Web App Pentest 667

Behind the Web, Advanced Techniques in Penetration Testing

Web App Penetration testing

Table of **Content:**

Program **Overview:**

The Web Application Security Course offers a wide range of topics related to web pentesting and security for IT Professionals who want to push their IT Skills to another level with the techniques and knowledge of Web Pentesting. This specially organized course is dedicated to clearing the topics on web security infrastructure, troubleshooting methods, security solutions, and laws related to web application security for IT Professionals.

Program **Features:**

- ✓ 60 hours of instructor-led training or Live VILT classes.
- ✓ The course will be in both English and Hindi mediums.
- ✓ Learn from Industry-leading experts with extensive experience in Linux and as a system administrator.
- ✓ Hands-on practical exercises to learn with real-time problem-solving scenarios.
- ✓ Cutting-edge curriculum to stay at the forefront of web application security.
- ✓ Receive detailed study guides and resources designed to enhance your learning experience.
- ✓ Access course materials and live sessions through both online and offline modes to suit your learning preferences.
- ✓ Benefit from our continuous support even after completing the course, ensuring your long-term success.

Delivery **Mode:**

Online Bootcamp / Offline Classroom Training / Corporate Training Facility

Prerequisites of **Web Application Security:**

A beginner can definitely join this course, however, a basic knowledge of web tech, computing languages, and usual IT concepts can give you a better flow.

Target **Audience:**

- ✓ Developers
- ✓ Security Professionals
- ✓ System Administrators
- ✓ Quality Assurance/ Testers
- ✓ Project Managers
- ✓ IT Managers and Executives
- ✓ Students and Educators
- ✓ Freelancers and Consultants
- ✓ Entrepreneurs and Startups
- ✓ Anyone with an Interest in Cybersecurity

Key Learning **Outcomes:**

A web application security course can greatly benefit IT professionals in several ways:

- ✓ **Understanding Common Threats:** One will get a better knowledge of usual risks & loopholes that affect web apps, such as SQL injection, XSS, CSRF, and IDOR.

- ✓ **Secure Development Practices:** To create web applications with built-in security features and lower the possibility of introducing vulnerabilities throughout the development process, they will master secure coding methods and methodologies.
- ✓ **Effective Testing Methods:** The course will cover a variety of testing approaches and tools, such as vulnerability scanning, penetration testing, and code review procedures that are used for measuring the security posture of online applications.
- ✓ **Incident Response Skills:** IT workers will learn the necessary skills for incident identification, analysis, containment, and recovery in the event of a security incident affecting web applications.
- ✓ **Compliance and Regulations:** They will be aware of the appropriate regulations and laws about online application security compliance, including the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), and others.
- ✓ **Risk Management:** IT workers will be able to successfully identify, prioritize, and mitigate security threats by learning risk management principles that are relevant to web application security in this course.
- ✓ **Securing Infrastructure:** To defend web applications from outside threats, IT professionals will learn how to deploy and secure web servers, databases, and other infrastructure components.
- ✓ **Secure Deployment Practices:** To guarantee that web applications are deployed securely, they will learn about secure deployment methods, such as secure configuration management, patch management, and secure deployment pipelines.
- ✓ **Security Awareness Training:** To teach staff members about web application security and best practices for preserving security vigilance, the course may include modules on security awareness training.
- ✓ **Career Advancement:** Gaining expertise in web application security can boost an IT professional's credibility, increase their value to companies, and create prospects for career growth in cybersecurity areas.

Certification **Alignment:**

Web Application Security is a specially customized training program to develop the technical skills and knowledge of IT Professionals who want to follow a career path including cybersecurity & web application security. Moreover, a certification offered by Craw Security will let you strengthen your value in the IT Sector. You can go for the training & certification program by contacting Craw Security.

Certification **Details & Criteria:**

Certification Details -
After the completion of the Web Application Security course, one will be able to sit for the examination. This exam will testify to the skills and knowledge of professionals related to web application security. Moreover, after the examination, professionals will receive a certificate validating their performance for future demonstrations.

About the **Exam:**

- ✓ **Number of Questions:** 30-35 Questions
- ✓ **Exam Test Duration:** 1 Hour
- ✓ **Test Format:** Multiple Choice Question (MCQ)
- ✓ **Exam Cost:** 600 Inclusive Taxes

Craw Security **Certification Criteria:**

- ✓ Attend 75% of classes and obtain 50% marks in the corresponding examination.
- ✓ Please note that there is an additional fee for the FutureSkills Prime exam related to this course.

100% Placement with **1 Year Cyber Security Course:**

There is a specialized set of Terms and Conditions for a 100% Placement Guarantee with **our 1 Year Cybersecurity Diploma** that needs to be fulfilled by each and every student who is willing to benefit from features from Craw Security. However, we have jotted down all the necessary T&Cs that need to be completed to take the advantage of 100% Placement Guarantee from the Department of Training & Placement by Craw Security:

- ✓ Attendance of 75% should be mandatory.
- ✓ Marks for internal exams should be 80% mandatory.
- ✓ Fees for 1 Year Cybersecurity Diploma Course should be properly paid.
- ✓ Candidate can apply for a job after completion of 6 modules.
- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.
- ✓ Global certifications are required, if needed by companies for jobs.
- ✓ Candidate should be Graduate/Pursuing.
- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be liable to re-arrange the interview, and also Craw Academy will not be liable for any refund or future litigations or claims.
- ✓ Package as per candidate's skills or according to company norms.
- ✓ Ideal Candidates can apply for multiple jobs.
- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
  1. Documentation
  2. Offer Letter
  3. Joining Date/ Timeline of Joining

What to Choose After this **Course:**

A person can choose the 1 Year Cybersecurity Diploma Course after the completion of this course or even switch the current course to this 12-course bundle of 1 Year Cybersecurity Diploma Course by Craw Security whose maximum courses are accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India.

