

Forum:[Hack Forums](#)

Thread: [dorks for code injection XSS](#)

famedgod6 - September 12, 2024, 4:20 pm

does anyone have any google dorks to find website that will be vulnerable to URL XSS?

to find websites that I can potentially put Malicious code into the URL of a website?

#AfterDark - September 12, 2024, 4:49 pm

Please do some more research on reflected xss and persistent xss.

XSS is most common in form fields such as search fields and submission boxes. So to answer your question. Look for google dorks that target submission forms/ search forms ;)

eddie_1600 - September 12, 2024, 9:27 pm

Site metatags have no correlation to how input is processed on the backend, so to answer your question: what you're looking for doesn't exist.

famedgod6 - September 13, 2024, 2:31 pm

(Sep 12, 2024 09:27 PM)eddie_1600 Wrote: [\[CITE\]](#) Site metatags have no correlation to how input is processed on the backend, so to answer your question: what you're looking for doesn't exist.

URL XSS is like the most basic XSS that exists, in literally every tutorial that exists, it shows malicious code being put into the URL bar, and I have done it before

It exists because I have done it, here is a website I defaced by entering HTML code into a URL string: <https://tinyurl.com/lulzy86768>

so it clearly does

eddie_1600 - September 15, 2024, 12:49 pm

(Sep 13, 2024 02:31 PM)famedgod6 Wrote: [\[CITE\]](#) URL XSS is like the most basic XSS that exists, in literally every tutorial that exists, it shows malicious code being put into the URL bar, and I have done it before

It exists because I have done it, here is a website I defaced by entering HTML code into a URL string: <https://tinyurl.com/lulzy86768>

so it clearly does

Yes you're not wrong, but Google dorking is simply a tool which allows you to sort/filter search results using metadata about particular sites (domain name, metatags, body content, etc). But none of this information can be used to guess how input is processed on the backend or whether there is an XSS exploit, unless you are looking for some certain instances of web applications which have a known vulnerability. But it's unlikely you will find something this way which hasn't already been touched by the troves of newbs looking to prove themselves

hackermenace247 - September 16, 2024, 10:57 pm

(Sep 12, 2024 04:20 PM)famedgod6 Wrote: [\[CITE\]](#) does anyone have any google dorks to find website that will be vulnerable to URL XSS?

to find websites that I can potentially put Malicious code into the URL of a website?

Normally I use exploit-db.com on Google cause you can search for Google ddorks and find exploit details like how to reconstruct the attack and the type of vulnerability it has. So have fun but remember its www.exploit-db.com

AmadeusHF - September 17, 2024, 7:43 am

you can find a lot of working dorks in github pages

bbbbbbbfbfbfbbb - September 18, 2024, 7:57 pm

No point in responding if you don't know what you're talking about...

portswigger.net/research/exploiting-xss-in-hidden-inputs-and-meta-tags

[deleted] [warn]

Leeriz - September 20, 2024, 8:39 am

(Sep 13, 2024 02:31 PM)famedgod6 Wrote: [\[CITE\]](#) URL XSS is like the most basic XSS that exists, in literally every tutorial that exists, it shows malicious code being put into the URL bar, and I have done it before

It exists because I have done it, here is a website I defaced by entering HTML code into a URL string: <https://tinyurl.com/lulzy86768>

so it clearly does

can you say please how to use xss to deface the website entirely

mariomotva - November 28, 2024, 11:12 am

I buy a geolocation tool for cell phones.

[/quote]

private messages

Chorozon - November 29, 2024, 9:21 pm

(Sep 12, 2024 04:20 PM)famedgod6 Wrote: [\[CITE\]](#) does anyone have any google dorks to find website that will be vulnerable to URL XSS?

to find websites that I can potentially put Malicious code into the URL of a website?

Use something like subfinder (github.com/projectdiscovery/subfinder)

Scan the site and list the subdomains and use something like XSSStrike or Subzy to scan the sites for XSS vulns