

# Forum:[Hack Forums](#)

Thread: [SQLMAP-Gettin Blocked](#)

**cloudz4me** - September 26, 2020, 10:24 pm

any suggestion not getting blocked again?

```
sqlmap.py -u "http://website.com" --no-cast --batch --level 5 --risk 3 --technique E --dbs -risk 3 -level 5 -tamper space2comment,randomcase,between -drop-set-cookie
```

<https://prnt.sc/uolhph>

**INBA** - September 26, 2020, 11:59 pm

install and use it with --tor , probable the IP get blocked

**cloudz4me** - September 27, 2020, 1:17 am

(Sep 26, 2020 11:59 PM)INBA Wrote: [\[CITE\]](#) install and use it with --tor , probable the IP get blocked ok thanks but theirs another problem a captcha before login.

**INBA** - September 27, 2020, 1:18 am

try optain the host real IP with different methode and put in sqlmap the direct link (with the IP)

**SUDOCODES** - September 27, 2020, 9:08 am

you will most likely get a captcha if you use a service like tor because all tor exist nodes are know. Rather use socks proxy or a VPN, you have better chances of it not asking for a captcha.

**cloudz4me** - September 27, 2020, 9:19 am

(Sep 27, 2020 09:08 AM)SUDOCODES Wrote: [\[CITE\]](#) you will most likely get a captcha if you use a service like tor because all tor exist nodes are know.

Rather use socks proxy or a VPN, you have better chances of it not asking for a captcha. captcha makes this difficult it wont intercept even burpsuite.

<http://prntscr.com/uot5gy>

anyone how to bypass this captcha?

**linkinpork** - October 6, 2020, 12:36 am

(Sep 26, 2020 10:24 PM)cloudz4me Wrote: [\[CITE\]](#) any suggestion not getting blocked again?

Hope I'm not too late for the party.

You need to make your requests as normal as possible. Start with a "normal" user agent like Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/79.0, then make sure your requests are delayed in such a way that you seem like you're just browsing the website normally.

The --risk argument also sends more "abnormal" requests, and in my experience ends up giving me more false positives.

Finally in my work it's very rare I find an SQLi vector in the URL. Best you intercept and inject in the POST data.

Have fun.

**cloudz4me** - October 6, 2020, 4:39 am

(Oct 6, 2020 12:36 AM)linkinpork Wrote: [CITE](#) Hope I'm not too late for the party.

You need to make your requests as normal as possible. Start with a "normal" user agent like Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/79.0, then make sure your requests are delayed in such a way that you seem like you're just browsing the website normally.

The --risk argument also sends more "abnormal" requests, and in my experience ends up giving me more false positives.

Finally in my work it's very rare I find an SQLi vector in the URL. Best you intercept and inject in the POST data.

Have fun.

thanks sent you some pm

**niqscann** - October 11, 2020, 3:01 am

i think nothing to do with that.

catchpa bypass is hard.

i even tried with browser than copied made a file to work with sqlmap , exactly same infos as browser and again catchpa appeared