QuillAudits

Audit Report
March, 2023

For

NEO LEGAL | Blockchain Australia® | NEO VIRTUAL TECH

Table of Content

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

	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

Request

Raw | Params | Headers | Hex

```
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

Raw | Headers | Hex

```
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_81pGO-53vV0Ho8ya-iYyxeoeQ.Tit7VgsQYvcRWQLIE7u%2FXuqWhgBuHBRc
MBFboLuK9CE; Path=/; HttpOnly

{"statusCode":200,"message":"User Login
successfully","data":{"auth":true,"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ
pZCI6IjYzZjMzY2RhOWUzNWNjZWI2NmVlZTBjYSIsInNSb2xlIjoidXNlciIsImlhdCI6MTY3Njg4NTIyOS
wiZXhwIjoxNjc3MTQ0NDI5fQ.zbwYXk4kffg3sVRmEmeCi5dfJAGD9Yb7b06sC1wbyyQ","sWalletAddre
ss":"0x445e5Bc684708266CB849CB653D2885AB9d12a6d","userId":"63f33cda9e35cceb66eee0ca
","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 addess, website and bio of the other person.

3. 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"}

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

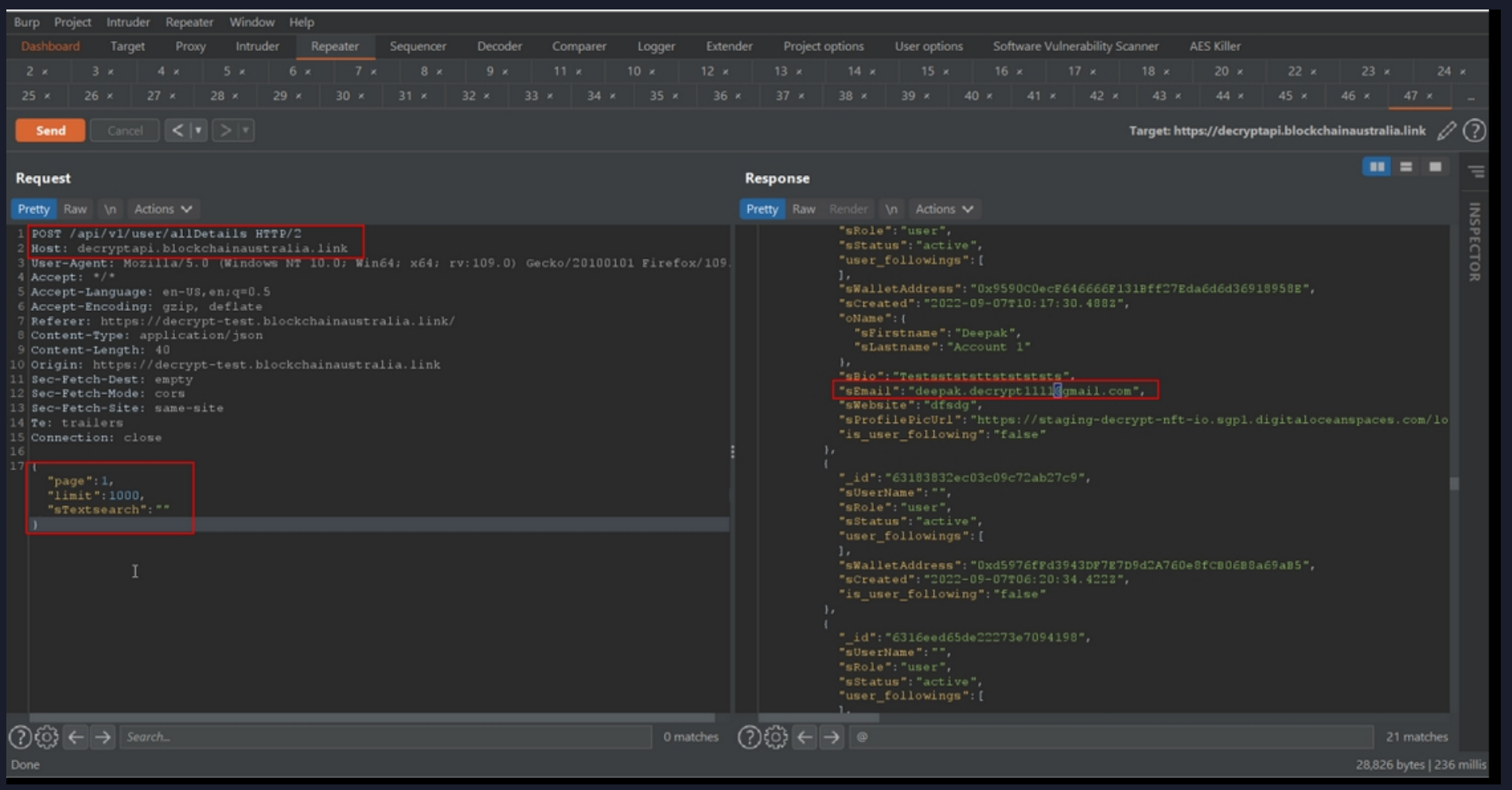
   POST /api/v1/bid/fetchBidNft HTTP/2
   Host: decryptapi.blockchainaustralia.link
   User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Referer: https://decrypt-test.blockchainaustralia.link/
   Content-Type: application/json
   Authorization: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjYzZTY5ZThkOWUzNWNjZWI2NmVlZDI3ZiIsInNSb2xlIjoidXNlciIsImlhdCI6MTY3NjM5MzMwNCwiZXhwIjoxNjc2NjUyNTA0fQ.a4nLac2Oo7DJL5yQjzh5dXnRKcDoZ9kpl0_zWykxBkw
   Content-Length: 86
   Origin: https://decrypt-test.blockchainaustralia.link

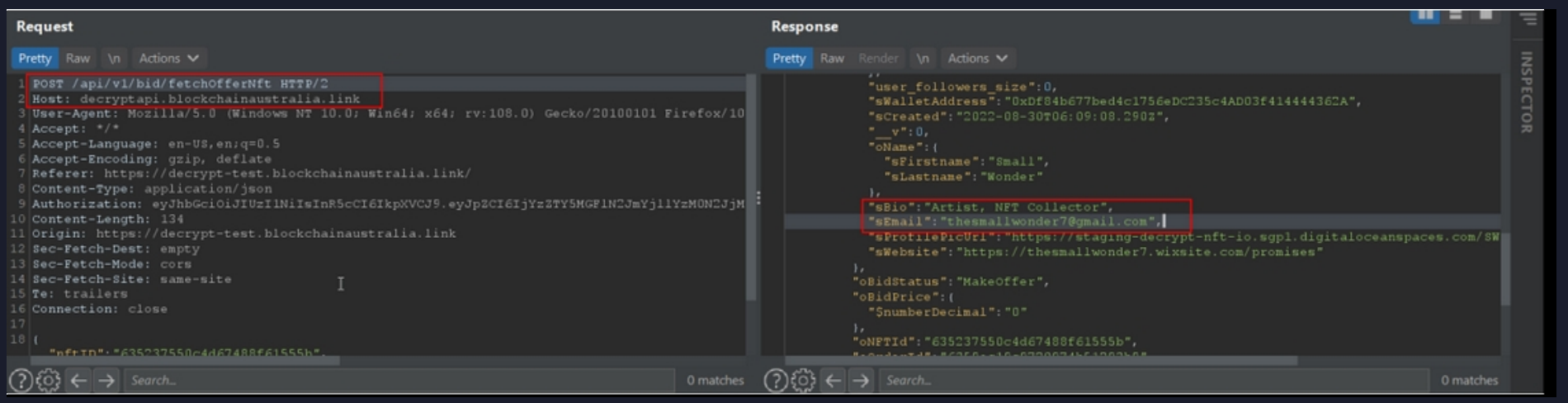
   {"nftID":"635237550c4d67488f61555b","orderID":"All","buyerID":"All","bidStatus":"All"}

