Toyin Ayanleye

ayanleyetoyin@outlook.com nulcell.github.io

SKILLS & INTERESTS

- **Skills:** Python; Bash; C; C++; JavaScript; SQL; NoSQL; Information & Network Security; Web Application Security; Vulnerability Assessment; Application Security Automation; AWS, CI/CD; CloudFormation; Linux; Kibana; Docker; Burp Suite Pro; Metasploit; Wireshark; Nessus; Postman; Git; DAST; SAST; OWASP Top 10; SANS Top 20; Vulnerability Remediation; Bug Bounty; Raspberry Pi; API Testing; Unit & Integration Testing; Scrum; Agile; Jira; Confluence; Stack Overflow (ctrl+c - ctrl+v)
- **Interests:** Gaming (largely esports titles); Movies; Music; Reddit

WORK EXPERIENCE

AMMP Technologies B.V. **Jun. 2022 – Present**

Data Engineer *Amsterdam, NL*

- Led the management and maintenance of AWS-based data services and CI/CD pipelines using GitHub Actions and CodePipeline
- Developed and maintained a suite of Python libraries for internal applications and led data integrations with external APIs and data analysis tools
- Conducted frequent log analysis to identify system states and potential areas for optimization, resulting in increased efficiency and cost savings
- Implemented security checks into the CI/CD pipelines of core services, specifically our API, resulting in the identification and fixing of major security issues within our applications
- Reduced AWS ECS cost by improving memory management, reducing compute waste, and migrating to ARM64 compute, resulting in a significant reduction in our infrastructure expenses

HackerOne **Apr. 2022 – Present**

Bug Bounty Hunter *Remote*

- Conducted thorough analysis of frontend JavaScript to steal user credentials and API keys through a MITM attack due to a misconfigured login functionality
- Successfully discovered and exploited XXE & SSRF vulnerabilities within a Java application to steal AWS access keys in a compute cluster by testing the API's handling of non-JSON input data
- Uncovered leaked API keys in live and archived pages, leading to complete control of all customer accounts and resulting in a significant payout through the bug bounty program
- Collaborated with a team of highly skilled bug bounty hunters to test and secure a variety of web applications

Tereta **Mar. 2022 – Apr. 2022**

Cybersecurity Analyst *Florida, US*

- Provided expert consultation on penetration tests for a range of clients in various industries
- Assisted with PCI DSS v4 compliance checks for clients, ensuring their payment systems were secure and compliant
- Conducted comprehensive vulnerability assessments and proposed effective remediation strategies to secure clients' systems and data

Security Contractor **Dec. 2021 – Mar. 2022**

Application Security Engineer *Remote*

- Discovered exposed /.git directories via direct IP address access and successfully dumped source code, leading to the identification of multiple vulnerabilities during analysis
- Exploited leaked credentials to gain code execution through a successful phpMyAdmin SQL injection attack,

allowing me to compromise other domains hosted on the server
- Compromised an insurance admin portal containing sensitive client data through the exploitation of misconfigured redirects and IDORs
- Discovered and exploited SQL injection and SSRF vulnerabilities, exposing internal systems and information of a major Nigerian government organization
- Accessed the WordPress Admin page through the reuse of passwords and weak credentials, then gaining code execution by uploading a malicious WordPress plugin, leading to the identification of multiple vulnerabilities when analyzing the source code on the server

Projects

Application Security Audit Service
Private (for now) and under active development
- Building an innovative AWS-hosted SaaS application to automate the tedious process of reconnaissance, enumeration, testing, exploitation, and reporting of common and unusual vulnerabilities in web applications, networks, and cloud infrastructure
- Constantly improving and expanding the capabilities of the tool through ongoing development
- Initial funding provided by AWS after a successful proposal

Bug Bounty Recon Script
Open source
- Developed highly efficient Python and Bash scripts to streamline the initial recon phase of bug bounty hunting and identify quick wins on live and archived pages
- Optimized the script to run smoothly on a VPS, saving time and physical resources

Security Tools Install Script
Open source
- Created a quick and easy script to set up any Linux VPS or virtual machine with a comprehensive suite of essential tools for application security and penetration testing, simplifying the setup process and saving valuable time

EDUCATION

University of Ibadan
BSc, Electrical and Electronics Engineering *Oyo, NG*
- Cybersecurity Lead of the Google Developer Student Club chapter

ACTIVITIES

M4xH3dr00m **Jun. 2021 – Present**
Team Member *Oyo, NG*
- Group of CTF players, ethical hackers, and cybersecurity professionals

AWARDS

Cybersecurity Hackathon **2021**
American Business Council
Nigerian National Cyber Security CTF **2021**
CyberTalents