

**Finding Name:** Unencrypted Communications.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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**

Input returned in response (reflected)

The value of the URL path filename is copied into the application's response.

**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. |

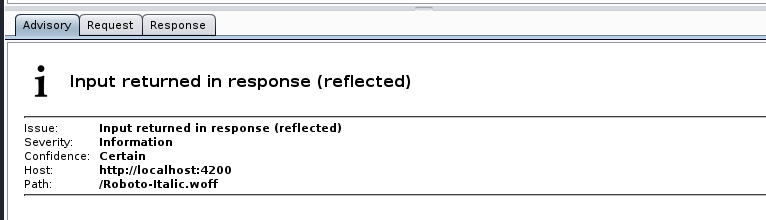
**Business Impact**

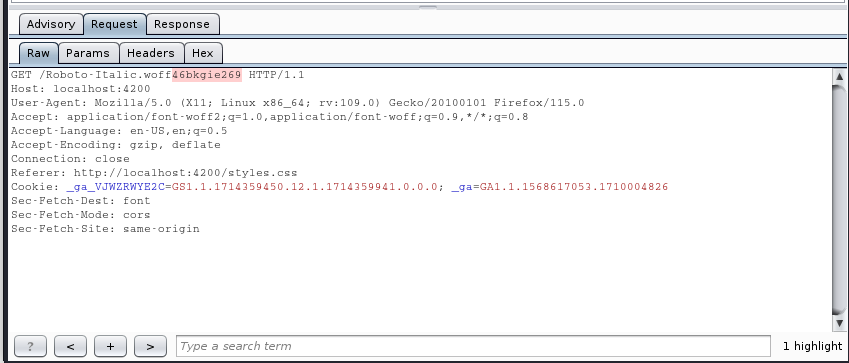
1. **Brand Reputation: If input reflected in the response is manipulated by attackers to display inappropriate, offensive, or misleading content, it could damage the reputation of the business. Users may lose trust in the brand, leading to decreased customer loyalty, negative publicity, and potential loss of revenue.**
2. **Customer Trust: Insecure handling of input reflected in the response undermines customer trust in the security and reliability of the application. Customers expect their data to be handled securely, and any indication of vulnerabilities may lead to concerns about the safety of their information. This erosion of trust can impact customer retention and acquisition efforts.**
3. **Legal Compliance: Depending on the nature of the content being reflected and the industry regulations, there may be legal implications for failing to adequately protect against vulnerabilities related to reflected input. Non-compliance with data protection laws or industry standards could result in fines, legal actions, and damage to the business's reputation.**

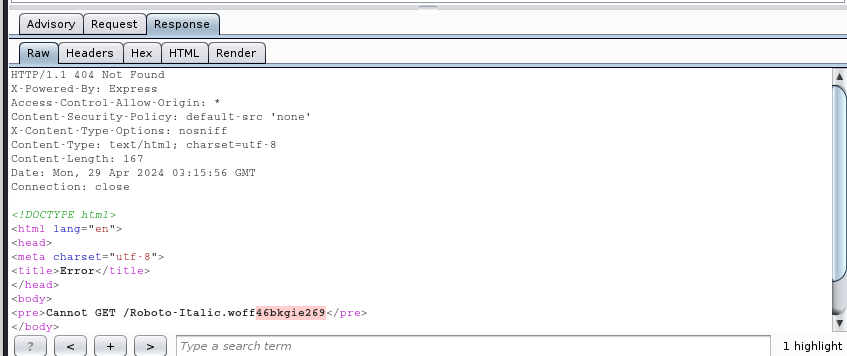
**Affected Assets**

1. **User Data: Input reflected in the response could include sensitive user data, such as usernames, email addresses, or personal information. If attackers manipulate this input, they could expose sensitive user data to unauthorized parties, leading to privacy breaches, identity theft, and financial fraud.**
2. **Application Integrity: Manipulating input reflected in the response could also impact the integrity of the application itself. Attackers may inject malicious code or scripts into the response, leading to various security issues such as cross-site scripting (XSS) attacks, session hijacking, or malware distribution. This compromises the reliability and functionality of the application.**
3. **User Experience: If input reflected in the response is manipulated to display misleading or deceptive content, it could negatively affect the user experience. Users may be tricked into clicking on malicious links, submitting sensitive information to unauthorized parties, or engaging in actions that compromise their security. This can lead to frustration, loss of confidence in the application, and ultimately, reduced user engagement.**

**Evidence**

****

****

****

**Remediation Advice**

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

Input being returned in application responses is not a vulnerability in its own right. However, it is a prerequisite for many client-side vulnerabilities, including cross-site scripting, open redirection, content spoofing, and response header injection. Additionally, some server-side vulnerabilities such as SQL injection are often easier to identify and exploit when input is returned in responses. In applications where input retrieval is rare and the environment is resistant to automated testing (for example, due to a web application firewall), it might be worth subjecting instances of it to focused manual testing.

**References**

[**https://cwe.mitre.org/data/definitions/20.html**](https://cwe.mitre.org/data/definitions/20.html)

[**https://cwe.mitre.org/data/definitions/116.html**](https://cwe.mitre.org/data/definitions/116.html)

**Contact Details**

Name: Mohnish Sharma

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.