CRED SHiELDS

Solidity Scan

Solidity Scan

Powered by

CRED SHIELDS

Starting into Smart Contract Security

About Me

- I am Shashank, CEO & Co-founder of Credshields.com which is a web3 security company and we are building SoldityScan.com a cloud based Smart Contact Security Scanner.
- In past I have worked as a security analyst at HackerOne and security engineer at Deriv.
- I have over 12 years of experience in security, starting as a bugbounty hunter in 2013.
- Security Consultant for Avalanche

Why Smart Contract Security

- It is called the web 3.0 the successor of web2
- Financial Loss > Data loss
- More challenging
- Huge Demand
- Higher payouts for a Bug Hunter (https://immunefi.com/explore/)
- https://code4rena.com

Solidity Scan

Powered by

CRED SHIELDS

Solidity Programming

- Why Solidity Programming is important?
- Resources

  Beginner:
  https://cryptozombies.io/en/course/

  Advance:
  https://solidity-by-example.org

Understanding Basics of Solidity

- Solidity is similar to any OOP with minor differences.

- Pragma
- Contracts
- Constructor
- Function
- Visibility
- Modifier
- Fallback
- Receive
- Import
- Inheritance
- Comments (NatSpec)
- Variables
- Events

What are Smart Contracts

- Smart contracts are programs stored on a blockchain that runs when predetermined conditions are met.
- Ethereum is the world's computer.
- https://etherscan.io/contractsVerified

Common Smart Contract Vulnerabilities

- https://swcregistry.io (It is like OWASP for Smart Contracts)

Read Audit Reports

Solidity Scan

Powered by

CRED SHIELDS

- https://github.com/Credshields/Audit-Reports
- https://github.com/peckshield/publications/tree/master/audit_reports
- https://blog.openzeppelin.com/security-audits/
- https://consensys.net/diligence/audits/

Solidity Scan

Powered by

CRED SHiELDS

Read blogs and Hack Analysis

- https://blog.solidityscan.com
- https://blog.credshields.com
- https://medium.com/immunefi
- https://blocksecteam.medium.com
- https://slowmist.medium.com
- https://hacken.io/category/case-studies/

Solidity Scan

Powered by

CRED SHiELDS

Practice

- https://ethernaut.openzeppelin.com - Challenges
- https://blog.dixitaditya.com/series/ethernaut - Solutions
- https://www.damnvulnerabledefi.xyz

Missing Access Controls

- Administrative functions may have public or external visibility.
- Modifiers like “onlyOwner” missing from these functions
- Spelling mistakes in modifier names
- Missing “require” validations inside functions
  https://blog.solidityscan.com/access-control-vulnerabilities-in-smart-contracts-a31757f5d707

Decoding the ShadowFi Hack

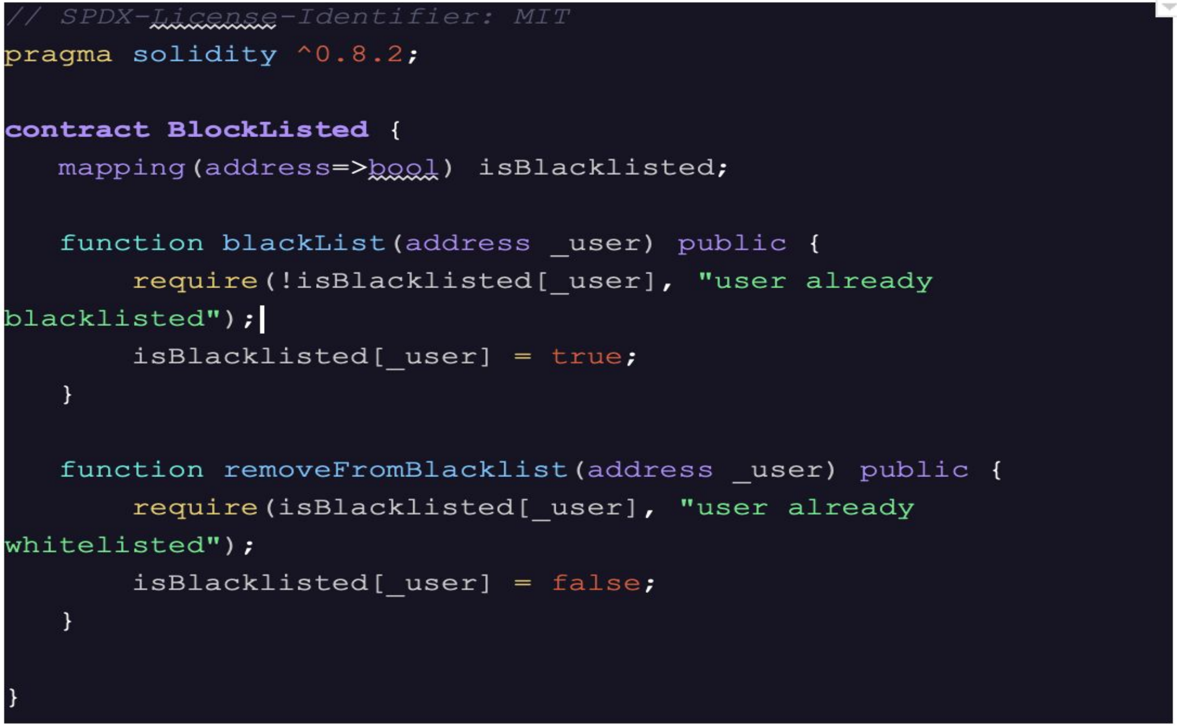
- https://bscscan.com/tx/0xe30dc75253eecec3377e03c532aa41bae1c26909bc8618f21fb83d4330a01018 [Hacker’s address]

- https://bscscan.com/address/0×10bc28d2810dD462E16facfF18f78783e859351b#code [Line 962]

Solidity Scan

Powered by CRED SHIELDS

Missing Access Control



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.2;

contract BlockListed {
   mapping(address=>bool) isBlacklisted;

   function blackList(address _user) public {
       require(!isBlacklisted[_user], "user already
blacklisted");
       isBlacklisted[_user] = true;
   }

   function removeFromBlacklist(address _user) public {
       require(isBlacklisted[_user], "user already
whitelisted");
       isBlacklisted[_user] = false;
   }

}
```

Solidity Scan

Powered by

CRED SHiELDS

Connect with Me :)

- https://twitter.com/cyberboyIndia
- https://www.linkedin.com/in/shashank-in/

Company Profiles:

- https://twitter.com/credshields
- https://twitter.com/solidityscan
- https://www.linkedin.com/company/credshields/
- https://www.linkedin.com/company/solidity-scan/