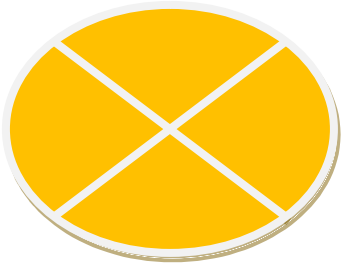

4/Oranges
Security LLC

VulnLawyers
Web Application Penetration Testing Report

Restricted – Authorized Personnel Only

Tester: Dario Tavarez
Assignment Date: 07/15/2025
Completion Date: 07/19/2025

Table of Contents

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 15–28, 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` (1rst Flag)
  - Discovered subdomain: `data.cassandra.ctfio.com/users (2do Flag)`
  - Exposed API returning usernames and emails

3.2 Application Enumeration

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

3.3 Authentication Testing

- **Manual Browsing & Burp Proxy:**
  - `/lawyers-only` login page discovered
  - Found in HTML (3er Flag)
- **Credential Spraying (Burp Intruder):**
  - Valid credentials: `jaskaran.lowe@vulnlawyers.ctf : summer`

3.4 Exploitation

- **Authenticated User Panel:**
  - `/Portal /profile` tabs reviewed (4th Flag)
- **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 (5th Flag)
- **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)

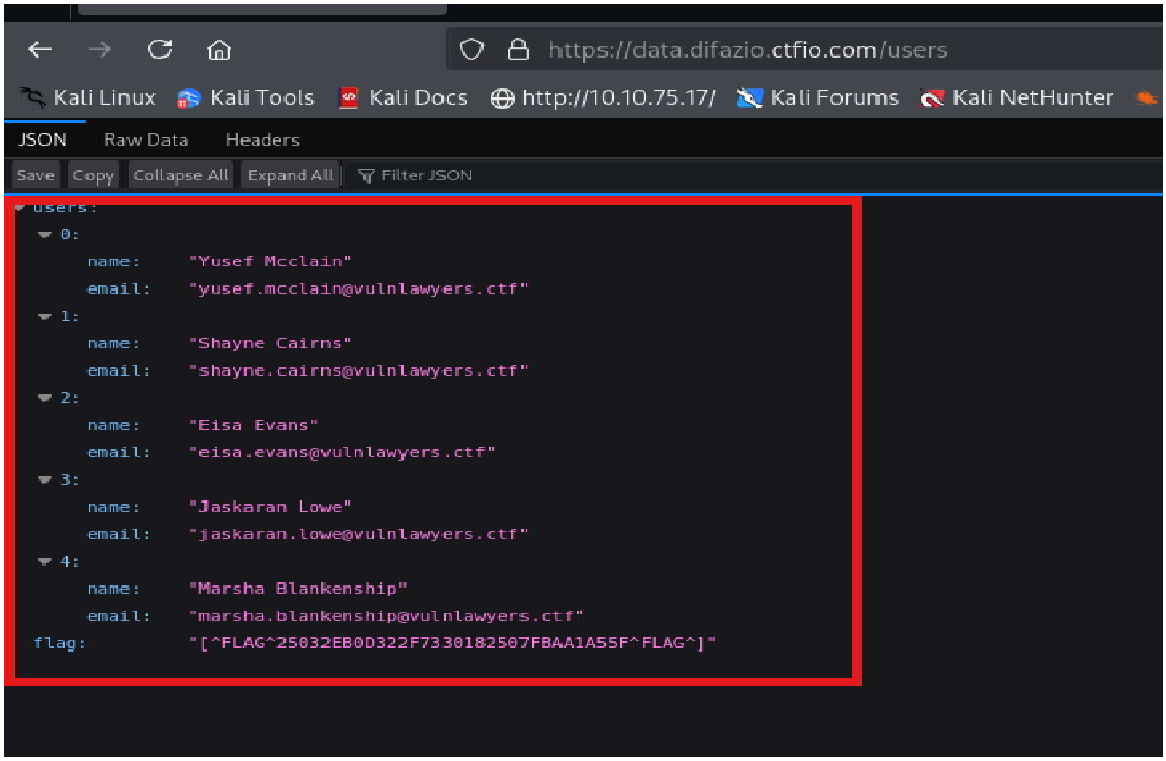

Figure 1: Screenshot showing API response revealing user emails

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

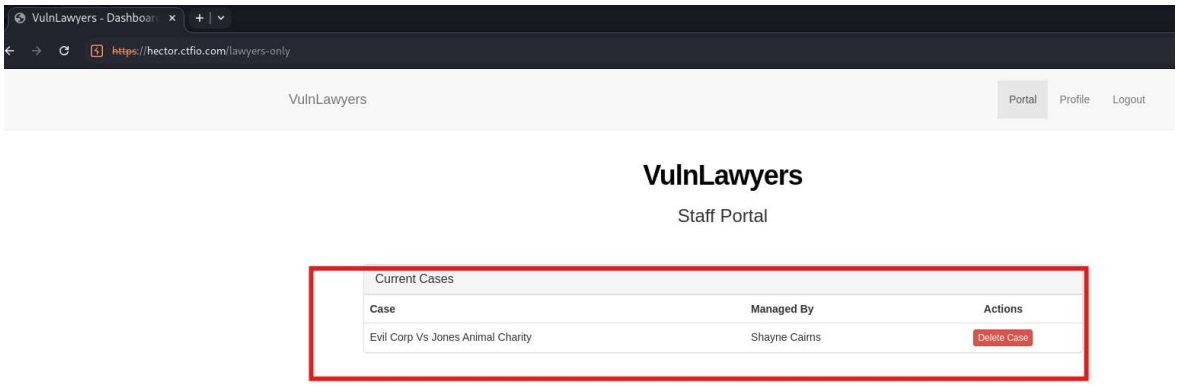

Figure 3: Showing successful case deletion

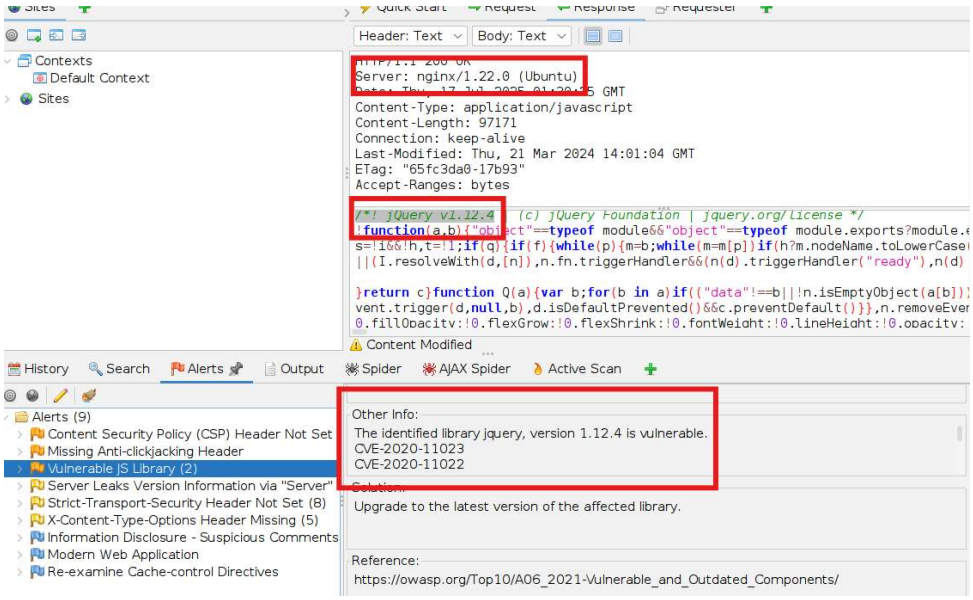

Figure 4: Outdated JavaScript

6. Summary Table

#	Title	Severity	Affected URL
1	Exposed API	High	`https://data.cassandra.ctfio.com/users`
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.

Notes:

1 - 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.

2 - The primary objective of this assignment was to locate all hidden flags within the target environment. As a result, the assessment prioritized application-layer exploration and exploitation techniques over deeper research into server configuration, infrastructure fingerprinting, or outdated JavaScript libraries. These areas were noted but not analyzed in depth, in order to focus on achieving the core goal of flag discovery.

*3 - This report does not list all tools and commands used during the engagement. Some were omitted intentionally for simplicity, clarity, and to protect proprietary methodologies developed by **4 /Orange Security LLC**. The techniques and findings presented reflect the essential steps taken to achieve the assessment objectives without disclosing sensitive internal practices.*

Final Thoughts

This assessment provided valuable insights into the web application's security posture and highlighted key areas for improvement. While the focus was on flag discovery, the process reflected real-world adversarial behavior, emphasizing the importance of secure coding, access control, and continuous monitoring. 4 Orange Security LLC remains committed to supporting organizations in strengthening their defenses through practical, goal-driven testing.