



18 August 2021.

# AMPLITUDE CLINICAL SERVICES LTD WEB APPLICATION PENETRATION TEST REPORT



The CPD Standards Office  
CPD PROVIDER: 22052  
2020 - 2022  
[www.cpdstandards.com](http://www.cpdstandards.com)



HM Government  
**G-Cloud**  
Supplier

## Document Control

Document Title:	Amplitude Clinical Services Ltd Web Application Penetration Test Report
Classification:	Commercial in Confidence
Date:	18 August 2021

## Consultant Information

Company Name:	Mitigate Cyber
Consultant Name:	Daniel Pollard
Address:	Mitigate Cyber InfoLab 21 Lancaster University Lancaster Lancashire LA1 4WA
Telephone Number:	+44 (0)333 323 3981
E-mail	daniel.pollard@mitigatecyber.com

## Client Information

Organisation Name (legal entity):	Amplitude Clinical Services Ltd
Address:	Woodend House Grafton Flyford Worcestershire WR7 4PH
Point of Contact name:	Tristan Salisbury
Telephone Number:	0333 014 6363
Email address:	tristan.salisbury@amplitude-clinical.com

## 1.0 Distribution List

© Mitigate Cyber, all rights reserved 2021.

This document contains confidential and proprietary information. It is intended for the exclusive use of Amplitude Clinical Services Ltd. Unauthorised use or reproduction of this document is prohibited.

The current test has been conducted by Mitigate Cyber's security experts. Mitigate Cyber assures that findings in this report are true to the extent that can be verified remotely.

This Vulnerability Assessment & Penetration Test reveals all relevant vulnerabilities known up to the date of this report. As new vulnerabilities continue to be found and the introduction of new security threats, it is suggested that security assessments be conducted after every major change in the Information System and periodically in 3 to 6 month intervals.

### Revision History

Version	Date	Author	Comment
0.1	18 <sup>th</sup> August 2021	Lee Smith	Initial Draft
0.2	18 <sup>th</sup> August 2021	Daniel Pollard	QA
1.0	20 <sup>th</sup> August 2021	Lee Smith	Release to Customer

## 2.0 Nondisclosure

### 2.1 Nondisclosure Statement

This report is the sole property of the customer. All information obtained in the security audit about the customer's operations and assets is deemed privileged information and not for public dissemination. The customer and Mitigate Cyber jointly and severally pledge their commitment that this information will remain strictly confidential. It will not be discussed or disclosed to any third party without the express written consent of the customer. Mitigate Cyber strives to maintain the highest level of ethical standards in its business practices.

### 2.2 Nondisclosure agreement

The customer has accepted that Mitigate Cyber can perform a security audit of their Internet facing infrastructure. All information in this document is subject to change without notice and should not be construed as any form of commitment by Mitigate Cyber. Mitigate Cyber takes no responsibility for any errors that may appear in this document. Similarly, an audit of a company's Internet infrastructure should not be construed as a definitive review of the organisation's security. Mitigate Cyber advise that differing security vulnerabilities might be gleaned through using additional scanning and enumeration techniques. Mitigate Cyber cannot be held liable for any performance issues that occur during or after the audit.

## 3.0 Report Structure

The remainder of this report is organised as follows:

### **Section 4.0: Executive Summary**

The executive summary highlights the main findings from the report and provides an indication as to the level of security of the target environment.

### **Section 4.1: Summary of Findings**

This section shows a summary of the issues found on each target accompanied by a bar chart to demonstrate the number of vulnerabilities found on each target and their severity.

### **Section 4.2: High level technical recommendations**

This section provides high level technical recommendations based on the test results.

### **Section 5.0: Introduction**

This section overviews the test and includes a summary of the test scope, a table of findings by severity by target system and the overall test methodology.

### **Section 6.0: Summary of Findings & Remediation Action**

A more detailed version of the summary of findings. An easy to view table of all findings is provided with reference to any remediations that have been made during or after the test.

### **Section 7.0: Vulnerability breakdown**


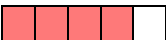



This section lists the open ports found for each target and contains the low to serious vulnerabilities. Each vulnerability includes an indication of its impact, a description, results and how it can be resolved. Whenever possible, an exploit for the identified vulnerability will be supplied. References to different web pages with additional information has also been supplied for extra supporting material. Screenshots are provided where possible within the table but for larger screenshots or multiple URLs or patch links then this will be provided in an appendix at the end of the report. If the vulnerability is detected on multiple ports, then the vulnerability count will reflect this.