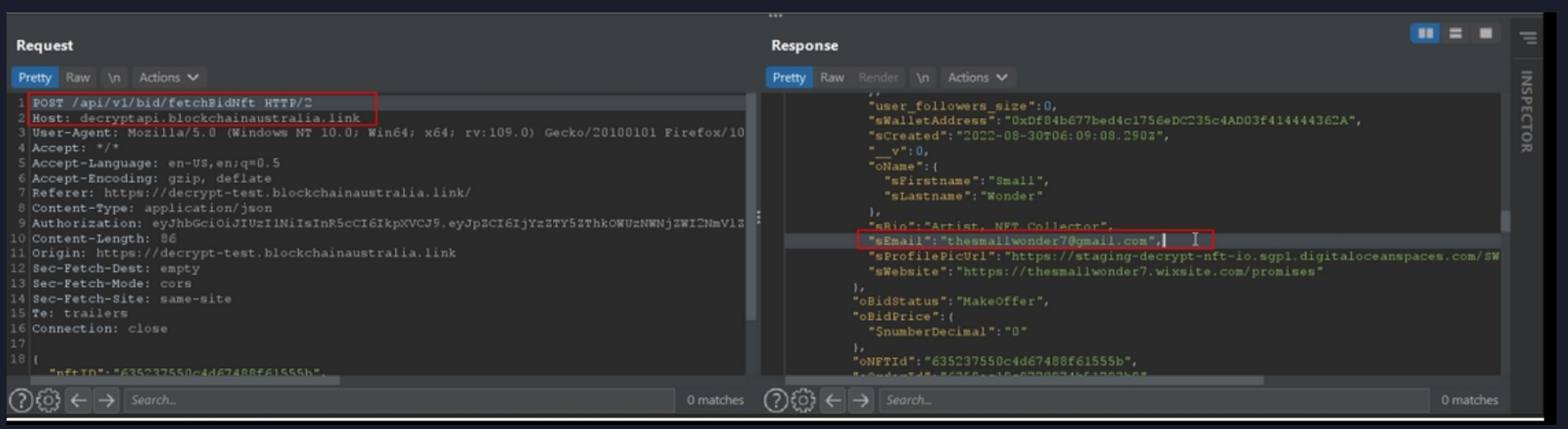
Recommended Fix

- 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







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

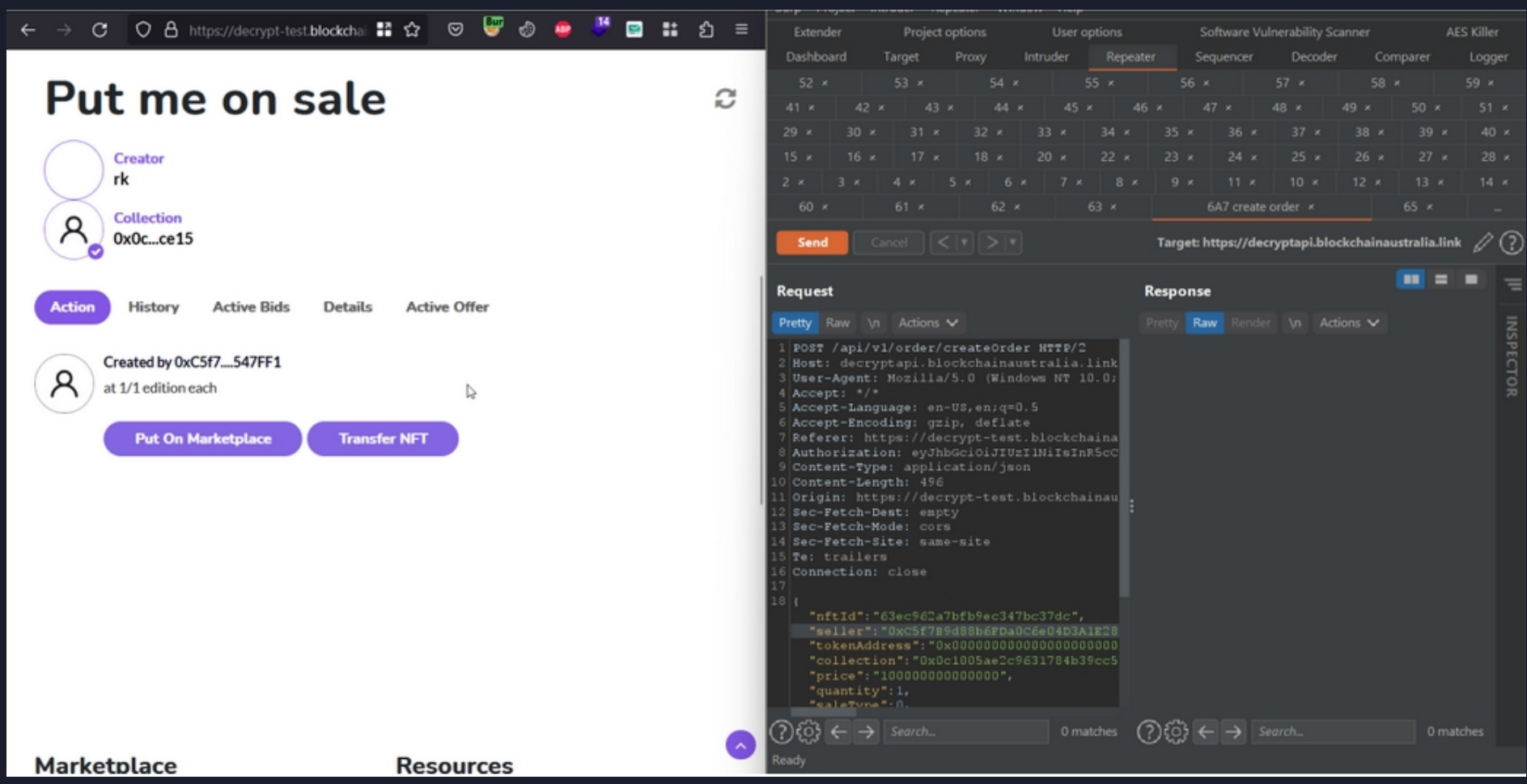
{"nftId":"63ec913f9e35cceb66eeda60","seller":"0x6A76dA346B7CC20f57A5f422b7E9C775692ff069","tokenAddress":"0x0000000000000000000000000000000000000000","collection":"0x1b88b7eb63a553e2ab838d2a58d1f98ee1866f9e ","price":"100000000000000","quantity":1,"saleType":0,"validUpto":2214189165,"signature":[28,"0x28838b1810ffdaac42e1979c0375a29f488942fbf1a82e9d0ff932ce3759e2b7","0x7e7ada1d7643109a947814d3ce93006331e8dc4a2087fc462353cb9ffd9411c3"],"tokenId":6,"auctionEndDate":"01/03/2040","salt":9760577}

