SEC542

Web App Penetration Testing and Ethical Hacking

Fall 2025 Update: Testing Modern Web Applications With an Expanded End-to-End CTF

The latest update to SEC542 brings modern web application penetration testing into today's real attacker landscape. This Fall 2025 refresh modernizes the methodology, labs, and tooling to reflect how adversaries exploit web applications, APIs, authentication flows, and server-side logic in real environments.

Co-authored by Eric Conrad, Timothy McKenzie, and Bojan Zdrnja, the revised course expands coverage of API exploitation, modern injection techniques, client-side attacks, authentication and authorization bypass, and advanced vulnerability chaining. Every section has been updated with current tools, real-world techniques, and attacker-driven workflows. A student who sits for SEC542 can comfortably test not only web applications but also web services after the course.

This release also introduces a significantly enhanced Capture the Flag experience, giving students the opportunity to apply the full methodology — from reconnaissance to exploitation — across realistic, multi-stage web applications. The CTF now mirrors the complexity of modern offensive engagements and reinforces the repeatable testing process students develop throughout the week.

New Content

- Expanded real-world API exploitation, authentication & federated identity testing (OAuth, OIDC, SAML, JWT)
- Updated modules on SQLi, NoSQLi, command injection, XXE, SSRF, and authentication/ authorization bypass
- Deepened client-side exploitation: DOM-XSS, Prototype Pollution, CORS, AJAX, browser developer tools
- New insecure deserialization & SSTI chains leading to file access and remote code execution
- Added content on OWASP Top 10 for LLM Applications and modern web logic flaws

Updated Features

- Fully rewritten 31+ hands-on labs emphasizing modern tooling & attacker workflows
- Streamlined instructions for clarity, stronger guidance, and real practitioner context
- Updated toolchain: Burp Suite Pro, ZAP, ffuf, Bruno, sqlmap, flask-unsign, JtR, CeWL, Metasploit
- Stronger integration of Python scripting for automation (Requests/httpx + custom tools)
- We have added the use of ChatGPT to develop advanced payloads to several labs: Command Injection and XSS

Lab Refresh

- Modernized exploitation labs covering SQL/NoSQL injection, prototype pollution, XSS chains, and CSRF attacks
- New end-to-end exploitation sequences showing chaining (e.g., deserialization → file inclusion → RCE)
- Enhanced authentication & authorization bypass labs (BOLA, BFLA, privilege escalation)
- Updated browser-exploitation exercises using DOM Invader and BeEF
- Strengthened CTF experience applying full methodology across multiple web apps

"Students regularly come to SEC542 frustrated with scanners producing thousands of false positives. Seeing them leave with the skills and mindset to perform real, focused, high-value assessments is one of the most rewarding parts of teaching this course."

— Eric Conrad, Timothy McKenzie & Bojan Zdrnja | SEC542 Authors

For more information: sans.org/SEC542

SANS | GIAC CERTIFICATIONS