QuillAudits

Audit Report
May, 2024

For

GANGSTER ARENA

Table of Content

Overview

Project Overview	Gangster Arena is a gamefi ecosystem that rewards users for gaming.
Scope of Audit	The scope of this pentest was to analyze Web Applications for quality, security, and correctness.
In Scope	*https://blaststaging.gangsterarena.com/game*
Date	20th May 2024 - 29th May 2024

Number of Issues per Severity

	High	Medium	Low	Informational
Open Issues	0	0	0	0
Acknowledged Issues	0	0	0	0
Partially Resolved Issues	0	0	0	0
Resolved Issues	0	1	5	0

Checked Vulnerabilities

We scanned the application for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that we considered:

- Improper Authentication
- Improper Resource Usage
- Improper Authorization
- Insecure File Uploads
- Insecure Direct Object References
- Client-Side Validation Issues
- Broken Access Controls
- Insecure Cryptographic Storage
- Insufficient Cryptography
- Insufficient Session Expiration
- Information Leakage
- Third-Party Components
- Rate Limit
- Input Validation
- Injection Attacks
- Cross-Site Request Forgery
- Broken Authentication and Session Management
- Insufficient Transport Layer Protection
- Malware
- Denial of Service (DoS) Attacks
- Cross-Site Scripting (XSS)
- Security Misconfiguration
- Unvalidated Redirects and Forwards

And more...

Techniques and Methods

Throughout the pentest of Gangster Arena Platforn, care was taken to ensure:

- Information gathering – Using OSINT tools information concerning the web architecture, information leakage, web service integration, and gathering other associated information related to web server & web services.
- Using Automated tools approach for Pentest like Nessus, Acunetix etc.
- Platform testing and configuration
- Error handling and data validation testing
- Encryption-related protection testing
- Client-side and business logic testing

Tools and Platforms used for Pentest:

- Burp Suite
- DNSenum
- Dirbuster
- SQLMap
- Acunetix
- Neucli
- Nabbu
- Turbo Intruder
- Nmap
- Metasploit
- Horusec
- Postman
- Netcat
- Nessus and many more

Issue Categories

Every issue in this report has been assigned with a severity level. There are four levels of severity, and each of them has been explained below.

High Severity Issues

A high severity issue or vulnerability means that your web app can be exploited. Issues on this level are critical to the web app's performance or functionality, and we recommend these issues be fixed before moving to a live environment.

Medium Severity Issues

The issues marked as medium severity usually arise because of errors and deficiencies in the web app code. Issues on this level could potentially bring problems, and they should still be fixed.

Low Severity Issues

Low-level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

Informational

These are four issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Issues Found

Medium Severity Issues

1. CSRF To Twitter Account

Description

The application has no protection to prevent CSRF attack for connecting Twitter accounts. Hence, an attacker can send a forge link and connect his Twitter account with victim's game account.

Vulnerable URL

https://blaststaging.gangsterarena.com/verify/twitter?oauth_token=0y_...W&oauth_verifier=DE....PL

Steps to Reproduce

1. Click on "Link Twitter Account" and select your account
2. Intercept the request, you will find a GET Request made to https://blaststaging.gangsterarena.com/verify/twitter?oauth_token=..&oauth_verifier=...
3. Copy these link and open it in a different game account
4. Twitter in your second game account will be connected

Impact

Attacker can send a link and connect his Twitter Account with the victim's game accounts.

Recommendation

Implement a 'state' parameter containing anti-csrf token to mitigate this issue.

Status

Resolved

Low Severity Issues

1. Clickjacking

Description

Clickjacking is an attack that fools users into thinking they are clicking on one thing when they are actually clicking on another. Its other name, user interface (UI) redressing, better describes what is going onClickjacking is an attack that fools users into thinking they are clicking on one thing when they are actually clicking on another. Its other name, user interface (UI) redressing, better describes what is going on.

Steps to Reproduce

Visit https://clickjacker.io/test?url=https://blaststaging.gangsterarena.com/game
Your website will be rendered in a frame confirmin Clickjacking.

Impact

This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online. Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees.

