The Hacktivists

Hacking | Forensic | Security

SYLLABUS

AWAE

ADVANCED WEB SERVICE ATTACKS AND EXPLOITATION VERSION 1

The most practical and extensive training course on web service (API) pentesting

IT Security Professionals have chosen "THE HACKTIVISTS" as their best cybersecurity training provider.
We have trained professionals who are working in Fortune 500 companies and Best organization across 100+ countries around the globe.

wipro · hp · accenture · Infosys · Paytm · verizon · EY · Cognizant · HCL · amazon · Honeywell · PhonePe · Mindtree · Mphasis · Deloitte. · pwc

INTRODUCTION

2021

COURSE DESCRIPTION

The Advanced Web Service Attacks And Exploitation (AWAE)is an online training program that provides all the high-level skills required for professional penetration test against modern web services (API). This training includes the most advanced web service attacks, exploitation and pentesting techniques.

This training, although based on the offensive approach, provides the most excellent exercises to solve modern web service security issues discovered during bug bounty hunting and penetration testing.

PRE-REQUISITES

AWAE is advanced training that requires the following pre-requisites:

- Basic development skills needed.
- Ability to read and understand web application code will help, although it is not mandatory.
- One year in an information security role or equivalent experience is recommended.

The Hacktivists AWAE training provides most of the above pre-requisites.

WHO SHOULD TAKE THIS COURSE?

Advanced Web Service Attacks And Exploitation (AWAE) training is beneficial for:

- Bug Bounty Hunters
- Penetration Testers
- Application Developers
- IT Security professionals with a technical background

INTRODUCTION

2021

WILL I GET A CERTIFICATE ?

Once you satisfy the requirements of the final practical certification test, you will be awarded an "Advanced Web Service Attacks And Exploitation Expert" certificate and will hold the AWAE certification.

DETAILED COURSE CONTENT

AWAE training is to introduce candidates to the concept of discovering vulnerabilities in modernised web services and web applications. We demonstrate advanced exploitation techniques using real-world scenarios - all challenges and practicals showed on live secure and unsecured web applications.

Module 1 : An Introduction to APIs for the Security Testing

Module 2 : Rethink Governance in an API-First World

Module 3 : Lab Setup of API Security Testing environment

Module 4 : Testing APIs Code Quality and Build Settings

Module 5 : Getting Started with API Security Testing

Module 6 : MobileApp and WebApp APIs Security Testing

Module 7 : Discovering Leaky APIs and Hidden APIs - Reconnaissance

INTRODUCTION

2021

Module 8 : API Authentication and Authorization Vulnerabilities

Module 9 : API Manipulation and Parameter Tampering

Module 10 : API Security Testing according to OWASP Top 10

Module 11 : Modern APIs Vulnerabilities and Bug Bounty - Introduction

Module 12 : Modern APIs Vulnerabilities and Bug Bounty - Practicals

MODULES

2021

MODULE 1 An Introduction to APIs for the Security Testing

- What An API Is and Why It's Valuable
- Different Approach of API Security Testing
- Real-time Challenges of API Security Testing
- Tools and Frameworks for API Security Testing
- Types of Bugs that API Security testing detects
- Difference between Common API testing and API Security testing

MODULE 2 Rethink Governance in an API-First World

- Primary Goal of API Governance
- So Why Implement API Governance?
- What Should API Governance Include?
- Implementing an API Governance Approach
- Modern APIs Are Different Than Integration
- how governance can enable security and compliance
- All WebApp and MobileApp development is API development
- best practices to help organizations scale their API program
- API governance: Key element for security & scaling API programs
- How to execute API governance throughout design,implementation and runtime operations.

