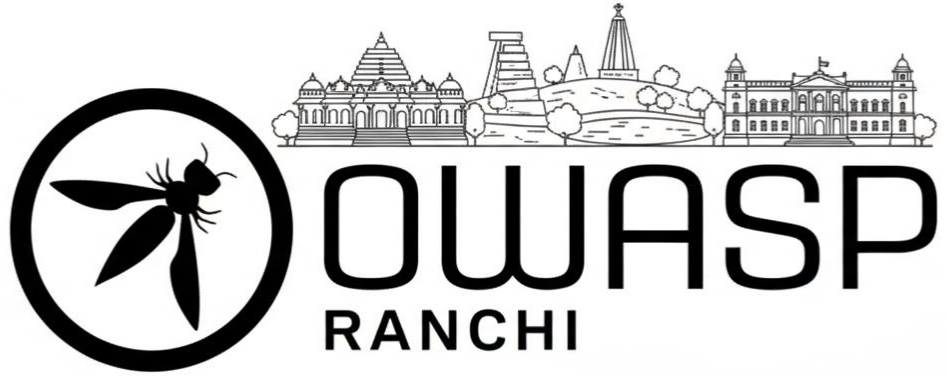
OWASP RANCHI

Join the WhatsApp Group!

Application Security Journey

A comprehensive guide to OWASP, Top 10 vulnerabilities, Lab exercises, and Bug Bounty programs for secure application development



Contents

OWASP RANCHI

What is OWASP

Open Web Application Security Project

A nonprofit foundation that works to improve software security through community-led open source projects, education, and awareness.

Global Community

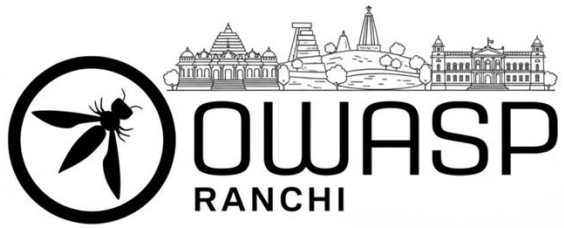
Worldwide network of security professionals and volunteers.

Open Source Tools

Free security tools and resources for developers.

Education Focus

Training materials and best practices documentation.



OWASP Key Projects

Comprehensive Security Ecosystem

OWASP provides numerous projects beyond Top 10,including tools, guides, and testing methodologies.

Security Tools

- ZAP (Zed Attack Proxy)
- WebGoat Training Platform
- Dependency-Check Scanner

Education

Cheat sheets and training materials

Standards

ASVS and SAMM frameworks

Testing Guides

- Testing Guide (WSTG)
- Mobile Security Testing
- API Security Testing

Vulnerability DB

Global security vulnerability database

OWASP RANCHI

Application Security

Application Security (AppSec) is the practice of **protecting software applications** from threats and vulnerabilities throughout their entire lifecycle—from development to deployment and beyond.

Key Activities

- **Secure Coding** : Writing code that avoids common flaws.

- **Scanning for Vulnerabilities** : Using scanners like SAST , DAST , SCA etc.

- **Threat Modelling** : Identifying, analyzing, and mitigating potential security threats and vulnerabilities in a system or application before attackers can exploit them

- **Pentesting** : Penetration testing is when security experts try to safely hack into a system to find and fix weaknesses before real attackers do.

OWASP RANCHI

OWASP Top 10 (A01 – A05)

- **A01: Broken Access Control** - Users act outside their intended permissions, gaining unauthorized access to resources or actions.

- **A02: Cryptographic Failures** - Weak or absent encryption exposes sensitive data to unauthorized parties.

- **A03: Injection** - Untrusted input interpreted as code enables attackers to execute malicious commands.

- **A04: Insecure Design** - Flawed architecture or logic creates exploitable security weaknesses in application flow.

- **A05: Security Misconfiguration** - Improperly configured systems leave vulnerabilities exposed to attackers.

