THREATiNTELLiGENCE

THREAT INTELLIGENCE PTY LTD

P: 1300 809 437
E: info@threatintelligence.com
HQ: 11 York Street
Sydney NSW 2000
W: threatintelligence.com
ABN: 43 156 362 300

To Whom It May Concern:

Threat Intelligence conducted a detailed penetration test of iFactFind's Web Application in April 2020.

The outcome of this engagement was for iFactFind to understand the priority risks associated with these assets and how to mitigate them to minimise the likelihood and impact of a security breach. The following web application URL's were in scope for this review:

- test.ifactfind.com.au
- test.ifactfind.com.au/afsl
- test.ifactfind.com.au/client

As per standard industry practice, Threat Intelligence did not attempt to perform any denial of service testing against the application.

The test standard used was the OWASP Application Security Verification Standard 4.0 at Verification Level 2, which consists of testing up to 131 positive security controls as defined by the standard.

For these tests, the following categories were tested:

Application Security Verification Standard Category	Controls Tested
Authentication	27
Session Management	14
Access Control	9
Validation, Sanitization and Encoding	27
Data Protection	6
Communications Security	3
Business Logic	4
File and Resources	14
API and Web Services	10
Configuration	17
Controls Tested	**131**

If there are any queries as to the nature of this testing, please contact Ty Miller, Managing Director on 0409 713 735 or ty.miller@threatintelligence.com.

Certified by

 On behalf of Ty miller

Ty Miller

Managing Director

22 June 2020

Web Application Penetration Test Report

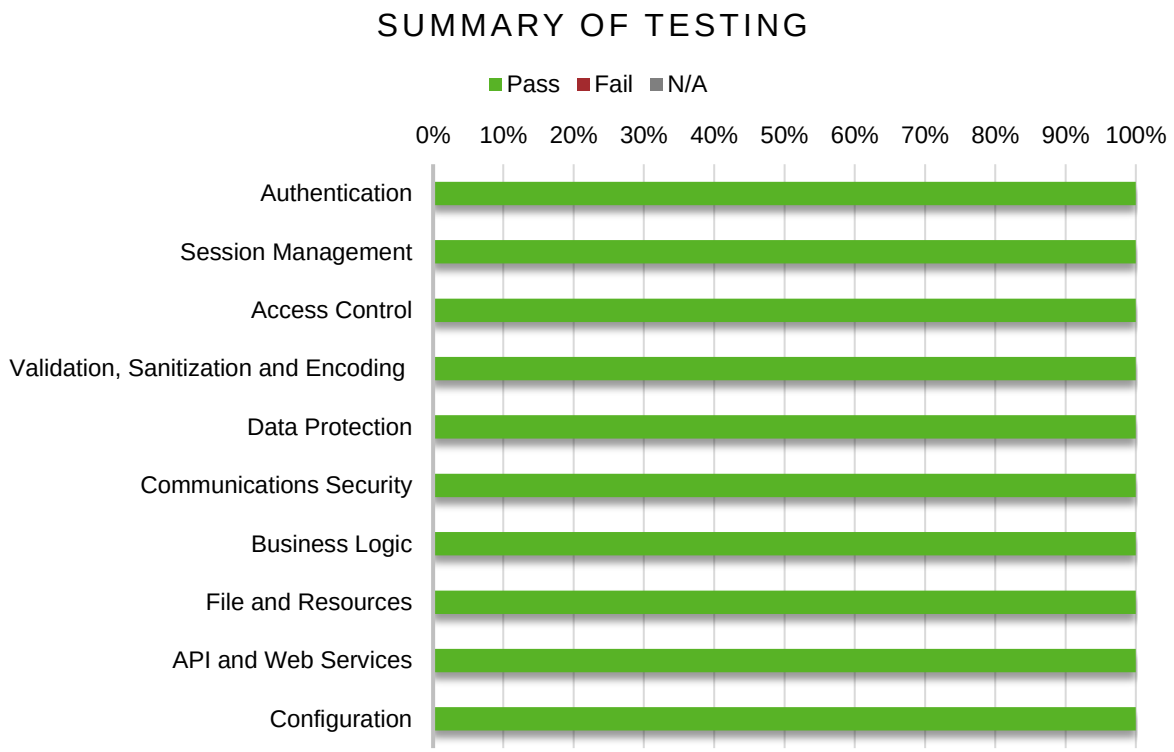
IFACTFIND

17 APRIL 2020

5.2 ASVS 4.0 LEVEL TI-2 RESULTS SUMMARY

We assessed the application using OWASP's Application Security Verification Standard 4.0 at the custom Level TI-2. This customised level includes testing of all ASVS L2 items that otherwise does not require access to systems, source code, logs, configuration data or documentation. This allows TI-2 to be a major superset of ASVS L1, whilst allowing for penetration testing without necessarily resorting to source code or hybrid review.

The complete results of our testing are detailed in the corresponding Appendix (Test Plan Results). All 131 issues were found to be in line with the standard.



.