

SHREYAS KALYANI

Cybersecurity | Bug Bounty Hunter | Penetration Tester (Android, iOS & Web).

PROFILE SUMMARY

Cybersecurity professional with a strong foundation in Web & Application Security, specializing in OWASP Top 10 vulnerabilities (XSS, SQLi, SSRF, CSRF, CORS, HHI) and offensive security techniques using tools such as Burp Suite, Metasploit, SQLmap, and Nmap. Proficient in Red Team operations, including social engineering, phishing simulations, OSINT, and privilege escalation, to identify and mitigate threats proactively.

Experienced in threat detection, incident response, and system hardening through real-time monitoring and SIEM tools. Adept at collaborating with developers and IT teams to embed security into the software development lifecycle (SDLC). Knowledgeable in the MITRE ATT&CK framework, leveraging adversary TTPs for effective security assessments. Actively engaged in the cybersecurity community through bug bounty programs (HackerOne, Bugcrowd) and CTF platforms (TryHackMe, Hack The Box), continually refining both offensive and defensive security skills.

WORK EXPERIENCE

- Conducted comprehensive web application security assessments, identifying and mitigating vulnerabilities such as XSS, SQLi, SSRF, CSRF, and CORS.
 - Utilized Burp Suite Professional for penetration testing, payload analysis, and vulnerability exploitation to enhance overall security posture.
 - Performed both manual and automated security testing to uncover weaknesses beyond standard scanning methods, strengthening application resilience.
 - Developed proactive security strategies to mitigate potential cyber threats, reducing the risk of exploitation and data breaches.
 - Collaborated with cross-functional teams, including developers and IT, to integrate security best practices into the Software Development Lifecycle (SDLC).
 - Provided actionable security insights and recommendations to support risk management and ensure compliance with cybersecurity standards.
 - Leveraged tools such as Nmap, OWASP ZAP, Nikto, and Nessus for continuous security monitoring and network vulnerability assessments.
 - Monitored security logs, analyzed intrusion detection alerts, and supported incident response activities to enhance threat detection and mitigation.
-

CORE COMPETENCIES

- Penetration Testing and Ethical Hacking.
- Vulnerability Assessment & Risk Mitigation.
- Threat Intelligence & Incident Response.
- Red Teaming & Offensive Security.
- Web Application & Network Security.

- Security Audits & Cyber Risk Management.
 - SIEM, Log Analysis, and Forensics.
 - Bug Bounty & Exploit Development.
 - Security Awareness.
 - Cross-Functional Collaboration.
-

TECHNICAL SKILLS

- Web & Network Security: OWASP Top10 (XSS, SQLi, CSRF, SSRF, CORS, HHI, IDOR), Web Application Security, Network Security, Secure Coding Practices, Firewall & IDS/IPS Configuration, Zero Trust Security.
 - Security Tools & Exploitation Frameworks: BurpSuite, Metasploit, SQLmap, Nmap, Nikto, Acunetix, Zaproxy and the MITRE ATT&CK framework.
 - CTF & Bug Bounty: Capture The Flag (CTF), (TryHackMe, HackTheBox), Bug Bounty (HackerOne, Bugcrowd) Exploit Development.
 - Network and Communication: Nmap, Nikto, Nessus, Msfconsole, Bindshell, Reverseshell, DoS and DDoS.
-


EDUCATION & CERTIFICATION

- 2021 -2022 - EDUCATION (10TH) GOVT- BOYS HIGH SCHOOL ANDJR.COMP GULEDGUDD.
 - 2022-2024 - Government Industrial Training Institute, Guledgudda Education Is:- Electrician Trade.
 - Certified Ethical Hacker(CEH), (Registration No: WS/2024/1/15043).
 - Certified Penetration Tester by WsCubeTech, (Registration No: WS/2025/1/35197).
-

CONTACT DETAILS

✉ shreyaskalyani53@gmail.com

☎ 91+ 8317437885

 www.linkedin.com/in/shreyas-kalyani-cybersecurity

PERSONAL DETAILS

- Date of Birth: 29-08-2006
- Languages Known: Kannada and Hindi
- Address: Guledudda, Bagalkot, Karnataka