VulnLawyers

Security Assessment Findings Report

Business Confidential

Date: July 27th, 2025
Project: VulnLawyers
Version 1.0

Table of Contents

Confidentiality Statement

This article is the sole property of VulnLawyers and Tech With Z (TWZ). This document includes private and confidential information. Duplication, dissemination, or use, in whole or in part, in any form, requires the permission of both VulnLawyers and TWZ.

VulnLawyers may share this material with auditors under non-disclosure agreements to verify compliance with penetration testing requirements.

Disclaimer

A penetration test is viewed as a snapshot in time. The findings and recommendations are based on the information obtained during the evaluation and do not include any changes or revisions made beyond that period.

Time-limited engagements do not allow for a comprehensive assessment of all security controls. TWZ prioritized the evaluation to find the most vulnerable security controls an attacker may exploit. TWZ suggests that similar assessments be conducted on an annual basis by internal or third-party assessors to verify that the controls remain effective.

Contact Information

Tech With Z		
Name	Title	Contact Information
Zandro Dadulla Jr.	Penetration Tester	zandro@techwithz.com

Assessment Overview

VulnLawyers engaged Tech With Z to assess the security status of its Web Application in relation to the latest industry standards, which involved conducting a web application penetration test. The testing conducted is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and tailored testing frameworks.

Phases of penetration testing activities include the following:

- Planning – Customer goals are identified, and rules of engagement are established.
- Discovery – Perform scanning and enumeration to identify possible vulnerabilities, weak points, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation, then conduct additional discovery with new access.
- Reporting – Document all discovered vulnerabilities and exploits, unsuccessful attempts, and company strengths and weaknesses.
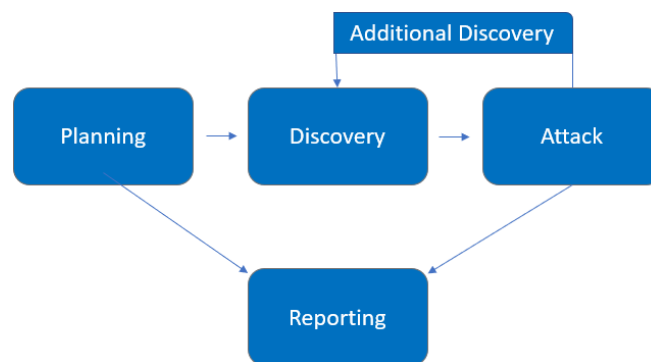
Assessment Components

Web Application Penetration Test

This web application penetration test was conducted to simulate an attacker with no internal access or prior knowledge of the environment attempting to compromise the organization's exposed web assets. The objective was to identify security weaknesses that could be exploited to gain unauthorized access to sensitive data or application functionality.

The assessment involved active reconnaissance, including scanning and enumeration of the target's publicly accessible web infrastructure. Discovered endpoints, directories, and services were analyzed for common vulnerabilities, misconfigurations, and access control flaws. The testing process focused on identifying issues that could result in unauthorized data exposure, authentication bypass, privilege escalation, and improper access to application resources.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Medium	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, the attacker's skill level, and the client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Web Application Penetration Test	mu.ctfio.com *.mu.ctfio.com

Scope Exclusions

TWZ did not conduct any of the following attacks during testing:

- Denial of Service (DoS) attacks against production infrastructure.
- Phishing / Social Engineering attacks.

Client Allowances

VulnLawyers provided a set of wordlists to assist with enumeration and password attacks.

Executive Summary

On July 21st, 2025, TWZ performed a web application penetration test targeting VulnLaywers' publicly accessible systems. The objective of this assessment was to evaluate the security posture of VulnLaywers' web application by identifying vulnerabilities and assessing the effectiveness of implemented security controls. This report provides a high-level overview of the findings, including both successful and unsuccessful exploitation attempts, as well as identified strengths and weaknesses in the application's security architecture.

Scoping and Time Limitations

Throughout the engagement, TWZ did not performed denial of service or social engineering in any testing components.

Testing was limited in duration. Web application penetration testing was approved until July 28th, 2025.

Testing Summary

The assessment evaluated VulnLawyers' web application security posture. From an external perspective, the TWZ team performed information gathering techniques to identify possible entry points for future attacks and gather sensitive information. This includes names, emails, and hidden endpoints.

The TWZ team discovered a vulnerable API endpoint which disclosed all emails registered to the website (Finding WPT-006). Using this information, the TWZ team discovered one critical severity finding due to insufficient password complexity (Finding WPT-001). During testing, TWZ was able to successfully password spray the VulnLawyers Staff login page due to no lockout policy in place (Finding WPT-003). In result of this attack, the TWZ team was able to identify the password and successfully logged in to the compromised account due to the absence of Multi-Factor Authentication (MFA) in the environment (Finding WPT-004).

After gaining access to the account, the TWZ team discovered that it is possible to access other users' information by modifying the user ID in the HTTP request (Finding WTP-005). This is due to the Insecure Direct Object Reference (IDOR) vulnerability present in the user profile page. This allowed TWZ to gather sensitive information such as names, emails, and plain text passwords (Finding WPT-002). This led the TWZ team to gain access to one of the accounts with elevated permissions that allows a case to be deleted.

In addition to the aforementioned compromise, the TWZ team also discovered a hidden endpoint by analyzing the HTTP response (Finding WPT-007) and the Web application discloses server information via HTTP response headers (Finding WPT-008). For further details on the findings, please see the Technical Findings section.

Tester Notes and Recommendations

During testing, a few things stood out: a poor password policy, insufficient authentication controls, lack of authorization controls on endpoints, and storing of credentials in plain text. The weak password policy and absence of Multi-Factor Authentication (MFA) resulted in an initial compromise of the account and is typically one of the first footholds an attacker seeks to employ in a network. The lack of authorization controls resulted in discovering sensitive information for all users and storing passwords in plain text allows an attacker to easily compromise an account.

We advise that VulnLawyers review its current password policy and consider a policy of 15 characters or more. We also urge that VulnLawyers look into utilizing Privilege Access Management (PAM) solutions. We also advise to implement and review authorization controls for the application's endpoints and avoid storing passwords in plain text.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Effective protection against injection attacks (XSS, SQLi).

The following identifies the key weaknesses identified during the assessment:

1. Insufficient password policy.
2. Insufficient Authentication controls.
3. Insufficient controls for preventing information disclosure.
4. Passwords are stored in plain text within the application, posing a significant security risk if unauthorized access is achieved.

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Web Application Penetration Test Findings

3	3	2	0	0
Critical	High	Medium	Low	Informational

Finding	Severity	Recommendation
Web Application Penetration Test		
WPT-001: Insufficient Password Complexity	Critical	Implement CIS Benchmark password guidelines / PAM solution.
WPT-002: Plaintext Password Storage	Critical	Implement secure password hashing using modern algorithms.
WPT-003: Insufficient Lockout Policy	Critical	Restrict logon attempts against VulnLawyers Staff login portal.
WPT-004: Insufficient Authentication Controls – MFA	High	Implement Multi-Factor Authentication (MFA).
WPT-005: Insecure Direct Object Reference (IDOR) Leading to Information Disclosure and Privilege Escalation	High	Implement Object-Level Access Control (OLAC) checks and UUIDs.
WPT-006: Information Disclosure via Unauthenticated API Endpoint	High	Enforce authentication and authorization checks for all sensitive API endpoints.
WPT-007: Hidden Endpoint Exposure via HTTP Response	Medium	Ensure all deprecated or internal endpoints are properly removed or access controlled.
WPT-008: Information Disclosure via HTTP Response Headers	Medium	Remove unnecessary information from HTTP response headers.

