CHARNYL ADARO

DIGITAL SECURITY ENGINEER

CONTACT

+639055667864

charnyladaro@gmail.com

https://charnyladaro.github.io/portfolio

Calamba, Laguna Ph.

EXPERTISE

- Vulnerability Assessment
- API Security Testing
- Scripting Languages
- Operating systems knowledge
- Penetration Testing
- Data Leakage Prevention
- Amazon Web Services
- Python Programming
- Web development projects
- PHP Programming
- Multilingual Abilities
- Cybersecurity knowledge

TOOLS

- Kali Linux
- Parrot Os
- Owasp Zap
- BurpSuite
- VEX
- Nmap
- Metasploit

CERTIFICATIONS

Verified Ethical Hacker (IBM) - April 12, 2024

ISC2 candidate(cybersecurity certification) - ISC2- April 2024

LANGUAGE

- English
- Japanese
- Tagalog

WORK EXPERIENCE

Bilingual - Digital Security Engineer

TMJPBPO Services Inc — November 2021 - Current

- Conduct Security Assessments: Performed comprehensive penetration tests on web applications, networks, and systems to identify security vulnerabilities.
- Vulnerability Analysis: Analyzed and interpreted security test results to determine the risk levels and potential impact of discovered vulnerabilities.
- Exploitation and Testing: Utilized advanced tools and techniques to exploit vulnerabilities, demonstrating potential attack paths and methods.
- Documentation and Reporting: Created detailed reports of findings, including the nature of vulnerabilities, potential impact, reproduction steps, and recommendations for remediation.
- Collaboration with Stakeholders: Worked closely with development and IT teams to explain findings, verify fixes, and provide guidance on remediation.
- Continuous Improvement: Stayed updated on the latest security threats, trends, and technologies to enhance testing methodologies and tools.
- Security Awareness: Assisted in developing and delivering security awareness training for employees to promote a culture of security within the organization.

Bug Bounty Hunter

HackerOne — April 2024 - Current

- Conducted Vulnerability Research: Performed in-depth research to identify security vulnerabilities in various web applications, mobile apps, and network systems.
- Executed Penetration Testing: Utilized a range of tools and techniques, such as Burp Suite, Nmap, and Wireshark, to test and exploit potential security flaws.
- Reported Findings: Documented vulnerabilities with detailed reports, including the nature of the issue, potential impact, steps to reproduce, and recommended remediation.
- Collaborated with Teams: Worked with development and security teams to verify, validate, and address reported vulnerabilities, ensuring timely and effective remediation.
- Maintained Ethical Standards: Adhered to ethical guidelines and legal requirements while performing security testing, ensuring responsible disclosure of vulnerabilities.
- Enhanced Skills: Continuously updated knowledge of the latest security threats, vulnerabilities, and attack vectors. Participated in security communities and ongoing learning.

Freelance Web Developer

Freelance — July 2018 - Current

- Client Communication: Maintained ongoing communication with clients throughout the development process to ensure project requirements and expectations were met.
- Continuous Learning: Stayed current with emerging trends and technologies in web development through continuous learning opportunities, ensuring the application of the latest best practices.
- Utilization of Modern Technologies: Applied modern web technologies such as HTML5, CSS3, and responsive design techniques to create dynamic and visually appealing web applications.