NETTITUDE

INTELLIGENT CYBER SECURITY & RISK MANAGEMENT

Penetration Test Management Report

Prepared for Amplitude

Authored by Dave Hardy

16 May 2016

Version 1.0

CREST

CHECK
IT Health Check Service

PCI Security Standards Council ™

NETTITUDE

INTELLIGENT CYBER SECURITY & RISK MANAGEMENT

Penetration Test Management Report

Nettitude provides a wealth of knowledge, expertise and experience in regards to Data Security. We provide comprehensive vulnerability assessment, penetration testing and application assessment services. Our team of dedicated security consultants deliver best in class testing capability as well as strong remediation advice and guidance.

NETTITUDE

REPORT CONTENTS

1 DISTRIBUTION LIST

Nettitude

Name	Title
Dave Hardy	Security Consultant
Lukasz Michalski	Security Consultant
Lauren Cole	Account Manager

Amplitude

Name	Title
Szymon Wnuk	Technical Testing Facilitator
Gary McCormack	Web Developer

Revision History

Version	Issue Date	Issued By	Comments
0.1	12 May 2016	Dave Hardy	Initial Draft
0.2	13 May 2016	Lukasz Michalski	Quality Assurance
0.3	13 May 2016	Lauren Cole	Quality Assurance
1.0	16 May 2016	Dave Hardy	Final

2 EXECUTIVE SUMMARY

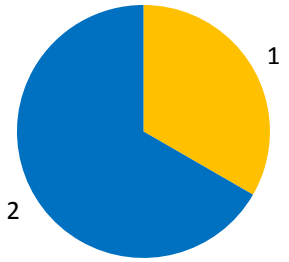
Background

Amplitude engaged with Nettitude in May 2016 in order to assess the overall security posture of their Amplitude registry application.

High Level Assessment

Based on the Amplitude's risk profile, primary security concerns and the vulnerabilities identified at the point of the engagement, Nettitude have found the application to be:

STRONG



Nettitude were able to…

- Identify out of date software
- Identify misconfigured web server settings

Primary Security Concerns

Nettitude worked with Amplitude, prior to this engagement, to investigate and understand the primary security concerns associated with the systems in scope.

These concerns are not exhaustive, but rather represent a method of helping to gauge the severity of the overall risk presented by the systems in scope.

Concern	Description	Data Category	Result
New software architecture	To ensure application is secure on the new architecture	Confidentiality Integrity	PASS
Security Best Practices	Issues identified during testing are not considered to be best practice	Confidentiality Integrity	PASS

Table 1 – Amplitude Primary Security Concerns

3 RISK AND ANALYSIS

Risk Profile

Nettitude present the following high level risk profile for Amplitude in order to help contextualise the reasoning behind each findings severity and the overall system rating of 'Strong'. This is Nettitude's own assessment, based on their knowledge and understanding of Amplitude, as an organisation.

How to understand the values below?

All risks should be run through your own internal risk register and methodology. The aim below is to provide you with a benchmark and a stake in the ground. We have only had a glimpse of the data you hold, and have based the impact on your business on industry equivalents. It's very important that you re-assess and understand these values according to your business and its risk appetite.

How do we calculate risk?

In brief, assets have values which if compromised will have an impact on your business (reputation, ability to function, fines, etc). Weaknesses (or vulnerabilities) allow threats to access/disrupt these assets. The location of the vulnerability will determine the likelihood of the weakness to be exploited.

Risk is a factor of the vulnerability, the impact and the likelihood. Threats need to be considered, but these are outside the scope of this work (See ISO31000 for a detailed methodology).

Risk and Priority Key

The following key shows how the level of risk and priority will be represented within this report.

Critical	
High	
Medium	
Low	

Amplitude Risk Details

The table below shows the values calculated for this environment.

Risk Factor	Grade	Reasoning
Impact		The application contains personally identifiable and sensitive information, being able to access this would severely impact not only the clients but the reputation of the company, which could also possibly lead to financial repercussions.
Vulnerability		A medium rated issue was identified, which relates to outdated software.
Likelihood		The likelihood of compromise is low given the identified issues.

Table 2 – Amplitude Risk Breakdown

Overall Risk Status

The overall risk for the environment under review for Amplitude is shown below:

Amplitude may perceive their risk profile to differ from what is presented in this section, in which case Nettitude would be happy to engage and discuss.

4 SYSTEM ANALYSIS

Nettitude were commissioned by Amplitude to assess the security posture of their Amplitude application and associated infrastructure.

A total of three issues were identified, the most severe being rated as a medium risk.

Before discussing the findings of the testing, it must be mentioned that the application on the whole is very well developed and free from the most common web application vulnerabilities e.g. SQL Injection, Cross Site Scripting and Cross Site Request Forgery etc.

The medium rated finding relates to the use of well-known library code to enhance the user experience or add functionality to the application; Nettitude identified that these were out-dated and subject to know security vulnerabilities, and should be updated, if possible, and added to the site patching regime.

Nettitude identified two low rated issues that relate to the configuration of the web server, the more significant of the two issues provides extra layers of security to the application and the users of the application.

Nettitude believe that the remediation steps outlined in the technical report will allow Amplitude to strengthen the security posture of the application. It is essential that the details of the technical report are understood prior to remediation, and also a formal debrief should be arranged to discuss the findings. A debrief can be arranged with your account manager directly.

5 NEXT STEPS

Post Engagement Actions

Nettitude recommends that Amplitude perform the following post engagement activities in the order of priority indicated.

	Activity	Description	Priority
1	Debrief from Nettitude	Nettitude will deliver a formal debrief to Amplitude in order to ensure that the findings of this engagement have been fully comprehended and to help assist in the formulation of a remediation plan.	
2	Update/patch outdated software	Update and/or apply vendor's software patches, implement a software patching solution and apply and update software at regular intervals.	
3	Reconfigure the web server	Apply the recommended web server configuration changes outlined in the technical report	

Table 3 – Post Engagement Activities

Nettitude recommend that the contents of this report are fully understood prior to progressing onto the technical report, which provides further information on the individual vulnerabilities identified, including how to fix them.