Technical Findings

Web Application Penetration Test Findings

Finding WPT-001: Insufficient Password Complexity (Critical)

Description	TWZ was able to determine the password of one of the VulnLawyers users using a password spraying attack.
CVSS Score	9.8 (Critical) – CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Risk	Likelihood: High - Simple passwords are susceptible to password-cracking attacks. Encryption provides some protection, but dictionary attacks based on common word lists often crack weak passwords. Impact: Critical – This can lead to full account compromise and access to the user's information and potentially denying access to user's account.
System	https://mu.ctfio.com/lawyers-only-login
Tools Used	Caido
References	CWE-521: Weak Password Requirements CIS Password Policy Guide: CIS Password Policy Guide Authenticator Management – Password-Based Authentication: NIST SP 800-53 Rev 5.1.1 IA-05(01)

Evidence / Steps to Reproduce

Using Caido, the usernames gathered (WPT-005), and the wordlist that VulnLawyers provided, the TWZ team was able to perform password spraying attack against the VulnLawyers Staff login page (*https://mu.ctfio.com/lawyers-only-login*).

TWZ was able to determine the password of one of the accounts which allowed the TWZ team to gain access to the account.
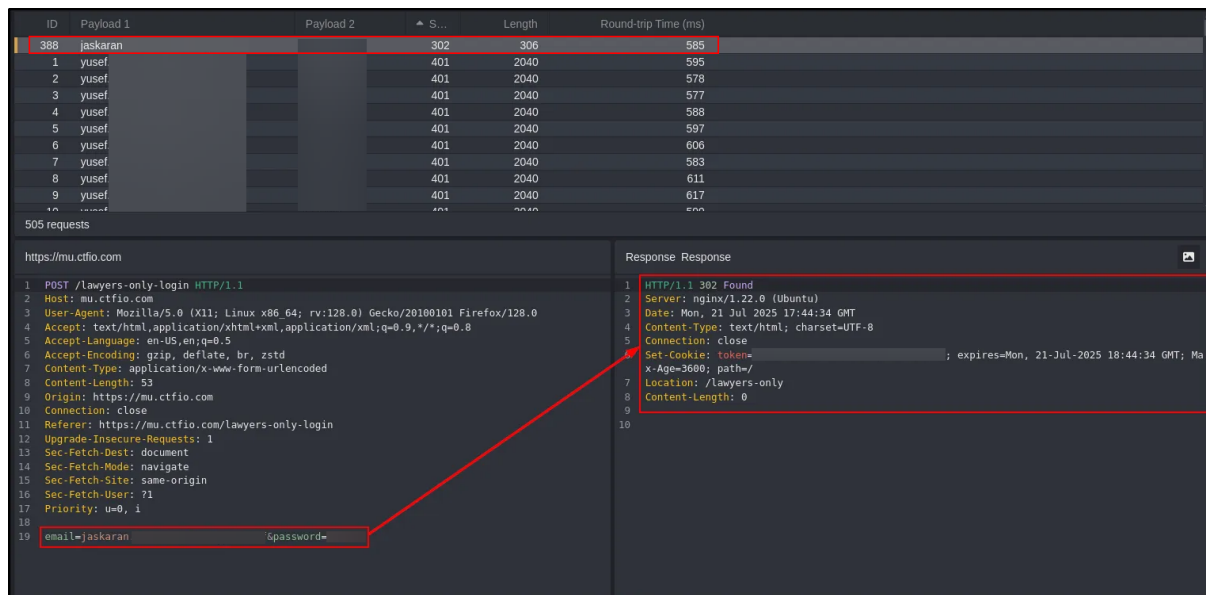
Figure 1: Caido Automate – Password Spraying.

TWZ then manually logged in using the compromised account credentials and gained access to the VulnLawyers Staff Portal (*https://mu.ctfio.com/lawyers-only*).
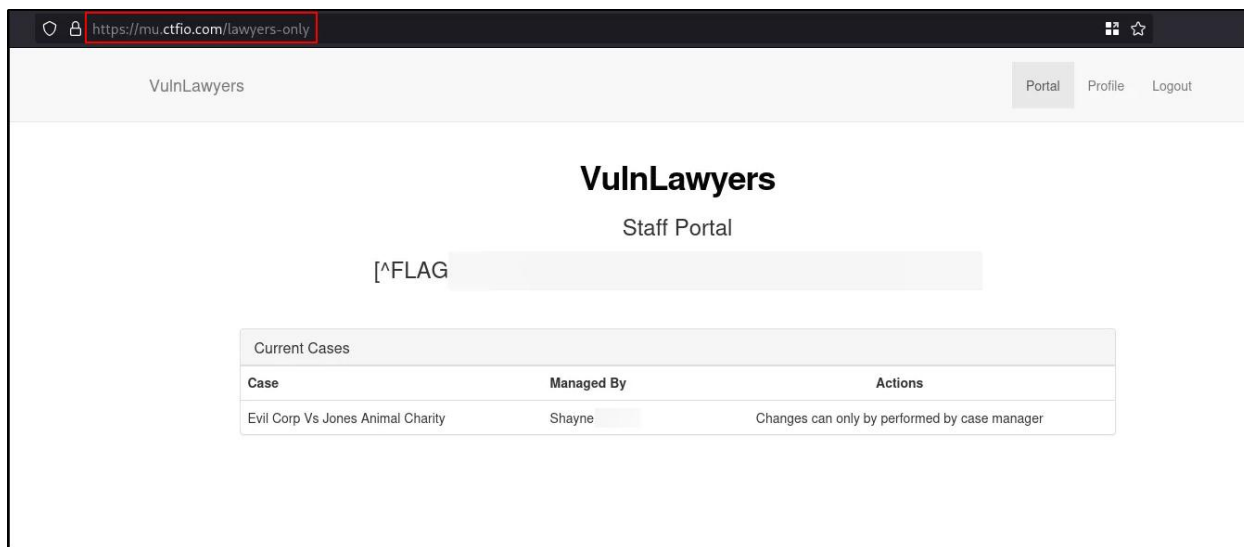
Figure 2: VulnLawyers Staff Portal.

Remediation

Implement CIS Benchmark password requirements / Privilege Access Management (PAM) solution. TWZ recommends that VulnLawyers enforce industry best practices around password complexity and management. It is also advised that users use a password filter to avoid using popular and easily guessed passwords.

Finding WPT-002: Plaintext Password Storage (Critical)

Description	While accessing user profile details during authenticated sessions, the application returned user passwords in clear text as part of the HTTP response. This implies that the application stores user passwords without hashing or encryption, which is a severe violation of security best practices.
CVSS Score	9.8 (Critical) – CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Risk	Likelihood: High - The information is visible in standard application responses. However, the attacker must be authenticated to view the data. Impact: Critical – Any user account could be compromised if data is intercepted or extracted.
System	https://mu.ctfio.com/lawyers-only-profile-details/
Tools Used	Caido, Manual Review
References	CWE-256: Plaintext Storage of a Password OWASP: A02 Cryptographic Failures - OWASP Top 10:2021 OWASP: Password Storage - OWASP Cheat Sheet Series NIST SP 800-63B, Section 5.1.1.2 – Password Storage Requirements: Web app pen test report

Evidence / Steps to Reproduce

During testing of Insecure Direct Object Reference mentioned in WPT-005, the TWZ team discovered that VulnLawyers user profile endpoint (*/lawyers-only-profile-details*) displays plain text password in the HTTP response which indicates that VulnLawyers stores passwords in plain text.
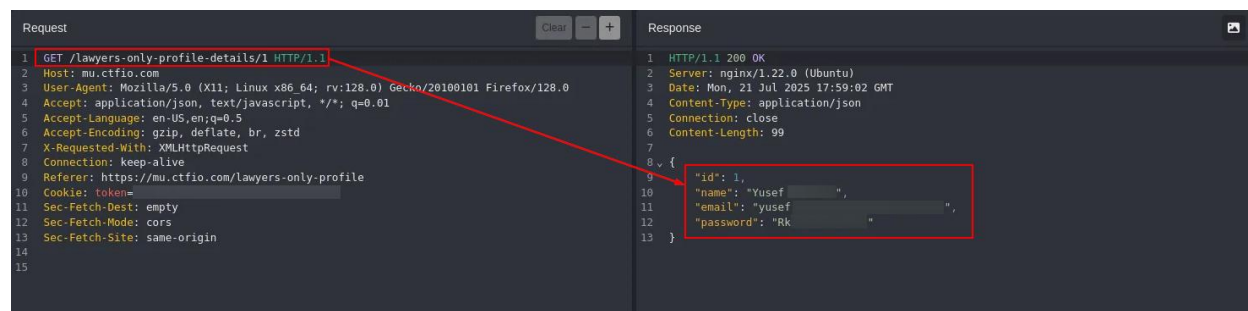
Figure 3: Plain Text Password in HTTP Response

Remediation

The TWZ team recommends removing all plaintext password display from responses and database storage and implement secure password hashing using modern algorithms such as bcrypt, Argon2, or PBKDF2.

