shieldify

Hopium

Penetration Testing

Date: 17 July 2024

CONTENTS

1. About Shieldify

Positioned as the first hybrid Web3 Security company, Shieldify shakes things up with a unique subscription-based auditing model that entitles the customer to unlimited audits within its duration, as well as top-notch service quality thanks to a disruptive 6-layered security approach. The company works with very well-established researchers in the space and have secured multiple millions in TVL across protocols, also can audit codebases written in Solidity, Vyper, Rust, Cairo, Move and Go.

Learn more about us at shieldify.org.

2. Disclaimer

The information in this document is confidential and meant for use only by the intended recipient. This security review does not guarantee bulletproof protection against a hack or exploit. The protocol, which this report is intended for, indemnifies Shieldify Security against any responsibility for any misbehavior, bugs, or exploits affecting the audited code during any part of the project's life cycle. It is also pivotal to acknowledge that modifications made to the audited code, including fixes for the issues described in this report, may introduce new problems and necessitate additional auditing.

3. About Hopium

The Hopium website (hopium.virtual.tech) is a Web2 application powered by Virtual Rollups, which are ZeroGas rollups offering one-click trading, millisecond finality, and user-validated execution. This platform is specifically designed to integrate with a smart contract on the backend. It enables players to participate in a coin flip game where bets are placed according to options provided by the interface. These bets are deducted from the session balance of a connected wallet. Players choose between options such as astroman or alien (equivalent to heads or tails), specifying their bet amount. They then await the application's response to determine if they have won or lost. Depending on the outcome, their wallet balance is adjusted accordingly, either increasing or decreasing based on the result of the coin flip game.

4. Methodology

Security assessment of the beecasino site between June 13, 2024 and June 18, 2024. The purpose of the assessment was to identify security vulnerabilities and recommend remediations.

The assessment was performed with a black-box, dynamic (browser based) approach. The assessment is conducted with the following phases:

- Pre-engagement Interactions
- Enumeration
- Vulnerability Discovery
- Exploitation
- Post Exploitation
- Reporting
- Post-Engagement Interaction

A combination of automated and manual methods and follows have been used as a testing methodology.

5. General Recommendations

To increase the security posture, the reporter recommends the following actions be taken:

1. Develop a plan of action and mitigation to remediate all other vulnerabilities according to a specific process of software patching. For more info: https://owaspsamm.org/model/operations/
2. Perform routine testing for the applications on a semi-annual basis.

6. Risk Classification

The risk score for Bitsight response scan is 7 of a possible 25, which is rated at **LOW RISK**.

A LOW risk score indicates the target system or data is at a very low risk of being compromised and no immediate action is required.

Table 1: Classification and Description of Vulnerabilities

Classification	Description
Catastrophic	Once a vulnerability is declared as Catastrophic, strict limits apply to the expected remediation timeline. Mitigations such as securing an asset behind a WAF or firewall and actively monitoring logs are the recommended immediate response.
Critical	This rating is given to flaws that could be easily exploited by a remote unauthenticated attacker and lead to system compromise (arbitrary code execution) without user interaction. These are the types of vulnerabilities that can be exploited by worms. Flaws that require an authenticated remote user, a local user, or an unlikely configuration are not classed as critical impact.
Important	This rating is given to flaws that can easily compromise the confidentiality, integrity, or availability of resources. These are the types of vulnerabilities that allow local users to gain privileges, allow unauthenticated remote users to view resources that should otherwise be protected by authentication, allow authenticated remote users to execute arbitrary code, or allow local or remote users to cause a denial of service.
Medium	This rating is given to flaws that may be more difficult to exploit but could still lead to some compromise of the confidentiality, integrity, or availability of resources, under certain circumstances. These are the types of vulnerabilities that could have had a critical impact or important impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations.
Low	This rating is given to all other issues that have a security impact. These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would give minimal consequences.

7. Assessment Objectives

The security assessment attempted to gain information in three areas:

1. Identify security risks and gain system level access.
2. Identify areas of infrastructure weakness.
3. Recommend remediations to mitigate risks and eliminate vulnerabilities.