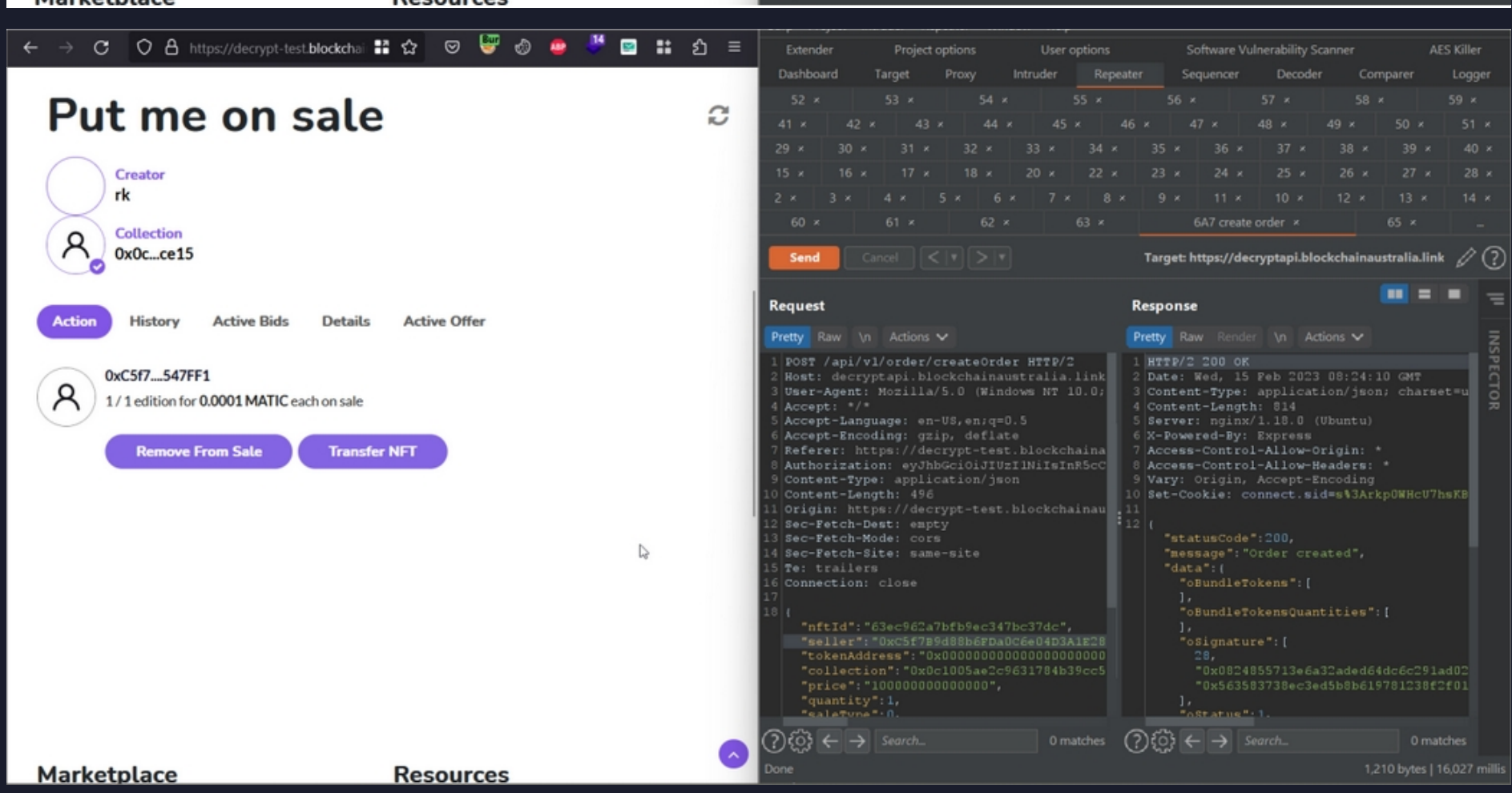
3. Replace seller, nftId, and collection with victim's deails in the request and send the request

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





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

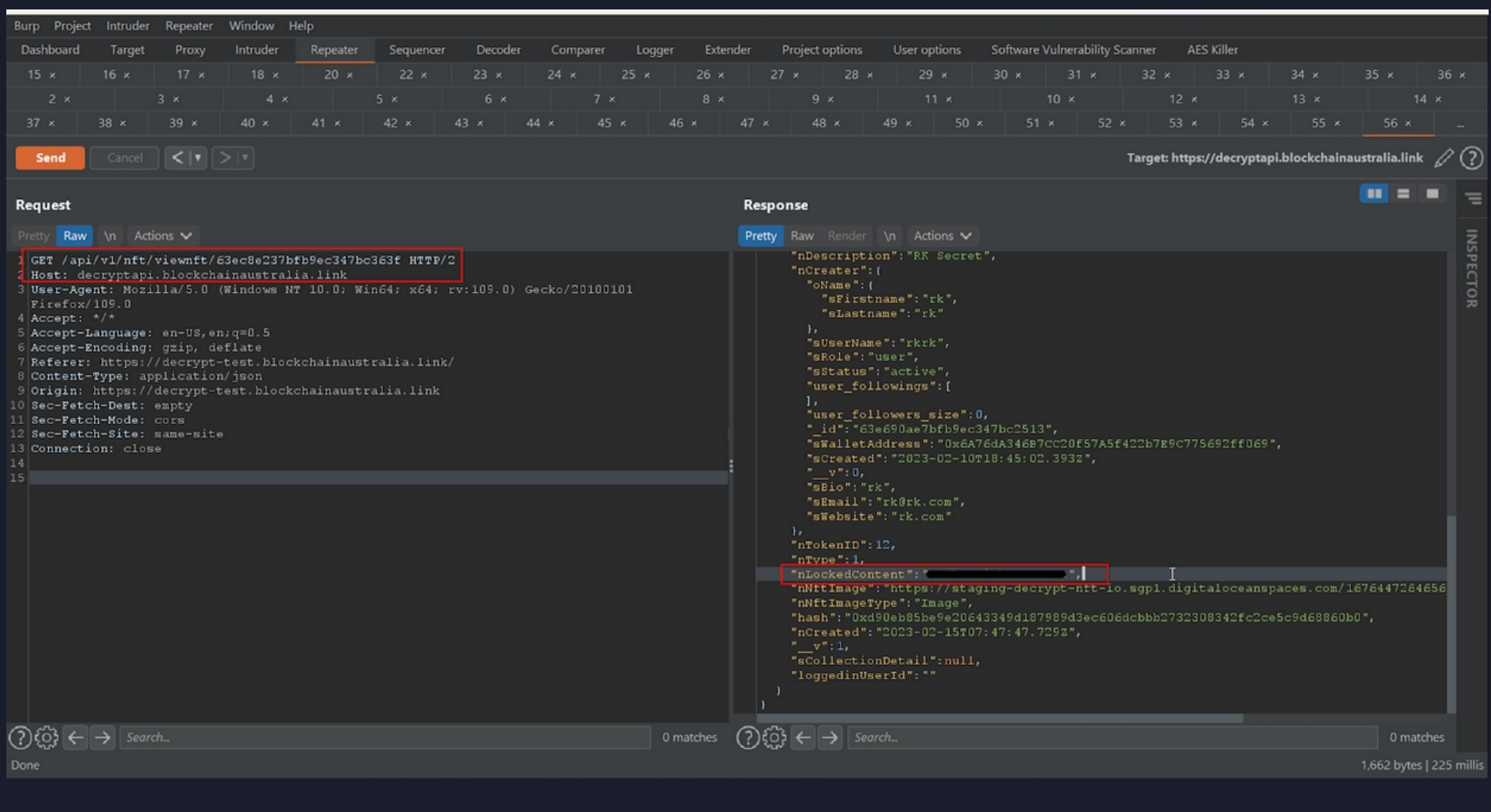
1. List an NFT with `Unlock once purchased` enabled
2. Send a GET request to https://decryptapi.blockchainaustralia.link/api/v1/nft/viewnft/nft_id]
   endpoint
3. You will find the secret content associated with the NFT in the response of the API call. Check `nLockedContent` parameter in the response