Finding WPT-003: Insufficient Lockout Policy (Critical)

Description	VulnLawyers allowed unlimited logon attempts against their Staff login portal (/lawyers-only-login). This configuration allowed brute force and password spraying attacks in which TWZ used to gain access to VulnLawyers' Staff Portal.
CVSS Score	9.1 (Critical) – CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Risk	Likelihood: High – An attacker can utilize readily available tools such as Burp Suite, Caido, THC Hydra, etc. to perform brute-force and password spraying attacks without any restrictions to login attempts. Impact: Critical – If successful and given unlimited time, an attacker can gain access to a user's account sensitive information.
System	https://mu.ctfio.com/lawyers-only-login
Tools Used	Caido
References	CWE-307: Improper Restriction of Excessive Authentication Attempts (4.17) Unsuccessful Logon Attempts: NIST SP 800-53 AC-07

Evidence / Steps to Reproduce

While performing the same password spraying attack mentioned in WPT-001, TWZ identified another vulnerability in VulnLawyers' Staff login portal (*https://mu.ctfio.com/lawyers-only-login*) where it allowed the TWZ team to continue the password spraying attack without getting the accounts locked out. The TWZ team sent 505 requests to the staff login page.

Figure 4: Caido Automate – Password Spraying Attack.
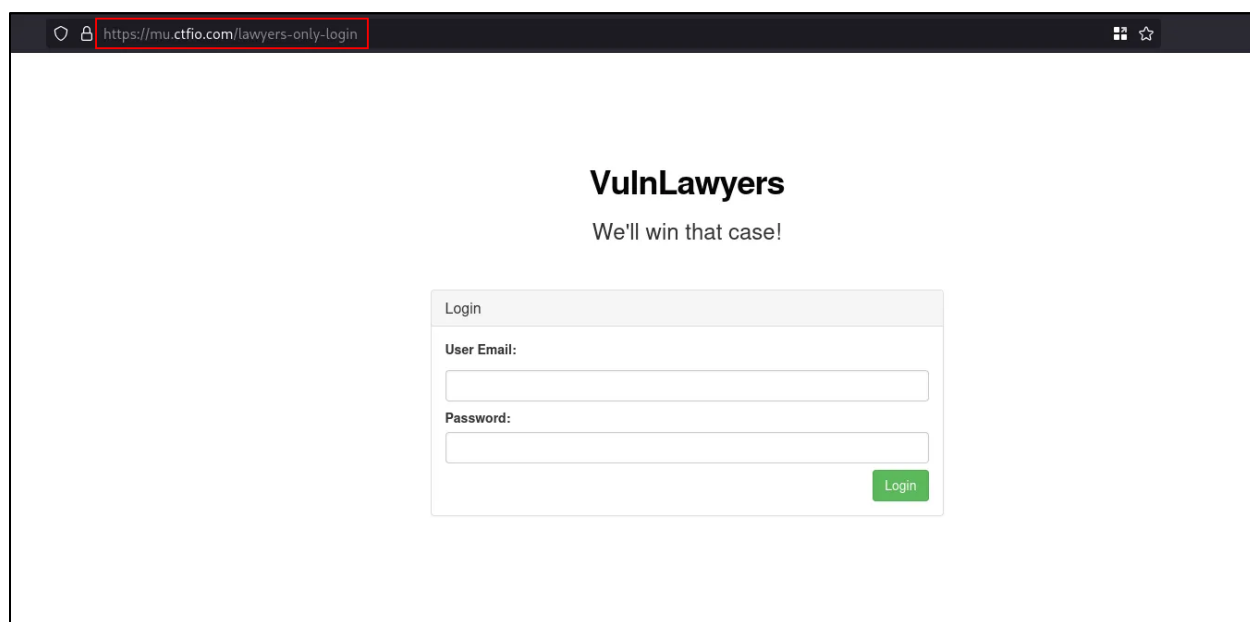
Remediation

TWZ recommends VulnLawyers to implement lockout policy and apply rate limiting and delay mechanisms to prevent or slow down any brute-force attempts.

Finding WPT-004: Insufficient Authentication Controls – MFA (High)

Description	VulnLawyers does not require multi-factor authentication for sensitive services. An attacker can acquire access to sensitive systems, such as email, by employing common techniques such as credential stuffing and password spraying. The TWZ team was able to access one (1) account via password spraying and manual login and gained access to the staff portal.
CVSS Score	8.8 (High) – CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Risk	Likelihood: High – The Staff Portal login page is accessible from the internet. Impact: High – If exploited, an attacker can gain access to a user's account without additional protective measures.
System	https://mu.ctfio.com/lawyers-only-login
Tools Used	Caido, Manual review
References	CWE-308: Use of Single-factor Authentication Identification and Authentication (Organizational Users) | Multi-Factor Authentication to Non-Privileged Accounts: NIST SP800-53 IA-2 (02) OWASP MFA Cheat Sheet: Multifactor Authentication - OWASP Cheat Sheet Series

Evidence / Steps to Reproduce

Once the credentials were confirmed from the password spraying attack mentioned in WPT-001, TWZ manually logged in to the Staff login portal (*https://mu.ctfio.com/lawyers-only-login*) and was able to access the compromised account without being prompted for Multi-Factor Authentication (MFA).
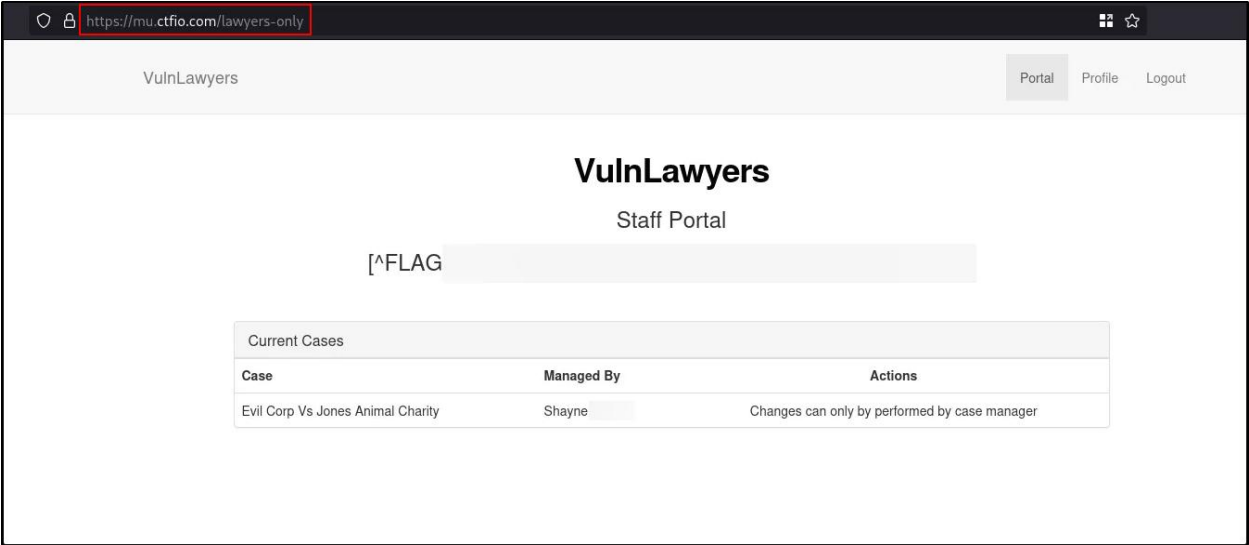

Figure 5: VulnLawyers Staff Login.

