Advance WEB HACKING APPLICATION 2023

Driving out Security Vulnerabilities & Improving the Resilience of your Infrastructure

2-3 MARCH 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 virtual-lead 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 9+ 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

Supported by:

ENCIPHERS

Exclusively by:

THOMVELL international

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) I Chaining of security vulnerabilities.

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

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

Involved 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

Module 1 (Day 1):
(Basics & Client Side Vulnerabilities)

Trainer will explain how the training lab is structured and how to approach it as a target for penetration test. The major points covered would be:

- Using virtual private servers for pentesting
- Setting up the lab access (SSH & RDP)
- Enumeration of target application and infrastructure
  - Port and service scanning
  - Finding all the entities
- Easy to find security vulnerabilities in web application:
  - Misconfgurations
- Missing security controls

Module 2 (Day 1):
(Finding Low Severity Vulnerabilities)

- Discovering and exploiting some of the web application vulnerabilities:
  - Cross Site Scripting
    - Stored XSS
    - DOM XSS
    - Blind XSS
- Using cross site scripting to takeover account
- Understanding Cross Site Request Forgery
- Discovering insecure entry points in the application
- Understanding authentication & authorization in the target app
- Basics of JSON Web Tokens

Module 3: (Day 2)
(Exploiting Server Side Vulnerabilities)

- Basics of 0auth flow and common issues
- Hacking the authentication
  - Cracking the JWT key
  - Other JWT related security issues
- Hacking the authorization:
  - Insecure Direct Object Reference
  - Bypassing UUID identifiers for exploiting IDOR
  - Mass Assignment vulnerabilities
- SQL Injection:
  - SQL Injection in web apps
  - Exploiting SQL injection in GraphQL
- XML External Entity Attack
  - File extraction with XXE
  - Out Of Band exploitation of XXE

Module 4: (Day 2) (Taking reverse shells)

- Server Side Request Forgery
  - SSRF exploitation scenarios
  - Exploiting SSRF for data ex-filtration
  - SSRF to AWS compromise
- Server Side Template Injection:
  - Testing for SSTI vulnerabilities
  - Getting reverse shell with SSTI
- Remote file inclusion
- RFI to reverse shell
- Remote code execution:
  - Hacking Insecure Jenkins to get reverse shell
- Command Injection
  - Command injection to reverse shell
- Insecure De-serialization
  - Reverse shell with insecure de-serialization

Pre-requisites:

- **Delegates MUST have understanding of:**
  - Basic usage of Burp Suite proxy
  - Security testing methodology - OWASP Top 10
  - Linux Operating system, ssh, remote desktop etc.
- Laptop with 4 GB RAM or higher, Preferably a SSD based laptop, with administrator/root privileges

Speaker Biography:

Abhinav Mishra a.k.a 0ctac0der, is an Application Security Researcher with 10+ years of experience in penetration testing of web, mobile and infrastructure. He is the founder of ENCIPHERS, a cyber security top consulting company 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. He also holds numerous accolades & rewards for finding security issues through responsible disclosure programs. Abhinav is a well-known trainer, speaker, cyber security strategist and ethical hacker in the information security community, where he majorly talks about the offensive security/penetration testing/responsible disclosures. Recently, he authored the book "Mobile App Reverse Engineering".

Who Should Attend

This security training course is addressed to all companies that have a software development department, in particular to testing and software development professionals who want to include security in software development life cycle.

- Web penetration testers
- Red team members
- Vulnerability assessment personnel
- Network penetration testers
- Security consultants
- Developers
- QA testers
- System administrators
- IT managers
- System architect

WORKSHOP TIMING