

Authenticated Cross Site Scripting (XSS) Vulnerability

Summary:

Vulnerable Endpoint:

Platform management > Edit Pages

Vulnerable Parameter:

Editor

Description:

A Stored Cross-Site Scripting (Stored XSS) vulnerability has been identified in the web application's "Edit pages" page. This vulnerability allows an attacker to inject malicious scripts into web pages that are stored on the server and later served to other users. When these malicious scripts are executed in the context of a user's browser, they can lead to data theft, session hijacking, defacement, and other malicious activities.

There are some protections in place that do not allow `<script>` tags, however these are bypassed by using the syntax found in the attack path. `<audio src/onerror=alert(1)>` is an example, but there are others that bypass the filter.

Mitigation:

- Implement strict input validation and sanitization to ensure that any user-supplied data does not contain malicious scripts. This can be done using libraries or frameworks that automatically escape or filter input.

References:

- <https://portswigger.net/web-security/cross-site-scripting>
- <https://owasp.org/www-community/attacks/xss/>

Attack Path:

Editing pages in Platform management > Edit pages allows Cross Site Scripting. The following payload works and displays an error.

```
<audio src/onerror=alert(document.cookie)>
```

The screenshot shows the 'Administration > Edit pages' interface. At the top, there's a header with a hamburger menu and the text 'Administration > Edit pages'. Below this is a section 'Choose page to edit' with a dropdown menu showing 'XSS Test'. To the right of the dropdown are several icons: a plus sign, a floppy disk, a trash can, a pencil, a circular arrow, a hamburger menu, and an eye. The main area is split into two panels: 'Editor' on the left and 'Preview' on the right. The 'Editor' panel contains a text area with the payload `<audio src/onerror=alert(document.cookie)> |`. The 'Preview' panel is currently empty. At the bottom of the interface, a dark grey notification box is displayed. It contains a globe icon followed by the text '192.168.230.128:8080', and below that, 'XSRF-TOKEN=7e4e8d16-a7b7-4ea8-b4c7-b05540789c49'. An 'OK' button is located in the bottom right corner of the notification box.

Administration > Edit pages

Choose page to edit
XSS Test

Editor

```
<audio src/onerror=alert(document.cookie)> |
```

Preview

192.168.230.128:8080
XSRF-TOKEN=7e4e8d16-a7b7-4ea8-b4c7-b05540789c49
OK