

## Security Assessment: Website AI Staking

February 17, 2024

- Audit Status: **Fail**
- Audit Edition: **Advance**



# Project Overview

## Token Summary

Parameter	Result
Address	0x
Name	Website AI
Token Tracker	Website AI (WEBAIS)
Decimals	18
Supply	0
Platform	ETHEREUM
compiler	v0.8.20+commit.a1b79de6
Contract Name	WEBAISTAKING
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	
Payment Tx	Corporate

## Main Contract Assessed Contract Name

Name	Contract	Live
Website AI	0x	Yes

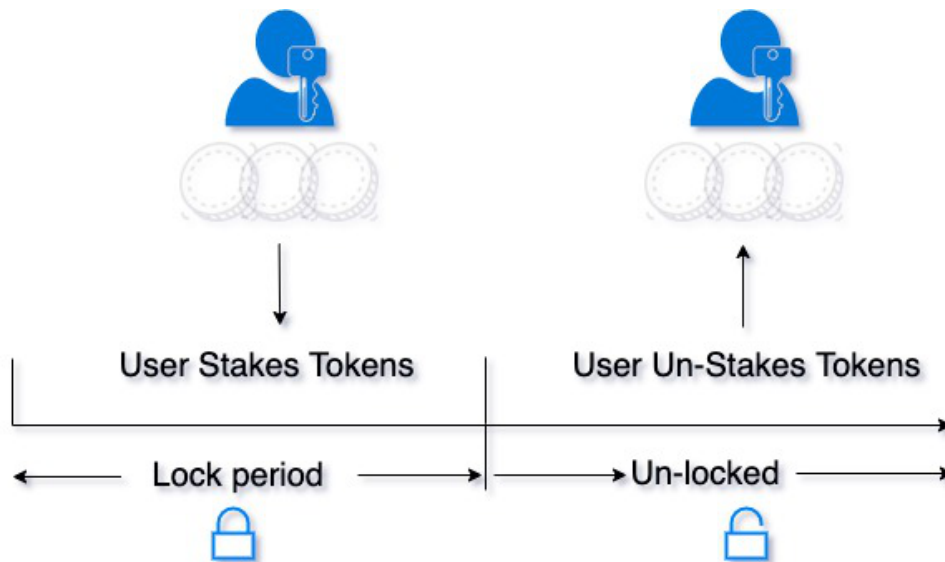
## TestNet Contract was Not Assessed

### Solidity Code Provided

SolidID	File Sha-1	FileName
WebAIStaking	0bd10417379ce26541e7edd7c112d25d20460364	WebAIStaking.sol
WebAIStaking		
WebAIStaking		
WebAIStaking		
WebAIStaking		
WebAIStaking	undefined	

# What is a Staking Contract

A smart contract which allows users to stake and un-stake a specified ERC20 token. Staked tokens are locked for a specific length of time (set by the contract owner at the outset). Once the time period has elapsed, the user can remove their tokens again.



# Smart Contract Vulnerability Checks

**The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) while overlaying a wide range of weakness variants that are specific to smart contracts.**

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	WebAISTaking.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	WebAISTaking.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	WebAISTaking.sol	L: 0 C: 0
SWC-103	Low	A floating pragma is set.	WebAISTaking.sol	L: 10 C: 0
SWC-104	Pass	Unchecked Call Return Value.	WebAISTaking.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	WebAISTaking.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	WebAISTaking.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	WebAISTaking.sol	L: 0 C: 0
SWC-108	Low	State variable visibility is not set..	WebAISTaking.sol	L: 863-866 C: 12
SWC-109	Pass	Uninitialized Storage Pointer.	WebAISTaking.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	WebAISTaking.sol	L: 0 C: 0
SWC-111	Pass	Use of Deprecated Solidity Functions.	WebAISTaking.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	WebAISTaking.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	WebAISTaking.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	WebAISTaking.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-115	Pass	Authorization through tx.origin.	WebAISTaking.sol	L: 0 C: 0
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	WebAISTaking.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	WebAISTaking.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	WebAISTaking.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	WebAISTaking.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randomness.	WebAISTaking.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	WebAISTaking.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	WebAISTaking.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	WebAISTaking.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	WebAISTaking.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	WebAISTaking.sol	L: 0 C: 0
SWC-126	Pass	Insufficient Gas Griefing.	WebAISTaking.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	WebAISTaking.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	WebAISTaking.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	WebAISTaking.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U+202E).	WebAISTaking.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	WebAISTaking.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	WebAISTaking.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	WebAISTaking.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	WebAISTaking.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	WebAISTaking.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	WebAISTaking.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry-standard security scanning tools.

