A logo of a nuclear explosion

Description automatically generated

Robert A. Kalka Metropolitan Skyport

Security Assessment Report

|  |
| --- |
| National University Cybersecurity Competition Team |

<Time>

**Confidentiality Statement:** The information contained within this report is considered proprietary and is Confidential Information. Inappropriate and unauthorized disclosure of this report or portions of it could result in significant damage or loss. This report should be distributed to individuals on a need-to-know basis only.

TABLE OF CONTENTS

[EXECUTIVE SUMMARY 3](#_Toc150531284)

[IMPACT 3](#_Toc150531285)

[RECOMMENDATIONS 3](#_Toc150531286)

[SECURITY TESTING OVERVIEW 3](#_Toc150531287)

[TESTING SUMMARY 4](#_Toc150531288)

[Scope 4](#_Toc150531289)

[PROJECT TEAM 4](#_Toc150531290)

[METHODOLOGY 4](#_Toc150531291)

[VULNERABILITIES 5](#_Toc150531292)

[CRITICAL 5](#_Toc150531293)

[HIGH 5](#_Toc150531294)

[MEDIUM 5](#_Toc150531295)

[LOW 5](#_Toc150531296)

[INFO 5](#_Toc150531297)

[ATTACKCHAINS 6](#_Toc150531298)

[APPENDIX: OVERVIEW EXPLAINED 7](#_Toc150531299)

[APPENDIX: SEVERITY DEFINITIONS 8](#_Toc150531300)

[APPENDIX: TESTCASES <take out if not needed> 9](#_Toc150531301)

[APPENDIX: VULNERABILITY-TO-ASSET MAPPING 10](#_Toc150531302)

[<Vulnerability Name> 10](#_Toc150531303)

[APPENDIX: ASSET-TO-VULNERABILITY MAPPING 10](#_Toc150531304)

[<Asset Name/IP> 10](#_Toc150531305)

# EXECUTIVE SUMMARY

<Exec Summary>

## IMPACT

<Impact on organization>

## SECURITY STRENGTHS

<List security strengths observed during assessment>

## RECOMMENDATIONS

<Recommendations at exec level detail>

## SECURITY TESTING OVERVIEW

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TOTAL UNIQUE VULNERABILITIES**  **0** | | | | | |
| **CRITICAL**  **0** | **HIGH**  **0** | **MEDIUM**  **0** | | **LOW**  **0** | **INFO**  **0** |
| **ZERO-DAY**  **0** | | | **EASILY-EXPLOITABLE**  **0** | | |

# TESTING SUMMARY

|  |  |  |
| --- | --- | --- |
| START  Sat 11 Nov 2023 | PROGRESS  0% | END  Sat 11 Nov 2023 |
| TOTAL VULNERABILITIES FOR ALL ASSETS: **0**  TOTAL CRITICAL VULNERABILITIES FOR ALL ASSETS: **0**  TOTAL HIGH VULNERABILITIES FOR ALL ASSETS: **0**  TOTAL MEDIUM VULNERABILITIES FOR ALL ASSETS: **0**  TOTAL LOW VULNERABILITIES FOR ALL ASSETS: **0**  TOTAL INFO VULNERABILITIES FOR ALL ASSETS: **0** | | |

## OBJECTIVES

<List/discuss objectives>

## Scope

1. <CIDR Ranges>
2. <Domains>

## PROJECT TEAM

1. <Teammates and Roles>
2. <Include RAKMS POC>

## METHODOLOGY

<Talk about methodology or methodologies used>

# VULNERABILITIES

## CRITICAL

<Crit vulns. These sections should contain the vulnerability, CVSS, Applicable Risk (EPSS), Description, Exploitation (if any), and Remediation. Include applicable screenshots>

## HIGH

<High vulns>

## MEDIUM

<Medium vulns>

## LOW

<Low vulns>

## INFO

<Info vulns>

# ATTACKCHAINS

<Specific attack paths/chains>

# DETAILED FINDINGS AND RECOMMENDATIONS

<This is where we can discuss in detail our exploitation paths, how to recreate it, and exact fixes. Goal should be to have something someone with decent technical knowledge could recreate>

# APPENDIX: OVERVIEW EXPLAINED

A screenshot of a computer

Description automatically generated

# APPENDIX: SEVERITY DEFINITIONS

A screenshot of a computer

Description automatically generated

# APPENDIX: TESTCASES <take out if not needed>

COMPLETED

<Completed>

IN PROGRESS

<In Progress>

NOT TESTED

<Not Tested>

NOT APPLICABLE

<N/A>

# APPENDIX: VULNERABILITY-TO-ASSET MAPPING

## <Vulnerability Name>

<List of Assets>

# APPENDIX: ASSET-TO-VULNERABILITY MAPPING

## <Asset Name/IP>

<Vuln 1>