7.1 Assessment Scope

The assessment was performed on hopium.virtual.tech

7.2 Assessment Approach

The assessment was conducted in five phases:

1. Reconnaissance and information gathering.
2. Review reconnaissance data and perform analysis.
3. Using Tools like proxies and interceptors to test injections and other issues.
4. Assess systems and determine which may be vulnerable to exploitation.
5. Documentation of findings and recommendations.

8. Findings Summary

The following number of issues have been identified, sorted by their severity:

- **Critical** and **High** issues: **0**
- **Medium** issues: **3**
- **Low** issues: **0**
- **Informational** issues: **2**

9. Findings

ID	Title	Severity	Status
[M-01]	Deposit Function Should be Disabled Before Starting a Game	Medium	-
[M-02]	Lack of Input Validation in Deposit Function will Trigger 0 Value Transactions	Medium	-
[M-03]	Decimals not Required in the Deposit Function	Medium	-
[I-01]	Strict Transport Security Not Enforced	Informational	-
[I-02]	Reset Function is Redundant	Informational	-

[M-01] Deposit Function Should be Disabled Before Starting a Game

Severity

Medium Risk

Description

Enabling the deposit function before initiating the game with “Start Game” can lead to unnecessary transactions and potential gas griefing.

Location of Affected Code

hopium.virtual.tech

Recommendation

Ensure that the deposit function is disabled for the user before starting a game.

[M-02] Lack of Input Validation in Deposit Function will Trigger 0 Value Transactions

Severity

Medium Risk

Description

The deposit function can trigger transactions even if the amount field is empty or if the user inputs special characters instead of numbers. These transactions result in gas griefing by consuming gas without transferring any value.

Location of Affected Code

hopium.virtual.tech

Proof of Concept

When a user is depositing assets, the amount field is not properly sanitized to accept only numeric values. Although there is a warning message stating that the input should be a positive number, a user can still input any value (or leave it empty), triggering a zero-value transaction that only consumes gas. Moreover this transaction is occurring without Starting a game which is required before depositing an amount.

