Greejith K

Kerala | greejithmiui12@gmail.com | 9809930419 | www.greejith.in | linkedin.com/in/greejith-k-64b28a241
github.com/Greejith-k

About

Cybersecurity / Penetration Testing Professional with 2+ years of hands-on experience conducting comprehensive security assessments across Web Applications, APIs, IoT, OT/SCADA, Networks, Infrastructure, Malware analysis, and Active Directory. Proven track record of delivering end-to-end penetration testing engagements for government, healthcare, finance, defense, and education sectors. Backed by 5+ years of continuous independent research and self-driven learning in offensive security, vulnerability research, and emerging threats.

Achievement

- Recognized in multiple Hall of Fame acknowledgments across leading organizations, including Zoho, Bosch, and others.
- Earned **2**0+ security bounties, demonstrating strong vulnerability research and exploit-finding skills.
- Successfully conducted penetration testing on India's top 3 power plants, strengthening critical ICS infrastructure security.

Experience

Cyber Security Analyst - Mirox Cyber Security and Technology PVT LTD, Technopark, Trivandrum, Kerala — Jan 2024– Ongoing

- Conducted web application and API penetration testing for government and private sector clients, identifying critical vulnerabilities and collaborating with development teams to implement OWASP-recommended secure coding practices.
- Performed comprehensive IoT and embedded device security assessments, including firmware and U-Boot analysis, reverse engineering of custom binaries, and configuration hardening reviews across routers, switches, firewalls, PLCs, ICS systems, servers, and other networked devices, covering hardware, firmware, and network-level attack surfaces.
- Performed comprehensive network and infrastructure audits for multiple organizations, including India's leading healthcare provider and provident fund, assessing security posture across diverse sectors and critical infrastructures.
- Conducted comprehensive threat hunting and performed both static and dynamic malware analysis for large-scale organizations, supporting rapid detection, investigation, and remediation of advanced threats.
- Submitted detailed proofs of concept (PoCs) and vulnerability details, including vulnerable endpoints, parameters, remediation impact, and reference links to the reporting team for further documentation and client communication.

Tools And Expertise

- **Web Security Testing** : OWASP Top 10 vulnerability assessment, manual and automated penetration testing, and comprehensive API security evaluations. Proficient with industry-standard tools including Burp Suite, SQLMap, OWASP ZAP, Gobuster, Nmap, Wfuzz, and Postman. Experienced in source code review.
- **Embedded Device Security Testing Expertise** : Hands-on experience assessing embedded systems using UART, SPI, I^2C, JTAG, CAN, Modbus. Skilled in Bootloader analysis, firmware extraction and reverse engineering, OTA update security, working with OpenWrt and Embedded Linux environments. Proficient with Binwalk, Firmadyne, Ghidra, IDA Pro, QEMU, and FAT
- **Networking and Infrastructure Security** : Perform vulnerability assessments and penetration testing (VAPT), configuration and architecture reviews, network segmentation assessments, firewall and IDS/IPS evaluations, VLAN and routing analysis, Wi-Fi security testing, traffic inspection. Proficient with Nmap, Wireshark, Tcpdump, Nessus, OpenVAS, Metasploit, Netcat

- **ICS/SCADA Security Testing** : OT network assessments, PLC/RTU security reviews, SCADA architecture evaluation, protocol analysis (Modbus, Profibus), ICS firewall and switch configuration audits, HMI security testing, asset discovery, OT threat hunting, with hands-on exposure to Siemens, ABB, and Allen-Bradley PLC ecosystems, using tools such as Wireshark, Tcpdump, PLC scanning utilities, Nmap, and industrial control system assessment frameworks.
- **Active Directory** : Performed Active Directory security assessments including domain enumeration, GPO and privilege review, Kerberos/NTLM analysis, password policy auditing, AD misconfiguration detection, and lateral movement identification using tools such as BloodHound, CrackMapExec, Rubeus, Impacket, and other AD auditing frameworks.
- **Configuration Review** : Conduct security configuration assessments and hardening for network switches, routers, firewalls, ICS switches and firewalls, PLCs, servers, desktops, and IoT devices to identify misconfigurations, enforce security baselines
- **Malware Analysis** : Static and dynamic analysis, memory forensics, behavioral profiling, and incident investigation, with proficiency in tools such as Velociraptor, YARA, Autoruns, FLARE VM, REMnux, Volatility, and MemProcFS

Projects

ARP SPOOFER Link

- Powerful and flexible ARP spoofing toolkit GUI. Designed for network penetration testing,

KEY LOGGER Link

- Advanced keylogger in Python capable of capturing keystrokes and collecting browsing history.

BATXSS Link

- Advanced Reflected XSS Finding Tool with 100% Accurate Rendering-Based Detection

Education

- Bachelor of Computer Applications 2023-Ongoing Final Year (Amrita Vishwa Vidyapeetham) - Online mode
- Higher Secondary 2017 - 2019 (Sree Krishna Higher Secondary School)
- SSLC 2016 - 2017 (Sree Krishna Higher Secondary School)

Certification

- CCNA (CISCO)
- CC (ISC2)
- 210W-07 ICS (Cybersecurity and Infrastructure Security Agency)
- Fortinet Certified Associate Cybersecurity (Fortinet)
- Certified Social Engineering Defense Practitioner (CSEDP)
- Python Essentials 1 and 2 (CISCO)
- Certified Cybersecurity Educator Professional (CCEP) (Red Team Leaders)