RED-AT

AUDIT REPORT FOR

Westie Doge ($WESTY)

PERFORMED FOR CONTRACT

0xfbde2dd798350dcf3991259abd1503e2cf1b9513

SIGNED AT BLOCK

13167171

THIS IS AN OFFICIAL RED-AT SECURITY AUDIT

DISCLAIMER

RED-AT provides security audits for various DEFI projects. RED-AT does not guarantee that a project is not a scam. RED-AT only does the security testing portion and provides the public with technical information about the degree of security of the project in a format that is easy to understand for the average individual or business.

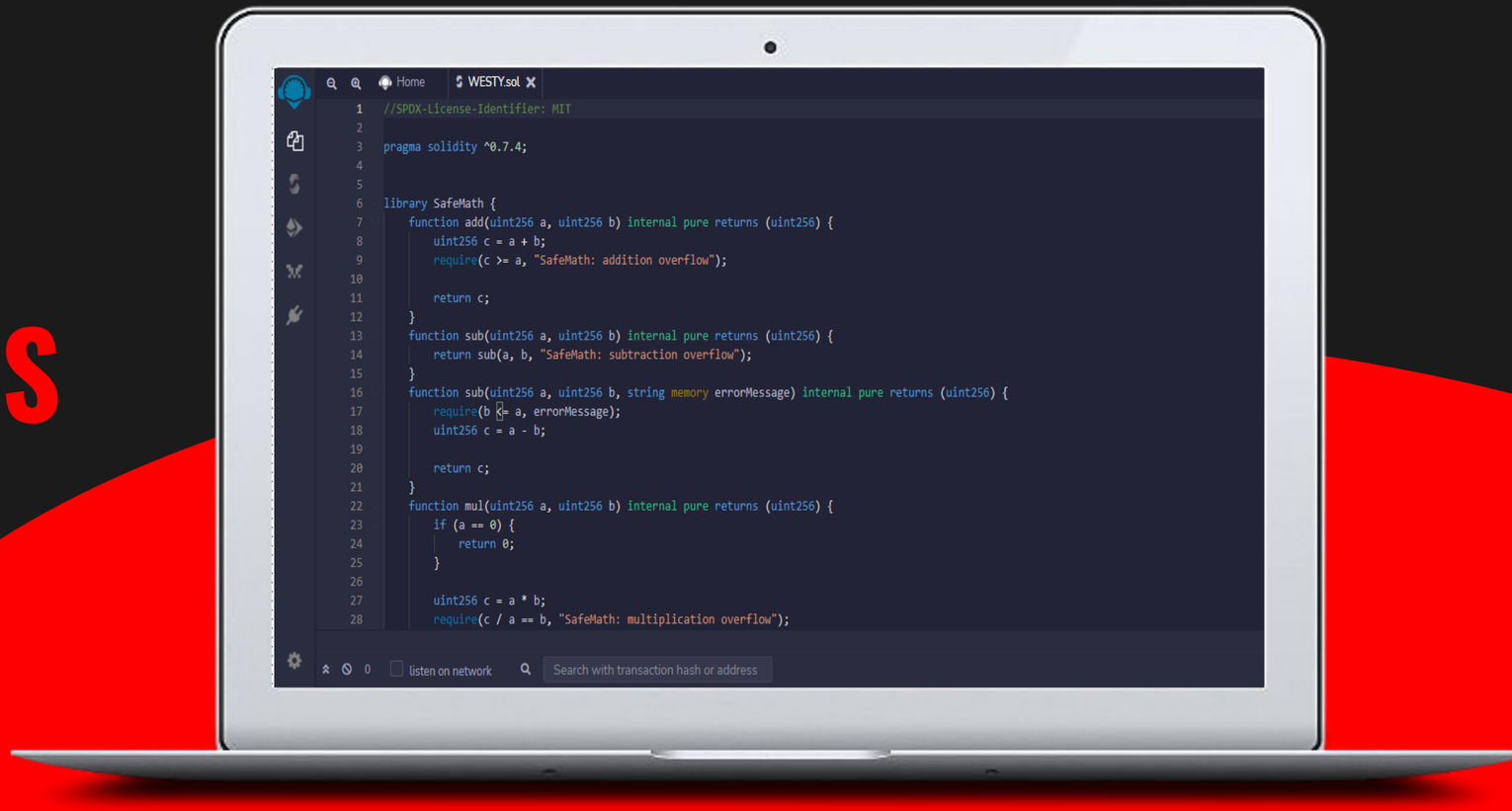
Agreeing to a security audit can be seen as the first sign of trust for a project, but in no way guarantees that a team will not pull all the money ("Rug Pull"), sell the chips, or completely withdraw from the scam. There is also no way to stop private sale holders from selling their tokens. It is eventually your responsibility to read all the paperwork, social media posts and contractual code for each of the individual projects to come to your own decisions and define your own risk tolerance.