OWASP RANCHI

OWASP Top 10 (A06 – A10)

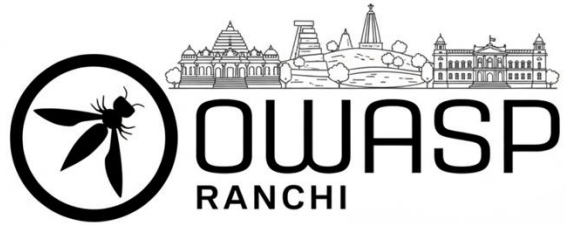
- **A06: Vulnerable and Outdated Components** - Use of unsupported or unpatched libraries introduces known security flaws.

- **A07: Identification and Authentication Failures** - Weak authentication mechanisms compromise user identities and access controls.

- **A08: Software and Data Integrity Failures** - Unverified updates or data manipulation enables unauthorized code execution.

- **A09: Logging and Monitoring Failures** - Insufficient logging hinders incident detection, response, and forensic investigation.

- **A10: Server-Side Request Forgery (SSRF)** - Attackers manipulate server requests to access unauthorized internal resources.



Bug Bounty Programs

• Bug bounty programs are initiatives where companies reward ethical hackers for finding security vulnerabilities.

• They help organizations strengthen security by crowd-sourcing vulnerability research.

• Bounties are monetary rewards or public recognition for responsibly reporting valid bugs.

• Programs often have clear rules on what types of vulnerabilities and in-scope systems qualify.

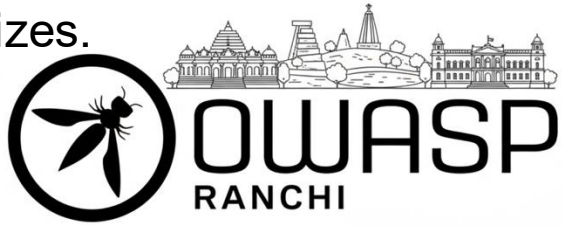
Example Bug Bounty Platforms

•**HackerOne:** Popular global platform connecting companies with ethical hackers.

•**Bugcrowd:** Large community and managed programs for organizations of all sizes.

•**Synack:** Invitation-only platform with vetted security researchers.

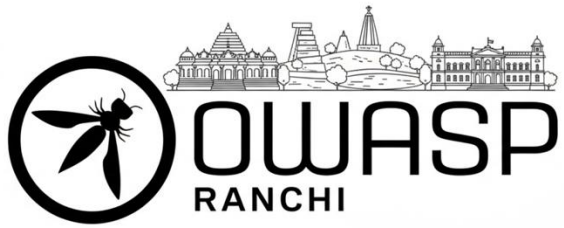
•**YesWeHack:** European-based bug bounty platform with global reach.



Resources & Lab Exercises

Tools Needed to get started

- OS – Linux (Kali preferably)
- Proxy Tool – Burp Suite
- Browser Add-on for Routing via Proxy Tool - FoxyProxy



Resources & Lab Exercises

Online Labs

- **Hacker101:** Popular global platform connecting companies with ethical hackers.
- **PortSwigger Academy:** Free online learning platform with dozens of interactive labs.
- **TryHackMe:** Hands-on cyber security and web application security labs .
- **Hack The Box (HTB) :** Popular for pentesting and web security labs in a realistic environment.

OWASP RANCHI

Resources & Lab Exercises

Offline Labs

- **OWASP Juice Shop:** An intentionally insecure web app designed as a security training ground.
- **DVWA (Damn Vulnerable Web Application):** A classic vulnerable web application for security testers to practice.

Books

- **The Web Application Hacker's Handbook** by Dafydd Stuttard & Marcus Pinto
- **Bug Bounty Bootcamp:** Very practical guide, covers how to find web vulnerabilities, how to report them.

OWASP RANCHI

OWASP
RANCHI

Adarsh Kumar

Product Security Engineer

Splunk

`>_ mrcatalyst`

LinkedIn

Twitter

OWASP RANCHI

ABOUT ME

I am an experienced **Security Enthusiast** with **7+ years** in Application & Product Security. Currently securing products at **Splunk**, I specialize in bridging the gap between Development and Security through automation and empathy.

CORE COMPETENCIES

AppSec & ProdSec

Threat Modeling, SAST/DAST, Secure Code Review

AI Security

Securing AI/ML pipelines & Automating defenses

Development

C# / .NET background, Python scripting for automation

Community

Creator of *mrcatalyst.space* & listMerGer

INTERESTS

Darknet Diaries | Reading Books | Automation | OWASP