SECURITY OVERALL CHECK-UP

AGENDA

Offer for Security Overall Check-up.

Package Check-up.

Package Overall Review.

What should be provided before the security check-up?

Steps of Security and Infrastructure Testing.

Steps of Front-end / Back-end Security Audit.

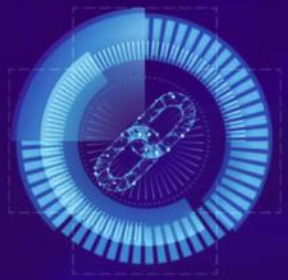
OFFER FOR SECURITY OVERALL CHECK-UP

Emerging frontiers like blockchain technology are never without their risks. More and more security holes are appearing on blockchain, while smart contracts add to the complexity of conducting audits on blockchain platforms. The vulnerability issues in the smart contracts account for as much as 40% of all potential risks of hack attacks.

482.solutions offers unique security packages to conduct a full check-up of your blockchain products and give companies an overview of the critical security gaps in infrastructure, frontend, backend, and smart contracts. We believe that each blockchain product should undergo such a procedure to avoid risks and vulnerabilities while searching for funds.

Our ultimate arm is to ensure the code is processing transactions effectively and securely.

We also provide our own software designed to automate the comprehensive security assessment of smart contracts and blockchain code upon request.



Protocols: Fantom, BSC, Polygon, ETH, Celo, and other EVM compatible protocols.

PACKAGE CHECK-UP

PACKAGE OVERALL REVIEW

PACKAGE CHECK-UP

SPECIALISTS ENGAGED:

- Senior DevOps Expert
- Senior Blockchain Security Expert

SECURITY CHECK-UP INCLUDES:

1. Infrastructure Security Audit
2. Smart Contracts Security Analysis

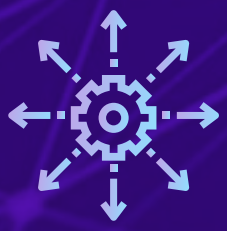
PACKAGE OVERALL REVIEW

SPECIALISTS ENGAGED:

- Security Engineer
- Senior Blockchain Security Expert
- Senior DevOps Expert
- Senior Solidity Smart Contract Expert

SECURITY CHECK-UP INCLUDES:

1. Infrastructure security audit. We will test cloud services for potential security flaws and data leaks.
2. Smart contracts & dApps audits for EVM compatible protocols.
3. Frontend & Backend Security Audit
4. Web Application Security Assessment
5. Penetration Testing
6. Access Control (key protections)
7. Database Assessments



WHAT SHOULD BE PROVIDED BEFORE THE SECURITY CHECK-UP?

- White Paper
- Technical Documentations
- JS tests
- Access to the infrastructure
- Provide token source code, merged in one file
- Provide a token name
- Provide a token symbol
- Is the token preminted? Answer Yes / No
- Could additional tokens be minted? Answer Yes / No
- Provide a solidity contract version (or we may require 0.8.x)
- Provide existing contracts, each smart contract merged in one file
- Provide a GitHub link with a contracts security audit
- Which blockchain token is deployed / will be deployed?
- Provide token owner address (if any). We will check if it is an EOA or multisig account
- Provide a treasury address (if any). We will check if it is an EOA or multisig account

STEPS OF SECURITY AND INFRASTRUCTURE TESTING

1 Testing of Web Application potential vulnerabilities

OWASP Top 10 vulnerability testing using scanners:

- Nessus
- InsightAppSec
- Nikto
- and other related tools from Vulnerability Scanning Tools list

2 Testing of Infrastructure vulnerabilities

Tools:

- Nessus
- Acunetix
- Metasploit
- ETTERCAP
- Netsparker

3 Checking of social engineering vulnerabilities

(if previous steps got some data of internal accounts)

Tools:

- Maltego
- SET (social-engineer-toolkit)

4 Creation and distribution of Detailed Reports

STEPS OF FRONT-END / BACK-END SECURITY AUDIT

- Test of userID (personal identification)
- ACL testing (access level control)
- Control sessions (tests)
- Three-Pronged Approach (forgery of permission to sign)
- Request intercept testing with Burp
- Testing of the login process with Bloom (sign the post data inputs)
- Testing of the reinitialization of the wallet owner (initWallet)

FIRST EVALUATION

1. White Paper
2. Tokennomics (if not in WP)
3. User Flow
4. Finance Flow (if no tokenomics or if there are any issues)
5. Pitch
6. Site (product or company)
7. FE/BE (accesses)
8. Repositories with Smart Contracts
9. Description of the project

LIST OF ADDITIONAL SOFTWARE USED FOR AUDIT

- mythx
- qualys
- burp suite
- maltego

SOLUTIONS

INNOVATIVE DECENTRALIZED
TRANSFORMATION

CONTACT US

+ 38 (073) 161-48-45
hello@482.solutions
www.482.solutions