# Ahmed "ahz" Sinada

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

## Education

**Sudan University,** School of Electrical and Nuclear Engineering *2017 - 2023 (expected)*
B.Eng. Electrical Engineering (Control)

## Technologies and Programming Languages

**Programming Languages:** C/C++, x86 Assembly, Solidity, Javascript, Python, Golang, BASH, PHP, JAVA.

**Technologies:** EVM, Smart contracts (across the stack), Ethers.js, Web3.js, Ganache, Hardhat, Nodejs, Express.js, Apollo, Pandas, Pyomo, API (REST, GraphQL), Git, Burp Suite.

**Database Systems:** PostgreSQL, MySQL, MongoDB.

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

## Summary


- Over 4 Years of Professional experience in Application Security, Penetration Testing, Design 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.
- Over 4 Years of Professional experience in building per-formant & high-assurance software across the stack.
- Developed internal automation scripts for security assessment and penetration testing (black-box, Grey-box & white-box) 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 and Vulnerability management for Open Systems and Middle-ware applications.
- Experienced in conducting both internal and external techniques based on partners' specifications and presenting security vulnerabilities reports.
- Well-versed with performing source code review (Solidity, Javascript, Python) and identifying and patching the immediate risks, vulnerabilities and the overlooked flaws through the different phases of development.
- 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 environment.
- Ready to adapt and master new technologies and solutions across the stack and the business model.

## Publications and Write-ups

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

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

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

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

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

## Projects

**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 data for analysis.

- Automated collecting and transferring for data analysis.
- Workflow integration.
- Middle-stage immediate availability.

## 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.
- Black-box testing.
- Source code review.
- Cryptography assessment.
- Reconnaissance.

## 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 Amazon's most critical systems and middlewares.

**HackerOne's The Climate Corporation Private Challenge Participant** *2020*

Participated in securing The Climate Corp critical routers, interfaces and API's, 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 severe flaws in the core infrastructure.

## Work Experience

**Security Researcher,** HackerOne *2020 - present*

- Performed scoping engagements, security and vulnerability assessment, threat modeling, design reviews, penetration testing of internal applications and external partner applications, mobile applications penetration testing of various stack and technologies.
- Coordinated with teams to ensure the closure of reported vulnerabilities by demystifying the exploitations, impact and the recommended security patches.
- Collaborated with teams defining requirements for applications security.
- Analyzed codebase and identifying potential vulnerabilities, defining patches for mitigating exploitations and ensuring the overall framework implementation.
- Updated with the new techniques and latest vulnerabilities to ensure the security of the core applications and identifying risks associated with new technologies or features.
- Worked with products teams to evaluate security, including products and architecture evaluations.

**Intraday Trader,** AHZ Capital *2022 - present*

- Market profile.
- Auction Market Theory.
- Order Flow Strategies.
- Enhancing predictive capability of new and existing models.
- Researching tools & applications for processing markets and trading data.
- Developing in-depth understanding of the quantitative analysis process.