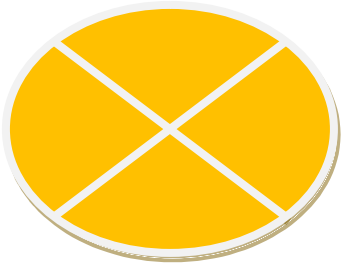

4/Oranges
Security LLC

VulnLawyers
Web Application Penetration Testing Report

Restricted – Authorized Personnel Only

Tester: Dario Tavarez
Assignment Date: 07/15/2025
Completion Date: 07/18/2025

Table of Contents

1. **Executive Summary** 3
2. **Scope of Engagement** 3
3. **Methodology** 3

    3.1 Reconnaissance 4

    3.2 Application Analysis 4

    3.3 Exploitation 4

4. **Detailed Findings** 4

    4.1 Exposed API Subdomain 5

    4.2 Outdated JavaScript Libraries 5

    4.3 Insecure Direct Object Reference (IDOR) 5

    4.4 Broken Access Control 5

5. **Evidence Screenshots ……..** 5
6. **Summary Table of Findings** 6
7. **Remediation Plan** 7
8. **Conclusion** 7

1. Executive Summary

- **Purpose:** Assess the security posture of VulnLawyers' web infrastructure.
- **Key Findings:**
  - Exposed subdomain revealing internal API and sensitive user data.
  - Outdated JavaScript libraries.
  - IDOR vulnerability on user profile data.
  - Broken access control allowing sensitive actions (e.g., deleting legal cases).
- **Overall Risk:** High
- **Recommendation Summary:**
  - Harden API access and restrict internal endpoints.
  - Implement proper access controls and object-level authorization.
  - Sanitize user input and session handling.

2. Scope

- **Target Domain:** `cassandra.ctfio.com`
- **OSINT Domain:** `vulnlawyers.co.uk`
- **Testing Window:** July 15–18, 2025
- **Testing Approach:** Black-box

---

3. Methodology

3.1 Reconnaissance

- **Nmap Scan:**
  - Open ports: 80, 443
  - HTTP headers revealed server stack
  - SSL cert revealed alternative DNS names
- **Directory Brute Force (Dirb):**
  - `/admincontrol`, `/login`, `/images`, `/denied` found
- **VHost Fuzzing (FFUF):**
  - Discovered subdomain: `data.cassandra.ctfio.com`
  - Exposed API returning usernames and emails
  - First FLAG discovered

3.2 Application Enumeration

- **OWASP Scan:**
  - Outdated JavaScript libraries detected

3.3 Authentication Testing

- **Manual Browsing & Burp Proxy:**
  - `/lawyers-only` login page discovered
  - Flag #2 found in HTML
- **Credential Spraying (Burp Intruder):**
  - Valid credentials: `jaskaran.lowe@vulnlawyers.ctf : summer`

3.4 Exploitation

- **Authenticated User Panel:**
  - `/portal` and `/profile` tabs reviewed
- **IDOR Exploitation:**
  - URL parameter `id=4` in `/lawyers-only-profile-details/4` revealed user data
  - Using another user's ID allowed viewing and manipulating others' data
- **Broken Access Control:**
  - Used Sayne Cains's credentials to delete a legal case
  - Final FLAG captured

---

4. Vulnerability Findings

Finding 1: Exposed API Subdomain

- **Severity:** High
- **Description:** API exposed without authentication; leaked sensitive data.
- **Recommendation:** Restrict access and require authentication for all API endpoints.

Finding 2: Outdated JavaScript Libraries

- **Severity:** Medium
- **Description:** Client-side libraries vulnerable to known CVEs.
- **Recommendation:** Upgrade or replace libraries with secure versions.

Finding 3: Insecure Direct Object Reference (IDOR)

- **Severity:** Critical
- **Description:** User ID in URL allowed access to other user profiles.
- **Recommendation:** Implement proper access controls for resource ownership.

Finding 4: Broken Access Control (Case Deletion)

- **Severity:** High
- **Description:** Logged-in user could delete another user's case data.
- **Recommendation:** Enforce role-based access checks on sensitive actions.

