Aiman Sam

Jr Penetration Tester

Aspiring cybersecurity professional with hands-on CTF experience and full-stack development skills. Ranked top 1% on TryHackMe and passionate about offensive security and automation.

CONTACT

Phone: +601137476496
Email: aimansammrsm@gmail.com
Linkedin: www.linkedin.com/in/aimansam
TryHackMe: https://tryhackme.com/p/zx10r

ACHIEVEMENT & PARTICIPATION

Bingo CTF 2025 | 3th Place

- Leading team score by solving advanced web exploitation, cryptography, and forensics challenges under time pressure.
- Collaborated with a 3-member team to figure the best idea to solve challenges
- Ranked among the top 3 out of 50 teams

TryHackMe | Top 1% Global Rank | 44th Malaysia Rank

- Completed over 350 rooms on penetration testing, web exploitation, and network-exploitation.
- Earned multiple learning paths including Jr. Penetration Tester and Pre Security.
- Documenting vulnerability assessment and report writing to simulate real-world pentesting.

MCMC Intervarsity Cyber Forensics Challenge 2025 Finalist | Top 10

- Demonstrated hands-on skills in digital forensics, incident analysis, and evidence handling under time-constrained scenarios.
- Applied forensic techniques including memory analysis, log analysis, file system forensics, and malware investigation.
- Collaborated in a team to analyze cyber incidents and present findings with clear technical justification.

Head of Technical Team & Challlenge Creator Codequest Coalition 2025

- Led the technical team in organizing and executing a large-scale university coding competition using the HackerRank platform
- Managed end-to-end challenge lifecycle, including creation, testing, deployment, and real-time troubleshooting during the event
- Ensured platform stability and fairness by monitoring submissions, preventing exploitation, and maintaining competition integrity

Challenge Creator DIV:IDE CTF 2026

- Designed and developed 7 Web Exploitation challenges and 1 Boot2Root machine, covering vulnerabilities such as SQL Injection (SQLite), Local File Inclusion (LFI), IDOR, and logic flaws
- Engineered and deployed scalable CTF infrastructure on Google Cloud Platform (Cloud Run & Compute Engine)
- Implemented secure architecture using Cloudflare tunneling to protect exposed services and reduce attack surface
- Integrated GitHub-based CI/CD workflow for efficient challenge deployment, updates, and version control

Speaker DIV:IDE Academy 2026

- Delivered a technical session titled "From URL to FLAG: Exploiting Your First Website" to introduce participants to web exploitation fundamentals
- Demonstrated hands-on techniques for identifying and exploiting common web vulnerabilities, including SQL Injection, LFI, and IDOR
- Translated complex cybersecurity concepts into clear, beginner-friendly explanations for improved audience understanding
- Showcased real-world attack scenarios to simulate industry-relevant web security challenges

Speaker Hack@10 CTF – DIV:IDE Academy 2026

- Conducted a live workshop "Click, Inject, Own – Web Exploitation Essentials" as part of International Hack@10 CTF preparation, focusing on beginner to intermediate web security skills.
- Introduced a structured CTF methodology for approaching and solving web exploitation challenges
- Demonstrated real-time analysis and manipulation of HTTP traffic using Burp Suite
- Explained common attack vectors such as injection flaws, access control issues, and input validation weaknesses through practical examples
- Designed interactive learning segments to help participants transition from theory to hands-on exploitation

Challenge Creator - International Hack@10 CTF 2026

- Designed and developed 2 web exploitation challenges focused on NoSQL Injection and JWT authentication bypass (pac4j-jwt vulnerability CVE-2026-29000)
- Engineered a vulnerable authentication system to demonstrate token manipulation and access control bypass techniques
- Conducted internal testing and created solution paths to validate exploitability and learning outcomes
- Enhanced participants' understanding of modern web security flaws through practical, scenario-based challenges

SKILLS

Cybersecurity

- Penetration Testing
- Network Security
- Web Exploitation (SQLi, XSS, LFI/RFI)
- Access Control Management
- Active Directory exploitation

Web Development

- HTML
- CSS
- React
- Javascript
- Next JS
- Node JS
- Postgresql
- MongoDB
- Flask
- SQLite

Scripting

- Python
- Bash

EDUCATION

Universiti Tenaga Nasional | October 2024 - October 2027

Bachelor of Computer Science (Cybersecurity)

- GPA: 3.80

CERTIFICATES

Certified Ethical Hacker (CEHv13) - EC Council

CCNA: Introduction to Networks - Cisco

Junior Penetration Tester - TryHackMe

Full-Stack Web Development Bootcamp - Udemy
HTML, CSS, JS, NextJS, React, Postgresql, MongoDB

Python & Bash for Ethical Hackers - Udemy