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



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>

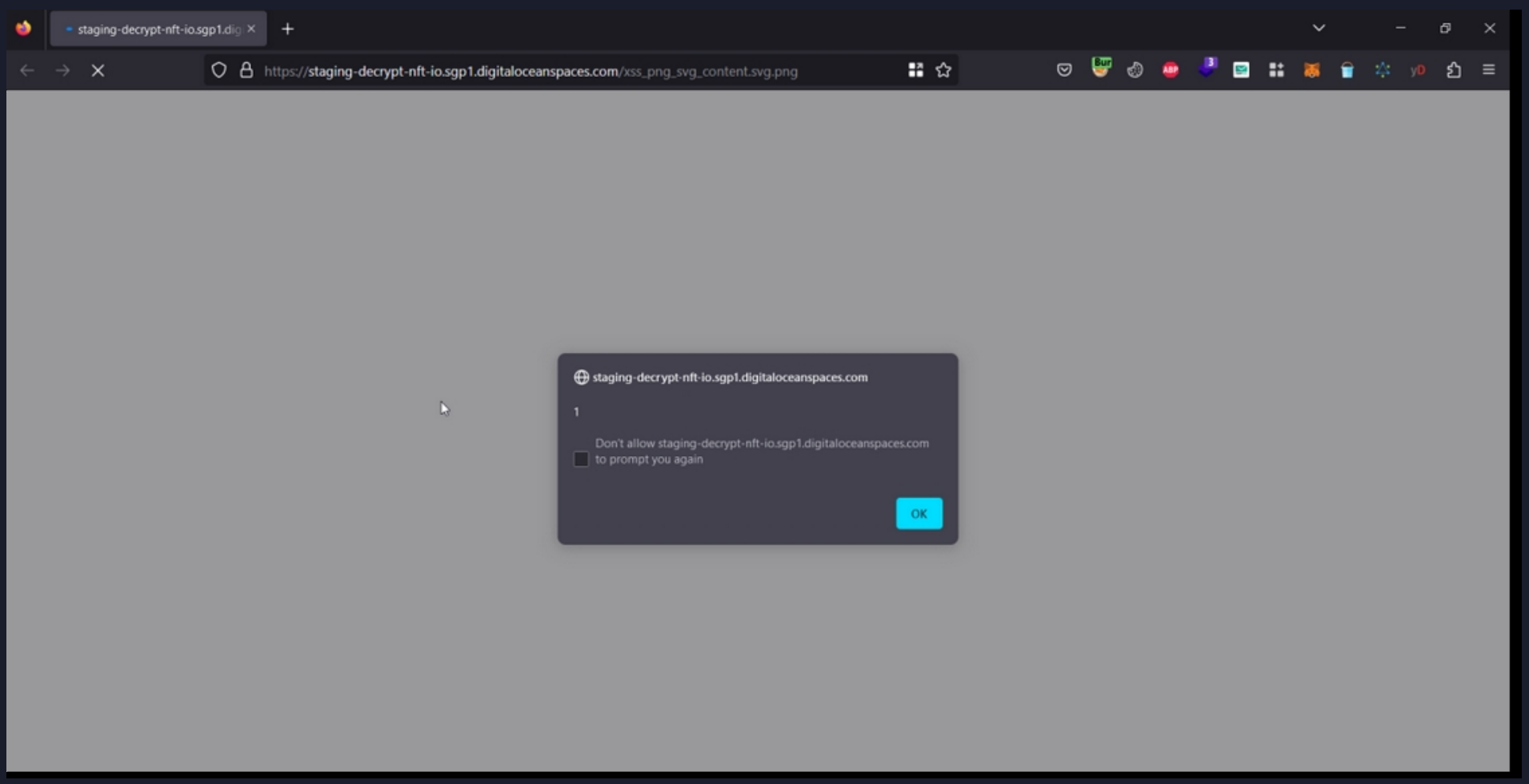
Open the uploaded file and you will the javascript executed in your browser

