Submitted to: Development Team  
Security Analyst: Security Analyst Team  
  
Date of Testing: 6/6/2021  
Date of Report Delivery: 6/6/2021

Security Assessment

|  |
| --- |
|  |

**Table of Contents**

Contents

[Security Engagement Summary 2](#_Toc47679235)

[Engagement Overview 2](#_Toc47679236)

[Scope 2](#_Toc47679237)

[Risk Analysis **Error! Bookmark not defined.**](#_Toc47679238)

[Recommendation **Error! Bookmark not defined.**](#_Toc47679239)

[Significant Vulnerability Summary 3](#_Toc47679240)

[High Risk Vulnerabilities 3](#_Toc47679241)

[Medium Risk Vulnerabilities 3](#_Toc47679242)

[Low Risk Vulnerabilities 3](#_Toc47679243)

[Significant Vulnerability Detail 4](#_Toc47679244)

[<< Vulnerability Name>> 4](#_Toc47679245)

[<< Vulnerability Name>> 5](#_Toc47679246)

[Methodology 6](#_Toc47679247)

[Assessment Toolset Selection 6](#_Toc47679248)

[Assessment Methodology Detail 6](#_Toc47679249)

# Security Engagement Summary

## Engagement Overview

<<

Explain the engagement.

* Who requested the engagement and why?
* What are the engagement’s goals?
* Who is complete the engagement?
* How often is assessment completed?

>>

The Udajuicer Development team that is responsible for the organization’s web-applications has requested a vulnerability assessment of a legacy web-application to help them understand what security risk the web-application is posing to the organization, and what mitigations are possible to increase the security posture and reduce the risk to the organization.

A security analyst working in the Information Security department at Udajuicer will be in charge of the engagement.

The assessment should be completed once every quarter.

## Scope

<<

In high-level terms, describe the scope of the engagement and why this scope is appropriate

>>

Frequent vulnerability and risk assessment operations are critical in understanding the potential risk of the information security infrastructure within an organization.

Vulnerability assessment can identify potential problems and weaknesses in an environment that, combined with a threat.

A vulnerability assessment of a legacy web-application will help to increase the security posture and reduce the risk to the organization.

## Executive Risk Analysis

<<

Summarize the overall risk that the report indicates for the scope. ( High | Medium | Low )

Explain why this risk level was reported. Include a summary of vulnerabilities in discussion (Executive Summary) form.

>>

## Executive Recommendation

<<

In discussion (Executive Summary) form, explain if remediation efforts are warranted. Describe at a high level how to best mitigate or remediate the highest-risk vulnerabilities Prioritize which vulnerability should be remediated first and why.

>>

# Significant Vulnerability Summary

<<

Provide a list of the highlighted vulnerabilities in descending order of assessed risk

High | Medium | Low

>>

### High Risk Vulnerabilities

### Medium Risk Vulnerabilities

### Low Risk Vulnerabilities

# Significant Vulnerability Detail

<<

For each significant vulnerability assessed, provide a summary of the vulnerability.

Include a page-break between each vulnerability in this section.

>>

## << Vulnerability Name>>

**<<RISK LEVEL HIGH | MEDIUM | LOW>>**

<<

Vulnerability detail

* Provide the assessed risk level (High | Medium | Low ) of the vulnerability.
* Discussion (Executive Summary) form, explain how the vulnerability was identified and validated.
* Provide evidence of validation (Screenshot, log excerpt, etc.)
* Discuss the probability of exploit/attack.
* Discuss who would be impacted if the attack was exploited (users-groups, departments, business-continuity/revenue)
* Discuss potential remediation

>>

## << Vulnerability Name>>

**<<RISK LEVEL HIGH | MEDIUM | LOW>>**

<<

Vulnerability detail

* Provide the assessed risk level (High | Medium | Low ) of the vulnerability.
* Discussion (Executive Summary) form, explain how the vulnerability was identified and validated.
* Provide evidence of validation (Screenshot, log excerpt, etc.)
* Discuss the probability of exploit/attack.
* Discuss who would be impacted if the attack was exploited (users-groups, departments, business-continuity/revenue)
* Discuss potential remediation

>>

# Methodology

<<

The remainder of the report is intended for technical practitioners, other security analysts, engineers, developers, and systems-administrators. Use of technical terms is appropriate.

The assessment methodology will be the longest single section of this report. It is written in a mostly chronological order starting with tool selection, followed be execution of tools, analysis of output, and validation of significant vulnerabilities.

Any significant vulnerabilities should be referenced in the earlier Significant Vulnerabilities Summary and Detail section, as well as discussed in the Risk Analysis and potentially in the Recommendation portions of this report.

>>

## Assessment Toolset Selection

<<

Provide a list of tools used during the vulnerability assessment and validation.

>>

## Assessment Methodology Detail

<<

Include evidence of the vulnerability assessment tool execution and sample output.

As tools are used, include either screenshots or specific command-line instructions.

Analysis of the tool output may identify significant vulnerabilities. Vulnerabilities that are considered significant should be validated manually. The process of manual validation is documented. The process documentation may include screenshots, tool commands. The process documentation should include evidence if the significant vulnerability is valid.

The methodology should include sufficient detail for a technical practitioner to arrive at the same risk conclusions as you present in earlier sections of the report.

>>

This concluded the vulnerability assessment methodology portion of this report.