RED-AT assumes no responsibility for potential losses, and does not encourage speculative investments. The information provided in this security audit is for informational purposes only and should not be considered as investment advice.

CONTENT

solidity

CONTRACT ANALYSIS



SMART CONTRACT INFORMATION

01

NAME (SYMBOL)

Westie Doge (WESTY)

02

CONTRACT ADDRESS

0xfbde2dd798350dcf3991
259abd1503e2cf1b9513

03

TOTAL SUPPLY

100,000,000,000 WESTY

04

CONTRACT DEPLOYER

0x98F774afA4F270E25aBF
fF9d506beFeecC1FD6F9

05

CONTRACT OWNER

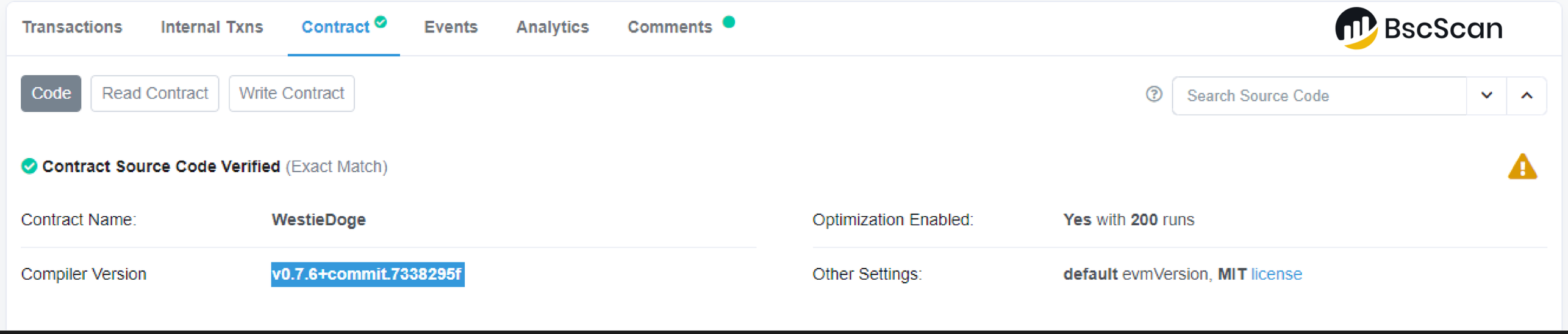
0x00659903fCcA548c4cB6
b83A1fD9A4EaBaF180A5

06

COMPILER VERSION

v0.7.6+commit.7338295f

SOURCE CODE VERIFICATION



CONTRACT

0xFBDE2dD798350DCF3991259abd1503E2cF1B9513

IS VERIFIED ON BSCSCAN

✔ VERIFIED

SMART CONTRACT VULNERABILITY ANALYSIS

TESTED VULNERABILITIES	AUTOMATED SCAN	MANUAL REVIEW	RESULT
INTEGER OVERFLOW IN ARITHMETIC OPERATION	COMPLETED	EXECUTED	✔ PASSED
INTEGER UNDERFLOW IN ARITHMETIC OPERATION	COMPLETED	EXECUTED	✔ PASSED
CALLER CAN REDIRECT EXECUTION TO ARBITRARY LOCATIONS	COMPLETED	EXECUTED	✔ PASSED
CALLER CAN WRITE TO ARBITRARY STORAGE LOCATIONS	COMPLETED	EXECUTED	✔ PASSED
DANGEROUS USE OF UNINITIALIZED STORAGE VARIABLES	COMPLETED	EXECUTED	✔ PASSED
ANY SENDER CAN WITHDRAW FROM THE CONTRACT ACCOUNT	COMPLETED	EXECUTED	✔ PASSED
USE OF "TX.ORIGIN" AS A PART OF AUTHORIZATION CONTROL	COMPLETED	EXECUTED	✔ PASSED