# Smart Contract Vulnerability Details

## SWC-103 - Floating Pragma.

### CWE-664: Improper Control of a Resource Through its Lifetime.

#### References:

#### Description:

Contracts should be deployed with the same compiler version and flags that they have been tested with thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively.

#### Remediation:

Lock the pragma version and also consider known bugs (<https://github.com/ethereum/solidity/releases>) for the compiler version that is chosen.

Pragma statements can be allowed to float when a contract is intended for consumption by other developers, as in the case with contracts in a library or EthPM package. Otherwise, the developer would need to manually update the pragma in order to compile locally.

#### References:

Ethereum Smart Contract Best Practices - Lock pragmas to specific compiler version.



# Smart Contract Vulnerability Details

## SWC-108 - State Variable Default Visibility

### CWE-710: Improper Adherence to Coding Standards

#### Description:

Labeling the visibility explicitly makes it easier to catch incorrect assumptions about who can access the variable.

#### Remediation:

Variables can be specified as being public, internal or private. Explicitly define visibility for all state variables.

#### References:

Ethereum Smart Contract Best Practices - Explicitly mark visibility in functions and state variables

# Inheritance

The contract for Website AI has the following inheritance structure.

The Project has a Total Supply of 0





## Privileged Functions (onlyOwner)

Please Note if the contract is Renounced none of this functions can be executed.

Function Name	Parameters	Visibility
renounceOwnership		Public
transferOwnership	address newOwner	Public
setDepositDeduction		External
setWithdrawDeduction		External
setEarlyPenalty		External
setStakeConclude		External

## WEBAIS-03 | Lack of Input Validation.

Category	Severity	Location	Status
Volatile Code	 Low	WebAISTaking.sol: L: 1077, C: 14,L: 1072, C: 14,L: 1067, C: 14,L: 1062, C: 14,L: 1057, C: 14,L: 1057, C: 14	 Detected

### Description

The given input is missing the check for the non-zero address.

The given input is missing the check for the missing required function.



### Remediation

We advise the client to add the check for the passed-in values to prevent unexpected errors as below:

```
...  
    require(receiver != address(0), "Receiver is the zero address");  
...  
...  
    require(value X limitation, "Your not able to do this function");  
...
```

We also recommend customer to review the following function that is missing a required validation. missing required function.

## WEBAIS-05 | Missing Event Emission.

Category	Severity	Location	Status
Volatile Code	 Low	WebAISTaking.sol: L: 1077, C: 14,L: 1072, C: 14,L: 1067, C: 14,L: 1062, C: 14,L: 1057, C: 14,L: 1057, C: 14	 Detected



### Description

Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes. The linked code does not create an event for the transfer.

### Remediation

Emit an event for critical parameter changes. It is recommended emitting events for the sensitive functions that are controlled by centralization roles.

## WEBAIS-07 | State Variables could be Declared Constant.

Category	Severity	Location	Status
Coding Style	 Low	WebAISTaking.sol: L: 863-866 C: 14	 Detected

### Description

Constant state variables should be declared constant to save gas.



```
maxDepositDeduction  
maxWithdrawDeduction  
maxEarlyPenalty  
minAPR
```

### Remediation

Add the constant attribute to state variables that never changes.

<https://docs.soliditylang.org/en/latest/contracts.html#constant-state-variables>

## WEBAIS-08 | Dead Code Elimination.

Category	Severity	Location	Status
Coding Style	 Low	WebAISTaking.sol: L: 89 C:14,L: 542 C:14	 Detected

### Description

Functions that are not used in the contract, and make the code s size bigger.



```
initialPool  
SafeERC20
```

### Remediation

Remove unused functions. dead-code elimination (also known as DCE, dead-code removal, dead-code stripping, or dead-code strip) is a compiler optimization to remove code which does not affect the program results. Removing such code has several benefits: it shrinks program size, an important consideration in some contexts, and it allows the running program to avoid executing irrelevant operations, which reduces its running time. It can also enable further optimizations by simplifying program structure.