Figure 6: VulnLawyers Staff Portal.

Remediation

Implement Multi-Factor Authentication (MFA).

Finding WPT-005: Insecure Direct Object Reference (IDOR) Leading to Information Disclosure and Privilege Escalation (High)

Description	The VulnLawyers Staff portal's profile endpoint (/lawyers-only-profile-details) allowed TWZ to access other users' data by modifying the user ID in the request. TWZ was able to capture all users' credentials as the password is shown in plain text, this also allowed TWZ team to access a privileged user account and performed administrative functions such as case deletion.
CVSS Score	8.8 (High) – CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Risk	Likelihood: Moderate – The attacker needs to be authenticated to be able to access the endpoint. Impact: High – Leads to full data exposure, account compromise, and privilege escalation.
System	https://mu.ctfio.com/lawyers-only-profile-details/
Tools Used	Caido, Manual Review
References	CWE-639: Authorization Bypass Through User-Controlled Key OWASP: A01:2021 – Broken Access Control OWASP IDOR Prevention Cheat Sheet: Insecure Direct Object Reference Prevention Cheat Sheet

Evidence / Steps to Reproduce

After logging in to the compromised account as mentioned in WPT-003, TWZ navigated to the user's profile page (*https://mu.ctfio.com/lawyers-only-profile-details/*).
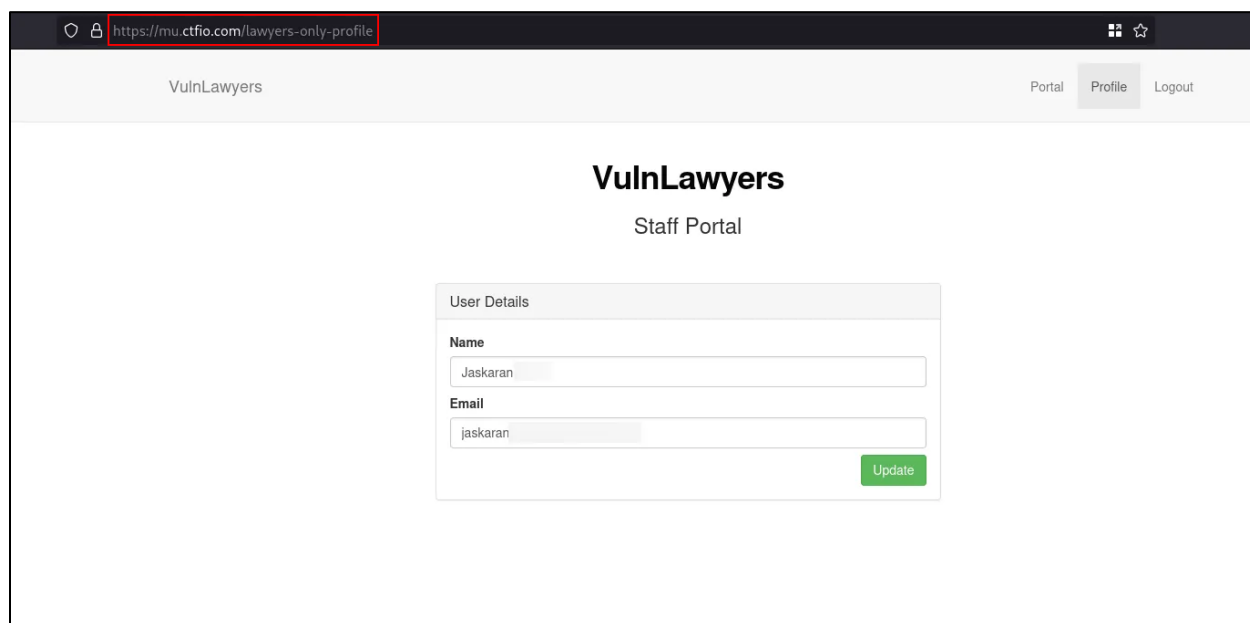
Figure 7: VulnLawyers Staff Portal – Lawyers Profile.

The TWZ team then used Caido to capture the HTTP request and analyzed its response. The HTTP response contains sensitive information of the user such as the Name, Email, and the plain text password. TWZ also noticed that the endpoint uses a numerical value for the user ID as shown in Figure 8.
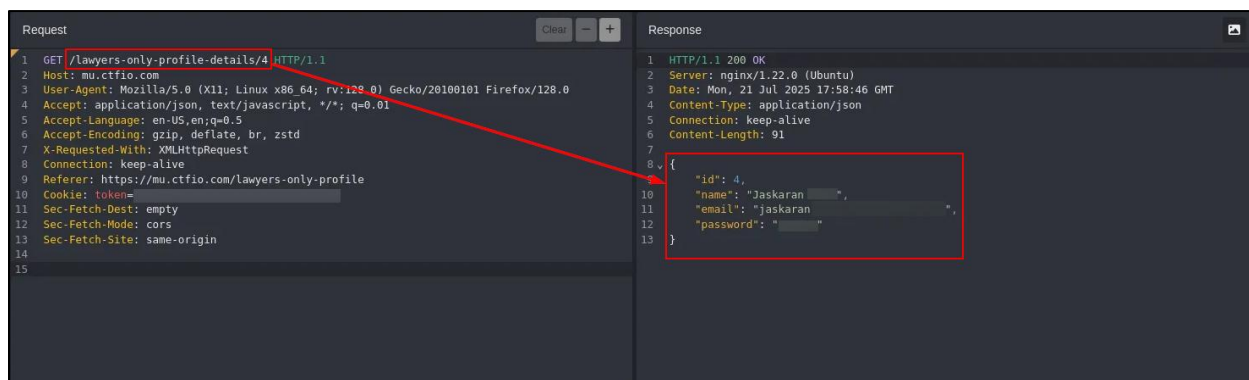

Figure 8: Caido – Lawyers Profile HTTP Request and Response for User ID 4.

The TWZ team then enumerated all users by changing the value of the user ID in the HTTP request (*/lawyers-only-profile-details/2*) which confirms the IDOR vulnerability. The user ID "2" as shown in Figure 8 is a user that TWZ specifically targeted as it may have admin privileges.
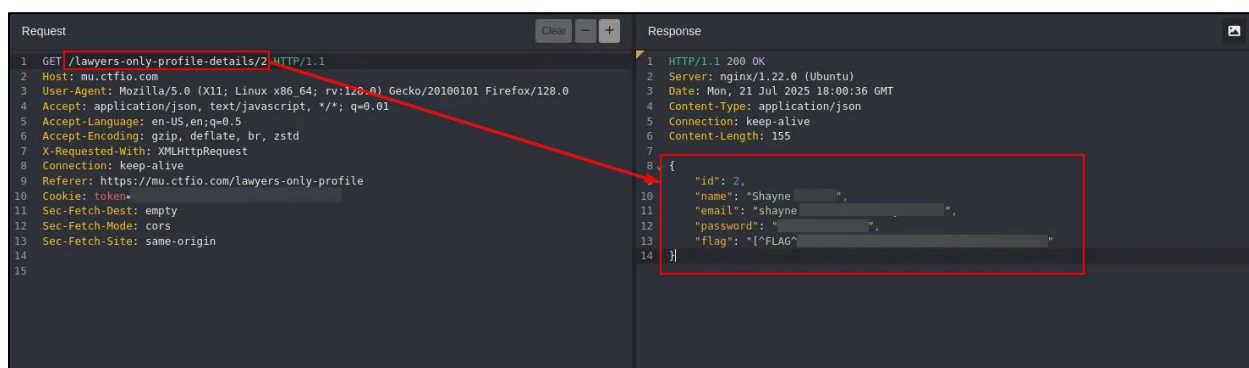
Figure 9: Caido – Lawyers Profile HTTP Request and Response for User ID 2.