VULNERABILITY ANALYSIS

II

TESTED VULNERABILITIES	AUTOMATED SCAN	MANUAL REVIEW	RESULT
DELEGATECALL TO A USER-SUPPLIED ADDRESS	COMPLETED	EXECUTED	✔ PASSED
CALL TO A USER-SUPPLIED ADDRESS	COMPLETED	EXECUTED	✔ PASSED
UNCHECKED RETURN VALUE FROM EXTERNAL CALL	COMPLETED	EXECUTED	✔ PASSED
BLOCK TIMESTAMP INFLUENCES A CONTROL FLOW DECISION	COMPLETED	EXECUTED	✔ PASSED
ENVIRONMENT VARIABLES INFLUENCE A CONTROL FLOW DECISIONS	COMPLETED	EXECUTED	✔ PASSED
LOOP OVER UNBOUNDED DATA STRUCTURE	COMPLETED	EXECUTED	✔ PASSED
IMPLICIT LOOP OVER UNBOUNDED DATA STRUCTURE	COMPLETED	EXECUTED	✔ PASSED

VULNERABILITY ANALYSIS

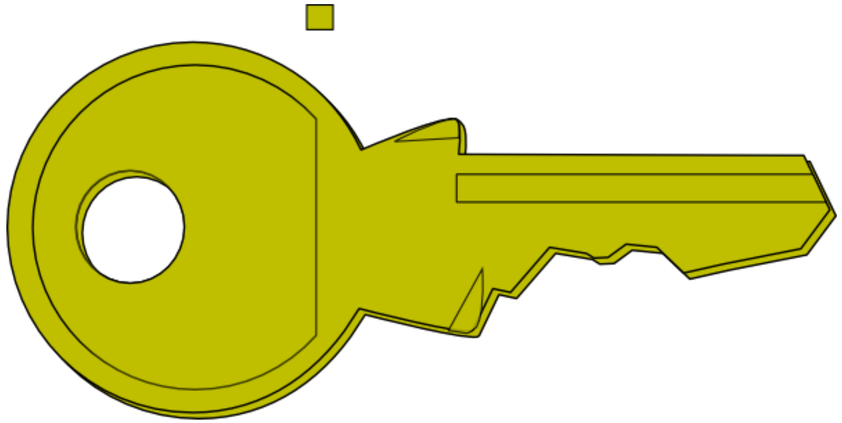
III

TESTED VULNERABILITIES	AUTOMATED SCAN	MANUAL REVIEW	RESULT
USAGE OF "CONTINUE" IN "DO-WHILE"	COMPLETED	EXECUTED	✔ PASSED
MULTIPLE CALLS ARE EXECUTED IN THE SAME TRANSACTION	COMPLETED	EXECUTED	✔ PASSED
PERSISTENT STATE READ FOLLOWING EXTERNAL CALL	COMPLETED	EXECUTED	✔ PASSED
PERSISTENT STATE WRITE FOLLOWING EXTERNAL CALL	COMPLETED	EXECUTED	✔ PASSED
ACCOUNT STATE ACCESSED AFTER CALL TO USER-DEFINED ADDRESS	COMPLETED	EXECUTED	✔ PASSED
RETURN VALUE OF AN EXTERNAL CALL IS NOT CHECKED	COMPLETED	EXECUTED	✔ PASSED
POTENTIAL WEAK SOURCE OF RANDOMNESS	COMPLETED	EXECUTED	✔ PASSED

