ZEALYNX SECURITY

Penetration Testing

Beecasino

Security Assessment

July 12th, 2024 - Prepared by Zealynx Security

Jose Fernando @0xMrjory

Disclaimer

The information in this document is confidential and meant for use only by the intended recipient. Every effort has been made to ensure that the information contained in this document is true and correct at the time of publication. However, the products, specifications, and content in general that are described in this document are subject to continuous development and improvement, and therefore the reporter cannot accept liability for any loss or damage of any nature whatsoever arising or resulting from the use of or reliance on outdated information or particulars.

Changelog

Revision	Date	Change
1	June 10, 2024	Initial revision

Contents

Executive Summary

Summary

The reporter performed a 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 reporter does not warrant that the material contained in this documentation is free of errors, please note that it is not possible to find all vulnerabilities and vectors during an assessment. This report should be taken as-is and not as an exhaustive list of all security issues. With the ever-changing environment of information technology, tests performed will exclude vulnerabilities in software or systems that are unknown at the time of the assessment.

Methodology

The assessment is conducted with the following phases:

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

The reporter uses a combination of automated and manual methods and follows a testing methodology based on the PTES Technical Guidelines and OWASP Testing Guide.

Findings Overview

Vulnerability Classification (see Appendix A)	No. of active vulnerabilities
Critical	0
High	1
Medium	0
Low	1
Informational	0

Key Findings

The penetration test identified **2 VULNERABILITIES** that require remediation:

1. Rounding issues
2.. Strict Transport not enforced

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/environment-management/stream-b/
2. Perform routine testing for the applications on a semi-annual basis.

Risk Score

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. (See Risk score calculation at the end of the report)

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.

Assessment Scope

The assessment was performed on beecasino.virtual.tech.

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.

Findings Summary

The tables below summarize vulnerabilities discovered during the assessment. More information about vulnerability classification can be found in PortSwigger.

	Severity	Remediated	Finding
	High	No	Rounding issues
	Informational	No	Strict transport not enforced

Application summary

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.

Technical Details

Decimals not handled by the application frontend

Summary

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.

Classification

High: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L

Affected Hosts

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.

Strict transport security not enforced.

Summary

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.

Classification

Informational

Affected Hosts

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.

References

- HTTP Strict Transport Security

Appendix A

Vulnerabilities Classification (based on Guidelines for Applying Security Patches)

Classification	Description
Catastrophic	This rating is assigned by the Vice President of Information Risk and Security. The rating will be rarely invoked, primarily for Known Exploited Vulnerabilities. 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 requiring 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.

Risk rating scale calculation (based on NIST and CVSS 3.1)

Rating	Scale
Critical	9 – 10
High	7.0 - 8.9
Medium	4.0 - 6.9
Low	0 - 3.9

Risk score calculation

Risk Score is calculated using the following equation:

Risk = Likelihood * Business Impact,

where Likelihood is calculated by taking the highest CVSS rated issue and dividing the rating by two, and Business Impact is selected from range 1 to 5 based on the following table.

In this case 7.1 was the highest divided by 2 = 3.55 with BI of 2 = 7.1 of risk score which is Low.

Business Impact	Explanation
1	System is isolated, only Public data and no means of pivoting or reputational harm being done
2	Public data, and no reputation harm when system compromised
3	Internal data with limited impact, pivoting only to systems with BI 1 and almost no reputation harm when system compromised
4	Internal data with limited impact, pivoting only to system with BI 3, moderate reputation harm when system compromised
5	Restricted(+PII) or customer data, or system can be used for pivoting to get to system with high value data/resources, or can be used for great harm reputation

Qualitative Risk Score	Qualitative Risk Level	Rating Definition
25	Critical	Critical risk score indicates the target system or data is at a very high risk of being compromised, and immediate action is required.
15 - 24	High	High risk score indicates the target system or data is at a significant risk of being compromised, and prompt action is required.
8 - 14	Medium	Medium risk score indicates the target system or data is at a moderate risk of being compromised, and ongoing monitoring and improvement is recommended.
4 - 7	Low	Low risk score indicates the target system or data is at a low risk of being compromised, but ongoing monitoring and improvement is recommended.
1 - 3	Very Low	Very Low risk score indicates the target system or data is at a very low risk of being compromised and no immediate action is required.