­

­

Penetration Test Report

Prepared By:

Prepared For:

Prepared On: undefined NaN,

ncrvoyix.com

Table of Contents

Section I

1.0 Executive Summary 3

1.1 Project Overview 3

1.2 Scope 3

1.3 Testing Accounts Provided 3

1.4 Assessment Team 3

1.4 Summary of the findings 4

1.5 Conclusion 4

# 1.0 Executive Summary

NCR AppSec team performed penetration testing of to find any security weaknesses in the application. This test was performed as of May 2024.

## 1.1 Project Overview

The AppSec team conducted a security assessment of the , employing both automated scanning and manual testing methodologies. The primary objective was to identify and address any potential vulnerabilities proactively, mitigating the risk of exploitation by malicious actors.

## 1.2 Scope

The following targets were provided to perform the scan:

|  |
| --- |
| List of in-scope items |
| Scope |

## 1.3 Testing Accounts Provided

|  |  |  |
| --- | --- | --- |
| User Type | User Id | Password/SSO |
| Internal | Id | SSO |

## 1.4 Assessment Team

|  |  |
| --- | --- |
| Name | Role |
| Name | Designation |

## 

## 1.4 Summary of the findings

|  |  |
| --- | --- |
|  | **■** Critical **■** High **■** Medium **■** Low **■** Info |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Vulnerability | Risk Rating | Application/System Impacted |
| 1 | XML External Entity (XXE) Injection | High |  |

# 1.5 Conclusion

Conclusion

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Vulnerability | Risk Rating | Application/System Impacted |
| 1 | XML External Entity (XXE) Injection | High |  |
| **Vulnerability Description:**  Exploiting vulnerable XML processors by including external entities. | | | |
| **Vulnerability Evidence:** | | | |
| **Impact:**  Data exfiltration DoS attacks and remote code execution. | | | |
| **Recommendations:**  Disable XML external entity processing Use libraries that protect against XXE Sanitize and validate all XML inputs. | | | |