VULNERABILITY ANALYSIS

IV

TESTED VULNERABILITIES	AUTOMATED SCAN	MANUAL REVIEW	RESULT
REQUIREMENT VIOLATION	COMPLETED	EXECUTED	✔ PASSED
CALL WITH HARDCODED GAS AMOUNT	COMPLETED	EXECUTED	✔ PASSED
INCORRECT ERC20/BEP20 IMPLEMENTATION	COMPLETED	EXECUTED	✔ PASSED
OUTDATED COMPILER VERSION	COMPLETED	EXECUTED	✔ PASSED
NO OR FLOATING COMPILER VERSION SET	COMPLETED	EXECUTED	✔ PASSED
USE OF RIGHT-TO-LEFT-OVERRIDE CONTROL CHARACTER	COMPLETED	EXECUTED	✔ PASSED
SHADOWING OF BUILT-IN SYMBOL	COMPLETED	EXECUTED	✔ PASSED

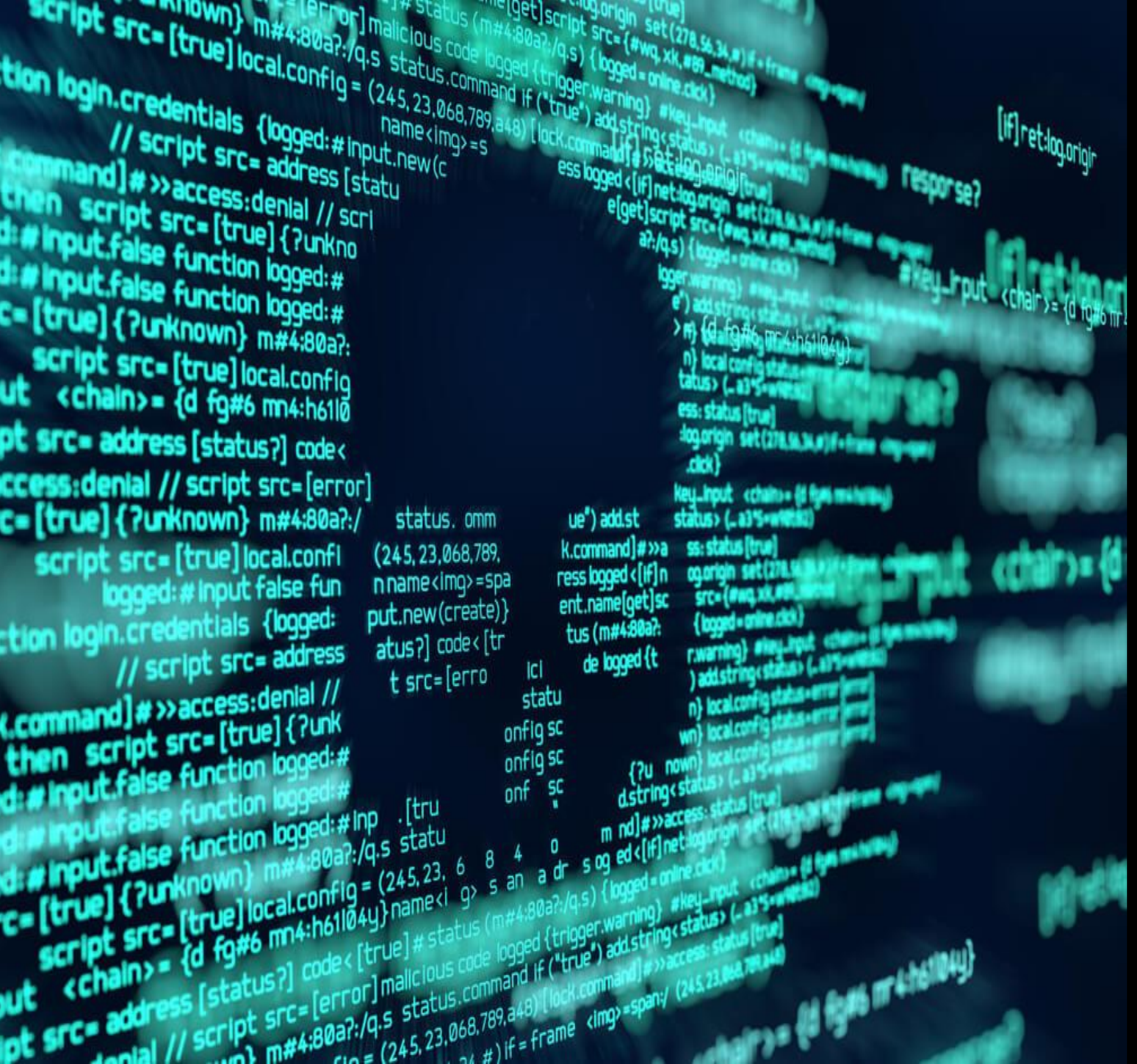


OWNERSHIP STATUS

Ownership of the contract was not renounced at the time of the audit.

