A close up of a dragon's face

Description automatically generated

**Finding Name: Cross site scripting**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Dev Patel | PT | Team member | EchoNet |  |  |
|  |  |  |  |  |  |

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

**Finding Description**

A stored Cross-Site Scripting (XSS) vulnerability was discovered in the application, specifically affecting the [Conservation request change]. This vulnerability occurs when user input is not properly sanitized and is subsequently rendered on the admin side without adequate validation or encoding. This allows an attacker to inject malicious JavaScript code into the application, which is then executed in the context of an authenticated admin user's browser session

**Risk Rating**  
Impact: Major  
Likelihood: High

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

Because of lack of proper encoding of output data/values, XSS attack is possible. This can lead to numerous client-side attacks including attempts to hijack a session or steal sensitive client-side data.

**Affected Assets**

Identify assets that are affected by this vulnerability.

**Evidence**

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

A screenshot of a computer

Description automatically generated

**Remediation Advice**

The application should have proper output encoding to avoid XSS injection attacks. The output encoding should be used consistently across all outputs to the client.

**References**

Burp-suite

**Contact Details**

DEV PATEL: - s222622553@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on