SHANTANU SAXENA

Penetration Tester

✉ shantanu17sept@gmail.com 🌐 https://j0ey17.github.io in https://linkedin.com/in/shantanusaxena1/

SUMMARY

Penetration tester and Security Researcher with almost 2 years of experience in testing networks and web applications / APIs.

An avid python programmer and an active CTF player who has achieved top ranks in multiple international Tournaments. Regularly creates HTB / THM machine walkthroughs on YouTube and writes blogs on medium.

Discovered CVE-2025-46047, a medium-severity 0-day vulnerability on a public CRM (Pending Publication).

SKILLS

Network and Web Pen Testing

- OWASP Top 10
- SOAP, REST, and GraphQL API
- Client and Server Side Vulnerabilities like IDOR, BOLA, XXE, SQL Injection, & SSTI
- OAuth and OpenID Connect
- Active Directory

Tools & Technologies

Coding Languages: Python, Bash, & PowerShell

Web Proxies: Burp Suite, Wireshark, & Postman

Tools: nmap, ffuf, kiterunner, sqlmap & more

Frameworks: Metasploit

EDUCATION

Northumbria University London

Master of Science
Cybersecurity
(2024-2025)

Research: ML-Based Detection of Golden and Silver Ticket using 'klist' output. Prototype model trained using the Random Forest Algorithm and built using Pandas Module.

WORK EXPERIENCE

Security Researcher (Freelance)

Synack Red Team & Public VDP (Current)

- Researched and provided remediations for security bugs on Bug Bounty and Vulnerability Disclosure Programs to secure web infrastructures of multiple companies.
- Found Reflected/Stored XSS, CSRF, SSRF, and more bugs, saving the client's sensitive data and systems from hacks which could have lead to considerable monetary damage.
- Created scripts to automate the discovery of hardcoded API keys and Sensitive data from HTML and JS files thus enforcing secure coding practices for clients.

Cyber Security Consultant

Astra Cyber Tech (Formerly W-CyberTeam)
(Mar 2022 – May 2023)

- Conducted Network, Web App, and Mobile Application VAPT assessments for BFSI and food service Industries.
- Delivered detailed technical and executive reports to communicate the results to relevant stakeholders, allowing them to make informed decisions.
- Participated in Red Team engagements and phishing campaigns against client's infrastructure.
- Provided consultations and tailored solutions to clients.
- Aided the company to receive the CERT-In accreditation.
- Conducted technical interviews and mentored Interns.

CERTIFICATIONS

- eWPTX - Web Application Penetration Tester eXtreme
- eWPT - Web Application Penetration Tester
- eJPT - Junior Penetration Tester
- Dante Pro Labs - HackTheBox
- Throwback Network - TryHackMe