LIQUIDITY STATUS

No liquidity was identified at the time of the audit



MALICIOUS FUNCTIONS

No malicious functions were identified during static and dynamic analysis of the smart contract source code

✔ **PASSED**

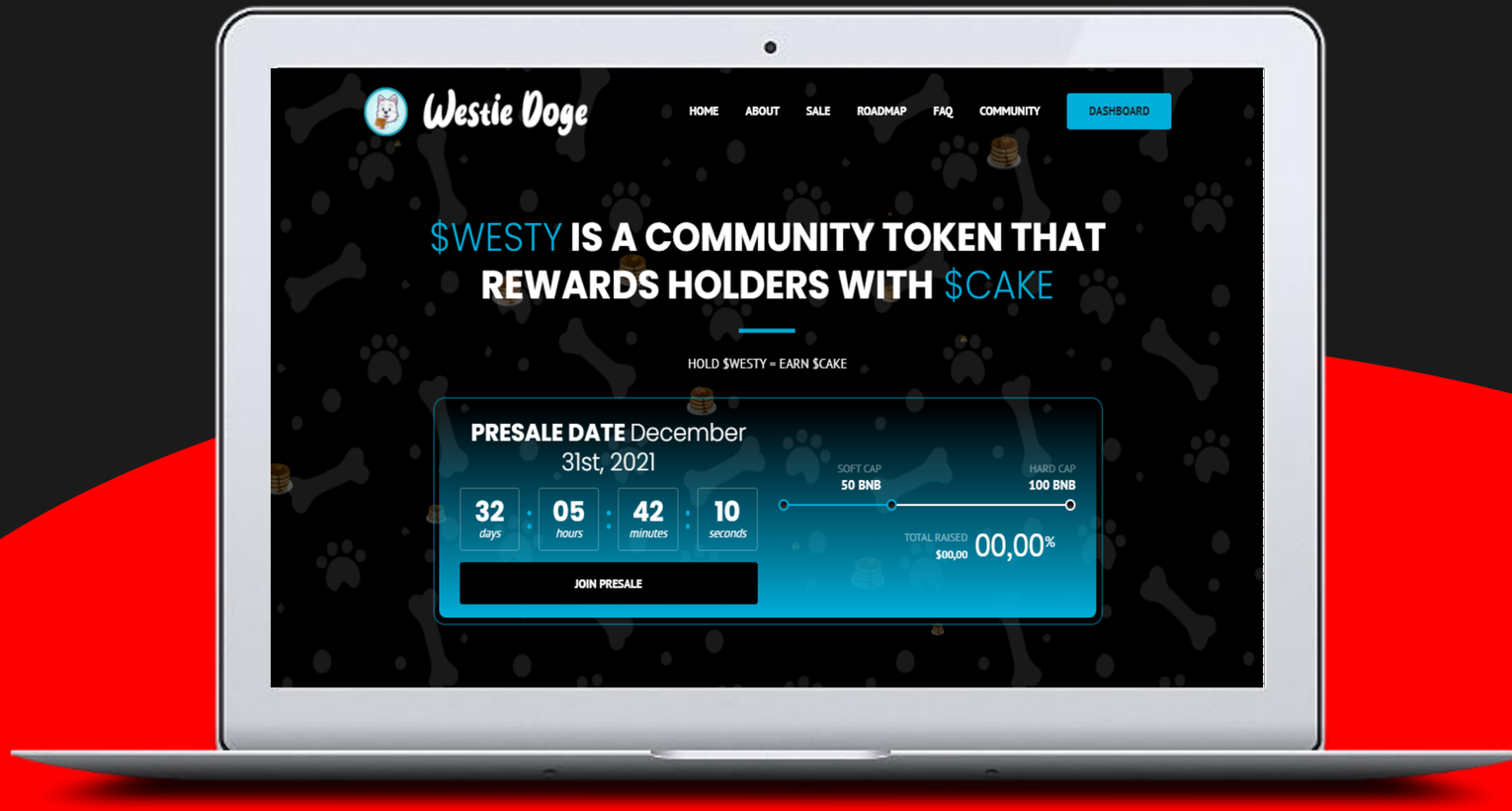
HONEYPOT ANALYSIS

Following our simulation of the smart contract source code in an isolated environment. We guarantee that the smart contract is not a honeypot, as it is possible to buy and sell the token without concerns.

