

Forum:[Hack Forums](#)

Thread: [Some XSS Dorks](#)

nondescriptoldie - November 25, 2014, 11:56 am

Hello HF members! Here I have some XSS Dorks for you guys! ;)

Code inurl:search.php?

inurl:find.php?

inurl:search.html

inurl:find.html

inurl:search.aspx

inurl:find.aspx

inurl:".php?cmd="

inurl:".php?z="

inurl:".php?q="

inurl:".php?search="

inurl:".php?query="

inurl:".php?searchstring="

inurl:".php?keyword="

inurl:".php?file="

inurl:".php?years="

inurl:".php?txt="

inurl:".php?tag="

inurl:".php?max="

inurl:".php?from="

inurl:".php?author="

inurl:".php?pass="

inurl:".php?feedback="

inurl:".php?mail="

inurl:".php?cat="

inurl:".php?vote="

inurl:search.php?q=

inurl:com_feedpostold/feedpost.php?url=

inurl:scrapbook.php?id=

inurl:headersearch.php?sid=

inurl:/poll/default.asp?catid=

inurl:/search_results.php?search=

Hope I helps some of you guys out! :)

la couille - November 25, 2014, 11:57 am

thanks you very much for this list :)

FI0urite - November 25, 2014, 11:58 am

You forgot guestbook, also, these look like they are only temporary XSS, anyway, thanks.

? ??s†??ß?? ? - November 25, 2014, 11:59 am

Great thread Darkcoreiscool,

This is a really helpful thread for all members! ?

?Smurf - November 25, 2014, 12:02 pm

Thank you for the list, very helpful indeed :)

nondescriptoldie - November 25, 2014, 12:30 pm

Thanks guys for your appreciation! :)

ExplodingKnees - November 25, 2014, 12:45 pm

They're completely pointless and you're wasiting your time.

Dr. Gonzo - November 25, 2014, 2:19 pm

Do you think that these would also work as SQLI dorks or no? Just wondering.

?Criminal - November 26, 2014, 6:37 am

(Nov 25, 2014 01:45 PM)ExplodingKnees Wrote: [\[CITE\]](#) They're completely pointless and you're wasiting your time.

holy shit I can't tell if you're trolling you can:

- send any GET/POST request on victims behalf just like a CSRF vuln except xss can parse CSRF tokens and make token protection for CSRF useless
- steal cookies(not as useful because most sites set the HTTPONLY flag which prevents cookie stealing nowadays)
- parse any javascript on a page which is useful for stealing facebook chat logs if you had a

facebook xss for example

- turn on victims webcam
 - geolocation to get someones exact address for a dox
- and many more fun things

dude I pwned a vbulletin site with a reflected XSS one time, coded a payload that priv escalated my self to the admin panel, sqli'ed a vuln parameter on one of the admin endpoints and the site got owned, you'd be suprised man.

ExplodingKnees - November 26, 2014, 7:44 am

(Nov 26, 2014 07:37 AM)maybeBlue Wrote: [\[CITE\]](#) holy shit I can't tell if you're trolling you can:

- send any GET/POST request on victims behalf just like a CSRF vuln except xss can parse CSRF tokens and make token protection for CSRF useless

- steal cookies(not as useful because most sites set the HTTPONLY flag which prevents cookie stealing nowadays)

- parse any javascript on a page which is useful for stealing facebook chat logs if you had a facebook xss for example

- turn on victims webcam

- geolocation to get someones exact address for a dox

and many more fun things

dude I pwned a vbulletin site with a reflected XSS one time, coded a payload that priv escalated my self to the admin panel, sqli'ed a vuln parameter on one of the admin endpoints and the site got owned, you'd be suprised man.I find the difference between your technical knowledge and your comprehension skills amusing. I never once stated XSS(Reflected, DOM, any other kind) is useless. XSS Dorks are. XSS is more of a subtle attack that aims towards being useful against clients of a website; dorking out random targets for websites nobody heard about is redundant. Targeting high-profile websites, mapping them out and delicately finding XSS holes is a different story. This thread is not how you exploit XSS.

?Criminal - November 26, 2014, 8:50 am

(Nov 26, 2014 08:44 AM)ExplodingKnees Wrote: [\[CITE\]](#) I find the difference between your technical knowledge and your comprehension skills amusing. I never once stated XSS(Reflected, DOM, any other kind) is useless. XSS Dorks are. XSS is more of a subtle attack that aims towards being useful against clients of a website; dorking out random targets for websites nobody heard about is redundant. Targeting high-profile websites, mapping them out and delicately finding XSS holes is a different story. This thread is not how you exploit XSS.

Oh lol I thought you meant XSS in general is useless you should of been more specific also XSS doesn't even need dorks OP is another retard who must be new to sqli pretty much any site that uses javascript with no input validation has an xss vuln somewhere there like so easy to find.

ExplodingKnees - November 26, 2014, 9:05 am

(Nov 26, 2014 09:50 AM)maybeBlue Wrote: [\[CITE\]](#) Oh lol I thought you meant XSS in general is useless you should of been more specific also XSS doesn't even need dorks OP is another retard who must be new to sqli pretty much any site that uses javascript with no input validation has an xss vuln somewhere there like so easy to find.I said: "They're"

They're = Plural. Thread title: XSS Dorks. I guess I could've been more clear, but that goes the same towards you.