importance of encryption and HTTPS.

TOPICS: Overview of the Web from a Penetration Tester's Perspective; Web Application Assessment Methodologies; The Penetration Tester's Toolkit; WHOIS and DNS Reconnaissance; Virtual Host Discovery; Open Source Intelligence (OSINT); The HTTP Protocol; Secure Sockets Layer (SSL) Configurations and Weaknesses; Interception Proxies; Proxying SSL Through BurpSuite Pro and Zed Attack Proxy

SECTION 2: Content Discovery, Authentication, and Session Testing

Section 2 begins with profiling the target(s) to understand the underlying configuration. The collected data is used to build a profile of each server and identify potential configuration flaws. The discussion is underscored through several practical, hands-on labs in which we conduct further reconnaissance. The exploitation is an opportunity to get deeper hands-on experience with BurpSuite Pro, cURL, and manual exploitation techniques. The system's configuration should involve proper logging and monitoring to ensure security-related events are not missed. We will briefly explore logging configuration and basic incident response testing.

TOPICS: Logging and Monitoring; Learning Tools to Spider a Website; Analyzing Website Content; Brute Forcing Unlinked Files and Directories via ZAP and ffuf; Web Authentication Mechanisms; Fuzzing with Burp Intruder; Username Harvesting and Password Guessing; Burp Sequencer; Session Management and Attacks; Authentication and Authorization Bypass; Mutillidae

SECTION 3: Injection AND XXE

After ending Section 2 with authentication bypass, we begin by exploring how web applications track authenticated users and ways to exploit weaknesses in session management. We will build on the information identified during the target profiling, spidering, and forced browsing exercises, exploring methods to find and verify vulnerabilities within the application. Students also begin to explore the interactions between the various vulnerabilities. This course section dives deeply into vital manual testing techniques for vulnerability discovery. We focus on developing in-depth knowledge of interception proxies for web application vulnerability discovery. Many of the most common injection flaws (command injection and local and remote file inclusion are introduced, and followed with lab exercises, to reinforce the discovery and exploitation.

TOPICS: Command Injection; 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; XML External Entity (XXE)

SECTION 4: XXE

After ending Section 3 by learning about and exploiting XXE, section four continues exploring exploitation flaws and spends time introducing Cross-Site Scripting (XSS) vulnerabilities, including reflected, stored and DOM-based XSS vulnerabilities. Manual discovery methods are employed during hands-on labs. Section 4 also introduces the Browser Exploitation Framework (BeEF) to students, which is used in multiple labs. The course continues with a detailed discussion of AJAX as we explore how it enlarges the attack surface leveraged by penetration testers. We also analyze how AJAX is affected by other vulnerabilities already covered in depth earlier in the course.

TOPICS: Cross-Site Scripting (XSS); Browser Exploitation Framework (BeEF); AJAX; XML and JSON; Document Object Model (DOM); API attacks; Data Attacks; REST and SOAP

SECTION 5: CSRF, Logic Flaws, and Advanced Tools

During SECTION 5, we launch actual exploits against real-world applications, expanding our foothold within the application, and extending it to the network on which it resides. As penetration testers, we specifically focus on ways to leverage previously discovered vulnerabilities to gain further access, highlighting the cyclical nature of web application penetration testing.

TOPICS: Cross-Site Request Forgery (CSRF); Logic Attacks; Python for Web App Penetration Testing; WPScan; ExploitDB; BurpSuite Pro scanner; Metasploit; When Tools Fail; Business of Penetration Testing

SECTION 6: Capture the Flag

During Section 6, 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.

Who Should Attend

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

"SEC542 shows a hands-on way of doing web app penetration testing – not just how to use this tool or that tool."

— Christopher J. Stover, **Infogressive Inc.**

"Knowing everything from the Internet is not enough. This class has a sequential structure to understand the basics of pen testing."

— Vinita Mhapsekar, **Kaiser Permanente**

GWAPT
Web Application Penetration Tester
giac.org/gwapt

GIAC Web Application Penetration Tester

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