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



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

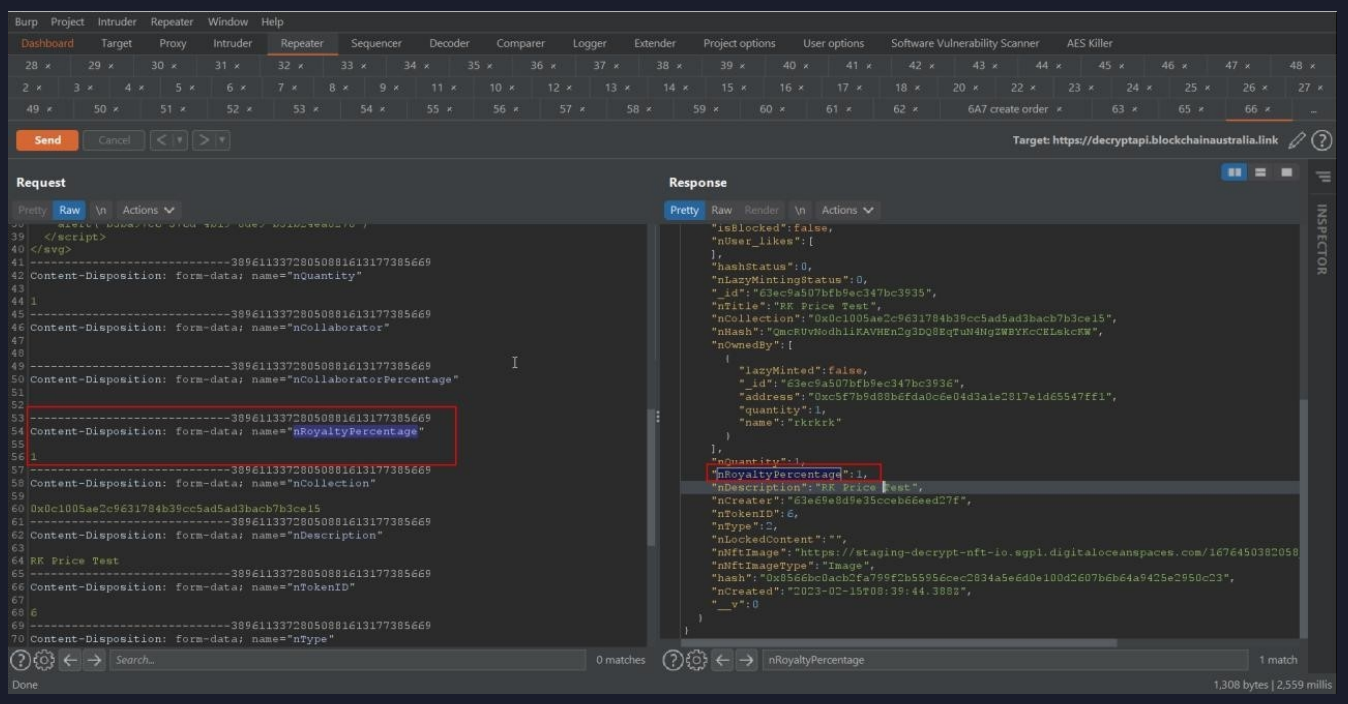
Steps to Reproduce

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



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/*

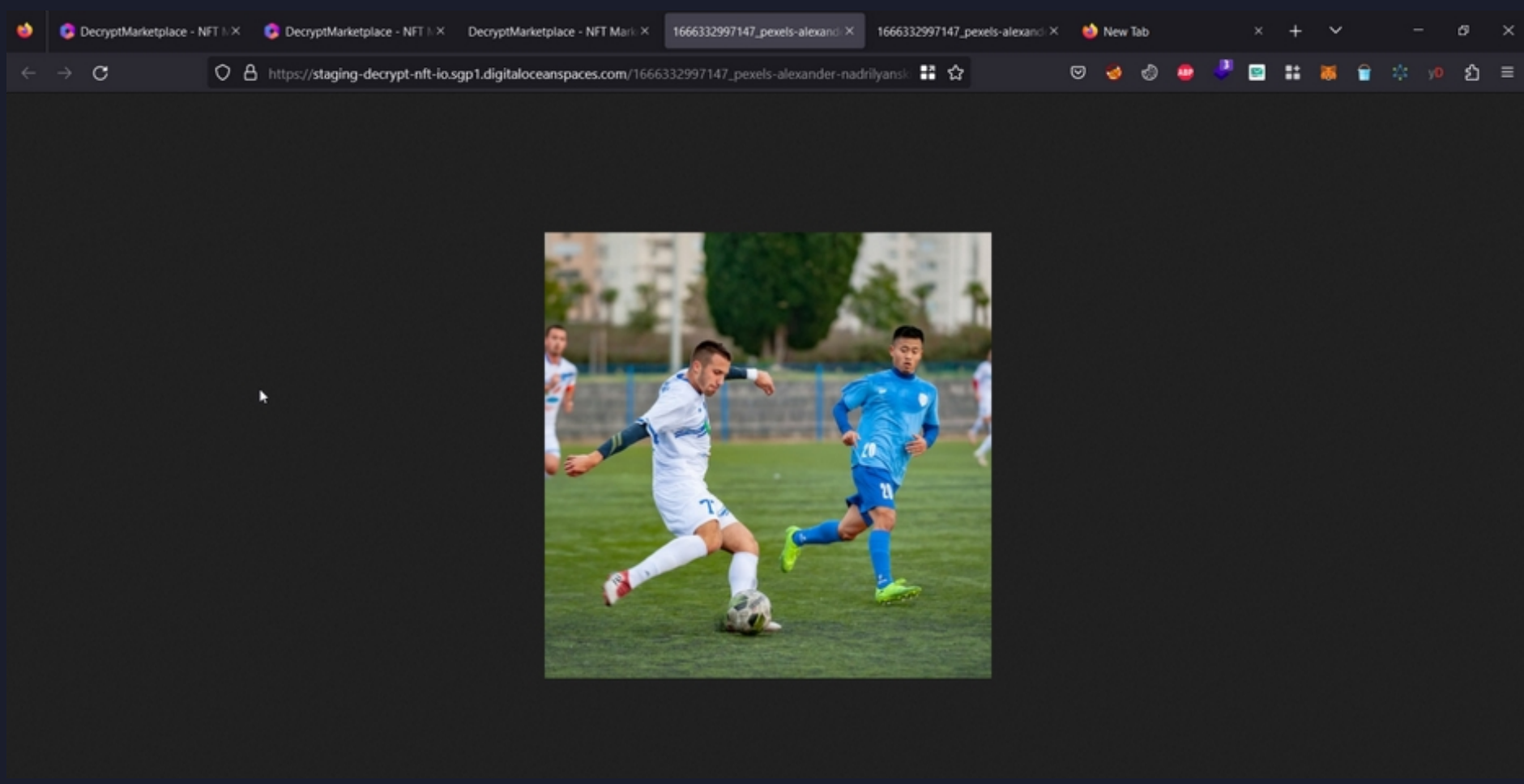
Steps to Reproduce

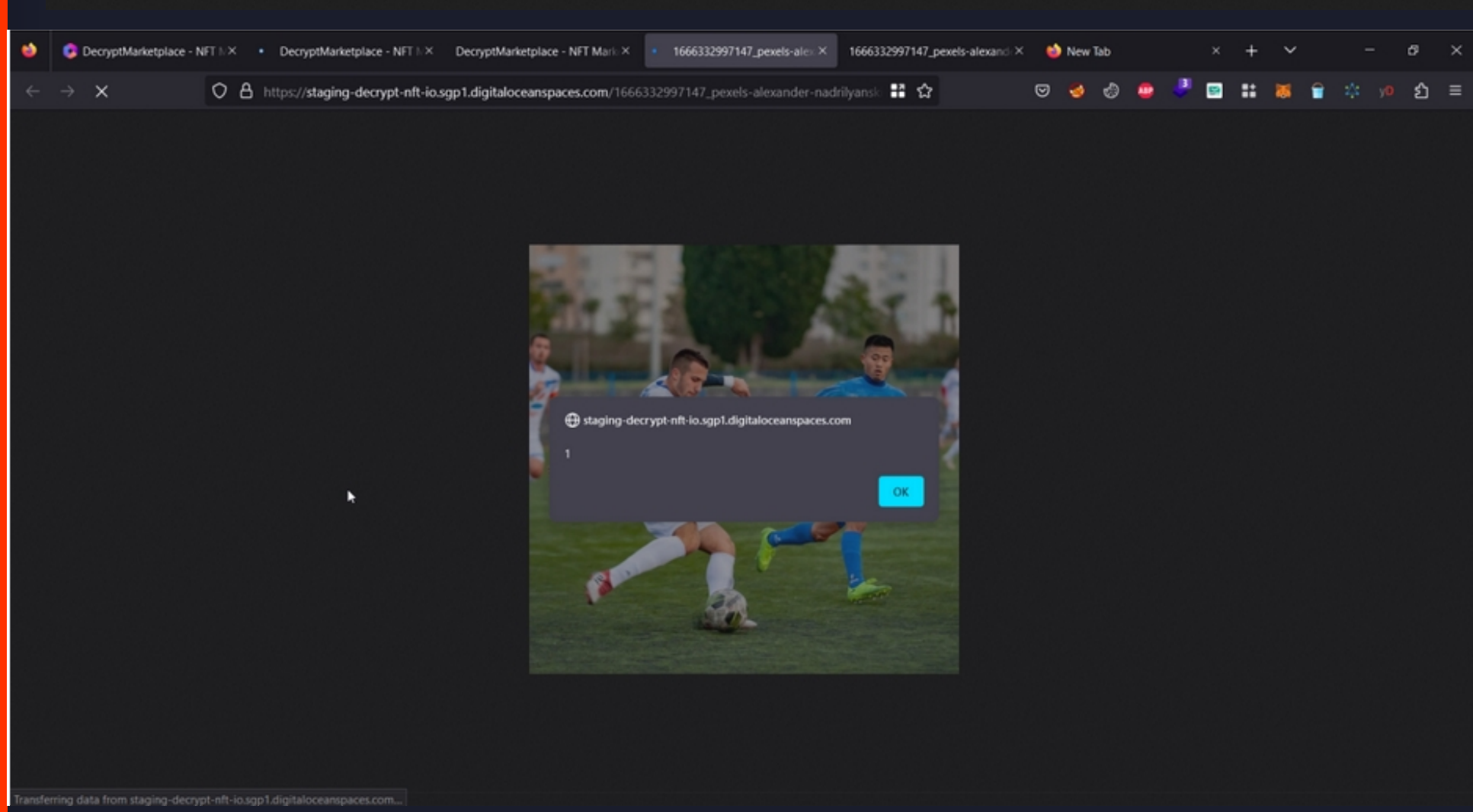
1. Create a new NFT and upload its image with filename `accountonenft.png` from first account
