UK Research and Innovation Penetration Testing Report

January 2020

Executive Summary

Introduction

The Penetration Testing team at Jisc is pleased to present the results of the penetration testing carried out for UK Research and Innovation. Extensive automated and manual testing was done against the REF submissions system and the related API covering all of the OWASP top 10 vulnerability classes.

Additionally, a phishing test was done against all REF contacts email addresses as provided to us. The testing and the results from the test are described separately in the Phishing Test section of this report.

The table below summarises the issues found and shows that the overall security posture of the REF submissions service is at an excellent level.

Risk Rating	Number of Findings
Critical	0
High	0
Medium	0

Low	0
Informational	4

Scope

The list of hosts covered by this assessment included:

- submissions.ref.ac.uk
- submissionsapi.ref.ac.uk

Conclusions and Recommendations

Submissions Site

As demonstrated by the summary of findings, no security issues above informational severity were found during the testing window. This is an exceptional and very rare result from a web application penetration test, and it is our pleasure to congratulate the UKRI REF team for the achievement. In this context, our main recommendation would be to ensure the high security standard of development is maintained.

A few informational issues which we don't qualify as vulnerabilities at present are discussed in the detailed findings below. A system should be implemented, if not already in place, to track all JavaScript libraries in use for updates, as these are not managed and part of the operating system updates. Any unexpected code behavior should be further investigated for security ramifications.

Submissions API

The supplied submissions API has a swagger interface (https://submissionsapi.ref.ac.uk/swagger/index.html) and this was used to obtain a list of possible endpoint URLs. Not all end points were found to be available for direct query, some were only available via the web user interface after authentication (with a valid Bearer Token).

Of the API URLs tested, all were found to be robust and free from any issues. The standard tests were performed, SQL Injection, Cross Site Scripting (XSS) and XML Entity injection. Part of the testing involved sending malformed data which all the end points handled properly. No unnecessary error code or descriptions were revealed, no debug output or stack traces were produced and any errors during processing were handled properly and without crashing the process.

The import process accepted malformed payloads, but according to the log files the processing failed gracefully. This is a good result as this can be a point of entry for an attacker. If the attacker can craft a specialised payload, they may be able to trigger an error condition in the parser that will execute commands or allow the attacker to upload a shell for remote access.

Phishing Exercise

A total of 291 emails were sent, 81 users clicked on the link and 61 users submitted login information. The validity of that login information was not checked, so it is possible that a section of those users submitted fake credentials. These results are the average for the sector based on our findings and highlight the importance of regular exercises to maintain user awareness and vigilance.