

**Finding Name: Missing Anti-Clickjacking Header**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Roocha Thakkar | Penetration Testing | Project Co-lead | Ontrack | Nabiha Masood & Oliver Powell |  |

|  |
| --- |
| **Was this Finding Successful?** |
| Yes |

**Finding Description**

Clickjacking is a harmful attack in which a deceptive website misleads users into clicking on unintended elements, allowing attackers to manipulate their actions. This can result in unauthorized activities and the exposure of sensitive information. Therefore, clickjacking poses a significant risk to internet users' security and privacy.

**Risk Rating**  
Impact: Minor  
Likelihood: Moderate

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact values** | | | | |
| **Very Minor** | **Minor** | **Significant** | **Major** | **Severe** |
| Risk that holds little to no impact. Will not cause damage and regular activity can continue. | Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity. | Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally. | Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally. | Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur and/or happens. | Event occurs at times and/or probably happens a lot. | Event is occurring now and/or happens frequently. |

**Business Impact**

Clickjacking, also called UI redress attack, deceives users into clicking on disguised elements, potentially leading to data theft or malware installation. Attackers exploit users' trust in the interface, tricking them into revealing sensitive information or unknowingly downloading malicious software.

**Affected Assets**

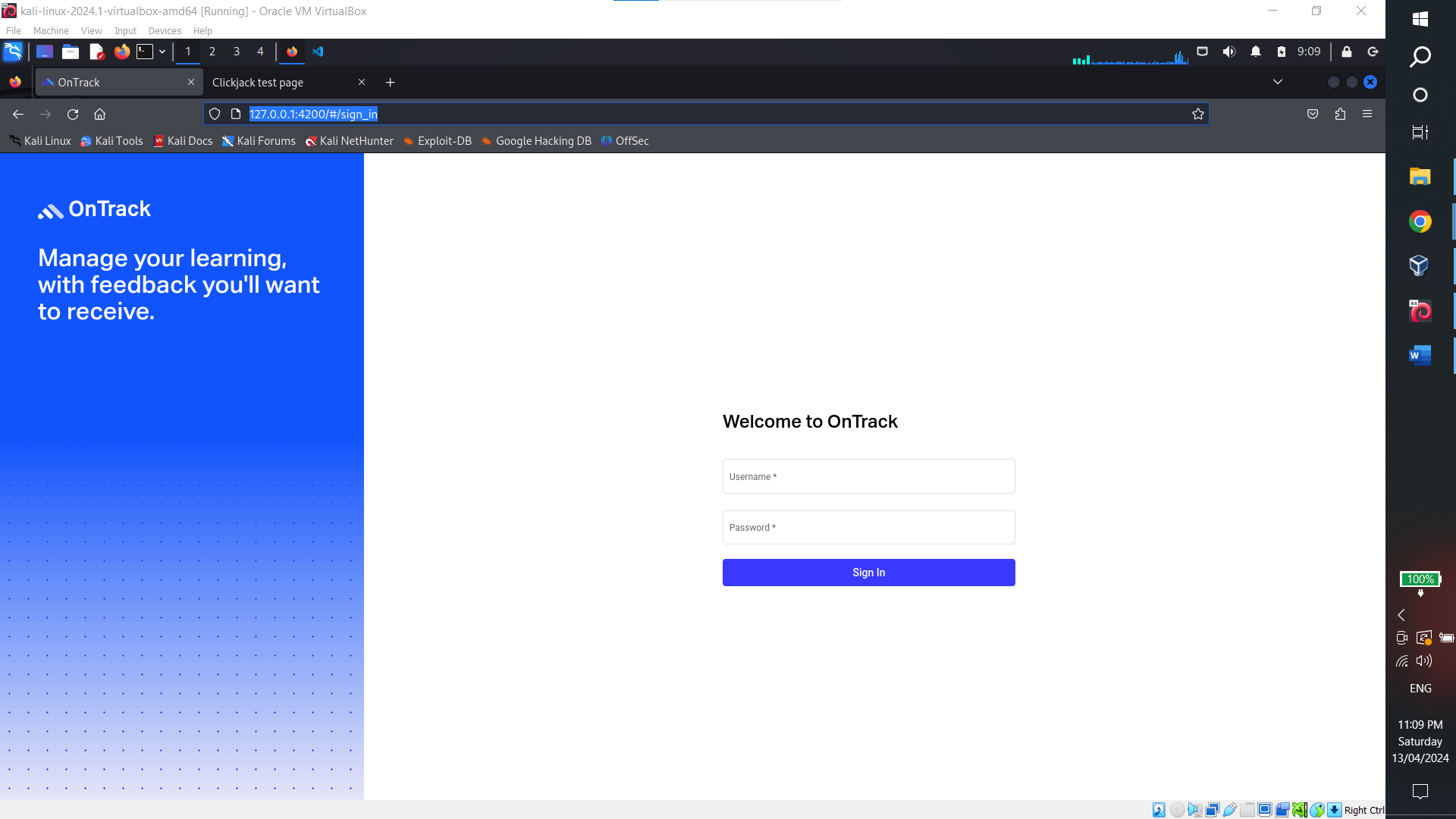
The following URLs are impacted:

* localhost:4200 (main application).

**Evidence**

Provide a step by step guide on how to reproduce the vulnerability with screenshots

**Step 1. Run the main application**

****

**Step 2. Create a webpage that fits the target site in an ifram using the following code**

<html>

<head>

<title>Clickjack test page</title>

</head>

<body>

<iframe src="http://127.0.0.1:4200/#/sign\_in" width="1500" height="1500"></iframe>

</body>

</html>

**Step 3. When you run the page the website will load on the page within the iframe and you can continue to login and operate as normal from with the frame which shows it is vulnerable to clickjacking**

**A screenshot of a computer

Description automatically generated**

**Remediation Advice**

Frame Busting and the "X-FRAME-OPTIONS" header are two common client-side methods used to protect web pages from clickjacking. Frame Busting involves embedding a script in each page to prevent it from functioning when loaded inside a frame, while the "X-FRAME-OPTIONS" header is sent from the server on HTTP responses to mark pages that shouldn't be framed. This header can have values like DENY or ALLOW-FROM origin.

**References**

<https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/11-Client_Side_Testing/09-Testing_for_Clickjacking>

<https://www.pingidentity.com/en/resources/cybersecurity-fundamentals/threats/clickjacking.html>

**Tools Used is OWASP ZAP For Web application Crawling**

**Contact Details**

Roocha Thakkar

[s222037199@deakin.edu.au](mailto:s222037199@deakin.edu.au)

**Pentest Leader Feedback.**

The lead will provide feedback to enact on