Ahmed "AHZ" Sinada

Sharg En Nile, Khartoum, Sudan
Website: https://ahzsec.github.io

Education

Sudan University, School of electrical and nuclear engineering — *2017- 2023*
B.Eng. Electrical Engineering (Control)

Technologies and Programming Languages

Programming Languages: C/C++, x86 Assembly, Solidity, JavaScript, Python, BASH, PHP, JAVA

Technologies: EVM, Smart contracts (across the stack), Nodejs, Express.js, Apollo, Pandas, Pyomo, API's (REST, GraphQL), Git, Burp Suite

Database Systems: MySQL, PostgreSQL, MongoDB

Skills: Penetration Testing, Application Security, Modern Cryptography, Optimization, Security and Vulnerability Assessment, Market profile and Order flow.

Work in progress: Rust, Golang, Typescript, Yul, Convex Optimization. *(Always learning, Can't stop)*

Summary

- Over 4 Years of Professional experience in Application Security, Penetration Testing, Designing reviews, Threat modeling, Security and Vulnerability Assessment of internal applications and external third-party applications identifying vulnerabilities and security defects using leading industry standards such PortSwigger, OWASP and ConsenSys.
- Over 4 Years of Professional experience in building per-formant & high-assurance software across the stack and technologies.
- Developed serious internal automation scripts for security assessment and penetration testing (blackbox, greybox & whitebox) methodologies.
- Hands-on experience in reviewing and defining requirements for Application Security solutions and mitigation techniques.
- Skilled in performing both manual and automated security testing for Web, Mobile applications and Smart contracts.
- Experienced in modern cryptography and hashing algorithms.
- Strong Experience in Security Checks, Vulnerability management for Open Application Systems and Middleware applications.
- Experienced in conducting both internal and external techniques based on partners' specifications.
- Well-versed with performing source code review (JavaScript, Solidity, Python, PHP) to find and patch the overlooked flaws through the different phases of development.
- Experienced in performing analysis of the source code review and penetration testing conclusions to identify the immediate risks and vulnerabilities.
- Generated and presented reports on Security Vulnerabilities to both internal and external partners.
- Good team player with excellent analytical, inter-personal, communication and written skills, problem-solving and trouble-shooting capabilities. Highly motivated and can adapt to work in any new environment.
- Ready to adapt and master new solutions and technologies across the stack and the business models.

Projects and Softwares

Phalanx: Automated weapon for penetration testers

Multi-stage penetration testing weapon for automating the security and vulnerability assessment process and the penetration testing methodologies.

- Black, Grey and White box.
- Reconnaissance & Scanning.
- Analysis & Exploitation.
- External, Internal, Blind & Double-blind testing.

Phalanx API: A data transferrer and collector for penetration testers

A pipeline for collecting and transferring the security and vulnerability assessment process data for analysis.

- Automate collecting and transferring.
- Data analysis.
- Workflow integration.
- Middle-stage immediate availability.

Publications and Write-ups

Demystifying Solidity Wargames: Smarx's capture the ether.
Ahmed "AHZ" Sinada, *2021.*

Demystifying Solidity Wargames: Openzeppelin's ethernaut.
Ahmed "AHZ" Sinada, *2021.*

THE GRINCH NETWORKS IS DOWN!.
Ahmed "AHZ" Sinada, *2021.*

Chaining vulnerabilities leads to account takeover.
Ahmed "AHZ" Sinada.
InfoSec Write-ups, 2020.

Bypassing OTP via reset password.
Ahmed "AHZ" Sinada.
InfoSec Write-ups, 2020.

Honors and Awards

HackerOne's Hackyholidays 2020-2021 Winner *2021*

After 28 days of non-stop hacking, and with over 100 hackers from all over the world, I was announced as the winner of HackerOne's Hackyholidays of 2020-2021.

- Security assessment.
- Penetration testing.
- Blackbox testing.
- Source code review.
- Cryptography assessment.
- Reconnaissance & Exploitation.

Challenges AND EVENTS

HackerOne's h1-2103 Participant

2021

Participated with the top 50 hackers from all over the world in securing Amazon's high, medium and low level private and public infrastructure, Maintaining full security and vulnerability assessment across Amazon's private subsidiaries and core assets and reviewing, auditing and performing analysis beyond the most critical Amazon's systems and middlewares.

The Climate Corporation Private Challenge Participant

2020

Participated in securing The Climate Corp critical routers, interfaces and APIs, Conducted security reviews across the multilevel multi-stack assets and subsidiaries, Utilized the products beyond the lack of documentations towards security assessment and responsibly disclosing serious flaws in the core infrastructure.

Work Experience

Intraday Trader 2022

- Market profile & Order flow.
- Enhancing predictive capability of new and existing models.
- Building research tools & applications for processing market and trading data.
- Developing in-depth understanding of the quantitative analysis process.

Bug Bounty Hunter, HackerOne 2020-2023

- Performed security and vulnerability assessment of various stack and technologies.
- Coordinated with development teams to ensure closure of reported vulnerabilities by demystifying the ease of exploitation and the impact.
- Collaborated with clients and company teams defining requirements for security and programs.
- Performed scoping engagements, vulnerability assessments, web penetration testing, mobile penetration testing.
- Access control and businesses logic testing to identify privilege escalation on various roles and ensuring the closure by overall framework implementation.
- Updated with the new hacking and latest vulnerabilities to ensure the security of the existing programs and systems.
- Participated in security architecture reviews to provide input on secure solutions.
- Analyzed applications codebase to identify potential vulnerabilities and developed solutions that mitigate the risk of exploitation.
- Provided technical expertise in identifying risks associated with new technologies or features.
- Worked with security product vendors to evaluate security, including product evaluations.
- Performed threat modeling, design reviews and penetration testing of internal web applications and external partner applications.