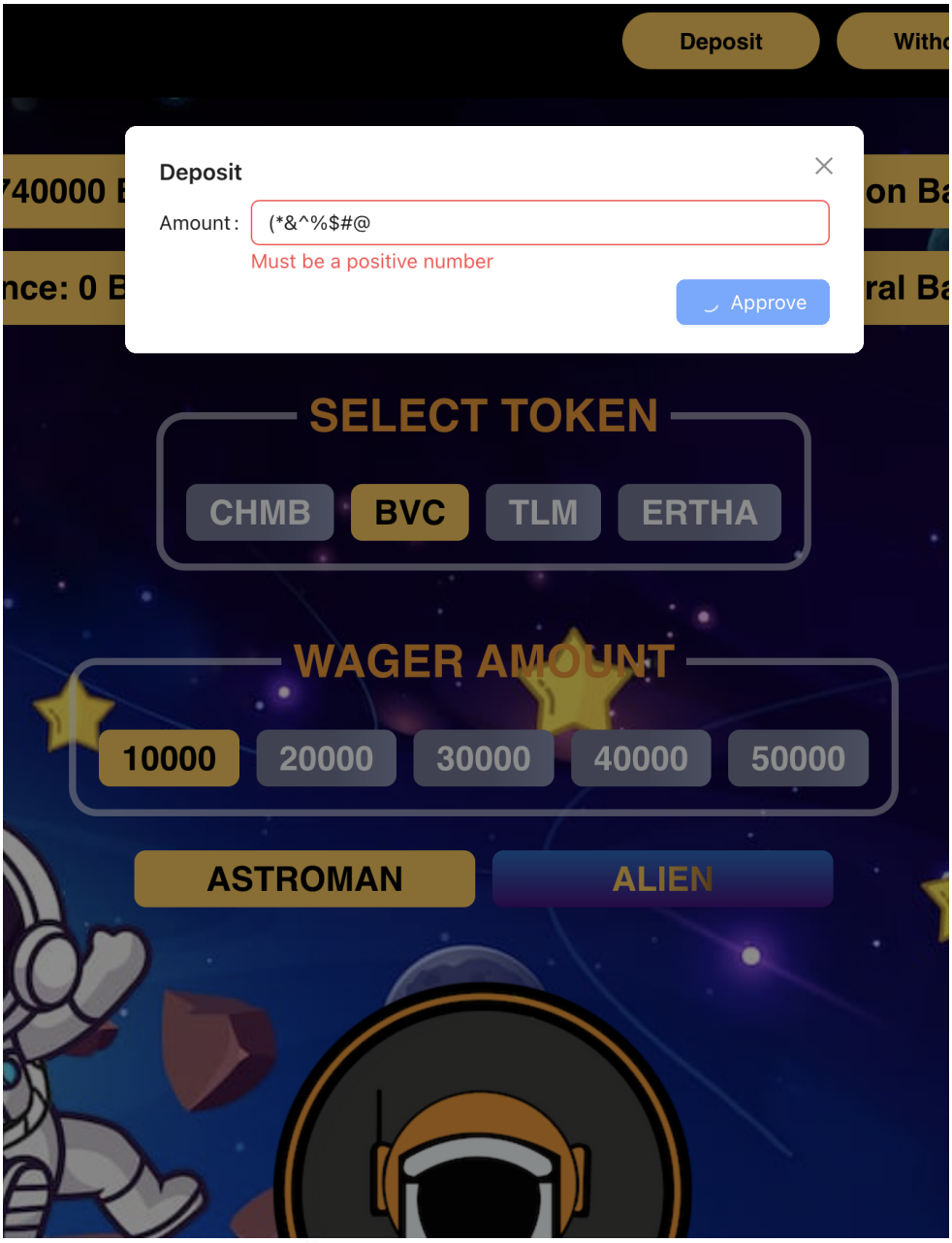

Figure 1: In the image: The current implementation allows a user to introduce special characters or an empty string, and the approve button will still process a transaction with a zero value, consuming only gas.

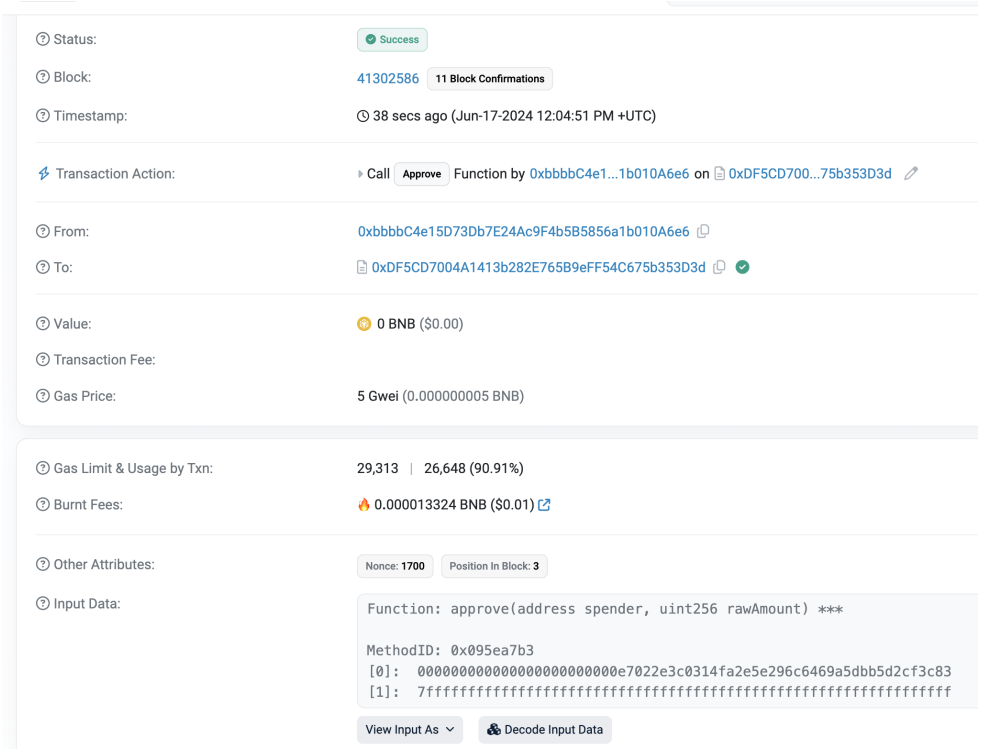

Figure 2: In the image: Details of the 0 value transaction from above.

