EC-Council

WEB APPLICATION HACKING & SECURITY

ICLASS.ECCOUNCIL.ORG

From the team that brought you **Certified Ethical Hacker**

C|EH™ Certified Ethical Hacker

THE COMPLETE HANDS-ON GUIDE TO **W**EB **A**PPLICATION **H**ACKING AND **S**ECURITY

Understand, Exploit, And Defend Yourself Against Topmost Web Vulnerabilities With A Comprehensive Hands-On, Lab-Based, Guided, Mastery Course Designed By The Team That Brought You C|EH

Table of Contents

From the team that brought you Certified Ethical Hacker

Test your skills and learn to hack applications with Web Application Hacking and Security. Whether you are a beginner or an experienced ethical hacker, the Web Application Hacking and Security course offers something for all skill levels. You will hack through a variety of challenges from SQL Injection, to Security Misconfigurations, to Cross-Site-Scripting, and more.

EC-Council

43,986
Exploits
in the Google Hacking Database

18,000
CVE
Published in 2020

Why Mastery of **Web Application Security** is Important

Most of the work we do on a day-to-day basis uses cloud-based apps that are vulnerable to cyber-attacks.

There are currently 43,986 exploits (and growing) in the Google Hacking Database[1] and the total number of Common Vulnerabilities and Exposures (CVE) is at a record high with over 18,000 published in 2020 alone!

Now, with so many published vulnerabilities, it is important to learn to defend and secure your web applications. Traditional protections like firewalls alone do not secure web applications. Defenders need a deep understanding of the most critical security risks to web applications such as the OWASP Top 10. And what better way to learn to gain familiarity and defend than to attack!

1-https://www.exploit-db.com/google-hacking-database

Course Description

Decoding Web Application Hacking and Security

Course Duration: 60 Hours

Web Application Hacking and Security has challenges derived from the iLab environments of EC Council – from Certified Ethical Hacker (C|EH) to the Certified Penetration Testing Professional (C|PENT); from Certified Application Security Engineer (C|ASE) .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 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 he does walkthroughs to help you learn Web Application Hacking and Security.

Play > Learn > Hack > Test

WHAT WILL YOU **LEARN?**

You will learn about application vulnerabilities and web application hacking. Even though this will prove useful for other CTF contests, and in cracking VVMs, it will be even more useful to your career as you learn to defend your applications and progress to Web Application Hacking and Security.

- 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
- CMS Vulnerability Scanning
- 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

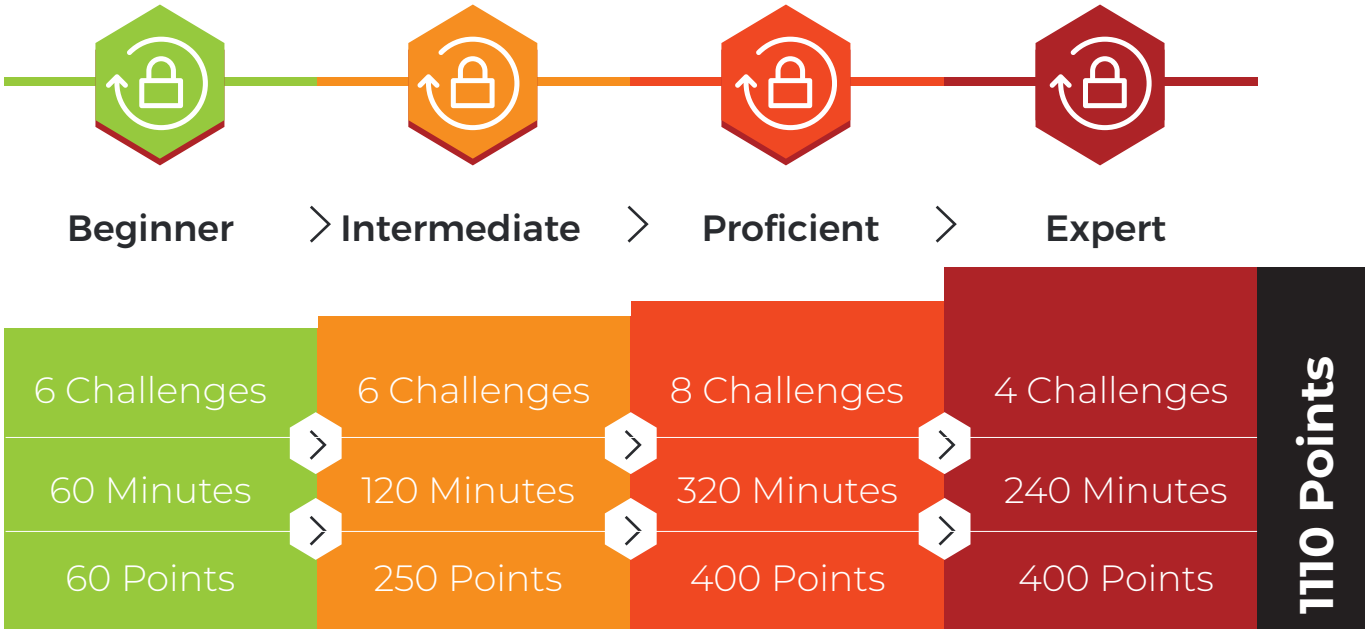
Learn by doing. Don't rely on the walkthroughs; challenge yourself and see how far you can get.

