TP 6: Smart Contract Security - 1 (180 minutes)

Smart Contract Security Workshop: Ethernaut Challenges

In this session, you will learn to analyze, exploit, and secure smart contracts by completing a series of challenges on **Ethernaut**, a gamified platform developed by OpenZeppelin. By interacting directly with contracts on a test blockchain, you will gain practical experience with common vulnerabilities and how to mitigate them.

By the end of this session, you will:

- Understand and exploit common vulnerabilities in Ethereum smart contracts.
- Learn how to interact with smart contracts using developer tools.
- Gain practical skills in debugging and securing Solidity code.

Cheating and looking for write ups on internet is prohibited.

Duration

180 minutes (approximately 20-30 minutes per challenge)

Setup

Before starting, ensure you have the following tools installed and configured:

1. **Metamask**: Connect to an Ethereum testnet or a local blockchain like Ganache.
    - Download: https://metamask.io/
2. **Remix IDE**: For analyzing and testing Solidity code.
    - Website: https://remix.ethereum.org/
3. **Ethernaut Platform**: Access Ethernaut at https://ethernaut.openzeppelin.com/.
4. **Infura or Alchemy Endpoint**: Optional, for connecting to Ethereum testnets.

Challenges Overview

You will attempt to solve 5-7 Ethernaut challenges during the session. Each challenge represents a real-world vulnerability, requiring you to think critically and interact with contracts using the developer console.

Challenges

1. Level 0: Hello Ethernaut (5-10 minutes)

- Objective: Set up your environment and complete the introductory level.
- Skills: Learn how to interact with the platform and understand the basics of contract interaction.

2. Level 1: Fallback (20 minutes)

- Objective: Gain ownership of a contract by exploiting its fallback function.
- Key Concepts: Fallback functions, contract ownership, sending Ether.

3. Level 2: Fallout (20 minutes)

- Objective: Claim ownership of a contract due to a constructor typo.
- Key Concepts: Constructors in Solidity, contract deployment.

4. Level 3: Token (30 minutes)

- Objective: Exploit a token contract to acquire an excessive balance.
- Key Concepts: Integer underflow/overflow, token balances.

5. Level 4: Delegation (30 minutes)

- Objective: Exploit a contract using delegatecall to hijack its ownership.
- Key Concepts: `delegatecall`, execution context, proxy patterns.

6. Level 5: Force (30 minutes)

- Objective: Force Ether into a contract that cannot receive it directly.
- Key Concepts: Contract destructors, transferring Ether without a fallback.

7. Level 6: Reentrancy(Bonus, 45 minutes)

- Objective: Exploit a reentrancy vulnerability to drain a contract's funds.
- Key Concepts: Reentrancy, contract security, modifiers.

Guidance and Rules

- **Read Carefully**: Each level includes hints and tips. Read the contract code provided thoroughly before making a move.
- **Use Developer Tools**: Leverage the browser console and Remix IDE for debugging and testing your solutions.
- **Collaborate and Learn**: If you're stuck, discuss strategies with peers or ask the instructor for additional hints. No outright solutions will be provided.

Assessment

- Completing at least 5 challenges is expected within the given timeframe.
- For students finishing early, attempt **Level 7: Denial** or revisit any incomplete challenges.

Resources

1. **Ethernaut Docs**: https://ethernaut.openzeppelin.com/
2. **Solidity Documentation**: https://docs.soliditylang.org/en/v0.8.20/
3. **Ethers.js**: https://docs.ethers.org/v5/
4. **OpenZeppelin Library**: https://docs.openzeppelin.com/contracts

Takeaways

At the end of this session, you should:

- Understand how real-world vulnerabilities are exploited and prevented.
- Be comfortable interacting with Ethereum smart contracts using the console and IDEs.
- Gain insights into the importance of secure coding practices in Solidity.

Activité précédente

Chapitre 06 : Introduction à la Sécurité des Smarts Contracts

Aller à…

Activité suivante

Chapitre 07 : Introduction à Solana