

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.

Copyright © Appsecco



Executive Summary

Appsecco was contracted by Law Firm Services to conduct Web Application Security Assessment to determine if there were security weaknesses in the LFS Portal application, the implementation of the Identity Server, the backend LFS API server and the tenant applications that can render the environment 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 testing was carried out on 11th August 2021 and 18th August 2021 on the testing setup of the LFS Hemmings and Walker application, LFS Identity Server and the associated API servers and web applications.

OWASP Top 10 2013, OWASP Top 10 2017 and CWE were used as the reference framework to evaluate and categorise the discovered security issues.

Common Vulnerability Scoring System (CVSS) 3.1 standard has been used to determine the severity of the discovered issues.

Summary of Results

No critical, high or medium severity issues have been discovered. One low severity issue has been identified.

The low severity issue identified arises because of unrestricted file upload in LFS Portal application.

The testing showed that the application has robust authentication and authorization mechanisms using Identity Server that is implemented with security in mind and prevents any unauthorised access to sensitive data.

The application is built with security in mind and can withstand attacks against common web application security vulnerabilities.

Copyright © Appsecco