Recommendation

Implement X-Frame-Options header.
Reference - https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Status

Resolved

2. Access other players Match Histories

Description

The API Endpoint - /api/v1/users/me/war-history/20240523-143000/did:privy:clwi2up2r06prghx0b7xb5h8e is vulnerable to an Insecure Direct Object Reference Vulnerability (IDOR). It allows one to see other user's match history by manipulating the did:privy ID.

Vulnerable URL

https://blstgapi.gangsterarena.com/api/v1/users/me/war-history/20240523-143000/did:privy:clwi2up2r06prghx0b7xb5h8e

Steps to Reproduce

Send the following HTTP Request using your Authorization: Bearer Token

```
GET /api/v1/users/me/war-history/20240523-143000/did:privy:clwi2up2r06prghx0b7xb5h8e HTTP/2
Host: blstgapi.gangsterarena.com
Sec-Ch-Ua: "Microsoft Edge";v="125", "Chromium";v="125", "Not.A/Brand";v="24"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJhbGciOiJFUz....4sAoAnky8A
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36 Edg/125.0.0.0
Sec-Ch-Ua-Platform: "Windows"
Origin: https://blaststaging.gangsterarena.com
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://blaststaging.gangsterarena.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=1, i
```

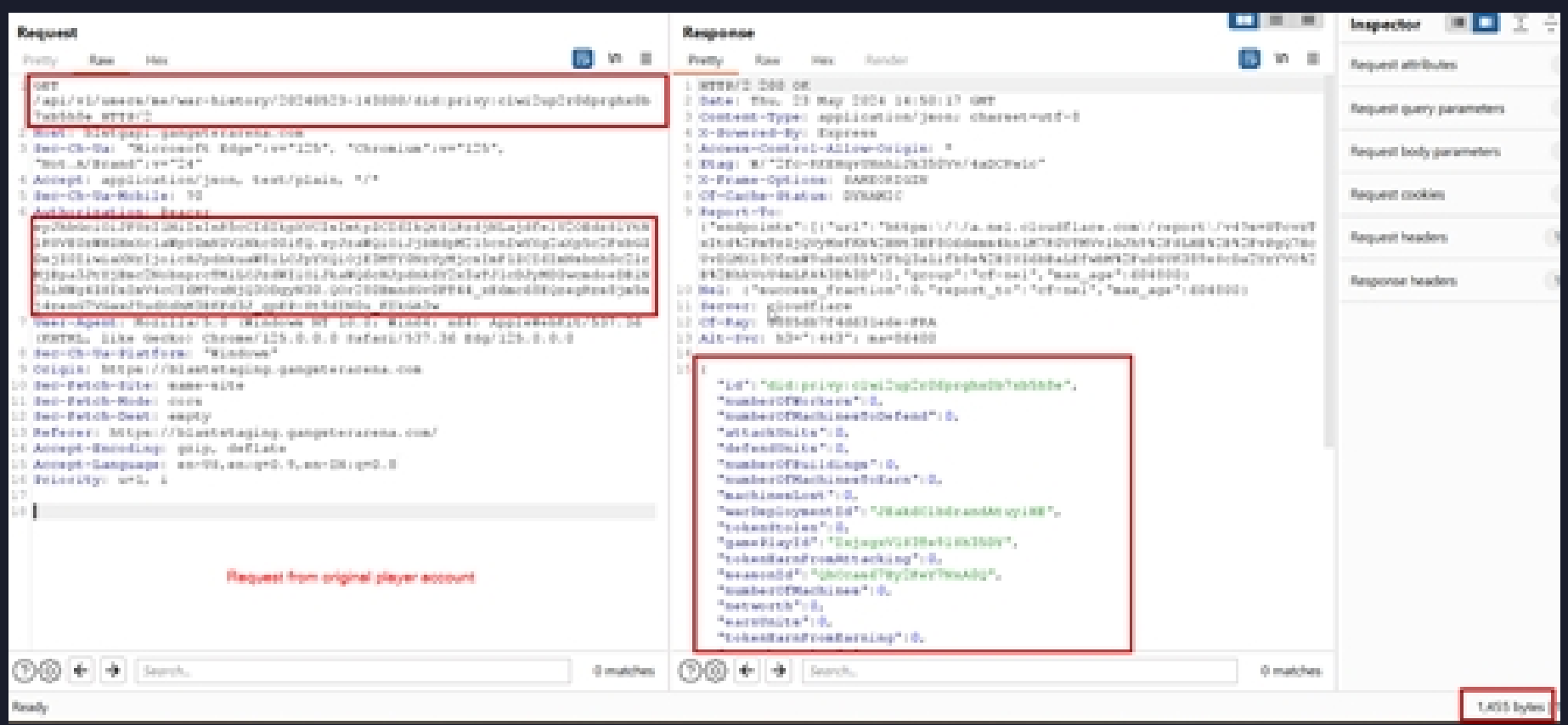
You should see the match history of another account.