BREAK THE C</>DE

Challenge yourself and hack your way to greatness

You will encounter security misconfigurations, SQL injection vulnerabilities, directory browsing vulnerabilities, enumeration vulnerabilities, and opportunities to escalate privileges and gain access to privileged information.

Each section of 'Break the Code' brings progressively more difficult challenges. There are always multiple paths to take, but few will get you the prize and move you up the leader board.



Watch your name rise on the leader board, a place where you'll see who's cracking the most challenges, who's making the most progress, who's cranking out the h@ck$!

WHO SHOULD ATTEND?

If you are tasked with implementing, managing, or protecting web applications, then this course is for you. If you are a cyber or tech professional who is interested in learning or recommending mitigation methods to a myriad of web security issues and want a pure hands-on program, then this is the course you have been waiting for.

- Penetration Tester
- Ethical Hacker
- Web Application Penetration Tester
- Security Engineer/Auditor
- Red Team Engineer
- Information Security Engineer
- Risk/Vulnerability Analyst
- Vulnerability Manager
- Incident Responder

EXAM OVERVIEW

A fully online, remotely proctored practical exam that challenges candidates through a grueling **6-hour performance-based, hands-on exam**. The exam assesses candidates' skills and proficiencies on a broad spectrum of **OWASP Top-10 web application vulnerabilities and attack vectors**. The assessment is not limited to only the understanding of automated exploitation frameworks but requires a deep understating of various web application technologies, their inherent and acquired vulnerabilities, and manual exploitation techniques.

CERTIFICATION

The exam focuses on candidates' proficiencies in performing a web application security assessment in real life stressful scenarios. Candidates who score more than **60%** will earn the **Certified Web Application Associate** certification, candidates who score more than **75%** will be awarded the **Certified Web Application Professional** certification and candidates who score more than **90%** attain the prestigious **Certified Web Application Expert** certification!

60% ASSOCIATE

75% PROFESSIONAL

90% EXPERT

Level Up Your Skills
Register Now ▶

- The Web Application Hacking and Security exam dashboard will be available for 30 days from time of activation. Launch your Exam Dashboard when you are ready to take on the exam.
- You will need to schedule the exam sessions and clear the exam from the Exam Dashboard within the validity period of 30 days.
- You will need a host machine with a virtual machine running your penetration testing toolkit to take the exam. Please read the Host System Requirement and Virtual Machine Resource Requirement carefully.

WEB APPLICATION HACKING & SECURITY

ICLASS.ECCOUNCIL.ORG

EC-Council