

CERTIFIED WEB APPSEC EXPERT 2023

Driving out Security Vulnerabilities & Improving the Resilience of your Infrastructure

4 - 5 DECEMBER 2023 | SHERATON IMPERIAL HOTEL KL

Web applications grow in complexity every day and it is extremely difficult to manage them from a security perspective. No system is bulletproof, but there are measures that, if implemented, can save companies millions from online frauds. This course helps organizations to understand the problems associated with web applications and the techniques used to address them providing crucial information to businesses and helping them identify and eliminate vulnerabilities without disrupting services.

This real-time immersive hands-on workshop uses a combination of lecture, real-world experiences, and hands-on exercises to teach you the techniques to test the security of tried-and-true internal enterprise web technologies, as well as cutting-edge Internet-facing applications



Abhinav Mishra is an Application Security Researcher with 12+ years of experience in penetration testing of web, mobile and infrastructure. He is the founder of ENCIPHERS, where he takes care of heading the penetration testing, training and other offensive security projects. Abhinav has been training security professionals on web, mobile and infrastructure hacking around the world.

Benefits of Attending:

- Understand & apply sophisticated web application testing techniques & identify vulnerabilities
- Interactive hands on training, where you get to practice a huge number of advance exploits
- Solve challenges and get personalised feedback, on dedicated platform - VantagePoint
- Learn about REST API security testing, advance exploitation methodology
- Ways to exploit web application vulnerabilities and taking reverse shell
- Learn methodology behind chaining vulnerabilities
- Learn ways to exploit an application vulnerability to get reverse shell
- Complementary 30 days access to VantagePoint, to solve challenges and practice
- Delegates will receive a Complementary **Certified Web AppSec Expert** exam voucher after completion of the training

Supported by:



Exclusively by:



Overview:

Web applications are the core of world wide web. Web applications handle data ranging from static content to extremely sensitive user data like personally identifiable information, personal health information, financial details and what not. This makes the web applications, a target for hacking and security breaches. A recent study shows that 41% of organizations suffered a possible web application attack in 2022. Hence, it is extremely important to ensure that the modern web applications are secure. Penetration testing is a process of testing applications/infrastructure etc for security issue.

This is a fully hands-on training designed to teach the skills required to find vulnerabilities in modern web apps. Delegates will be able to perform exploit and practice a lot of advanced level security attacks, on the state-of-art training lab. Some major vulnerabilities/topics covered:

SQL injection | Cross Site Scripting | XML Injection | XXE | Remote Code Execution | Command Injection | Server side request forgery | Server side template injection | Insecure direct object reference | Out of bound exploitation (XXE ,SSRF) | Chaining of security vulnerabilities.

Take-aways include: Presentation Slides | Lab Manual | Solution Sheet | Hackers Mind Map | Certification

Why Web Application Penetration Testing?

Verizon's annual data breach report shows most attackers are external, money remains their top motivator, and web applications and unsecured cloud storage are hot targets. According to the updated Verizon Data Breach Investigations Report, 45% of data breaches target the application layer. Even as digital transformation requires that software be built faster, application security is required to reduce your organization's overall business risk.

The Solution:

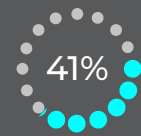
To counter this problem, Encipher team of trainers will conduct the 2 days hands-on interactive training on security risk assessment solution – Web Application Penetration Testing – to identify, analyze and report vulnerabilities in a given web application. Here, you will gauge how to adopt strong technology and process based approach supported by a well-documented methodology to identify potential security flaws in the web application and the underlying environment.

STATISTICS

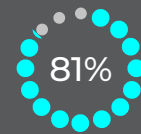
of total breaches reported



Involving attacks on web applications

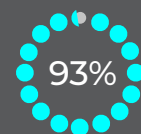


Featured hacking to exploit vulnerabilities

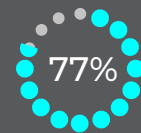


hacking related breaches that leveraged weak or stolen passwords

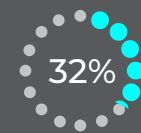
of attacks on Web Applications



financially motivated, perpetrated by organized criminal groups



carried out by botnets, not individuals



exploited SQL Injection errors

Source: Verizon Data Breach Investigations Report