## 3.1 Severity Scale

Vulnerabilities are supplied with ratings next to them giving an indication of their severity and are rated on a scale of one to five using the icons below. The rating that is applied to vulnerability is based on the information gathered during the testing and the threat to that specific environment under review.

A rating of five means that the vulnerability will enable an attacker to break into the server, a rating of one therefore is of low severity, possibly disclosing information that cannot be hidden.

A more detailed description containing examples of the ratings can be seen below:

Severity	Description
<b>Critical Risk:</b> 	<p>These findings identify conditions that could directly result in the compromise or unauthorised access of a network, system, application or information. Examples of High Risks include known buffer overflows, weak or no passwords, no encryption, which could result in denial of service on critical systems or services; unauthorised access; and disclosure of information.</p>
<b>High Risk:</b> 	<p>Vulnerabilities provide hackers with remote user access, but not remote administrator or root user capabilities. Vulnerabilities at level 4 may include full read access to files, potential backdoors, or a listing of all the users on the host. Level 4 vulnerabilities expose highly sensitive information.</p>
<b>Medium Risk:</b> 	<p>These findings identify conditions that do not immediately or directly result in the compromise or unauthorised access of a network, system, application or information, but do provide a capability or information that could, in combination with other capabilities or information, result in the compromise or unauthorized access of a network, system, application or information.</p>
<b>Low Risk:</b> 	<p>Warnings which may or may not be vulnerabilities, depending upon the patch level or configuration of the target. Typical low risk vulnerabilities might provide unnecessary or excessive information about a host or its operating environment</p>
<b>Informational:</b> 	<p>Attackers can gather information about the host (open ports, services, software packages and versions etc.) and may be able to use this information to discover other vulnerabilities.</p>

## 4.0 Executive Summary

This report presents the results of the penetration test of the target web application based on a grey-box test Methodology. This assessment was performed under the auspices of Mitigate Cyber’s certified and licensed penetration tester. The purpose of this assessment was to ascertain what vulnerabilities and exposures exist through the internet facing and identify areas where penetration may be possible.

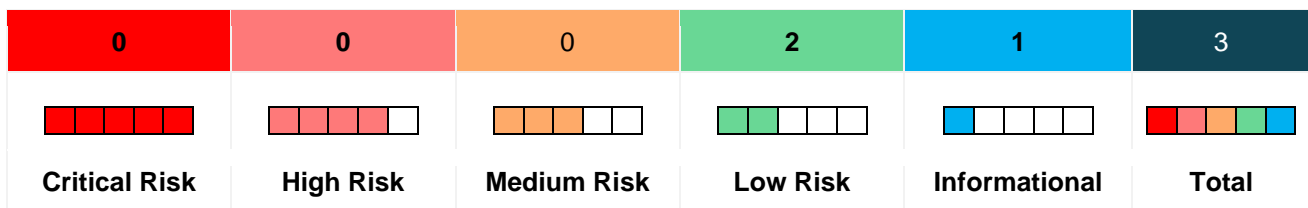
The findings in this report reflect the conditions found during the testing, and do not necessarily reflect current conditions.

### 4.1 Executive summary

This analysis is based on the technologies and known threats as of the date of this report. Mitigate Cyber recommends that all recommendations suggested in this document be performed to ensure the overall security of the internet facing environment.

The test was carried out from Monday 12<sup>th</sup> to Friday 16<sup>th</sup> July 2021.

The total numbers of vulnerabilities found by severity were:




### 4.2 Summary of Findings

Overall, the security of the Amplitude systems was found to be excellent. Following a retest, all the medium-rated issues have now been resolved, thus improving the security even further. The only issues that remain are either informational only, or low risk.

### 4.3 High level technical recommendations

In response to the detected vulnerabilities Mitigate Cyber recommend the following fix activity:

- Validate the functionality used to encode and process user inputs, in particular for the input string "<?".
- Disable password auto-complete.



**Full Report:** Please note, the pages following this page contain technical information and are therefore not to be shared in the public domain.

---