Using the credentials found, TWZ team logged in to the account that has admin privileges and confirmed that it has the permission to delete cases and was successful deleting a case as shown in Figure 11.
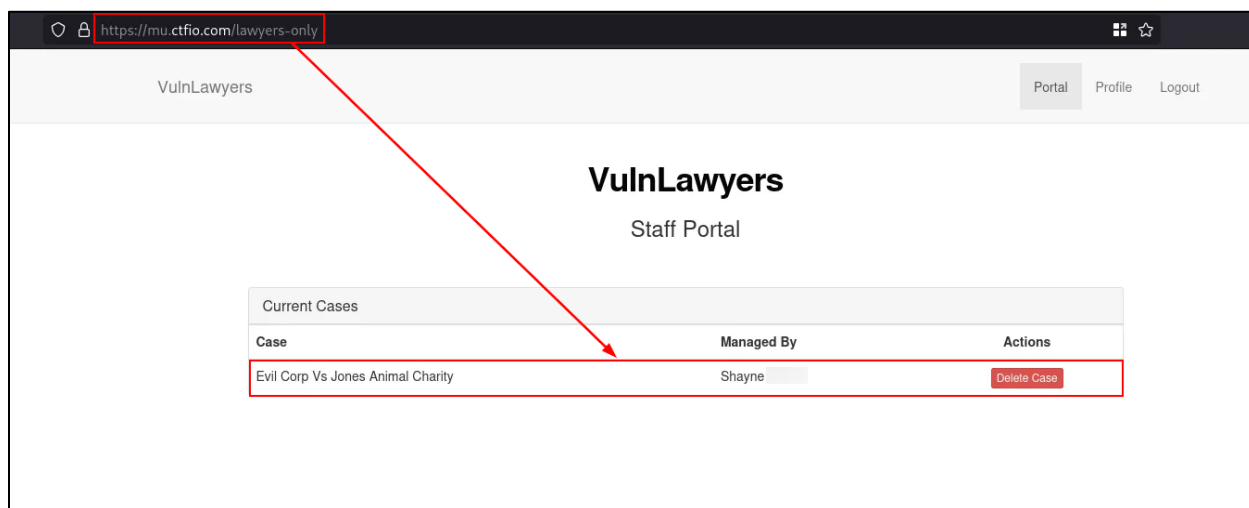
Figure 10: Staff Portal Dashboard for User ID 2.
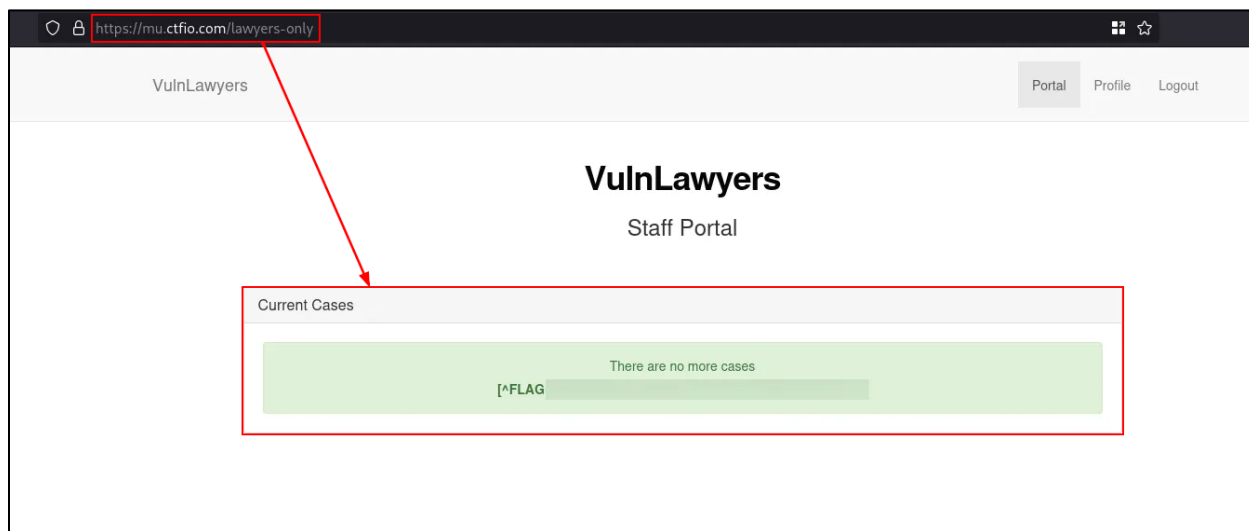
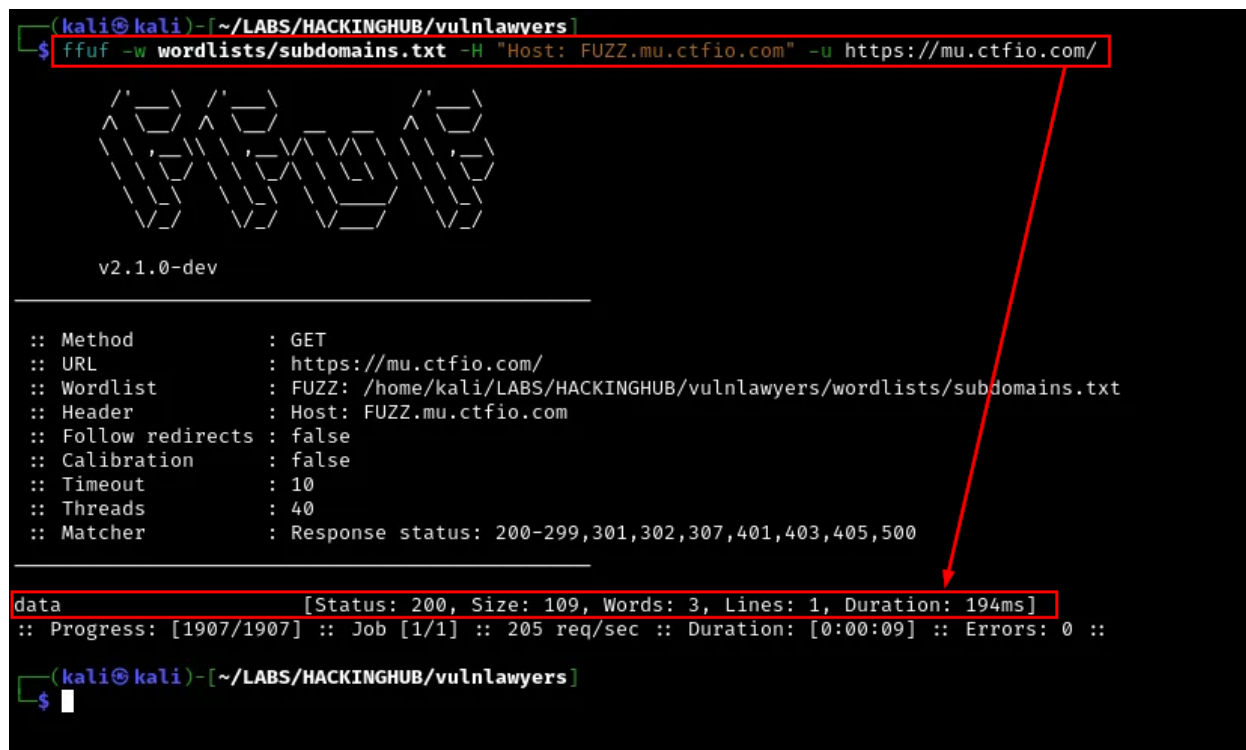*Figure 11: Case Deletion Performed Successfully.*

Remediation

TWZ recommends that VulnLawyers enforce object-level access control checks on all endpoints and use Universally Unique Identifiers (UUIDs) instead of the numeric User ID.

