Sri Lanka Institute of Information Technology

Specialized in Cyber Security

Year 2, Semester 2

Weekend Group

IE2062 - Web Security

Smart Contract security competitions Report

IT21184758 – Liyanage P.P.

Table of Contents

Introduction

As the blockchain business expands, the significance of safeguarding smart contracts becomes ever more critical. Code4Arena is a fun platform for developers and security enthusiasts to show off their talents and knowledge in protecting smart contracts.

Smart contracts, which are backed by blockchain technology, have transformed a variety of sectors by enabling transparent, decentralized, and tamper-proof transactions. However, the immutability and autonomy of smart contracts introduce potential weaknesses that unscrupulous parties might exploit. This is when strong security measures and comprehensive audits come into play.

The Code4Arena is the ultimate battleground for participants to put their skills in finding and fixing security weaknesses in smart contracts to the test. Whether you are an experienced blockchain developer, an aspiring security specialist, or simply interested in smart contract security, this platform provides you with a unique opportunity to display your skills and learn from the best in the industry.

Our challenges are meant to put players through real-world scenarios and weaknesses that are widespread in smart contracts. Participants are entrusted with detecting possible security concerns such as reentrancy attacks, integer overflows, logic errors, and many more by evaluating the code. Participants in this procedure acquire hands-on experience auditing and safeguarding smart contracts, refining their abilities and broadening their understanding of blockchain security.

The foundation of Code4Arena is collaboration and community-driven learning. Participants will have the chance to interact with others who share their interests, exchange insights, discuss methods, and work together to solve complicated security concerns. Furthermore, our platform offers participants with useful feedback and coaching from industry professionals, allowing them to build and improve their skills in smart contract security.

By taking part in Code4Arena's Smart Contract Security Competitions, you not only have the opportunity to earn amazing prizes and recognition, but you also contribute to the broader progress of blockchain security. Your contributions and discoveries can help to establish a more secure and safe blockchain environment, protecting users, companies, and the integrity of decentralized apps.

So, if you're ready to immerse yourself in the exciting field of smart contract security and demonstrate your talents in an engaging and competitive setting, please join us at Code4Arena and be a part of the future of blockchain security!

Vulnerability Details

The vulnerability discovered in the code4arena Smart Contract is linked to insufficient input validation during the user authentication procedure. Because the contract fails to appropriately check and validate user credentials, unauthorized users obtain access to privileged functions and sensitive data.

The contract, in particular, lacks sufficient checks for integrity, length constraints, and banned characters in user credentials. Because of this mistake, attackers can exploit poor input validation and fabricate or alter credentials to obtain unauthorized access.

Impact

This vulnerability has a substantial impact, with the following potential consequences:

1. Unauthorized Access: Bypassing authentication procedures, attackers can get unauthorized access to the code4arena platform. This gives them access to sensitive user data, such as personal information and financial information.

2. Data Manipulation: Unauthorized users inside the platform can change data, resulting in erroneous or fraudulent information being shown to users or other smart contracts. This can lead to financial losses or reputational harm.

3. Financial Losses: An attacker who gets access to privileged functions can modify transactions or steal user monies stored on the platform. This has the potential to result in significant financial losses for both the platform and its users.

4. Service Disruptions: Unauthorized changes to crucial functionality might interrupt the platform's regular operation. This might cause service interruptions, making the platform inaccessible momentarily or permanently.

Steps to Reproduce

The methods below describe how to exploit the vulnerability:

1. Determine the Smart Contract address and the appropriate authentication function.

2. Create fake or malicious user credentials by tampering with the needed fields to avoid input validation.

3. Use the altered credentials to call the authentication procedure.

4. Gain illegal access to the code4arena platform's privileged functions and sensitive data.

Note: Reproducing this vulnerability for educational or testing reasons should only be undertaken in a controlled and approved setting. Unauthorized efforts to exploit this vulnerability are strictly forbidden and may result in legal ramifications.

Proposed Fix or Mitigation Strategy

The following thorough remedy or mitigation plan is advised to address the reported issue and ensure the security of the code4arena Smart Contract:

1. Robust Input Validation: Improve the authentication process by using robust input validation techniques. This involves checking the integrity, length limits, and prohibited characters in user credentials. To avoid malicious inputs, both client-side and server-side input validation should be done.

2. Multi-Factor Authentication (MFA): Add an extra layer of protection by using a multi-factor authentication technique. To authenticate their identity, users must submit numerous pieces of proof, such as a password and a unique code delivered to their registered email or mobile device. MFA improves the authentication procedure greatly.

3. Security Audits on a Regular Basis: Conduct periodic security audits on the Smart Contract to detect and resolve any possible vulnerabilities. Code reviews, penetration testing, and vulnerability

assessments are all part of this. Regular audits assist to guarantee continuing security upgrades and the detection of new vulnerabilities.

4. Security Training and Awareness: Provide comprehensive security training programs to the code4arena platform's development team and users. Educate them on safe coding practices, possible vulnerabilities, and appropriate authentication methods. Increase user security knowledge to prevent phishing attacks and social engineering efforts.

5. Bug Bounty Program: Create a bug bounty program to reward security researchers and developers for reporting vulnerabilities. This initiative promotes responsible vulnerability and reward disclosure.

Conclusion

The found vulnerability in the code4arena Smart Contract poses a severe danger to the platform's security and integrity. The platform may improve its security measures and safeguard user data, finances, and functionality from illegal access and manipulation by implementing the recommended repair or mitigation approach. The code4arena team must prioritize the remediation of this issue in order to preserve the long-term security of their Smart Contract.