

What this report contains

Executive Summary

This section provides a non-technical overview of the scope of the project, the key findings from the testing work carried out and highlights the areas we see as most important or urgent in needing attention to improve the security of the system under test.

Target Information

This lists what was tested and the type of testing carried out.

Methodology

This is a short, technical description, of physical way that the testing was undertaken.

Issue Summary

This is a high level, technical, summary of each issue found. It's common for this section to contain multiple examples of the same type of issue as we list every instance of an issue we find so that there is a clear list of everything that needs to be fixed – i.e. If we find a form that is insecure it's possible that each individual field within the form has the same type of issue and so if the form has five fields; First name, Last name, Email address, Company name and comments these would be listed as 5 issues as each field needs attention.

Vulnerability by Severity

This is a visual representation of the different levels of issues found to provide a quick overview of the number of each type individually and in relation to the application as a whole.

Details of Individual Issues

This is a detailed list of each issue found containing, where possible:

- Affected assets – what in the system has the issues
- Severity – on a 5-point scale from 'Critical' to 'For information only'
- OWASP / CWE mapping – how the issue relates to security testing methodologies or databases
- Technical description – a detailed technical explanation of the issue
- Steps to reproduce – how to verify the issue exists and to check that it has been fixed
- Business impact – a non-technical description of the potential impact of the issue
- Solution and/or mitigation – what's required to fix the issue
- External technical reference links – additional information in the public domain to provide more insight into the type of issue, other ways to fix it etc.

As with the issue summary, every instance of an issue is listed individually to provide a detailed, step-by-step guide for all fixes required.



Executive Summary

Appsecco was contracted by Law Firm Services to conduct Web Application Security Testing to determine if there were security weaknesses in the **LFS Client Portal** website that can render the application insecure and allow an attacker to gain access to any data that is accessible via them or gain access to the underlying operating system. The assessment was carried out between 4th October, 2023 and 10th October, 2023 on the demo web application accessible at,

- https://tenant1.hemmings-walker.co.uk
- https://tenant2.hemmings-walker.co.uk

The identity servers were,

- https://account-ten1.hemmings-walker.co.uk
- https://account-ten2.hemmings-walker.co.uk

And, the API server was,

- https://api-demo.lawfirmservices.co.uk

OWASP Top-10 2017, 2021 and CWE was used as the reference framework to evaluate and categorize the security issues.

Summary of Results

As part of the testing of the applications in scope we identified multiple weaknesses that are listed below. During the assessment 2 Medium and 2 Low severity issues were discovered. The following 4 issues discovered, arise due to weak password policy, insufficient anti-automation, and missing security headers in the application. Here is a quick summary of the discovered issues.

One Medium severity issue arises due to weak password policy leads to the possibility of account takeover

One Medium severity issues arises due to lack of anti-automation leads to service disruption and allotted quota exhaustion

One Low severity issue arises due to lack of anti-automation leads to service disruption and allotted quota exhaustion

One Low severity issue arises due to missing security headers leads to protocol downgrade attacks.