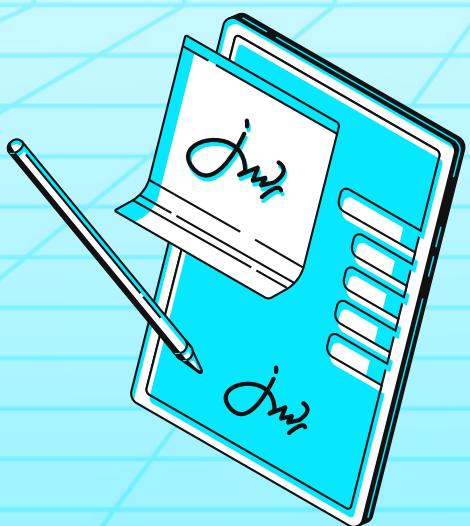


our shielding • Your smart contracts, our shielding • Your smart c



shieldify



Bee Casino

Penetration Testing

Date: 16 July 2024



CONTENTS

1. About Shieldify	3
2. Disclaimer	3
3. About Bee Casino	3
4. Methodology	3
5. General Recommendations	3
6. Risk Classification	4
7. Assessment Objectives	4
7.1 Assessment Scope	5
7.2 Assessment Approach	5
8. Findings Summary	5
9. Findings	5

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 Beecasino

The Beecasino (beecasino.virtual.tech) website is a Web2 application developed in Unity, designed to interface with a smart contract in the backend. This functionality enables players to participate in games by placing determined bets using tokens stored in the session balance of a connected wallet. Specifically, players engage by betting in USDC and await feedback from the application to determine the outcome of their wagers, either winning or losing.

4. Methodology

Security assessment of the beecasino site between June 10, 2024 and June 17, 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:

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 beecasino.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: **1**
- **Medium** issues: **0**
- **Low** issues: **0**
- **Informational** issues: **1**

9. Findings

ID	Title	Severity	Status
[H-01]	Rounding Issues	High	-
[I-01]	Strict Transport Security Not Enforced	Low	-

[H-01] Rounding Issues

Severity

High Risk

Description

The application is accepting decimals in the Deposit and Withdraw function which is reflected immediately in the session balance (and rollup balance later on):



While the bets are always in rounded numbers, and the deposit, withdraw and finish seem to handle the decimals at the end of the game correctly, the reason this is classified as a High severity issue is that it might still present a potential issue of balance mishandling that the application is not expecting from the user input, considering it does not explicitly enforce the use of decimals and the backend might not be able to tackle the decimal rounding situations.



In the image: session balance 0.1 USDC remaining after playing.



In the image: rollup balance of 5.0889.

Location of Affected Code

beecasino.virtual.tech

Recommendation

Revise the input deposit/withdrawal amount that the user is able to introduce in both functions considering the ability to input decimals. If the application does not expect them, then the user should not be able to introduce these partial amounts.

[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

beecasino.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](#)

our shielding • Your smart contracts, our shielding • Your smart c



shieldify



Thank you!

