

Forum:[Hack Forums](#)

Thread: [XSS vulnerabilities without dorks](#)

cybertoto - February 25, 2014, 11:28 am

Hello all

I want to know how to find XSS vulnerabilities without dork?

thanks a lot

tux1 - February 25, 2014, 11:40 am

It's not hard. In my experience most sites that have a search bar are vulnerable to xss. The site owners either don't understand xss or just don't care, probably a bit of both.

But any just find a site with a search bar and start seeing what you can input into it. Also look for other ways you can get the server to output your input.

cybertoto - February 27, 2014, 9:49 am

thanks mate for info :D a lot of web site have a search bar lol :D

Terry A. Davis - February 27, 2014, 10:18 am

(Feb 25, 2014 12:40 PM)tux1 Wrote: [\[CITE\]](#) It's not hard. In my experience most sites that have a search bar are vulnerable to xss. The site owners either don't understand xss or just don't care, probably a bit of both.

But any just find a site with a search bar and start seeing what you can input into it. Also look for other ways you can get the server to output your input.

So much this.

I can go to anysite, and if they have a search bar I am bound to check for XSS, hell even certain templateed contact forms have XSS problems in the E-mail feild.

Numinous - February 27, 2014, 10:19 am

DOMINOS - One Year OLD XSS

<http://www.dominos.co.in/blog/?s=\x3c\x2f\x74\x69\x74\x6c\x65\x3e\x3c\x73\x63\x72\x69\x70\x74\x3e\x61\x6c\x65\x72\x74\x28\x64\x6f\x63\x75\x6d\x65\x6e\x74\x2e\x64\x6f\x6d\x61\x69\x6e\x29\x3c\x2f\x73\x63\x72\x69\x70\x74\x3e>

HERE YOU GO :)