MODULE 3 Lab Setup of API Security Testing environment

- Installation of API Security Testing tools
- Installation of API Security Testing Frameworks
- Configuration and Testing builds of Live Test Cases

MODULE 4 Testing APIs Code Quality and Build Settings

- First, let's look at the APIs Documentations
- API Documentation Made Easy Security Testing
- Security Review of APIs Documentations
- Understanding API-Based Platforms

MODULES

2021

MODULE 5 Getting Started with API Security Testing

- Setup API Live Test Case Environment
- API Penetration Testing Methodologies
- API Security testing Checklists for Pentesters
- API Security testing Checklists for Developers
- API Security testing Checklists for Bug Hunters
- API Security testing according to API governance

MODULE 6 MobileApp and WebApp APIs Security Testing

- Complete Security testing of Web API Applications
- Complete Security testing of Mobile API Applications
- Covering Security Audit of MobileApp API and WebApp API

MODULE 7 Discovering Leaky APIs and Hidden APIs Recon

- Configure Fiddler to find Sensitive and leaky APIs
- Configure Burpsuite to Security test of Hidden APIs
- Proxying Device Traffic Through Fiddler | Burpsuite
- Discovering More About Mobile Apps via Fiddler
- Discovering Hidden APIs via Documentation Pages
- Discovering Hidden APIs via Search Engine
- Discovering Hidden APIs via robots.txt
- Discovering Leaky APIs - UserID Endpoint
- Discovering Leaky APIs - User Input Endpoint
- Discovering Leaky APIs - User Interaction Endpoint
- Personally Identifiable Information (PII) Disclosure

MODULES

2021

MODULE 8 API Authentication and Authorization Vulnerabilities

- A Practical Approach to Test: Various OAuth Misconfiguration
- A Practical Approach to Test: OAuth Authorization Bypass
- A Practical Approach to Test: Account takeover Issues
- Improper Restriction of Unprotected APIs Endpoint
- Transporting API Auth tokens as Cleartext Allowed
- Improper Restriction of Misconfigured API
- Insufficient Entropy For Random Values
- Leakage of API Authentication Tokens
- Improper Access Control

MODULE 9 API Manipulation and Parameter Tampering

- A Practical Approach to Test: XML External Entity (XXE) Processing
- A Practical Approach to Test: HTTP Parameter Pollution Attacks
- A Practical Approach to Test: Cross-site Scripting (XSS)
- A Practical Approach to Test: Common Injection Attacks
- A Practical Approach to Test: Command Injection
- A Practical Approach to Test: SQL injection
- Manipulating App Logic by Request Tampering
- Response Tampering

MODULE 10 API Security Top 10 according to OWASP

- OWASP API Security Vulnerabilities - Practicals
- Testing for Broken Function Level Authorization
- Testing for Broken Object Level Authorization
- Testing for Lack of Resources & Rate Limiting
- Testing for Broken User Authentication
- Testing for Improper Assets Management
- Testing for Security Misconfiguration
- Testing for Excessive Data Exposure
- Testing for Mass Assignment

MODULES

2021

MODULE 11 Modern APIs Vulnerabilities and Bug Bounty

- Why APIs Security Testing Important in Bug Bounty Hunting
- Why APIs Security Testing Important in WebApp Security Auditing
- Why APIs Security Testing Important in MobileApp Security Auditing

MODULE 12 Modern APIs Vulnerabilities & Bug Bounty Practicals

- A Practical Approach to Test: Insecure Direct Object Reference(IDOR)
- A Practical Approach to Test: Cross-Origin Resource Sharing (CORS)
- A Practical Approach to Test: Cross-Site Request Forgery (CSRF)
- A Practical Approach to Test: Open Redirection Vulnerability
- A Practical Approach to Test: Privilege escalation Issues
- A Practical Approach to Test: Local File Inclusion (LFI)
- A Practical Approach to Test: Remote File Inclusion(RFI)
- A Practical Approach to Test: Input validation Issues

ABOUT US

Our Company The Hacktivists™ (Leading IT Security Services & Training Providing Company) offers a wide range of courses & training in Information Cyber Security. We are a Fast-growing online information security training company based out of India.

We have a large number of professional instructors who are specialized and experienced in various Information/Cyber Security domains. Our Instructors holds a wide range of accreditation like OSCP, OSEE, OSCE, eCXD, eMAPT, eWPTX, eWDP, CEH, CHFI, CISSP, CISM, CISA.

The Hacktivists™ is one of the most trusted and reliable training providers in information/cybersecurity, providing exceptional unmatched Hands-on practical training to individuals and corporates worldwide. Our goal is to train, mentor, and support your career in cybersecurity.

We emphasize more on hands-on practical training which gives our clients and candidate an edge to grow and advance professionally in their respective career(s).

Contact details:
www.thehacktivists.in
info@thehacktivists.in