­

­

Penetration Test Report

Prepared By: vinay

Prepared For: app name

Prepared On: September 4, 2024

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 app name 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 app name, 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 |
| google.com |

**1.3 Testing Accounts Provided**

|  |  |  |
| --- | --- | --- |
| User Type | User Id | Password/SSO |
| Vinay | asdasdf | 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 | google.com |
| 2 | Clickjacking | Medium |  |

**1.5 Conclusion**

Conclusion

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

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Vulnerability | Risk Rating | Application/System Impacted |
| 2 | Clickjacking | Medium |  |
| **Vulnerability Description:**  Malicious technique of tricking a user into clicking on something different from what the user perceives. | | | |
| **Vulnerability Evidence:** | | | |
| **Impact:**  Unintended actions such as changing settings or initiating transactions. | | | |
| **Recommendations:**  Use X-Frame-Options header Implement frame busting techniques Educate users on the risks of clickjacking. | | | |