# WAHS WEB APPLICATION HACKING & SECURITY

EC-Council's Web Application Hacking and Security is a specialization certification that enables you to play, learn, hack, test, and secure web applications from existing and emerging security threats in the industry verticals.

Web Application Hacking and Security has challenges derived from the engaging iLab environments of EC Council – from Certified Ethical Hacker (CEH) to the Certified Penetration Testing Professional (CPENT); from Certified Application Security Engineer (CASE) .Net to Java. But Web Application Hacking and Security goes beyond this to more difficult scenarios as you advance through each problem.

Web Application Hacking and Security is like a Capture-The-Flag (CTF) competitions meant to test your hacking skills. But you can keep on trying until you achieve the goal. Test your skills and work alone to solve complex problems or follow the instructor as they do a walkthrough to help you learn Web Application Hacking and Security

## Content

- Advanced Web Application Penetration Testing
- Advanced SQL Injection (SQLi)
- Reflected, Stored and DOM-based Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF) – GET and POST Methods
- Server-Side Request Forgery (SSRF)
- Security Misconfigurations
- Directory Browsing/Bruteforcing
- Network Scanning
- Auth Bypass
- Web App Enumeration
- Dictionary Attack
- Insecure Direct Object Reference Prevention (IDOR)
- Broken Access Control
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- Arbitrary File Download
- Arbitrary File Upload
- Using Components with Known Vulnerabilities
- Command Injection
- Remote Code Execution
- File Tampering
- Privilege Escalation
- Log Poisoning
- Weak SSL Ciphers
- Cookie Modification
- Source Code Analysis
- HTTP Header modification
- Session Fixation
- Clickjacking