2. No go to second account. Upload its profile picture with filename `accountonenft.png` and save it. This file must be a different image but filename must be same.
3. Go back to first account and check its 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.

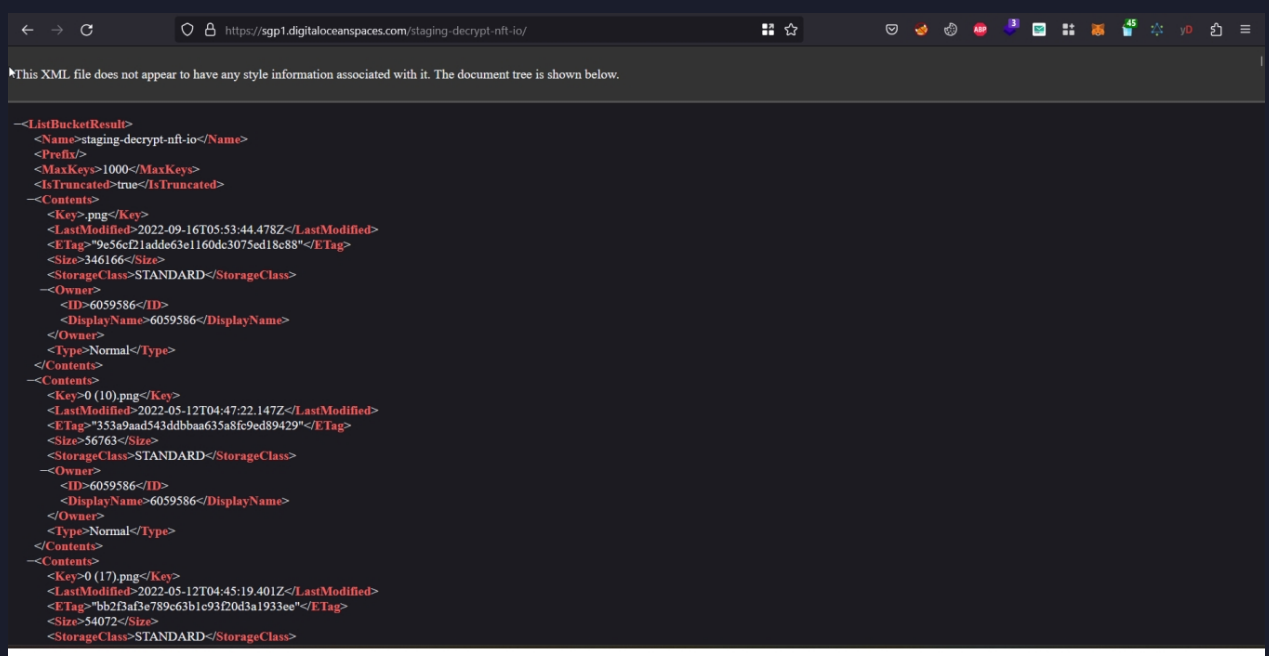
Access to a bucket on DigitalOcean can pose a security risk if unauthorized users are able to access it. This can lead to data leakage or loss, as well as potential damage to the reputation of the organization hosting the bucket.

