Aman Raj

7274017051 | iamanraj28@gmail.com | linkedin.com/in/amanraj28 | irainsec.github.io

Cybersecurity professional with experience in web and network penetration testing, source code reviews, and security tool development. Proven ability to identify and remediate vulnerabilities using industry-standard tools and methodologies. Looking to leverage technical expertise in a challenging security analyst role.

EXPERIENCE

Security Consultant Feb 2024 – Present

Altisec Technologies Pvt. Ltd. *Pune, Maharashtra*

- Web VAPT: Conducted penetration testing on web apps using Burp Suite, OWASP ZAP, and Nikto, identifying and exploiting vulnerabilities like SQLi, XSS, and CSRF. Provided detailed reports and risk assessments and remediation guidance based on OWASP Top 10.
- Network VAPT: Led network vulnerability assessments, using tools like Nmap, Nessus, and Metasploit to map networks, detect misconfigurations, identify open ports, and exploit vulnerabilities such as weak encryption, privilege escalation, and unpatched services to simulate real-world attacks.
- Source Code Review: Performed static code analysis with SonarQube, identifying security flaws like hardcoded secrets and improper error handling. Collaborated with dev teams to implement secure coding practices and reduce vulnerabilities.

Intern/Associate Consultant Oct 2023 – Feb 2024

CyberFrat *Dehradun, Uttarakhand*

- Assisted in developing a phishing simulation tool to create realistic attack scenarios for security awareness training
- Conducted testing and quality assurance, identifying bugs and ensuring tool functionality.
- Executed phishing campaigns targeting fellow students to assess awareness and improve phishing defense strategies

Cyber Security Trainee Aug 2023 – Feb 2024

Cyber Shikshaa *Dehradun, Uttarakhand*

- Assisted in conducting network and web app assessments using tools like Nmap, Nessus, and OpenVAS to identify vulnerabilities.
- Supported penetration testing efforts using Metasploit and Burp Suite to exploit vulnerabilities in test environments.
- Helped design and execute phishing campaigns using GoPhish to evaluate user awareness and security practices.
- Configured security tools for vulnerability scanning, reporting, and risk analysis.
- Participated in exploiting vulnerabilities and assessing risk severity to provide actionable recommendations.
- Contributed to generating detailed technical reports with findings, risk levels, and remediation steps.

PROJECTS

Malware Development | *Batchfile* July 2024 – Present

- Developed malware leveraging socat to bypass various solutions by establishing secure, encrypted communication channels for data exfiltration and reverse shell access.
- Employed evasion techniques such as dynamic payload delivery and traffic obfuscation using socat to avoid detection by traditional antivirus and security monitoring systems.
- Tested and refined the malware under controlled environments to ensure successful evasion of signature-based and behavioral detection methods, enhancing stealth capabilities against security tools.

Personal multitool | *Python, Batchfile* May 2024 – Present

- Developed a multifunctional tool for malware development, reverse shell creation, and network listening, streamlining penetration testing and exploitation tasks.
- Integrated reverse shell functionality to enable remote system control and facilitate post-exploitation activities in controlled testing environments.

PCST - Phishing Control Simulation Tool | *Go, JavaScript, HTML* Oct 2023 – Feb 2024

- Built a phishing simulation tool to replicate various phishing attacks (email spoofing, URL redirection, fake login pages) for testing security awareness.
- Developed automated reporting features to track user responses, identify vulnerabilities, and generate detailed analytics for improvement.
- Created customizable scenarios for different phishing techniques, enabling organizations to assess and strengthen their security defenses.

CERTIFICATIONS

- Ethical hacking Essentials (EHE) Certified by EC-Council.
- CISCO Networkings.
- SQL Injection Attacks by EC-Council.
- VAPT : Importance & Benefits for Securing Organizations from Cyberattacks by CyberFrat.
- Cybersecurity Workshop by Slog Solutions.

EDUCATION

Shivalik College of Engineering Dehradun, Uttarakhand
Bachelors of Technology in Computer Science *2020 – 2024*

TECHNICAL SKILLS

Penetration Testing Tools: Burp Suite, OWASP ZAP, Nikto, Metasploit, Acunetix, Kali Linux
Networks Scanning and Exploitation: Nmap, Nessus, OpenVAS, Wireshark, Netcat, Hydra, Aircrack-ng, tcpdump, Ettercap, Hping3
Web Application Security: OWASP Top 10, SQL Injection, XSS, CSRF, IDOR, Insecure Deserialization
Security Testing Methodologies: Black-box testing, White-box testing, Gray-box testing, Social Engineering