---

5. Evidence (Screenshots & Payloads)

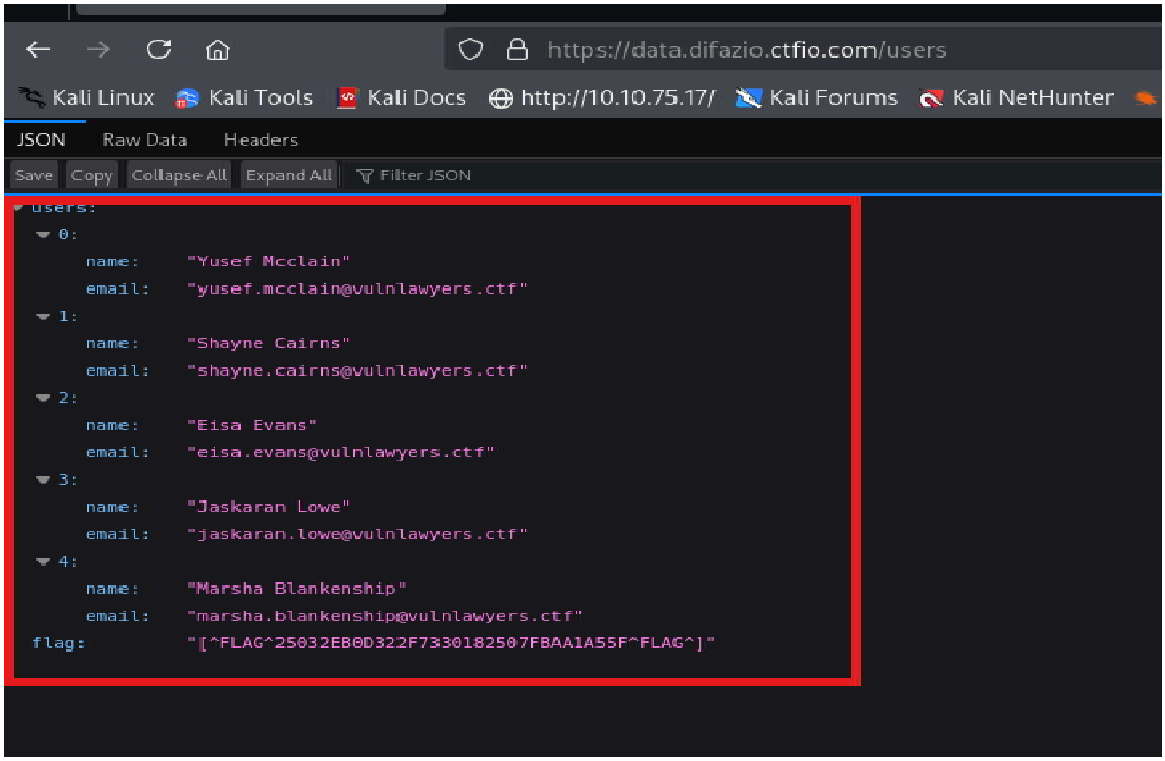

Figure 1: Screenshot showing API response revealing user emails

Figure 2: Burp capture of IDOR request to access other user profiles

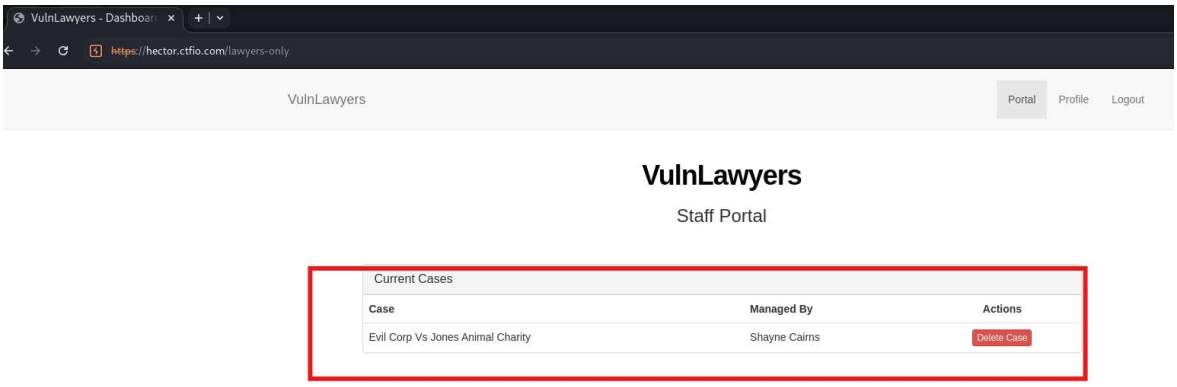

Figure 3: Burp request showing successful case deletion

---

6. Summary Table

#	Title	Severity	Affected URL
1	Exposed API	High	`https://data.cassandra.ctfio.com`
2	Outdated JavaScript	Medium	`https://cassandra.ctfio.com`
3	IDOR in profile endpoint	Critical	`/lawyers-only-profile-details/{id}`
4	Case deletion vulnerability	High	`/lawyers-only/case/delete`

---

7. Remediation Plan

- **Short-Term:**
  - Disable unauthenticated API endpoints.
  - Patch JS libraries.
- **Medium-Term:**
  - Implement proper object access validation.
  - Conduct internal code review.
- **Long-Term:**
  - Enforce RBAC and access logging.
  - Schedule recurring security assessments.

---

8. Conclusion

The assessment uncovered critical vulnerabilities that could lead to data leakage and unauthorized actions. Prompt remediation is advised, and security best practices (e.g., input validation, access controls) should be prioritized moving forward.

Note:

The testing environment generated a new domain on each launch, which caused differences between the domains shown in screenshots and those listed in the report. Additionally, some scans took longer than expected due to environment setup delays. These factors did not affect the validity of the findings.