✔ **PASSED**

```
43  mapping (address => mapping (address => uint256)) private _allowances;
44
45
46  uint256 private _totalSupply;
47  uint8 private _decimals;
48  string private _symbol;
49  string private _name;
50
51
52  constructor() public {
53    _name = "NAME HERE";
54    _symbol = "SYMBOL HERE";
55    _decimals =  DECIMALS HERE;
56    _totalSupply = TOTAL SUPPLY HERE;
57    _balances[msg.sender] = _totalSupply;
58
59
60    emit Transfer(address(0), msg.sender, _totalSupply);
61  }
62
63
64  /**
65   * @dev Returns the bep token owner.
66   */
67  function getOwner() external view returns (address) {
68    return owner();
```

WEBSITE ANALYSIS



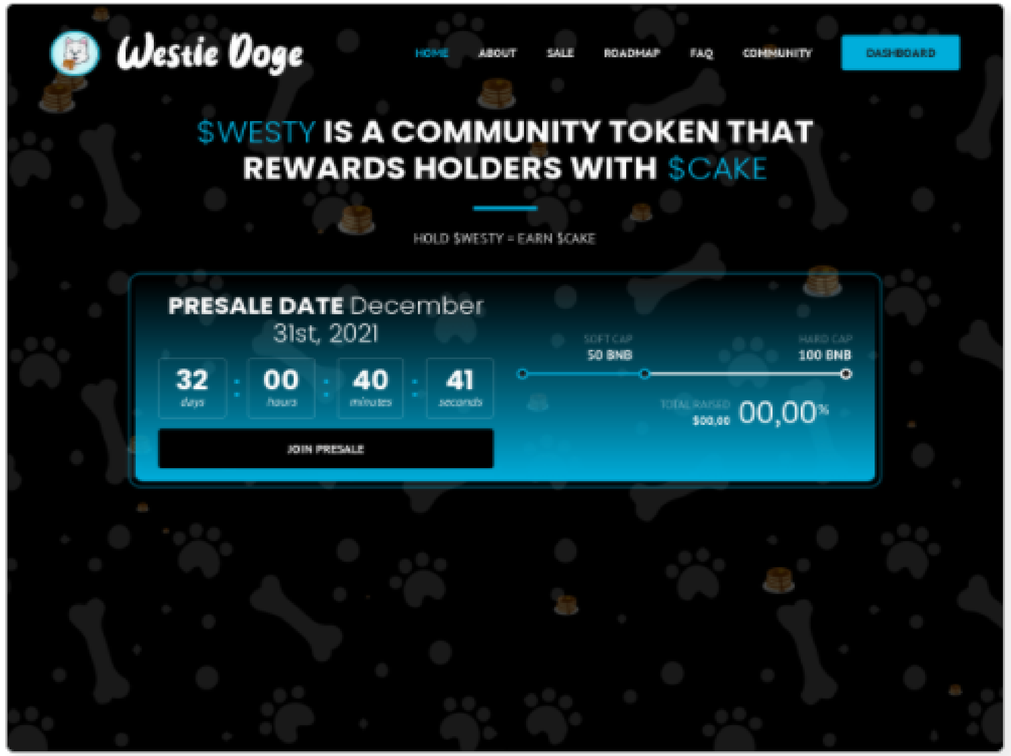
WEBSITE METADATA

www.westiedoge.com

AMAZON-02, US

Seen 1 times between November 28th, 2021 and November 28th, 2021.