<https://docs.soliditylang.org/en/latest/cheatsheet.html>

## WEBAIS-14 | Unnecessary Use Of SafeMath

Category	Severity	Location	Status
Logical Issue	 Medium	WebAISTaking.sol: L: 22, C: 13	 Detected

### Description

The SafeMath library is used unnecessarily. With Solidity compiler versions 0.8.0 or newer, arithmetic operations

will automatically revert in case of integer overflow or underflow.

library SafeMath {

An implementation of SafeMath library is found.

using SafeMath for uint256;

SafeMath library is used for uint256 type in contract.

### Remediation



We advise removing the usage of SafeMath library and using the built-in arithmetic operations provided by the

Solidity programming language

### Project Action



## WEBAIS-20 | Missing check for reward tokens vs staked tokens..

Category	Severity	Location	Status
Logical	 Critical	WebAIStaking.sol: L: 05 C: 14	 Detected

### Description

This could lead to a situation where the contract is unable to pay out the staked amount of users or users cannibalizing other user's funds. Recommend adding a check for the reward token balance before allowing a user to claim rewards and update reward balance on every deposit and withdrawal. Allowing anyone to add tokens to the contract as a reward balance and offsetting the staked amount in a separate variable to keep control.






### Remediation

review stake logic.






### Project Action

# Technical Findings Summary

## Classification of Risk

Severity	Description
 Critical	Risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
 High	Risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
 Medium	Risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform
 Low	Risks can be any of the above but on a smaller scale. They generally do not compromise the overall integrity of the Project, but they may be less efficient than other solutions.
 Informational	Errors are often recommended to improve the code's style or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

## Findings

Severity	Found	Pending	Resolved
 Critical	1	1	0
 High	0	0	0
 Medium	1	1	0
 Low	4	4	0
 Informational	0	0	0
Total	6	6	0

# Social Media Checks

Social Media	URL	Result
Twitter	<a href="https://twitter.com/WebsiteAI_ERC">https://twitter.com/WebsiteAI_ERC</a>	Pass
Other		Fail
Website	<a href="https://websiteai.io/">https://websiteai.io/</a>	Pass
Telegram	<a href="https://t.me/Website_AI">https://t.me/Website_AI</a>	Pass

We recommend to have 3 or more social media sources including a completed working websites.

**Social Media Information Notes:**

**Auditor Notes:** undefined

**Project Owner Notes:**



# Audit Result

## Final Audit Score

Review	Score
Security Score	50
Auditor Score	55

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 85 Points for a higher standard, if a project does not attain 85% is an automatic failure. Read our notes and final assessment below.

## Audit Fail



## Assessment Results

### Important Notes:

- - Plan Struct - `initialPool` is not used in the contract.␣
- - Library `SafeERC20` is declared but unused in the entirety of the contract.␣
- - The use of an abstract contract adds unnecessary complexity to the contract, recommended to use an interface instead.␣
- - Although solidity version `^0.8.0` is specified, the contract still uses `SafeMath` library. This is not necessary as the arithmetic operators are checked for overflow and underflow in the latest version of solidity.␣
- - The contract must use a specific pragma version.␣
- - `totalRewardsPerWalletPerPlan` check if this is used as something internal, if external only, would recommend removing it in favor of having a per Staking amount and calculated in an external function for the UI.␣
- - Recommend adding a `createPool` to add all the data in a single transaction.␣
- - Staking contract has a lot of unnecessary checks if the plan limit is only 1.␣
- - There are multiple instances of constants used in the contract. It is recommended to abstract these into a single location to make it easier to read.␣

- `e.g. uint256 public constant BASIS\_PERCENTAGE = 100;`

**Auditor Score =55**  
**Audit Fail**



# Appendix

## Finding Categories

### Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

### Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.

### Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how `block.timestamp` works.

### Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being invoke-able by anyone under certain circumstances.

### Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

### Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

### Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code, such as a constructor assignment imposing different requirements on the input variables than a setter function.

### Coding Best Practices

ERC 20 Coding Standards are a set of rules that each developer should follow to ensure the code meets a set of criteria and is readable by all the developers.

# Disclaimer

Assure Defi has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocacy for the Project, and users relying on this report should not consider this as having any merit for financial advice in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided 'as is, and Assure Defi is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will Assure Defi or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment services provided by Assure Defi are subject to dependencies and are under continuing development. You agree that your access or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.

