

Forum:[Hack Forums](#)

Thread: [Good XSS or SQL Bruteforce tool](#)

ernestmiller - January 3, 2018, 11:13 am

Anyone with any good suggestions??

CryptixHacking - January 3, 2018, 2:41 pm

(Jan 3, 2018 12:13 PM)ernestmiller Wrote: [\[CITE\]](#) Anyone with any good suggestions??
<http://sqlmap.org>

Is usually known as the best or one of the best software for this.

Works on all OS's and has easy command line access.

Also its python language allows you to easily add to the programs features or create custom plugins.

Now cant say it uses any XSS as cross site scripting isnt of much value on most sites anymore as they have many features in place now on most sites to block such script injection.

For XSS your probably better off going with
<https://xsser.03c8.net/>

Which is also coded in python and supports Tor proxy.

_____ - January 3, 2018, 2:43 pm

Use Kali Linux. It has loads of these types of programs installed under relevant headings

CryptixHacking - January 3, 2018, 2:45 pm

(Jan 3, 2018 03:43 PM)_____ Wrote: [\[CITE\]](#) Use Kali Linux. It has loads of these types of programs installed under relevant headings

Kali linux isnt required but yes it is a linux distro created to have many of these tools pre-installed.

ernestmiller - January 4, 2018, 2:38 am

That is half the fun though trying to bypass it, if its browser based protection for example just need to use another browser

I run Kali have all these tools built in already

[BLANK] - January 5, 2018, 9:51 am

Just use ZAP, it will scan an entire site for you and tell you if there is a common XSS or SQL issue. Then from there you can use other tools or manual methods of exploitation. Or use Burpsuite, scan the target, and test each parameter manually. There are also browser plugins that will test for xss. Lots of free tools out there.

ernestmiller - January 7, 2018, 3:14 am

Is ZAP a reliable scanner then it seems to be more reliable than Vega it does not pick up on strange

XSS and SQL that does not exist I have Kali but never actually used it before

javinzplayer - *January 7, 2018, 10:34 am*

Havij is a advanced SQL Database Tool. It is really good to find DBs that are vuln to SQL Injection. But good luck finding a clean version because nearly all of them are infected.

ernestmiller - *January 8, 2018, 8:26 am*

I read you can use Havij with Wine on Linux does anyone have a download of it that is not completely corrupted