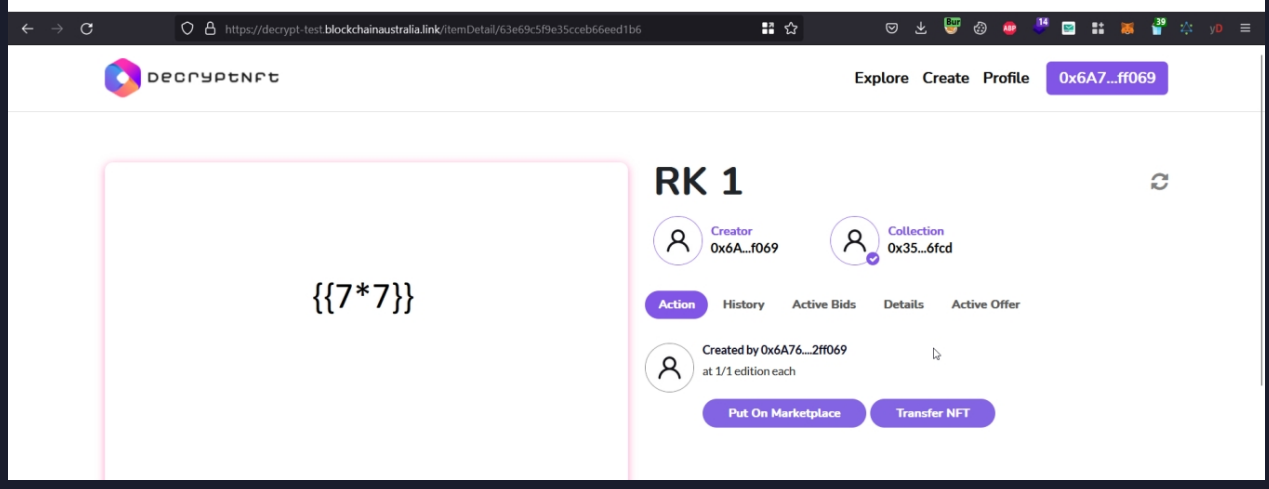
Vulnerable Endpoint

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

Recommendation

Disbale 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]

5. The response will list down all NFT details to you even though neither that NFT publicly listed nor its information is available anywhere

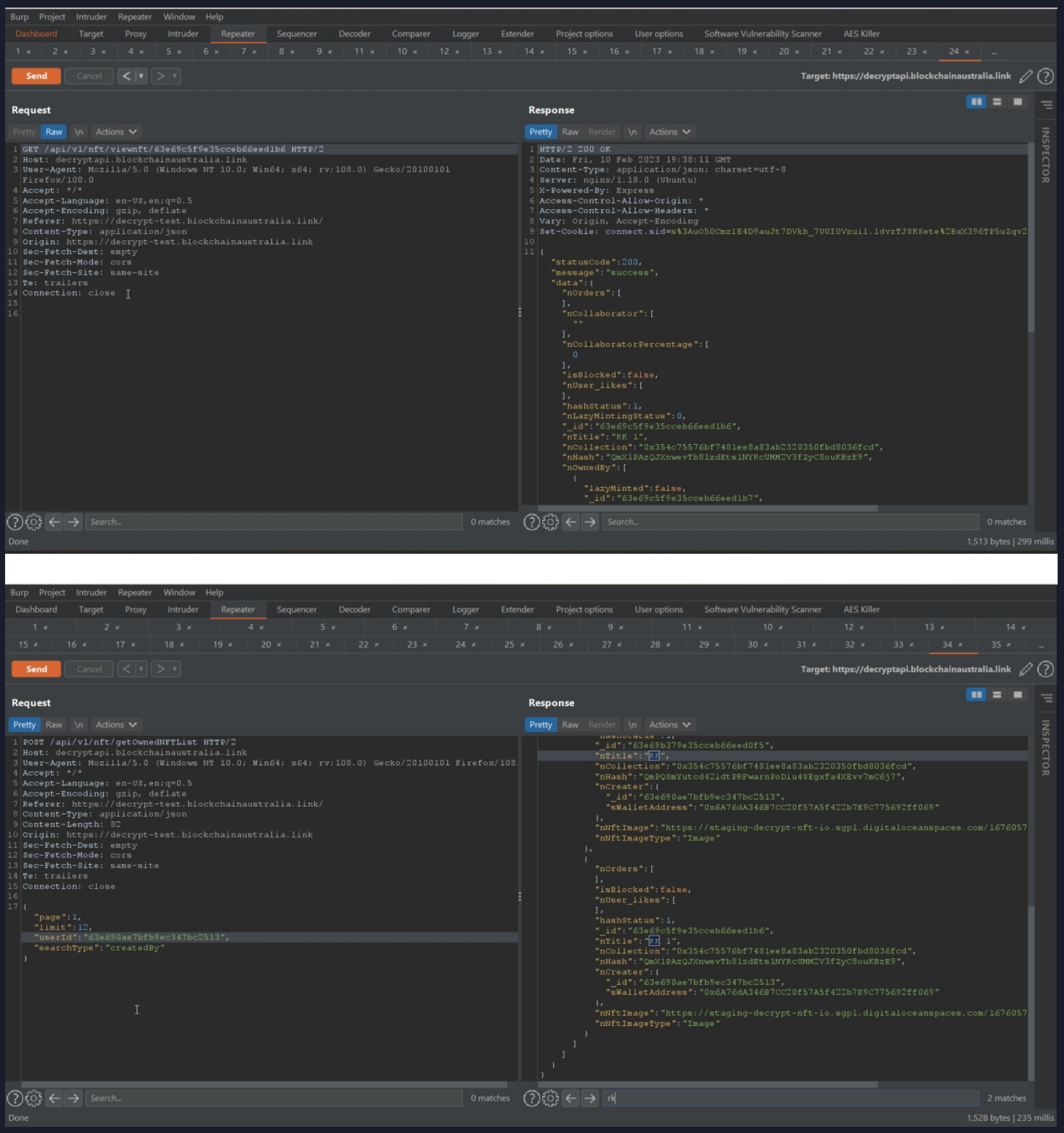
   GET /api/v1/nft/viewnft/63e69c5f9e35cceb66eed1b6 HTTP/2
   Host: decryptapi.blockchainaustralia.link
   User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0

6. Directly visiting the https://decrypt-test.blockchainaustralia.link/itemDetail/63ec913f9e35cceb66eeda60 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 an asily differentiate on bakend if the NFT is private or not and reply accordingly.

POC



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 impact 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.

Recommedation

- 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

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 requets to /api/v1/auth/checkuseraddress endpoint with a valid wallet address on `sWalletAddress` body parameter

