

# Forum:[Hack Forums](#)

Thread: [Managed to find a XSS vulnerable site. Now what?](#)

**randomUsername25214** - May 12, 2018, 9:49 am

So i managed to find a vulnerable site where it forgets to filter one of the variables and just echos it out. I have managed to make a simple alert but when i try to enter php code to add malicious code it just gets commenred out. Anyway of getting around this?

**Nexuslol** - May 12, 2018, 11:19 am

It'd help if you gave us some more information. Is it stored XSS or reflected? What kind of methods did you use to bypass the filters, if there are any in the first place?

**randomUsername25214** - May 12, 2018, 11:57 am

(May 12, 2018 11:19 AM)Nexuslol Wrote: [\[CITE\]](#) It'd help if you gave us some more information. Is it stored XSS or reflected? What kind of methods did you use to bypass the filters, if there are any in the first place?

I did not bypass any filter since it does not appear to have any. I do not know what you mean whit stored/reflective. I do beluve you would call if reflective since it does not store the info like in a comment.

**UnhealthyCharger** - May 12, 2018, 12:01 pm

(May 12, 2018 09:49 AM)KA34 Wrote: [\[CITE\]](#) but when i try to enter php code to add malicious code it just gets commenred out. Anyway of getting around this?

That is because XSS is used for client-side attacks and php is server side language, meaning you are executing code in browser of whoever visits affected website, not on server where website is hosted.

**randomUsername25214** - May 12, 2018, 1:39 pm

(May 12, 2018 12:01 PM)UnhealthyCharger Wrote: [\[CITE\]](#) That is because XSS is used for client-side attacks and php is server side language, meaning you are executing code in browser of whoever visits affected website, not on server where website is hosted.

So a XSS attack can never be used as long as nobody exept you sees it?

**0xB9** - May 13, 2018, 8:45 pm

(May 12, 2018 01:39 PM)KA34 Wrote: [\[CITE\]](#) So a XSS attack can never be used as long as nobody exept you sees it?

Depends if it's stored or reflected, if it's stored anyone who visits that page will automatically see the pop-up alert when visiting since the script would be stored in the sites code. But if it's just a reflected then you will need to craft the URL and send it to the victim, that way when they click the link they will be alerted with the pop-up basically reflecting what you see.