|  |
| --- |
| New Audit Demo |
| Vulnerability Report |
| Saturday, April 03, 2021 |

modifications history

| **Version** | **Date** | **Author** | **Description** |
| --- | --- | --- | --- |
| 1.0 | 04/03/2021 | Devi Jagannadh Kotha | Initial Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

1. General Information 4

1.1 Scope 4

1.2 Organisation 4

2. Executive Summary 5

3. Technical Details 6

3.1 title 6

4. Vulnerabilities summary 8

# General Information

## Scope

VIT-AP has mandated us to perform security tests on the following scope:

## Organisation

The testing activities were performed between 04/02/2021 and 04/14/2021.

# Executive Summary

# Vulnerabilities summary

Following vulnerabilities have been discovered:

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **ID** | **Vulnerability** | **Affected Scope** |
| High | IDX-002 | DOM XSS |  |
| Medium | VULN-001 | Clickjacking |  |

# Technical Details

## DOM XSS

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CVSS Severity** | **High** | | **CVSSv3 Score** | | **7.6** |
| **CVSSv3 criterias** | Attack Vector : | **Network** | Scope : | **Changed** | |
| Attack Complexity : | **Low** | Confidentiality : | **High** | |
| Required Privileges : | **Low** | Integrity : | **Low** | |
| User Interaction : | **Required** | Availability : | **None** | |
| **Affected scope** |  | | | | |
| **Description** | **DOM XSS** stands for Document Object Model-based **Cross-site Scripting**. ... All HTML documents have an associated **DOM** that consists of objects, which represent document properties from the point of view of the browser. When a client-side script is executed, it can use the **DOM** of the HTML page where the script runs. | | | | |
| **Observation** | 1)Open any url which you want to test let's say https://www.incrypts.com/   2) now just put <html> | | | | |
| **Test details** | | | | | |
| **Remediation** | USE USER INPUT VALIDATION AND WAF | | | | |
| **References** |  | | | | |

## Clickjacking

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CVSS Severity** | **Medium** | | **CVSSv3 Score** | | **6.3** |
| **CVSSv3 criterias** | Attack Vector : | **Network** | Scope : | **Unchanged** | |
| Attack Complexity : | **Low** | Confidentiality : | **Low** | |
| Required Privileges : | **Low** | Integrity : | **Low** | |
| User Interaction : | **None** | Availability : | **Low** | |
| **Affected scope** |  | | | | |
| **Description** | Clickjacking is a malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or allowing others to take control of their computer while clicking on seemingly innocuous objects, including web pages. A clickjack takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function. Clickjacking is an instance of the confused deputy problem, a term used to describe when a computer is innocently fooled into misusing its authority. | | | | |
| **Observation** | 1)Open any url which you want to test let's say https://www.incrypts.com/   2) now just put <html> | | | | |
| **Test details** | | | | | |
| **Remediation** | Use “X- Frame Options” | | | | |
| **References** |  | | | | |

## XSS

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CVSS Severity** | **None** | | **CVSSv3 Score** | | **0** |
| **CVSSv3 criterias** | Attack Vector : |  | Scope : |  | |
| Attack Complexity : |  | Confidentiality : |  | |
| Required Privileges : |  | Integrity : |  | |
| User Interaction : |  | Availability : |  | |
| **Affected scope** |  | | | | |
| **Description** |  | | | | |
| **Observation** |  | | | | |
| **Test details** | | | | | |
| **Remediation** |  | | | | |
| **References** |  | | | | |