Finding WPT-006: Information Disclosure via Unauthenticated API Endpoint (High)

Description	The API subdomain (*https://data.mu.ctfio.com*) exposed an unauthenticated */users* endpoint that publicly exposed a list of all users' email addresses. This endpoint allows anyone on the internet to harvest registered emails, posing a privacy issue and enabling follow-on attacks such as phishing or credential stuffing.
CVSS Score	7.5 (High) – CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Risk	Likelihood: High – The endpoint is accessible remotely and no privileges or user interaction required. Impact: High – The endpoint provides high confidentiality impact by exposing user data.
System	https://data.mu.ctfio.com/users
Tools Used	FFuF, Manual Review
References	CWE-306: Missing Authentication for Critical Function API3:2023: Boken Object Property Level Authorization

Evidence / Steps to Reproduce

During the reconnaissance phase, the TWZ team enumerated VulnLawyers' subdomain/vhost and discovered the subdomain *https://data.mu.ctfio.com* which turned out to be VulnLawyers' API as shown in Figure 13.

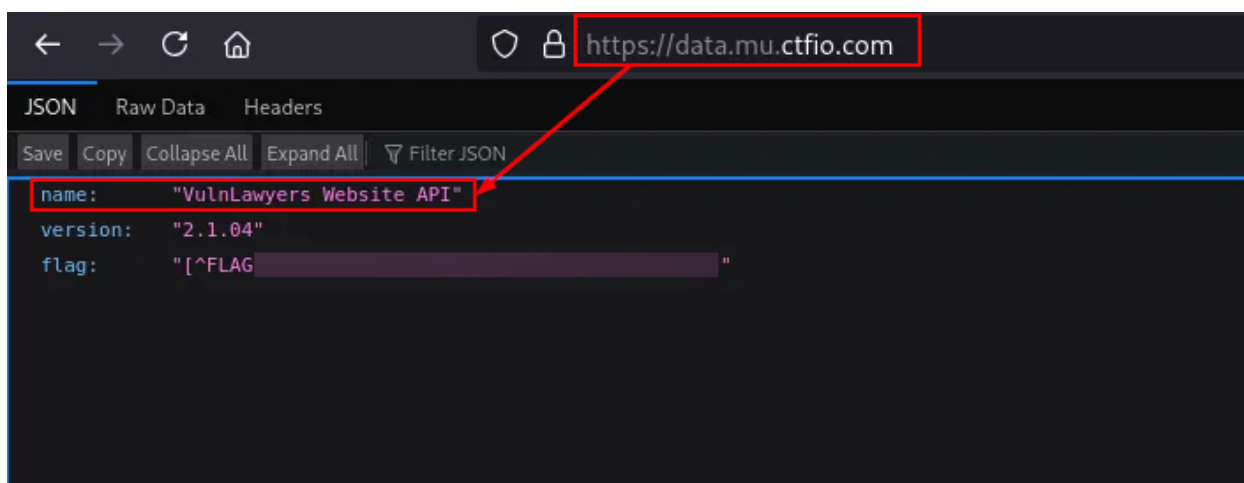*Figure 12: FFuF – Subdomain/Vhost Enumeration*

Figure 13: VulnLawyers API.

The TWZ team enumerated all possible endpoints of the API *https://data.mu.ctfio.com* and was able to find the "/users" endpoint.
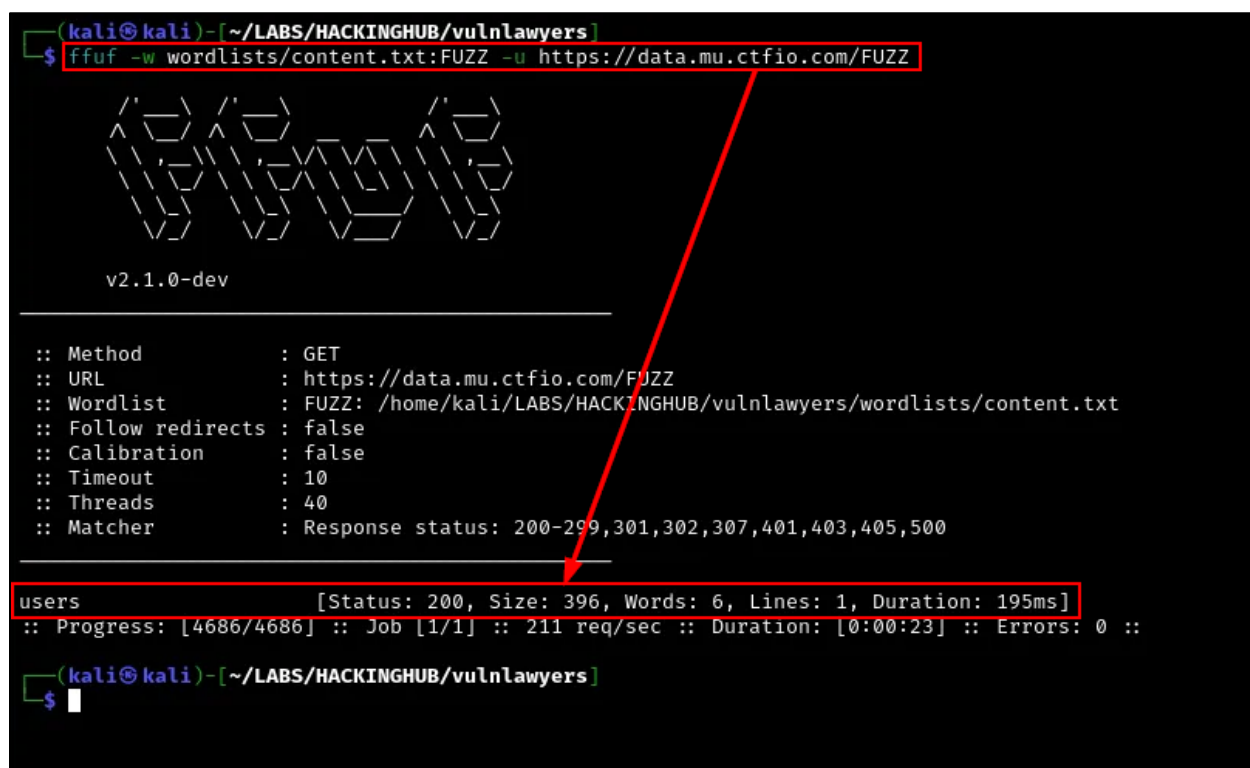

Figure 14: FFuF – API Endpoint Enumeration.