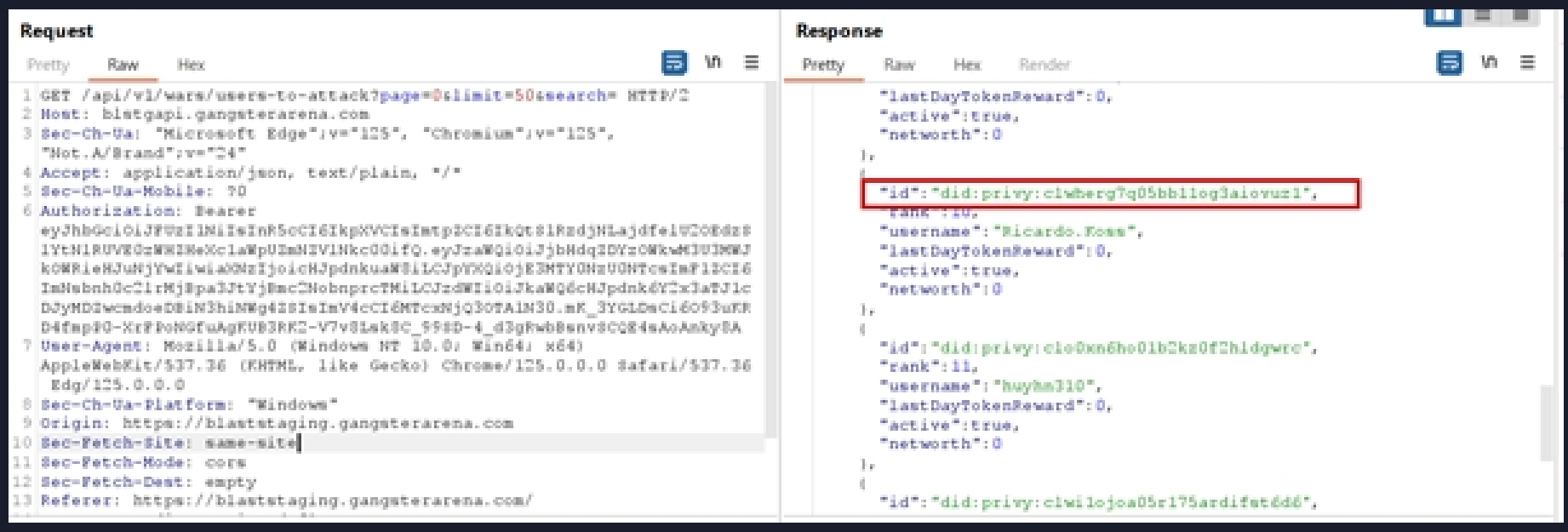
All did:privy IDs could be found by sending the following request -

```
GET /api/v1/wars/users-to-attack?page=0&limit=50&search= HTTP/2
Host: blstgapi.gangsterarena.com
Sec-Ch-Ua: "Microsoft Edge";v="125", "Chromium";v="125", "Not.A/Brand";v="24"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJhbGciOiJFUz.....SCQE4sAoAnky8A
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36 Edg/125.0.0.0
Sec-Ch-Ua-Platform: "Windows"
Origin: https://blaststaging.gangsterarena.com
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
```

Sec-Fetch-Dest: empty
Referer: https://
blaststaging.gangsterarena.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-
US,en;q=0.9
Priority: u=1, i

PoC





Impact

Match History of other players is disclosed. The game does not show the history of other players to each other

Recommendation

Apply proper Access Control on the API Endpoint. Verify who is initiating the request and if he is authorized to view the information.