Live Screenshot Hover to expand



General Info

Open in Search

Geo	Frankfurt am Main, Germany (DE) —	
Created	November 12th, 2021	
Domain	westiedoge.com	(The registered domain)
AS	AS16509 - AMAZON-02, US Note: An IP might be announced by multiple ASs. This is not shown.	
Registrar	ARIN	
Route	3.64.0.0/12	(Route of ASN)
PTR	ec2-3-67-234-155.eu-central-1.compute.amazonaws.com	(PTR record of primary IP)
IPv4	3.67.234.155 18.192.76.182	

WEBSITE SSL CHECK

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > www.westiedoge.com

SSL Report: www.westiedoge.com

Assessed on: Sun, 28 Nov 2021 23:21:08 UTC | **HIDDEN** | Clear cache

Scan Another >>

	Server	Test time	Grade
1	52.73.153.209 ec2-52-73-153-209.compute-1.amazonaws.com Ready	Sun, 28 Nov 2021 23:18:59 UTC **Duration:** 65.202 sec	A
2	54.205.240.192 ec2-54-205-240-192.compute-1.amazonaws.com Ready	Sun, 28 Nov 2021 23:20:05 UTC **Duration:** 63.774 sec	A

SSL Report v2.1.8

WEBSITE VULNERABILITY ANALYSIS

OWASP TOP 10

TESTED VULNERABILITIES	AUTOMATED SCAN	MANUAL REVIEW	RESULT
A1 - Injection	COMPLETED	EXECUTED	✔ PASSED
A2 - Broken Authentication	COMPLETED	EXECUTED	✔ PASSED
A3 – Sensitive Data Exposure	COMPLETED	EXECUTED	✔ PASSED
A4 – XML External Entities (XXE)	COMPLETED	EXECUTED	✔ PASSED
A5 - Broken Access Control	COMPLETED	EXECUTED	✔ PASSED
A6 - Security Misconfiguration	COMPLETED	EXECUTED	✔ PASSED
A7 – Cross Site Scripting(XSS)	COMPLETED	EXECUTED	✔ PASSED
A8 – Insecure Deserialization	COMPLETED	EXECUTED	✔ PASSED
A9 – Known Vulnerabilities	COMPLETED	EXECUTED	✔ PASSED
A10 – Insufficient Logging and Monitoring	COMPLETED	EXECUTED	✔ PASSED

SOCIAL NETWORKS

We were able to identify the following social networks

YOUTUBE

TWITTER

TELEGRAM

LOCATION

DEV TEAM IS
LOCATED IN CANADA

TEAM DOXING

THE IDENTITY OF THE DEVELOPERS OF THIS PROJECT HAS BEEN FULLY VALIDATED

✔ **DEV DOXED**

DISCLAIMER

The opinions expressed in this document are for general information purposes only and are not intended to provide specific advice or recommendations to any individual or particular investment. Other unknown security vulnerabilities are beyond our control. RED-AT is publishing this report only on the basis of attacks or vulnerabilities that already existed or occurred prior to the publication of this report. For the emergence of new attacks or vulnerabilities that exist or occur in the future, RED-AT does not have the ability to judge their possible impact on the security status of smart contracts, and therefore assumes no responsibility for them. The analysis of smart contracts and other contents of this report are based solely on documents and materials that the contract provider provided to RED-AT or that were publicly available prior to the issuance of this report (issuance of the report recorded via the block number on the cover page), if the documents and materials provided by the Contract Provider are missing, altered, deleted, concealed, or reflected in a situation that does not conform to the actual situation, or if the documents and materials provided are altered after the issuance of this report, RED-AT assumes no responsibility for the resulting loss or adverse effects. RED-AT provides no guarantee against the sale of team tokens or the outflow of cash by the project audited in this document. Even projects with a low risk score have been known to withdraw liquidity, sell all team tokens, or exit - scam. Please exercise caution when dealing with crypto-currency related platforms. The final interpretation of this statement is up to RED-AT. RED-AT strongly discourages the use of crypto-currencies as speculative investments and they should only be used for the utility they are intended to provide.

WE ARE A CANADIAN COMPANY FOCUSED ON BLOCKCHAIN CYBERSECURITY - WE PROVIDE SOLUTION-ORIENTED CONSULTING AND AUDITING SERVICES FOR DECENTRALIZED APPLICATIONS, INCLUDING SMART CONTRACTS

CONTACT

info@red-at.com