**{{ malcode }}**

**Dynamic Application Security Test (DAST)**

**{{ assement\_comp\_date }}**

Contents

[1. Executive Summary 3](#_Toc99805179)

[1.1 Overview 3](#_Toc99805180)

[1.1.1 Threat Overview 3](#_Toc99805181)

[1.2 Project Objectives 3](#_Toc99805182)

[1.3 Assessment Details 3](#_Toc99805183)

[2. Findings 5](#_Toc99805184)

[2.1 Severity Findings 5](#_Toc99805185)

[2.1.1 5](#_Toc99805186)

[3. Appendix 6](#_Toc99805187)

[3.1 Remediation Requirements 6](#_Toc99805188)

**Disclaimer**

<Replace me with Confidentiality policy>

# Executive Summary

## Overview

Full dynamic application security testing was conducted from {{ from\_date }} through {{ to\_date }}.

Automated dynamic application security testing using Burp Suite was performed on the {{ typeofappl }} due to Application Security Standard Requirements.

**Disclaimer:**

<Please fill if available>.

### Threat Overview

Overall, identified the following number of security issues:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Number of Observations by Threat Level** | | | | | | |
|  | **Total** | **Critical** | **High** | **Medium** | **Low** | **Informational** |
| **Open** | **0** | 0 | 0 | 0 | 0 | 0 |
| **Closed** | 0 | 0 | 0 | 0 | 0 | 0 |

| **Issue Name** | **Severity** | **Finding ID** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Project Objectives

The following IP/URLs were tested for security vulnerabilities:

* {{ host }} : {{ ip }}

## Assessment Details

|  |  |
| --- | --- |
| **Application Name:** | **{{ nameofappl }}** |
| **MAL Code:** | **{{ malcode }}** |
| **Line of Business:** | **{{ line\_of\_business }}** |
| **Application Owner:** | **{{ btrm\_name }}** |
| **Assessment Name:** | **Dynamic Scan for Web Application** |
| **Intake Request:** | **{{ appsec\_no }}** |
| **Requester Name:** | **{{ requester\_name }}** |
| **Assessor Name:** | **{{ assessor\_name }}** |
| **Assessment Completed Date:** | **{{ assement\_comp\_date }}** |
| **Technical Contact:** | **{{ tech\_contact }}** |
| **Project Identifier / Ref:** | **{{ clarity\_code }}** |

# Findings

## Critical Severity Findings

|  |  |
| --- | --- |
| {% for item in document\_obj %} | |
| {% if ‘Critical’ in item.keys() %} | |
| {%tr for key, value in item.items() %} | |
| {{ value.name }} | |
| Severity: {{ value.severity }} | |
| CVSS Vector: 0.00 | |
| Remediation State*:* Open | |
| Affected Asset | |
| URL | PARAMETER(S) |
| {{ value.host }} | {{ value.port }} |
| Affected URLs | |
| URL | PARAMETER(S) |
| {{ value.path }} | {{ value.param }} |
| Vulnerability Details | |
| {{ value.issueDetail }} | |
| {{ value.issueBackground }} | |
| Recommendation | |
| {{ value.remediationBackground }} | |
| References | |
|  | |
| {%tr endfor %} | |
| {% endif %} | |
| {% endfor %} | |

## High Severity Findings

|  |  |
| --- | --- |
| {% for item in document\_obj %} | |
| {% if ‘High’ in item.keys() %} | |
| {%tr for key, value in item.items() %} | |
| {{ value.name }} | |
| Severity: {{ value.severity }} | |
| CVSS Vector: 0.00 | |
| Remediation State*:* Open | |
| Affected Asset | |
| URL | PARAMETER(S) |
| {{ value.host }} | {{ value.port }} |
| Affected URLs | |
| URL | PARAMETER(S) |
| {{ value.path }} | {{ value.param }} |
| Vulnerability Details | |
| {{ value.issueDetail }} | |
| {{ value.issueBackground }} | |
| Recommendation | |
| {{ value.remediationBackground }} | |
| References | |
|  | |
| {%tr endfor %} | |
| {% endif %} | |
| {% endfor %} | |

## Medium Severity Findings

|  |  |
| --- | --- |
| {% for item in document\_obj %} | |
| {% if ‘Medium’ in item.keys() %} | |
| {%tr for key, value in item.items() %} | |
| {{ value.name }} | |
| Severity: {{ value.severity }} | |
| CVSS Vector: 0.00 | |
| Remediation State*:* Open | |
| Affected Asset | |
| URL | PARAMETER(S) |
| {{ value.host }} | {{ value.port }} |
| Affected URLs | |
| URL | PARAMETER(S) |
| {{ value.path }} | {{ value.param }} |
| Vulnerability Details | |
| {{ value.issueDetail }} | |
| {{ value.issueBackground }} | |
| Recommendation | |
| {{ value.remediationBackground }} | |
| References | |
|  | |
| {%tr endfor %} | |
| {% endif %} | |
| {% endfor %} | |

## Low Severity Findings

|  |  |
| --- | --- |
| {% for item in document\_obj %} | |
| {% if ‘Low’ in item.keys() %} | |
| {%tr for key, value in item.items() %} | |
| {{ value.name }} | |
| Severity: {{ value.severity }} | |
| CVSS Vector: 0.00 | |
| Remediation State*:* Open | |
| Affected Asset | |
| URL | PARAMETER(S) |
| {{ value.host }} | {{ value.port }} |
| Affected URLs | |
| URL | PARAMETER(S) |
| {{ value.path }} | {{ value.param }} |
| Vulnerability Details | |
| {{ value.issueDetail }} | |
| {{ value.issueBackground }} | |
| Recommendation | |
| {{ value.remediationBackground }} | |
| References | |
|  | |
| {%tr endfor %} | |
| {% endif %} | |
| {% endfor %} | |

## Informational Findings

|  |  |
| --- | --- |
| {% for item in document\_obj %} | |
| {% if ‘Information’ in item.keys() %} | |
| {%tr for key, value in item.items() %} | |
| {{ value.name }} | |
| Severity: {{ value.severity }} | |
| CVSS Vector: 0.00 | |
| Remediation State*:* Open | |
| Affected Asset | |
| URL | PARAMETER(S) |
| {{ value.host }} | {{ value.port }} |
| Affected URLs | |
| URL | PARAMETER(S) |
| {{ value.path }} | {{ value.param }} |
| Vulnerability Details | |
| {{ value.issueDetail }} | |
| {{ value.issueBackground }} | |
| Recommendation | |
| {{ value.remediationBackground }} | |
| References | |
|  | |
| {%tr endfor %} | |
| {% endif %} | |
| {% endfor %} | |