1. Your Assessment

Your security assessment was carried out by Nick Simpson between 18/12/2019 and 19/12/2019. Nick has endeavoured to provide as much insight as possible, in line with the objectives, scope and constraints set out in this section.

1.1. Description

What were we asked to do?

Web Application Assessment

Through a mixture of black box and white box testing this assessment will attempt to identify security issues in the design and implementation of the authentication and file upload facilities of the web application. This will help build a picture of the applications resilience to attack.

Reporting and Analysis

With all security assessments the standard deliverable will be a report of findings. The intention of this document is to describe the penetration testing activities which took place, grade vulnerabilities which were discovered regarding their business risk, and supply appropriate summaries for managers and the board.

1.2. Scope

What was included in this assessment?

- https://xxx.myp11d.com – *xx.xx.xxx.xx*

1.3. Constraints

What were the limitations imposed on the assessment?

This engagement reviewed a snapshot in time of the systems in scope. Underlying configuration changes could result in the addition of new issues or a weakened security standpoint. New vulnerabilities and attack vectors are discovered on a daily basis encouraging the need for further security testing. Penetration testing is a security standard representative of both Secarma's security assessment methodology and attack techniques publicly known at the time of the engagement. As a project scope and time constraints do not limit real world attackers, it is possible that additional security weaknesses, which could not reasonably be identified during the engagement, may be present and exploited in the future.

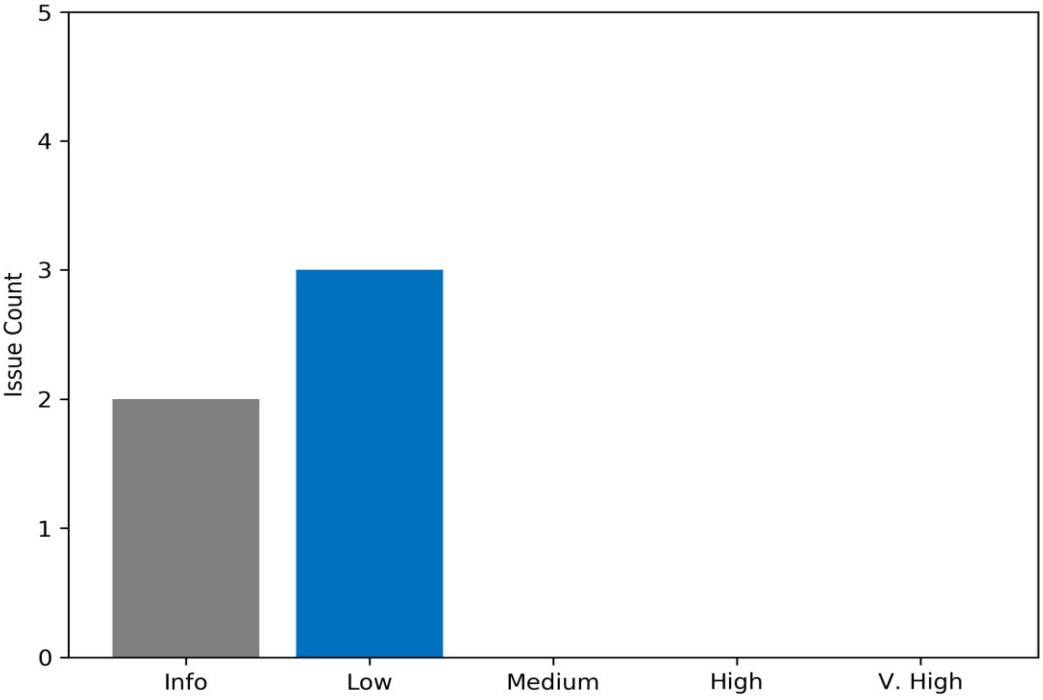
3. Technical Findings

As with all risk and vulnerability assessments, the findings that Nick has compiled in this report, may not all represent the same potential risk to PAS Ltd. Some will be purely informational, whilst others will expose the business to a varying degree of risk, depending on the associated technical and operational context. To aid you in deciding which of these issues require more immediate consideration, Nick has applied a risk rating scale, as well as their expert knowledge, in generating the following high level view of the known risks facing PAS Ltd.

3.1. Applied Risk Matrix

Total	**5**	This is the total number of issues that Nick has identified as part of your assessment.
Very High	**0**	If exploited, these issues may **critically undermine** the technical and operational capability, as well as the reputational credibility of your business.
High	**0**	The exploitation of these issues could result in **significant harm** to your business.
Medium	**0**	If exploited, the impact to your business would be **disruptive**, but not likely to significantly undermine normal business operations.
Low	**3**	These issues are difficult to exploit or would result in **little to no meaningful impact** to your business, if they were.
Info	**2**	These are technical or operational realities, which characterise a meaningful deviation from standard practice, **but do not represent a significant risk**.

3.2. Risk Overview


Issue Count
Info
Low
Medium
High
V. High