

Forum:[Hack Forums](#)

Thread: [How to check whether a site is vulnerable to XSS attack or not?](#)

GetASyncKeyState() - January 24, 2018, 2:01 am

Can someone recommend me a good way to do so?

I already have a good knowledge about SQL Injections , so I'm not definitely a noob when talking about web exploiting.

Thanks for your answers in advance.

Baud - January 24, 2018, 11:17 am

(Jan 24, 2018 03:01 AM)blurrybot Wrote: [\[CITE\]](#) I already have a good knowledge about SQL Injections , so I'm not definitely a noob when talking about web exploiting.

If all you know about web exploiting is SQL injection then yes, I'd say you're still a noob, there's so much more to this subject than SQL injection and XSS. But anyways... to test for XSS you have to inject JavaScript code inside input textboxes on a webpage, say for example a search box or a comment form. The most commonly used script to test it is something like this: (had to tweak it because of HF's firewall, change the double quotes into < and >)

Code "script>alert("Hello world!");"/script"

If when you press enter or submit the form a popup window appears, the input field you tested is vulnerable to XSS. Remember that a website can still be vulnerable even if at a first glance nothing appears, because it might be implementing a WAF (Web Application Firewall) which is blocking certain characters or strings, so in that case you will have to edit the script to bypass the WAF rules. If you wish to learn more about XSS, and I certainly hope so:

[https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

GetASyncKeyState() - January 24, 2018, 11:29 am

Thank you for your help.

Can you recommend me other web-exploiting techniques to learn more about besides XSS?

I'd like to become good in this field!

Baud - January 24, 2018, 12:03 pm

LFI, RFI, CSRF, SSI injection, directory traversal, path disclosure, just to name a few. Make sure you also study web-based programming languages like PHP, JavaScript, and all the likes because you need to understand how a vulnerability works before exploiting it. A good reference book you can read is The Web Application' Hacker's Handbook.

GetASyncKeyState() - January 24, 2018, 1:42 pm

Thank you so much for your help.

I started learning about XSS now.