Ajoy A G

Offensive Security Researcher | Junior Penetration Tester | Red Team Operator

Hosur, Tamil Nadu, India

📱 +91 6379243495 | ✉ ajoyag06@gmail.com | Portfolio | Github | LinkedIn

Professional Summary

I'm Ajoy A G (aka 0xprowl3r), a Junior Penetration Tester and Red Team Operator focused on offensive security, vulnerability research and exploit development. I work across web, API and internal network security, combining manual exploitation, automated recon and adversary simulation to uncover the weaknesses that scanners often miss.

I've built custom tools for recon, privilege escalation and post-exploitation, and I've disclosed real-world vulnerabilities through bug bounty and responsible disclosure programs. CTFs and lab-based red team exercises continue to sharpen my offensive problem-solving mindset.

I'm especially interested in red team tradecraft, exploit automation and the convergence of digital and physical attack surfaces.

Currently exploring opportunities in Red Teaming, Penetration Testing and Security Research.

Experience

HackerOne

India

Bug Bounty Hunter *07/2025 -*

- Discovered and reported **5 verified vulnerabilities** across web & API programs.
- Used Burp Suite, Nuclei & custom recon scripts to map targets and validate findings.

Mahindra University

Hyderabad

IDOR Vulnerability Disclosure (Independent Project) *07/2025 - 07/2025*

- Identified **critical IDOR exposing personal data of 1,000+ students** in university ERP.
- Authored technical report & SOP; disclosure adopted for future security audits.

Tata Electronics

Hosur

Information Security Intern *06/2025 - 07/2025*

- Built PowerShell-based audit automation tool for 1,000+ systems ▯ **90% reduction in manual audit time (~150+ hrs/month saved)**.
- Performed VAPT on internal web apps; identified critical vulnerabilities (IDOR, XSS, outdated dependencies) with actionable remediation.
- Designed phishing simulation for 150+ employees; post-awareness training resulted in **35% reduction in phishing success rate**.
- Monitored endpoints via CrowdStrike and escalated confirmed threats.

Datacom

Datacom — Cybersecurity Job Simulation *02/2025 - 02/2025*

Practiced incident analysis, threat hunting & vulnerability management; drafted triage reports aligned with SOC procedures.

Education

Mahindra University

Bachelor of Technology - BTech *08/2023 - 06/2027*

Sishya School, Hosur

PCMC *06/2009 - 04/2023*

Skills

- Network Security
- Web Application Security
- Privilege escalation
- Burp Suite
- Nessus
- Nuclei
- Wireshark
- Python
- Bash
- Kali Linux
- Windows Server / Active Directory
- VirtualBox
- Chrome DevTools
- Bug Bounty
- Security Audits
- Email Security
- API Security
- Post-exploitation
- Attack surface mapping
- Nmap
- Metasploit
- Scapy
- SQLmap
- PowerShell
- Prompt Engineering
- Ubuntu
- VMware
- Crowdstrike Falcon
- Kali Linux
- Qualys
- Electronics Security
- OSINT

Projects

0xprowl3r Scepter — Logic-Based Vulnerability Discovery Engine

Built a tool to identify vulnerabilities missed by traditional scanners by prioritizing **context-aware fuzzing over signature scanning**.

- Discovered **4 critical and 4 high-severity vulnerabilities** (including logic abuse and SPA bypass) in secured environments.
- Developed an engine capable of detecting flaws in **business logic and complex SPA applications**.
- Implemented a **risk-based reporting methodology** to prevent severity misclassification and clearly demonstrate business impact.
  Outcome: Improved exploit chain visibility, reduced false negatives, and showcased adversarial simulation value in real-world remediation efforts.

PktLens — Network Packet Sniffer & Traffic Analyzer

Developed a **terminal-based packet sniffer** to gain real-time insights into network traffic.

- Monitors and resolves **IPs/domains in real-time**, tracking top 5 talkers and top 5 domains.
- Detects **NXDOMAIN spikes and suspicious traffic patterns**.
- Minimal and full-feature modes for both quick snapshots and deep monitoring.
  Stack: Python, Scapy, Rich.
  Outcome: Lightweight and fast dashboard enabling on-prem network visibility for analysts.

Phishing Awareness Simulation Platform

Designed and executed a phishing simulation campaign to evaluate employee security awareness.

- Built realistic phishing emails and landing pages mimicking real-world attacks.

- Captured and analyzed campaign telemetry to identify user risk groups.
- Delivered post-simulation awareness sessions with the IT/security team.
  Outcome: Identified a **25% click-through rate** initially; follow-up simulations after training resulted in a **30% reduction in phishing susceptibility**.

Security Audit Automation — Active Directory Environment

Script-based automation framework to collect system/user state from multiple machines across an AD environment.

- Eliminated repetitive manual auditing tasks and reduced operational overhead.
- Integrated retry logic and CSV export for offline analysis.
  Outcome: Automated security audits across an enterprise environment, supporting internal red-team/blue-team workflows.

Burp Suite DAST Deployment & Configuration

Implemented end-to-end setup of **Burp Suite DAST (Enterprise Edition)** for automated security testing as part of an internship project.

- Configured scan pipelines, reporting modules, and vulnerability tracking workflows.
- Demonstrated practical CI-friendly dynamic security testing capability.

Windows Remote C2 Using Discord

Security research project demonstrating how attackers can use Discord as a **covert C2 channel** to remotely execute commands on compromised systems.
Goal: Raise awareness on double-use risks of trusted productivity platforms for cyberattacks.

Breaking Secure Web Gateway (SWG) with Last Mile Reassembly Attacks (LMRA)

Developed a simulation based on SquareX research to demonstrate how **Secure Web Gateways can be bypassed using LMRA** via dynamic UI manipulation.
Purpose: Educational project to help defensive teams understand SWG weaknesses and resilience improvements.