TWZ team then accessed the "/users" endpoint manually from a browser and discovered all users including their emails that were registered to the VulnLawyers Staff portal. The email addresses were then used for password spraying attack mentioned in WPT-001.
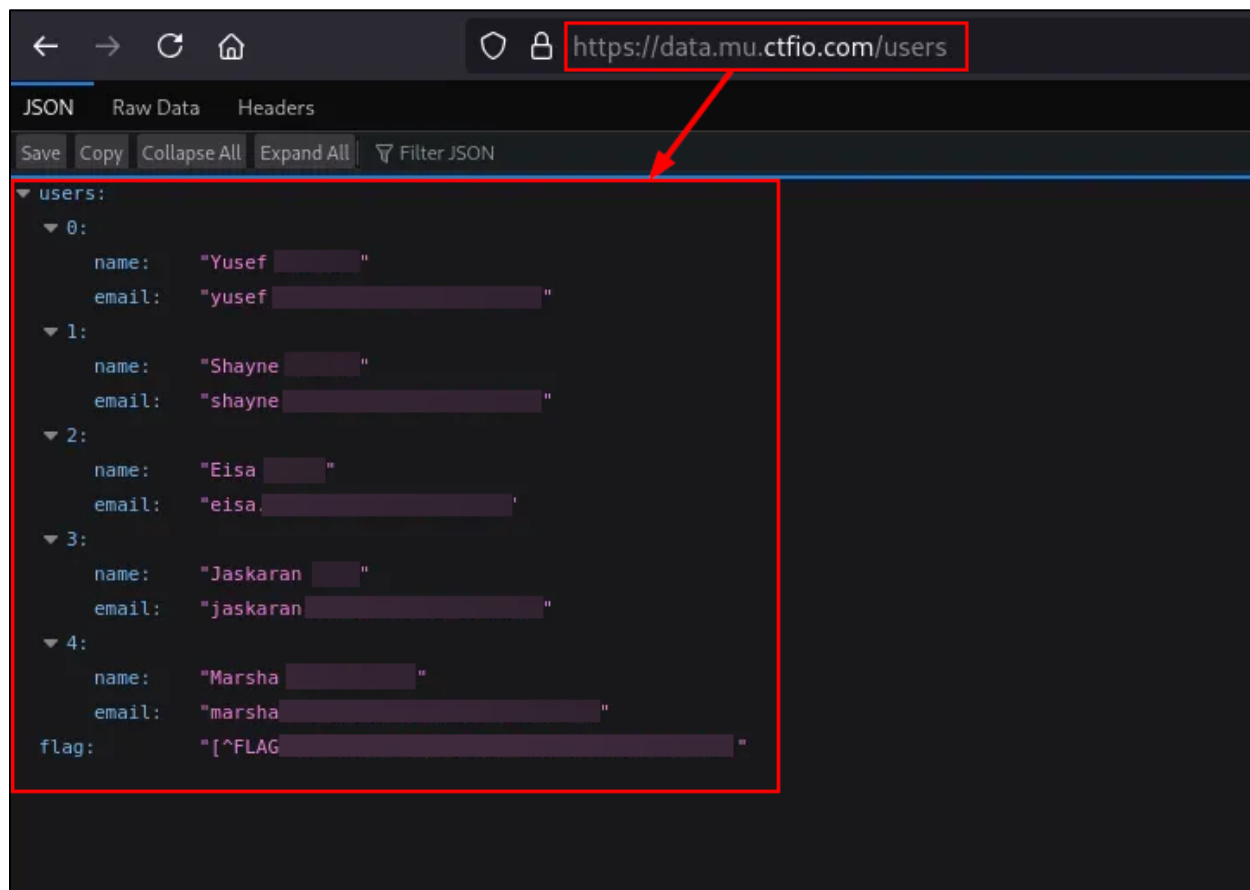

Figure 15: Discovered Emails on "/users" API Endpoint.

Remediation

TWZ recommends enforcing authentication and authorization checks for all sensitive API endpoints and minimize data exposure and avoid returning full user records unless necessary.

Finding WPT-007: Hidden Endpoint Exposure via HTTP Response (Medium)

Description	While the /login endpoint denied access, analysis of the response revealed another route (/lawyers-only) leading to the actual login portal. This leak of hidden or restricted paths allowed the TWZ team to access unintended entry points.
CVSS Score	5.3 (Medium) – CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Risk	Likelihood: Medium – This endpoint is accessible remotely but requires some manual inspection or automation. Attackers also routinely inspect HTML/JS for hidden routes. Impact: Medium – Leads to further attack surface discovery.
System	https://mu.ctfio.com/login
Tools Used	Caido, Manual Review
References	A05:2021: Security Misconfiguration OWASP Web Security Testing Guide: Review Webpage Content for Information Leakage

Evidence / Steps to Reproduce

During the reconnaissance phase, the TWZ team performed directory enumeration against the VulnLawyers' domain *https://mu.ctfio.com* and discovered some interesting directories/endpoints.

Figure 16: FFuF – Directory Enumeration.

TWZ navigated to the login page (*https://mu.ctfio.com/login*) of VulnLawyers' staff portal. The website redirected this request to the "Access Denied" page (*https://mu.ctfio.com/denied*).
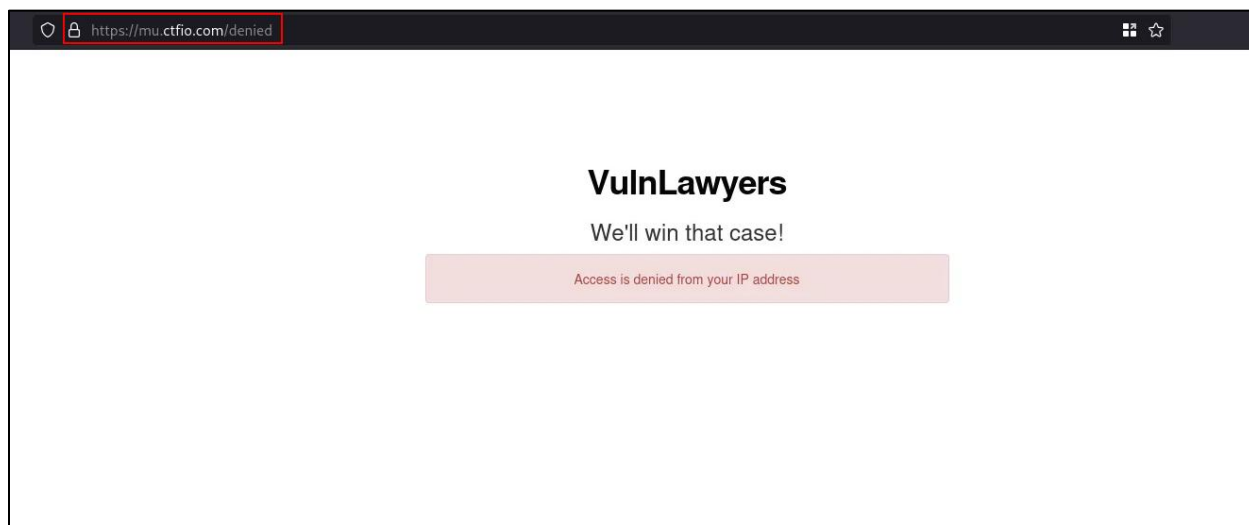

Figure 17: VulnLawyers "Access Denied" Page.