Status

Resolved

3. Response Manipulation Check Absent for In-Game Coins

Description

All the in-game details are brought on by Google Firestore and shown in game. Details such as eth balance, token (greed,xgreed) balance and such.
But if response manipulation takes place in response it shows directly in game without having a recheck on-chain that does this user have this many token or eth or not.

Recommended Fix

1. Coin Update on every refresh should also check for on-chain data.
2. Keep a cronjob for a profile to check balance after interval of time on-chain.

Steps to Reproduce

1. Check for tokenbalance parameter on the response in Burp (tool to check response and requests)

2. Make a config to change the value of tokenbalance in every request
   “doubleValue": 79xxxxx.xxxxxx (here the balance of user is 7.9M) to
   “doubleValue": 99xxxxx.xxxxxx (the new balance of user is changed to 9.9M)
3. But here it doesn’t check on chain if the user has 9.9M Greed or Not.

Impact

Minimal real world impact as such just that it can be used for fake manipulation by crypto-influencers and more and it’s better to fix such issues when you have such game that can update data on-chain.

Status

Resolved

4. Twitter Username still visible after unlinking accounts

Description

After a user unlinks a Twitter account from a Gangster Arena account, the leaderboard still showcases the player's Twitter username and profile photo. Thus personal information is still available even after the account is disconnected.

Vulnerable URL

https://blstgapi.gangsterarena.com/api/v1/gamePlays?page=0&limit=100

Steps to Reproduce

1. Link a twitter account
2. Do some activity in the game like buying assets and taking part in war
3. Unlink the twitter account
4. If your activities lead you to list on the leaderboard, your Twitter username will be displayed here

Impact

Even after unlinking account, Twitter account details of user are still visible including username and profile photo.

Recommendation

Make sure all Twitter information is immediately disconnected from the user account. Remove all cached information.

Status

Resolved

5. Machines can be manipulated

Description

While deploying for a war, the value of numberOfMachines can be manipulated.

Vulnerable URL

PUT/https://blstgapi.gangsterarena.com/api/v1/gamePlays/war-machines

Steps to Reproduce

1. Deploy for a war
2. You will find a PUT request made to -
   PUT /api/v1/gamePlays/war-machines HTTP/2

   Host: blstgapi.gangsterarena.com
   {"numberOfMachines":1,"numberOfMachinesToEarn":1,"numberOfMachinesToAttack":0,
   "numberOfMachinesToDefend":0}
3. Change the value of numberOfMachines to any random value you like

Impact

Not sure. Not sure what impact this has on war.

Recommendation

Validate data properly.

Status

Resolved

Closing Summary

In this report, we have considered the security of the GangsterArena web app. We performed our audit according to the procedure described above.

Some issues of medium and low severity were found, Some suggestions and best practices are also provided in order to improve the code quality and security posture. In the end, the Gangster Arena Team resolved all issues.

Disclaimer

QuillAudits Dapp security audit provides services to help identify and mitigate potential security risks in Gangster Arena Platform. However, it is important to understand that no security audit can guarantee complete protection against all possible security threats. QuillAudits audit reports are based on the information provided to us at the time of the audit, and we cannot guarantee the accuracy or completeness of this information. Additionally, the security landscape is constantly evolving, and new security threats may emerge after the audit has been completed.

Therefore, it is recommended that multiple audits and bug bounty programs be conducted to ensure the ongoing security of Gangster Arena Platorm. One audit is not enough to guarantee complete protection against all possible security threats. It is important to implement proper risk management strategies and stay vigilant in monitoring your Platform for potential security risks.

QuillAudits cannot be held liable for any security breaches or losses that may occur subsequent to and despite using our audit services. It is the responsibility of the Gangster Arena to implement the recommendations provided in our audit reports and to take appropriate steps to mitigate potential security risks.

About QuillAudits

QuillAudits is a secure smart contracts audit platform designed by QuillHash Technologies. We are a team of dedicated blockchain security experts and smart contract auditors determined to ensure that Smart Contract-based Web3 projects can avail the latest and best security solutions to operate in a trustworthy and risk-free ecosystem.

1000+
Audits Completed

$30B
Secured

1M+
Lines of Code Audited

Follow Our Journey

Audit Report
May, 2024

For

GANGSTER ARENA

QuillAudits

Canada, India, Singapore, UAE, UK

www.quillaudits.com

audits@quillhash.com