Muhammad Nur Irsyad

nurirsyad.naser@gmail.com • github.com/monsieurDuke • linkedin.com/in/muhammadnurirsyad

EDUCATIONS

Jakarta State Polytechnic *Depok, West Java*
Bachelor of Applied Science in Informatics *Jun 2018 – Jan 2023*
Major in Networking & Multimedia; Minor in Information & System Security
GPA: 3.58/4.0

Center for Computing and Information Technology - University of Indonesia *Depok, West Java*
Professional Certificate in Network and System Administration *Jun 2018 – Jun 2020*
In Association with Cisco Networking Academy Training
GPA: 3.34/4.0

TECHNICAL SKILLS

Burp Suite • Wireshark • Level-of-Detail • Secure Coding Practice • Risk Assessment • Vulnerability Management • Report Writing • Network Administration • Network Security • Penetration Testing • Scripting & Automation • REST API • HTML/CSS/JavaScript • Python • Java • Go • SQL/RDBMS • Linux • Git • Docker

CERTIFICATIONS

- **BNSP** Junior Cyber Security Specialist; Junior Network Administrator
- **Cisco** Networking Academy Training Completion
- **CompTIA** Security+; Linux+
- **EC-Council** Certified Application Security Engineer (CASE) - Java
- **Google** IT Support; Cybersecurity (Assets, Threats, and Vulnerabilities)
- **NIIT** HIT Software Engineering

INTERNSHIP EXPERIENCE

Automate All *(Robotic Process Automation Start-up)* *Bandung, West Java*
Software Security Developer Intern *Oct 2021 – Dec 2021*

- Performed security testing on development-stage REST API using OWASP Testing Guide while following the Non-Disclosure Agreement on the testing capabilities and the information that are being fetched
- Mapped founded vulnerabilities with CVSS to give a proper based environment threat & risk analysis
- Constructed a technical report alongside its appropriate recommendation that is suitable for the technology that's being used, which is passed to be discussed with the Backend Developer

HONOR

2nd - Red Team Cyber Range *(InfraDigital Foundation)* *South Jakarta, DKI Jakarta*
Team Leader - Red Teaming *Jan 2023 – May 2023*

- Organized a 5-man team on building a Cyber Range alongside a fully-structured executive summary
- Solved undocumented End-of-Life service policy by CentOS Web Panel in an injury time before the final presentation by reverting the system clock, resulting in continuing the work in parallel to finish the overall project in time with excellent outcome while still till have rooms for improvement.

PROJECTS

CVE-2022-44877 - CentOS Web Panel Vulnerability Analysis ↗ *Feb 2023 – Apr 2023*
Bash; Go; Apache ModSecurity WAF; Mikrotik; PTES; OWASP Web Security Testing Guide

- Developed an exploit tool that integrated seamlessly with REST API to perform advanced & modular TTP
- Performed a full-phase penetration testing based on PTES, which included threat modeling, using an attack tree, to the post-exploitation, such as bypassing the firewall to installing a dynamic reverse shell backdoor
- Designed a functional defense & detection mechanism from the application-level to its network that accomplished by using ModSecurity WAF, File Integrity Monitoring, and traffic management in Mikrotik

CVE-2021-44228 - Log4Shell Vulnerability Analysis *(Thesis)* ↗ *Mar 2022 – Jan 2023*
Bash; Java; Go; Arduino; OpenLDAP; Apache Log4j; BadUSB; PTES

- Developed a Proof-of-Concept on integrating Log4Shell vulnerability into a BadUSB device to build a service-based Remote Access Trojan with a 100% false negative rate on 3 different tested physical systems
- Built a curated payload and a central config via REST API, which makes all the modern Linux system that at least have Java 8 installed in any build-version of it, is fully exploitable and capable on achieving multiple remote access simultaneously via a simple HTTP request