TWZ then analyzed the HTTP response of the "/login" endpoint and discovered that there is another endpoint (*/lawyers-only*) embedded in the HTML body of the, indicating a route not intended for regular user access. When accessed it redirects to (*/lawyers-only-login*). This would then be used by TWZ team to perform attacks mentioned in WPT-001 and WPT-004.
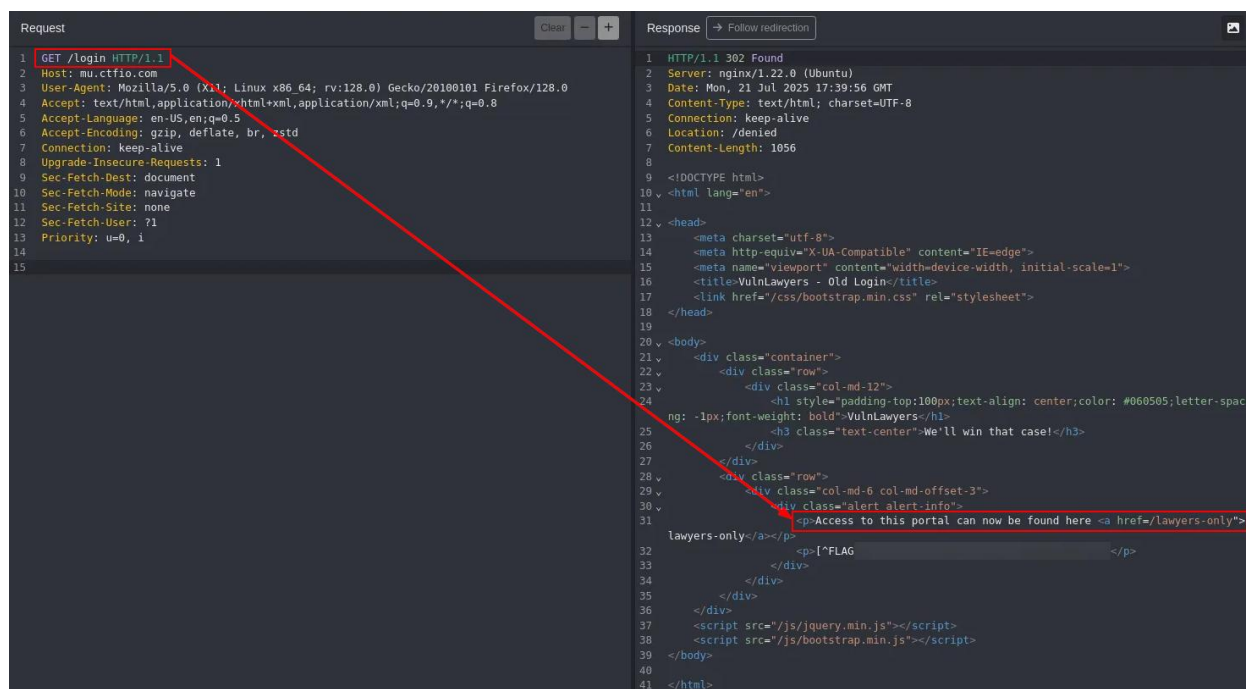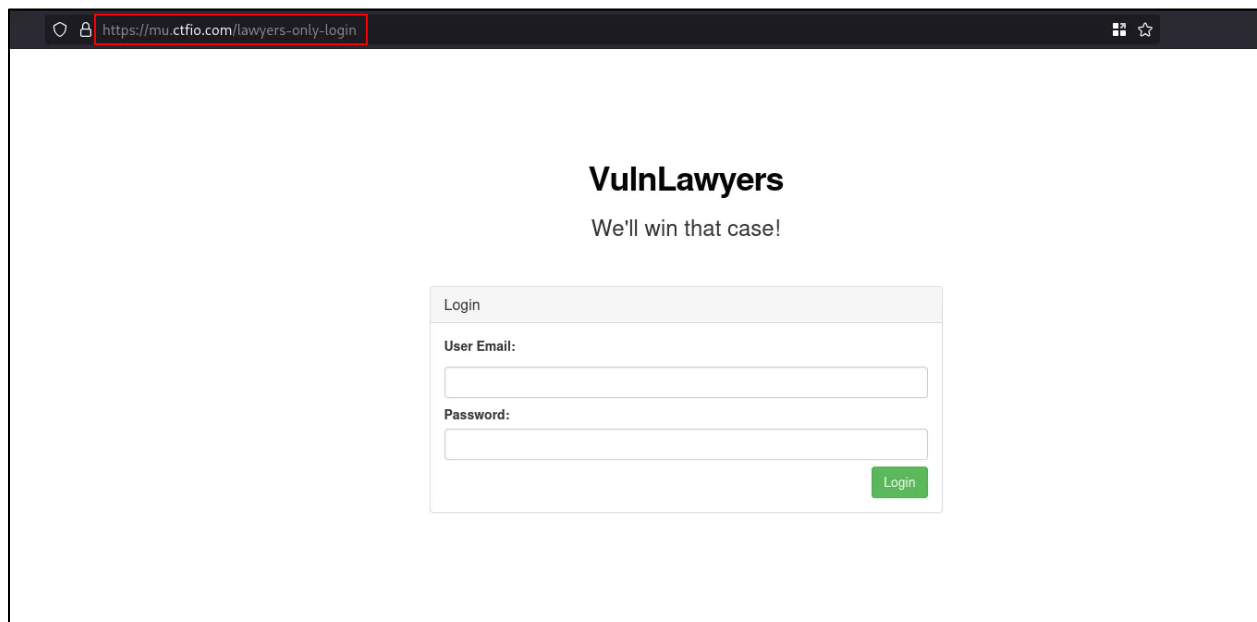

Figure 18: VulnLawyers Login Page HTTP Response.

Figure 19: VulnLawyers Lawyers Only Login Page.

Remediation

Perform routine code and content audits to identify outdated or unused endpoints. Ensure all deprecated or internal endpoints are properly removed or access controlled.

Finding WPT-008: Information Disclosure via HTTP Response Headers (Medium)

Description	VulnLawyers' web server disclosed unnecessary information within HTTP response headers returned to client requests.
CVSS Score	5.3 (Medium) – CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Risk	Likelihood: High – The system is accessible from the internet and is passively observable with any HTTP client or proxy tool. Impact: Medium – This information could allow an attacker to fingerprint the web server to better target future exploit attempts.
System	https://mu.ctfio.com/*
Tools Used	Caido, Manual Review
References	CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere OWASP Secure Headers Project: OWASP Secure Headers Project | OWASP Foundation Nginx: Module ngx_http_headers_module

Evidence / Steps to Reproduce

While analyzing HTTP response headers of the VulnLawyers website, the TWZ team discovered that the web server reveals the server version running which is unnecessary and could allow attackers to fingerprint the server.
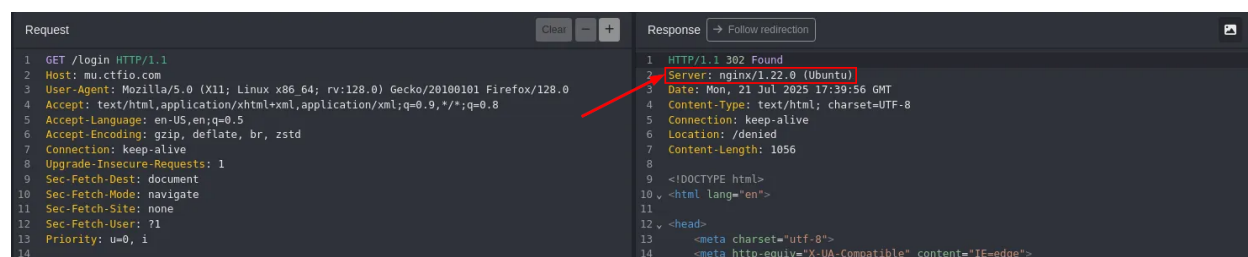

Figure 20: HTTP Response Header Showing the Server Version.

Remediation

TWZ recommends removing unnecessary information from HTTP response headers. Additionally, VulnLawyers can modify the *nginx.conf* and add the directive *server_tokens off;*

Conclusion & Next Steps

The VulnLawyers application exhibits several critical vulnerabilities, particularly around authentication, authorization, and sensitive data exposure. These findings present real-world risks that could be exploited by malicious actors to gain unauthorized access to user accounts, administrative functionalities, and sensitive data.

The most severe risks stem from insecure password practices, lack of account lockout policies, missing multi-factor authentication, and insecure direct object references (IDOR) that allow privilege escalation.

Immediate actions should be taken to address the following critical and high-risk issues:

- Enforce strong password complexity requirements.
- Implement account lockout and rate-limiting policies.
- Enable Multi-Factor Authentication (MFA) for all user accounts, especially administrative roles.
- Apply strict object-level access controls and remove all plaintext password storage.

To strengthen the overall security posture of the VulnLawyers' application:

- Apply the remediation actions outlined in each technical finding.
- Conduct a follow-up penetration test after remediations are applied to validate fixes.
- Consider integrating security monitoring and alerting mechanisms to detect future intrusion attempts.

LAST PAGE