Although the user is required to approve this zero-value transaction, if the application warns the user to use only valid positive numbers, it should enforce this by accepting only valid input for approval.

Recommendation

Ensure that user input is restricted to only the expected values (numbers) before allowing the approval of any transaction.

[M-03] Decimals not Required in the Deposit Function

Severity

Medium Risk

Description

When a user deposits an amount into any of the tokens, allowing input of decimal numbers is unnecessary since the wages are fixed in rounded numbers.

Location of Affected Code

hopium.virtual.tech

Proof of Concept

When a user initiates a game and proceeds to deposit, it is possible to enter amounts with decimals.

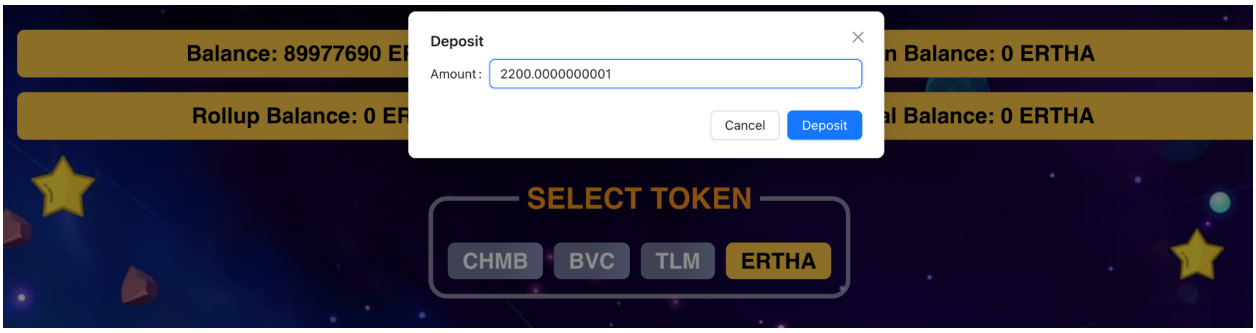

Figure 3: In the image: The application processes decimals in the Session Balance.

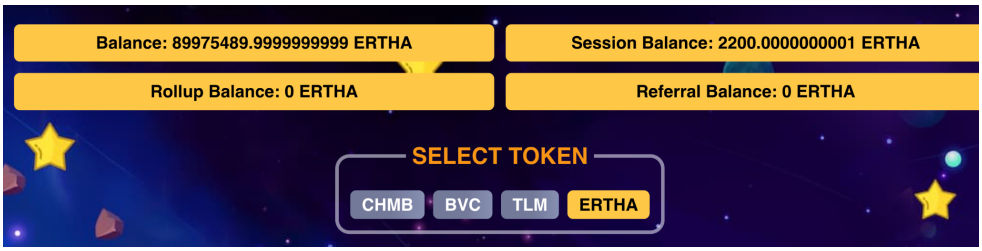

Figure 4: In the image: The application processes decimals in the Session Balance.

Although the application seems to manage calculations involving decimal numbers in the rollup/withdrawal process, allowing users to input decimal numbers is unnecessary. This is because the application enforces a fixed wager amount for each available token.

Leaving the decimals might cause rounding issues in the backend, in this way the input must be properly constrained.

Recommendation

Consider restricting users from entering decimal amounts when making deposits.

[I-01] Strict Transport Security Not Enforced

Severity

Informational

Description

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a

compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Location of Affected Code

allyourbase.virtual.tech

Recommendation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict- Transport-Security' and the value 'max-age=expireTime' , where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate. Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header , and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header , and submit the domain for review by browser vendors.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

References

HTTP Strict Transport Security

[I-02] & Reset Function is Redundant

Severity

Informational

Description

The Reset function is redundant as it merely changes the selection from " Alien" to " Astroman" a task that users can already perform through the existing user interface.

Location of Affected Code

hopium.virtual.tech

Recommendation

If the Reset function only changes the selection, it can be removed to streamline and simplify the user interface.

shieldify

Thank you!