

**Finding Name: Frameable response (potential clickjacking)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Mohnish Sharma | PT | Senior Team Member | Ontrack |  |  |
|  |  |  |  |  |  |

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

**Finding Description**

**Frameable response (potential clickjacking)**

**Risk Rating**  
Impact: Significant  
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. |

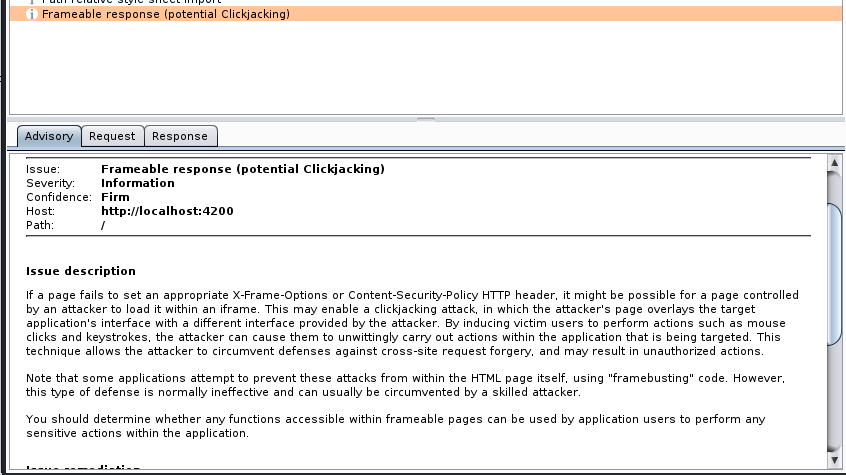
**Business Impact**

* **Data Integrity and Confidentiality: Without appropriate protection against clickjacking, sensitive data within the application may be compromised. This could include customer information, financial data, or proprietary business information. Maintaining the integrity and confidentiality of this data is crucial for compliance, customer trust, and competitive advantage.**
* **Brand Reputation: A successful clickjacking attack could result in unauthorized actions being carried out within the application, potentially damaging the reputation of the business. If customers perceive the application as insecure or untrustworthy, they may lose confidence in the brand, leading to decreased usage, customer churn, and negative publicity.**
* **Legal and Regulatory Compliance: Depending on the nature of the application and the industry it operates in, there may be legal and regulatory requirements regarding the protection of user data and prevention of unauthorized access. Failure to implement adequate safeguards against clickjacking could lead to non-compliance penalties, fines, legal actions, and reputational damage.**

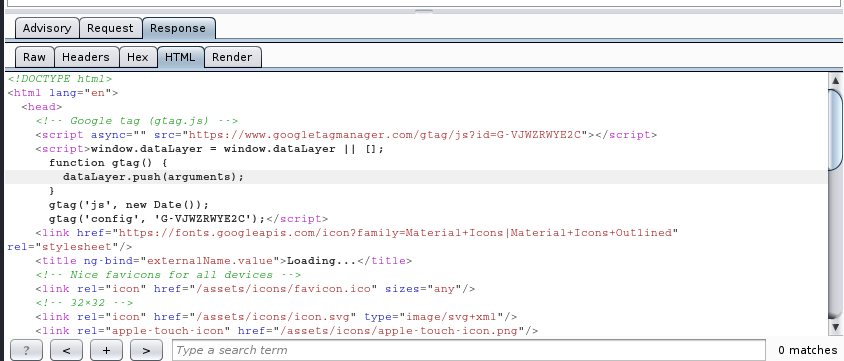
**Affected Assets**

* **User Accounts and Credentials: Clickjacking could allow attackers to manipulate user interactions within the application, potentially leading to unauthorized access to user accounts and credentials. This could result in identity theft, financial fraud, or unauthorized access to sensitive information stored within user accounts.**
* **Transaction Processing: Applications that involve financial transactions or sensitive operations could be affected by clickjacking. Attackers could manipulate user actions to carry out unauthorized transactions, modify transaction details, or compromise the integrity of the transaction process, leading to financial loss and reputational damage.**
* **Application Functionality: Clickjacking attacks can also impact the functionality of the application itself. By overlaying a malicious interface, attackers could manipulate how users interact with the application, potentially causing disruptions, errors, or unintended consequences. This could affect user experience, productivity, and overall satisfaction with the application.**

**Evidence**



****

****

**As we can see the absence of the X-Frame-Options or Content-Security-Policy HTTP headers is there, which should be set in the HTTP response to prevent clickjacking attacks.**

**Remediation Advice**

**To effectively prevent framing attacks, the application should return a response header with the name X-Frame-Options and the value DENY to prevent framing altogether, or the value SAMEORIGIN to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.**

**References**

**https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options**

**Contact Details**

Name: Mohnish Sharma

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.