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)>
```