CERT NO. RCWP

PROFESSIONAL CERTIFICATION PROGRAM

REDSPECTOR

// RCWP · ADVANCED WEB PENTEST TRACK

Redspector Certified

Web Pentester

PROFESSIONAL PROGRAM

An elite, hands-on certification for offensive security engineers
mastering web application exploitation — from OWASP to real-world attack chains.

10 MODULES

40+ LABS

07 TOOLKITS

01

```
~/redspector/rcwp

redspector~$ web_pentest --scope owasp-top10 --mode red-team

> burp + payload chain + real-world methodology verified.

> target compromised. RCWP eligible.
```

ENROLL NOW

WWW.REDSPECTOR.COM · TEAM@REDSPECTOR.COM · +91 80783 28520

“Building the Next Generation of Cybersecurity Professionals”

// 01 ABOUT

Course Overview

TheRedspector Certified Web Pentester(RCWP) program is a hands-on, practitioner-grade certification for offensive security professionals mastering modern web application penetration testing. Students move from web and protocol fundamentals through OWASP Top 10 exploitation, Burp Suite mastery, PortSwigger labs, and a full real-world pentest methodology — building the mindset, toolkit and reporting discipline required to break and secure production web targets.

10	40+	07	01
CORE MODULES	HANDS-ON DRILLS		

// WHO SHOULD JOIN

Built for Web Pentesters & Bug Hunters

Aspiring Pentesters

Beginners entering offensive security through the web attack surface.

Bug Bounty Hunters

Researchers targeting real-world OWASP vulnerabilities and payouts.

Security Analysts

Blue-team professionals learning the attacker mindset for defense.

Developers

Engineers writing secure code by understanding how it is broken.

CS Students

Learners building a career foundation in offensive web security.

Red Teamers

Operators extending capability into modern web exploitation chains.

// 02 PATH

Learning Journey

Astructured,six-stageprogressionfromwebfundamentals to real-world pentest methodology.

01

WEB FUNDAMENTALS

HTTP,client-servermodel,sessions, cookies & protocols

02

FRONTEND SURFACE

HTML,CSS,JavaScript,DOM& client-side security controls

03

DATA LAYER

SQLfundamentals,query logic & injection foundations

04

OWASP TOP 10

Injection,brokenaccess, SSRF, misconfig & modern web risks

05

TOOLING & RECON

Reconnaissance,subdomain enumeration & Burp Suite mastery

06

EXPLOIT & REPORT

AdvancedOWASP,PortSwigger labs & real-world pentest flow

// PROGRAM CURRICULUM

Modules 01–04

Foundations—protocols,frontendsurface and the data layer.

MOD 01

WEB & INTERNET FUNDAMENTALS

- How the Internet Works
- Client-Server Model
- HTTP vs HTTPS
- HTTP Methods & Status Codes
- Cookies & Sessions Basics

LABS
Protocol Traffic Analysis
HTTP Request Dissection

MOD 02

HTML & CSS BASICS FOR HACKERS

- HTML Structure & DOM
- Forms and Input Fields
- Hidden Fields
- CSS Selectors (class, id)
- Client-Side Validation Basics

LABS
DOM Inspection Drills
Hidden Field Exploitation

MOD 03

JAVASCRIPT BASICS

- JavaScript Fundamentals
- DOM Basics
- Event Handling
- Client-Side Security Controls
- Intro to DOM XSS Concept

LABS
Client-Side Bypass Lab
DOM XSS Discovery

MOD 04

SQL FUNDAMENTALS

- Database Basics
- SELECT, INSERT, UPDATE
- Login Query Logic
- Intro to SQL Injection

LABS
Auth Bypass via SQLi
Query Logic Exploitation

// PROGRAM CURRICULUM

Modules 05–08

Coreexploitation—OWASP,recon,Burp Suite and advanced attack chains.

MOD 05

OWASP TOP 10 OVERVIEW

- What is OWASP?
- Top 10 Vulnerabilities Overview
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable Components
- Authentication Failures
- SSRF & Logging Failures

LABS
OWASP Top 10 Assessment
Vulnerability Classification

MOD 06

RECONNAISSANCE & INFO GATHERING

- What is Reconnaissance?
- Passive Reconnaissance
- Subdomain Enumeration
- WHOIS & DNS Analysis
- Technology Fingerprinting

LABS
Target Recon Simulation
Subdomain Discovery

MOD 07

BURP SUITE MASTERY

- Introduction & Setup
- Proxy Interception
- Repeater
- Intruder
- Decoder
- Comparer
- Real Traffic Analysis

LABS
Full Burp Workflow
Live Traffic Manipulation

MOD 08

ADVANCED OWASP EXPLOITATION

- Advanced SQL Injection
- XSS Deep Dive
- IDOR Vulnerabilities
- Authentication Bypass
- File Upload Vulnerabilities
- Real-World Attack Chains
- Secure Development Practices

LABS
Attack Chain Simulation
Exploit Development

// PROGRAM CURRICULUM

Modules 09–10

Appliedmethodology—PortSwiggerlabs and real-world pentest flow.

MOD 09

PORTSWIGGER LABS WALKTHROUGH

- Introduction to PortSwigger Labs
- Guided Lab Solving
- Methodology Building
- Payload Crafting
- Real-World Mindset

LABS Guided Lab Series
Payload Engineering

MOD 10

REAL-WORLD PENTEST METHODOLOGY

- Step-by-Step Testing Flow
- Target Mapping
- Vulnerability Validation
- Reporting Basics
- Pentester Mindset
- Important Tools

LABS End-to-End Pentest
Professional Reporting

// FINAL CAPSTONE

Live Web Application Pentest

Studentsexecuteafullengagementagainstaproduction-grade target.

0 Scoping & Rules of Engagement
1 OWASP-Aligned Vulnerability Discovery
0 Attack Chain Construction
3
0
5

0 Reconnaissance & Target Mapping
2 Exploit Development with Burp Suite
0 Professional Pentest Report
4
0
6

// CERTIFICATION

Benefits, Value & Contact

An industry-ready credential built for elite web security roles.

CERTIFICATION BENEFITS

- Professional RCWP Certification
- OWASP Top 10 Mastery Credential
- Burp Suite Practitioner Skills
- Real-World Pentest Portfolio
- Bug Bounty Career Readiness
- Verifiable Industry Recognition

WHY REDSPECTOR?

1. Industry-Focused Training
2. Hands-On, Lab-Driven Learning
3. Expert-Led Curriculum
4. Real-World Methodologies
5. Bug-Bounty-Grade Skill Development
6. Recognized Certification Program

CONTACT US

Start Your Web Pentest Journey

WEBSITE
www.redspector.com

EMAIL
team@redspector.com

PHONE
+91 80783 28520

"Building the Next Generation of Cybersecurity Professionals"

REDSPECTOR

// RCWP·WEBPENTESTERPROFESSIONAL

"Building the Next Generation of Cybersecurity Professionals"

WWW.REDSPECTOR.COM · TEAM@REDSPECTOR.COM · +91 80783 28520

CERT NO. RCWP-2026 · STATUS VERIFIED