Aaditya Vinayak

+91 9950866267 | vaaditya320@gmail.com | linkedin.com/in/vaaditya320 | Portfolio | Jaipur, IN

Summary

Cybersecurity student with hands-on experience in web application penetration testing, vulnerability assessment, and security reporting. Passionate about ethical hacking, bug bounty hunting, and continuous skill development in cybersecurity. Proven ability to identify real-world vulnerabilities and deliver clear, actionable remediation reports.

Technical Skills

Security Testing: Web Application Pentesting, Vulnerability Assessment, OWASP Top 10

Tools: Burp Suite, Nuclei, Subfinder, HTTPx (ProjectDiscovery Suite), Nmap

Scripting: Python, JavaScript, Bash

Reporting: Security Documentation, Risk Analysis, Proof-of-Concept Writing, Remediation Guidance

Experience

Cyberops Infosec LLP Jaipur, Rajasthan

Intern *Jun 2026 – July 2026*

- Performed VAPT assessments on web applications and API endpoints, identifying critical vulnerabilities including account takeovers, broken access controls, and authentication bypasses.
- Performing end-to-end security assessments across web and API surfaces using Burp Suite, Nuclei, and manual testing methodologies.
- Documenting findings with detailed proof-of-concepts, CVSS severity ratings, and actionable remediation guidance.

Intern *Jun 2025 – Aug 2025*

- Participated in multiple penetration testing engagements and security audits, identifying and reporting vulnerabilities across web and cloud environments.
- Prepared detailed security audit reports with proof-of-concepts, severity ratings, and actionable remediation steps.
- Enhanced technical skills by applying manual testing techniques with Burp Suite and other tools in real-world assessment scenarios.

Certifications

Ethical Hacker Cisco Networking Academy

eWPT INE Security *(In Progress)*

Projects

BLHify | *Burp Suite Extension API, Regex*

- Built a passive Burp Suite extension that scans HTTP traffic and extracts social media profile URLs using regex pattern matching.
- Automatically checks and verifies if extracted usernames are unclaimed across X (Twitter), Instagram, and Facebook to detect broken social link hijacking.
- Successfully used in live bug bounty engagements to identify and report broken social link hijack vulnerabilities.

Education

Poornima Institute of Engineering and Technology Jaipur, Rajasthan

B.Tech in Computer Science and Engineering

Interests

Bug Bounty Hunting: Actively hunting on platforms like HackerOne, focusing on web application vulnerabilities.

Capture-the-Flag (CTF) Challenges: Participating in CTF competitions to sharpen offensive security skills across web, Cryptography, and Steganography categories.

Achievements

Reported security issues in multiple bug bounty programs, earning bounties for identifying broken access control issues and preventing account takeover / social engineering scenarios.