PIYUSH PALIWAL

OFFENSIVE SECURITY CONSULTANT

+91 87585 10856 | PiyushThePal@gmail.com | India | www.piyushpaliwal.com

SUMMARY

Offensive security consultant and bug bounty hunter with 7 years of experience testing web applications, APIs, networks, and Active Directory environments. Reported 300+ vulnerabilities across client engagements and bounty programs. Discovered and disclosed CVE-2026-43935, a host header injection in the e107 CMS that allowed pre-authentication account takeover. OSCP certified, member of the Synack Red Team, and an active open-source contributor.

WORK EXPERIENCE

Offensive Security Consultant | Worknest Secure — May '26 - Present

- Conduct web application, API, network, and Active Directory penetration tests for clients, handling each engagement from scoping through to the final report.
- Write engagement reports covering both the technical detail for engineering teams and a clear summary for client leadership.
- Built internal tooling to handle repetitive engagement tasks, freeing up time for manual testing.
- Support newer pentesters through engagement reviews and methodology walkthroughs.

Penetration Tester | Bulletproof — Dec '24- May '26

- Tested web applications, APIs, networks, and Active Directory environments for some of the biggest UK and EU based clients.
- Documented findings in reports for both technical teams and non-technical stakeholders.
- Contributed to the team's testing methodology and built reusable patterns adopted by other consultants.

Associate Security Consultant | SecureLayer7 — Apr '23 - May '24

- Performed penetration testing on Android applications, Windows and PowerShell environments, and network infrastructure.
- Reported 100+ vulnerabilities across client applications.
- Adopted AI tools into the testing workflow to improve efficiency.

Intern Security Consultant | SecureLayer7 — Oct '22 - Apr '23

- Carried out source-code audits, API testing, and web application assessments.
- Wrote reports suited to both technical and non-technical readers.

Bug Bounty Hunter & Security Researcher — Jun '19 - Present

- Report vulnerabilities on HackerOne, Bugcrowd, and private programs, focused on web and API targets.
- Vetted member of the Synack Red Team since 2024, testing enterprise customer targets across web applications, APIs, and hosts.
- Discovered and disclosed CVE-2026-43935, a host header injection in the e107 CMS password reset flow that allowed account takeover without authentication. Rated CVSS 8.1 and fixed in e107 2.3.4 with researcher credit.

OPEN SOURCE PROJECTS

SeBackup-Privilege github.com/PiyushThePal/SeBackup-Privilege

A reference for abusing the Windows SeBackupPrivilege. Covers local exploitation (robocopy bypass, SAM/SYSTEM dump, ntds.dit via diskshadow) and the remote path. Useful for CTFs and AD work.

PA-Pentest_Automation github.com/PiyushThePal/PA-Pentest_Automation

A Bash pipeline that runs a set of common web security checks: host header injection, broken-link hijacking, backup-file discovery, SSL/TLS audit, JS secret hunting, and request smuggling.

Mass-XSS github.com/PiyushThePal/Mass-XSS

Bash tool for finding XSS at scale. Pulls URLs from gau, waybackurls, katana, and hakrawler, filters for parameters, and tests payloads with qsreplace and airixss.

prototype-polluter github.com/PiyushThePal/prototype-polluter

Go tool that checks a list of URLs for client-side prototype pollution. Released as v0.1.0, installable with go install.

PUBLICATIONS & DISCLOSURES

CVE-2026-43935 — Host Header Injection in e107 CMS May '26

github.com/e107inc/e107/security/advisories/GHSA-7pmw-jwvr-cq2x

Pre-authentication account takeover via host header injection in the e107 CMS password reset flow. CVSS 8.1 (High), patched in e107 2.3.4 with researcher attribution. CWE-20 (Improper Input Validation).

CERTIFICATIONS

OffSec Certified Professional (OSCP) | OffSec Jul '24

Credential ID: (OS-101-42177)

Certified Network Pentester (CNPen) | The SecOps Group Mar '24

Credential ID: (8545962)

Junior Penetration Tester (PT1) | TryHackMe Aug '25

Credential ID: (a808170d-a68f-4222-b414-ab4c872e48a2)

AWARDS & ACHIEVEMENTS

CVE-2026-43935 May '26

Disclosed pre-auth account takeover via host header injection in e107 CMS (CVSS 8.1)

Bugcrowd Black Hat USA CTF — 31st Place (Team Finish) Aug '24

Competed alongside global researchers under time pressure

Speaker @ The Hackers Meetup India Surat Chapter Apr '24

Delivered a presentation on advanced penetration testing techniques - Certificate of Appreciation

First Bounty Jun '21

Received from HackerOne

TECHNICAL SKILLS

Penetration Testing:- Web Application, API Pentesting, Network Pentesting, Forensics, Source-Code Auditing, Windows Active Directory Pentesting
Programming Languages:- Python, Bash, Go
Standards:- OWASP Top 10, OWASP API Top 10, MITRE ATT&CK, NIST

EDUCATION

Higher Secondary Education Jun '17
Metas MCD School Of S.D.A