Security Testing Report

PROJECT A

General information	
Customer	<Project name>
Created by (Author)	
Preparation date	
Version	
Status	

Revision History					
Version	Description	Author	Date	Approved by	
				Author	Date

Content

1. Introduction

1.1 Testing Methodology

Description of the methodology.

1.2 Security testing plan

1	Tools selection
2	Environment preparation
3	Security testing
4	Results analysis
5	Preparation of a report and a list of recommendations for resolving found vulnerabilities

1.3 Tools

The list of tools used during the execution of security testing:

1	Modify Headers for Firefox
2	Nmap
3	….
4	….
5	….

2. Security Testing Report

2.1 Web application infrastructure configuration

During collecting of information about the infrastructure there were found 1 domains hosted on the server:

Host	Server

All the ports of the application servers were scanned, the following data was obtained:

Server	Port	Status	Service	Version
	80/tcp	open	http	-
	443/tcp	open	ssl/https	….

Risk level: high

Recommendations for security improving: We recommend to...

2.2 Using components with known vulnerabilities

Also scanners show that server type is Apache/2.4.33 (Amazon) and OpenSSL/1.0.2k-fips PHP/5.6.36. This version of Apache, OpenSSL and PHP have a lot of known vulnerabilities. List of them is presented below in the table:

<table>

To improve the security of the system, you should follow the updates of the components used, frameworks, server operating system.

Risk level: medium

Recommendations for security improving: We recommend to...

2.3 Password fields with auto-complete

In typical form-based web applications, it is common practice for developers to allow autocomplete within the HTML form to improve the usability of the page. With autocomplete enabled (default), the browser is allowed to cache previously entered form values.

For legitimate purposes, this allows the user to quickly re-enter the same data when completing the form multiple times.

When autocomplete is enabled on either/both the username and password fields, this could allow a cyber-criminal with access to the victim's computer the ability to have the victim's credentials automatically entered as the cyber-criminal visits the affected page.

It was discovered that the affected pages contain forms containing a password field that has not disabled autocomplete.

<screens>

Risk level: low

Recommendations for security improving: We recommend to...

2.4 Next type of checking

2.5 Next type of checking

2.6 Next type of checking

3. Recommendations for security

During testing several problems were discovered in security of the web application. Based on the information available, the security testing team suggests possible solutions to the problems listed in the table below.

<recommendations>