Course **Curriculum:**

Module 01: Introduction

- ✓ Lesson 01: Networking and protocol
- ✓ Lesson 02: HTTP & HTTPS

Module 02: Owasp top 10

- ✓ Lesson 01: Briefing about various frameworks
- ✓ Lesson 02: Explaining the OWASP top 10

Module 03: Recon for bug hunting

- ✓ Lesson 01: Subdomains enumeration
- ✓ Lesson 02: Domains filtration
- ✓ Lesson 03: Endpoints enumeration
- ✓ Lesson 04: Grepping responses

Module 04: Advanced SQL Injection

- ✓ Lesson 01: Union based SQLI
- ✓ Lesson 02: SQL Authentication Bypass
- ✓ Lesson 03: Error based SQLI

- ✓ Lesson 04: Time-based SQLI
- ✓ Lesson 05: In-band and out-of-band SQLI
- ✓ Lesson 06: Create our own script to automate the process of Blind SQLi

Module 05: Command injection

- ✓ Lesson 01: DVWA source code review
- ✓ Lesson 02: PHP command injection with various functions
- ✓ Lesson 03: Filter bypass

Module 06: Session Management and Broken Authentication Vulnerability

- ✓ Lesson 01: Cookie hijacking
- ✓ Lesson 02: HSTS policy bypass

Module 07: CSRF – Cross-Site Request Forgery

- ✓ Lesson 01: protection bypass

Module 08: SSRF – Server Site Request Forgery

- ✓ Lesson 01: Filter bypass
- ✓ Lesson 02: Server-side configuration check

Module 09: XSS – Cross-Site Scripting

- ✓ Lesson 01: Explaining JavaScript
- ✓ Lesson 02: Reflected JavaScript
- ✓ Lesson 03: Stored JavaScript
- ✓ Lesson 04: DOM-based JavaScript

Module 10: IDOR – Insecure Direct Object Reference

- ✓ Lesson 01: UUID protection

Module 11: Sensitive Data Exposure and Information Disclose

- ✓ Lesson 01: GIT source code disclosure
- ✓ Lesson 02: Client-side source code review

Module 12: SSTI – Server Site Template Injection

- ✓ Lesson 01: Template engine Explaining
- ✓ Lesson 02: Various exploitation techniques with various Template engine

Module 13: Multi-Factor Authentication Bypass

- ✓ Lesson 01: Brute-force attacks
- ✓ Lesson 02: Creating wordlists
- ✓ Lesson 03: Logic errors bypass

Module 14: HTTP Request Smuggling

- ✓ Lesson 01: Explaining HTTP/1.1 and HTTP/2
- ✓ Lesson 02: CL-TE attack
- ✓ Lesson 03: TE-CL attack
- ✓ Lesson 04: TE-TE attack

Module 15: External Control of File Name or Path

✓ Lesson 01: Whitelisting and blacklisting
✓ Lesson 02: Bypassing blacklisting
✓ Lesson 03: Brief on regex

Module 16: LFI – Local File Inclusion and RFI – Remote File Inclusion

✓ Lesson 01: Traversal payload
✓ Lesson 02: Bypass WAF
✓ Lesson 03: Reading and inclusion difference

Module 17: Directory Path Traversal

✓ Lesson 01: Path traversal payload to read the file

Module 18: HTML Injection

✓ Lesson 01: Explaining HTML web page
✓ Lesson 02: Reflected HTML injection
✓ Lesson 03: Stored HTML injection

Module 19: Host Header Injection

✓ Lesson 01: Apache config brief
✓ Lesson 02: Host header Explaining

Module 20: File Upload Vulnerability

✓ Lesson 01: POST method explain
✓ Lesson 02: Encoded POST method
✓ Lesson 03: Various headers related to file upload

Module 21: JWT Token Attack

✓ Lesson 01: JWT tokens algorithms
✓ Lesson 02: Brute force on HS256 algo
✓ Lesson 03: Logic error bypass

Module 22: Flood Attack on Web

✓ Lesson 01: XXE vulnerability to cause DOS
✓ Lesson 02: Business logic to cause DOS

Module 23: Report Writing

✓ Lesson 01: POC (proof of concept)
✓ Lesson 02: Executive and Management Report
✓ Lesson 03: Technical Report For IT and security Department

About us:

Craw Security is India's leading cybersecurity training institute, dedicated to developing the next generation of cybersecurity professionals. With a focus on practical, hands-on training, we offer a wide range of courses tailored to all skill levels. Our mission is to enhance the cybersecurity posture of individuals and organizations worldwide.

For more information, please visit our course page website:
https://www.craw.in/learn-web-application-security-course-in-delhi/

Contact **us:**

Craw Cyber Security Private Limited, India (Head Office)

1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station, Said-ula-jab, New Delhi – 110030, India

Email id: training@craw.in | info@craw.in
Contact Number: +91 9513805401
Connect on WhatsApp: +91 8448897124

Visit our website: www.craw.in | www.crawsecurity.com
Get Latest Cyber Security updates: www.nesw4hackers.com

Connect on Social media

Facebook: https://www.facebook.com/CrawSec/
Twitter: https://twitter.com/crawsec
YouTube: https://www.youtube.com/c/crawsecurity
LinkedIn: https://www.linkedin.com/company/crawsec

Join Our Community

WhatsApp Channel: Join Whatsapp Channel