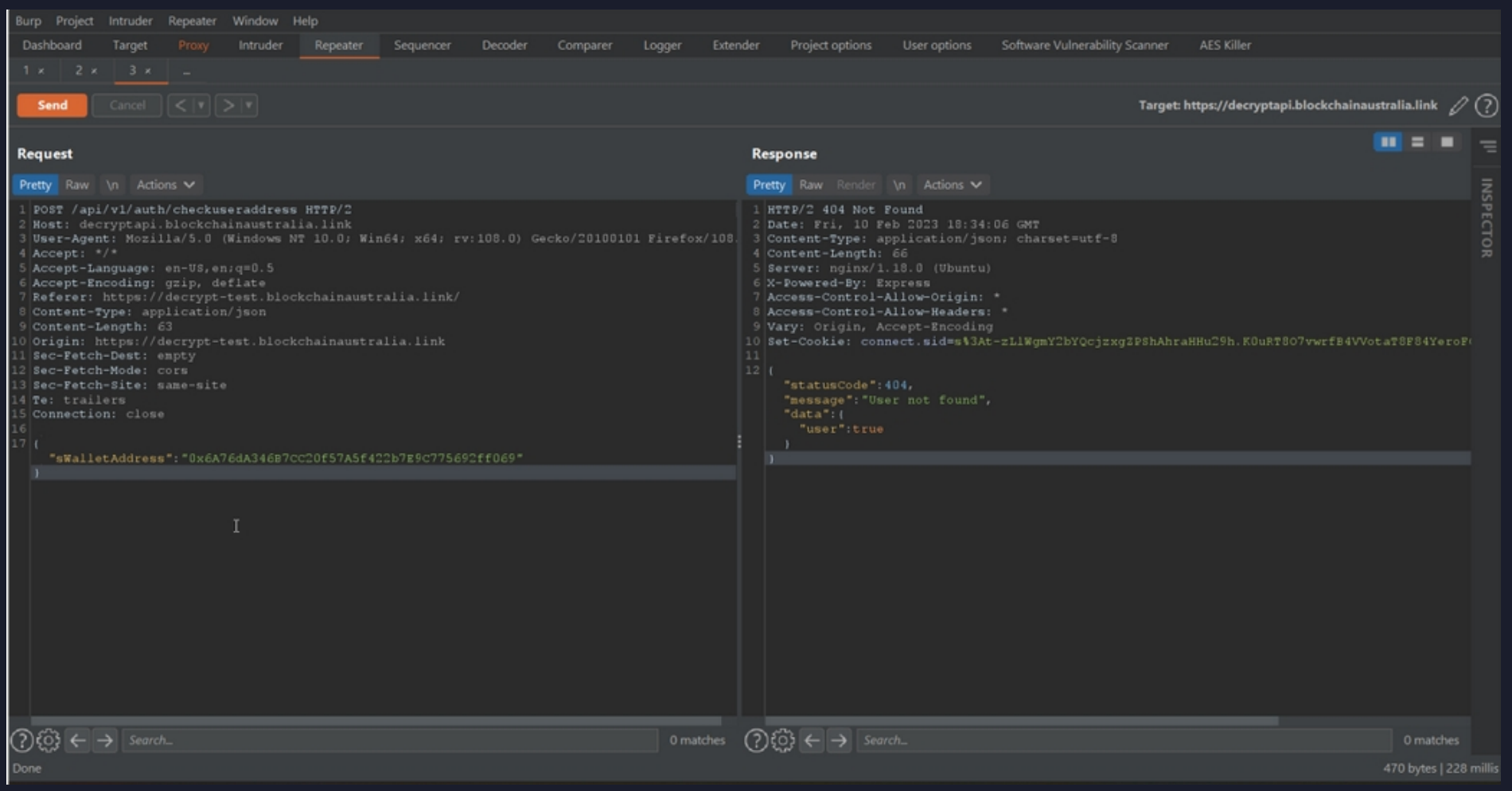
2. If the user exists, the application will respond with 200- User Found Successfully else , the application will respond with 404 - User not found
   POST /api/v1/auth/checkuseraddress HTTP/2
   Host: decryptapi.blockchainaustralia.link
   User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
   Connection: close

   {"sWalletAddress":"0x6A76dA346B7CC20f57A5f422b7E9C775692ff069"}

Recommendation

Disbale 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



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

Recommedation

- 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

```
HTTP/2 200 OK
Date: Wed, 15 Feb 2023 08:51:32 GMT
Content-Type: text/html; charset=utf-8
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%3Afr19SssXjleUQTx6EOEJpga_q_NFZOg7.Vg%2BSZ4h89o0f1PuwDeYSqIk5W
```

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

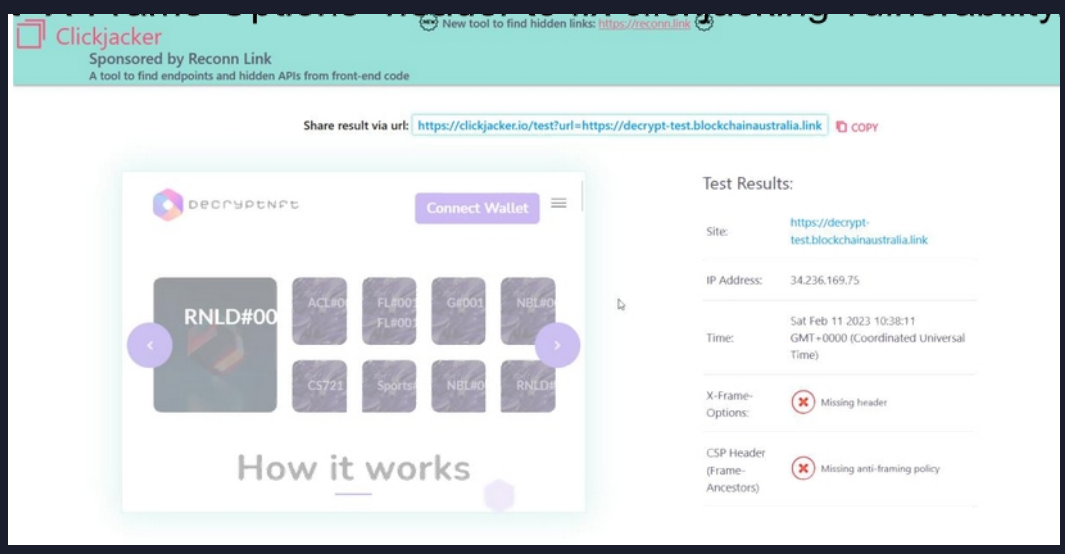
1. Save the following PoC code as `poc.html` and open it in your browser
2. You will find your website `https://decrypt-test.blockchainaustralia.link/` `iframed` in a box

```
<!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>
```

Recommedation

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

POC



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: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Authorization: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjYzZTY5ZThkOWUzNWNjZWI2NmVlZDI3ZiIsInNSb2xlIjoidXNlciIsImlhdCI6MTY3NjQ1MDUzMCwiZXhwIjoxNjc2NzA5NzMwfQ.NQ7nILHlQfv0RuAo-G7_SWFZnFetwWnUPYu436f2-6g
Content-Type: application/json
Connection: close

{"nftId":"63ec9b3e9e35cceb66eedce1","seller":"0xc5f7b9d88b6fda0c6e04d3a1e2817e1d65547ff1","tokenAddress":"0x0000000000000000000000000000000000000000","collection":"0x0c1005ae2c9631784b39cc5ad5ad3bacb7b3ce15","price":"10000000000000","quantity":1,"saleType":0,"validUpto":2214189165,"signature":[27,"0xb6c9d0902f534ca28e64bc688e54ef8e1a6ca99e0133f6f0bf7526cefdca97fc","0x65207be78f482dce6d3f7bd2aff60f55e93077788b2ccfe54dc559fe63b86cd5"],"tokenId":20,"auctionEndDate":"01/03/2040","salt":470267}
```


Recommedation

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

NEO LEGAL | Blockchain Australia® | NEO VIRTUAL TECH

QuillAudits

Canada, India, Singapore, United Kingdom

audits.quillhash.com

audits@quillhash.com