

Forum:[Hack Forums](#)

Thread: [\[Tutorial\]Cloudflare Bypass](#)

fLQZ - August 16, 2015, 6:08 am

Hey Guys,
today I am going to show you how to bypass the cloudflare protection.

Target: tv.com.pk

Step 1:

Paste your target URL at the end of this URL to get the real IP:

ht tp://api.predator.wtf/cfresolve/?arguments=YOURTARGET
(without http and www)

Example:

ht tp://api.predator.wtf/cfresolve/?arguments=tv.com.pk

Now you will see the real IP.

Step 2:

Open c:\windows\system32\drivers\etc\ and edit the "hosts" file.

Like this:

.
.

127.0.0.1 localhost

173.192.32.248 tv.com.pk

Notice: This will not work on every Website

Krew - August 16, 2015, 6:12 am

This Domain Is Not Vulnerable To Our Method!

Luckily mine isn't.

fLQZ - August 16, 2015, 6:15 am

Quote:This Domain Is Not Vulnerable To Our Method!

Luckily mine isn't.

Yeah like I said not every website is vulnerable, but did you check your website without http and www?

Krew - August 16, 2015, 6:47 am

(Aug 16, 2015 06:15 AM)fLQZ Wrote: [\[CITE\]](#) Yeah like I said not every website is vulnerable, but did you check your website without http and www?

Yep. Should be 100% safe. ?

SIM-2223238 - August 16, 2015, 6:49 am

Wow 90% of the websites does not work, try again later.

n000b

fLQZ - August 16, 2015, 7:06 am

(Aug 16, 2015 06:49 AM)Aggron Wrote: [\[CITE\]](#) Wow 90% of the websites does not work, try again later.

n000b

Not 90% I actually found a lot, and I did say that it does not work all the time

BassheadHF - August 16, 2015, 12:28 pm

Wow Great share man thanks for this!! =)

UnKnOwN333 - August 16, 2015, 7:26 pm

Its work with my domain :D thnx bro :P its cool keep up

Aur3xis - August 16, 2015, 7:31 pm

Well, this works sometimes...

Actually like 5%~ of the times unfortunately.

beachkid - August 16, 2015, 7:41 pm

works for mylol.com mwahahaha XD

Buried Alive - August 17, 2015, 1:43 pm

Explain a bit more

i get this

```
aspmx.l.google.com => 74.125.20.26
alt2.aspmx.l.google.com => 173.194.206.26
alt1.aspmx.l.google.com => 173.194.193.26
aspmx3.googlemail.com => 173.194.206.27
aspmx2.googlemail.com => 173.194.193.27
```

and what does step 2 do ?

fLQZ - August 17, 2015, 2:21 pm

(Aug 17, 2015 01:43 PM)Buried Alive Wrote: [\[CITE\]](#) Explain a bit more

i get this

```
aspmx.l.google.com => 74.125.20.26
alt2.aspmx.l.google.com => 173.194.206.26
alt1.aspmx.l.google.com => 173.194.193.26
aspmx3.googlemail.com => 173.194.206.27
aspmx2.googlemail.com => 173.194.193.27
```

and what does step 2 do ?

If you get this, your website isn't vulnerable. This are just some subserver.

Step 2 makes that you can access the website without cloudflare even if you type the hostname so you do not have to type the IP manually

Learner Boy - August 18, 2015, 10:58 am

This Domain Is Not Vulnerable To Our Method!

Bad Luck

Anyways

Thanks for this

Th3PonyWizard - August 18, 2015, 11:23 am

I don't get how the hosts file is related. Explain.

fLQZ - August 18, 2015, 11:39 am

(Aug 18, 2015 11:23 AM)Th3PonyWizard Wrote: [\[CITE\]](#) I don't get how the hosts file is related. Explain.

You do not need to do the step with the host file. It just makes it easier for you so if you do the step you can write the hostname and you connect to the unprotected IP

FFY00 - August 19, 2015, 2:38 pm

.-. It is easy to do but is more easy to access the website in the browser to generate the cookies, then use these cookies in the HTTP request on the exploit.

(Aug 18, 2015 11:23 AM)Th3PonyWizard Wrote: [\[CITE\]](#) I don't get how the hosts file is related. Explain.

When u access a domain it will connect with the ns servers to resolve the dns, the hosts file is used to bypass it, if u set a specific ip for a domain it wouldn't resolve the domain in the dns server, the computer will use the ip address specified in that file.

fLQZ - August 19, 2015, 2:42 pm

(Aug 19, 2015 02:38 PM)FFY00 Wrote: [\[CITE\]](#) .-. It is easy to do but is more easy to access the website in the browser to generate the cookies, then use these cookies in the HTTP request on the exploit.

Yeah but I wanted to show this way

FFY00 - August 19, 2015, 2:50 pm

(Aug 19, 2015 02:42 PM)fLQZ Wrote: [\[CITE\]](#) Yeah but I wanted to show this way

So ol, xD but my method is more easy and just few people use it. I posted because very few websites can't be resolved and my method will work on those cases...

Th3PonyWizard - August 19, 2015, 3:05 pm

(Aug 19, 2015 02:38 PM)FFY00 Wrote: [\[CITE\]](#) .-. It is easy to do but is more easy to access the website in the browser to generate the cookies, then use these cookies in the HTTP request on the exploit.

When u access a domain it will connect with the ns servers to resolve the dns, the hosts file is used to bypass it, if u set a specific ip for a domain it wouldn't resolve the domain in the dns server, the computer will use the ip address specified in that file. I still don't get it. Your job is to get that IP address in the first place. What's the point accessing the domain from your computer if your whole point is to get the IP to further attack it? If you already have the IP to put in the hosts file, you've already bypassed CF.

FFY00 - August 19, 2015, 11:56 pm

(Aug 19, 2015 03:05 PM)Th3PonyWizard Wrote: [\[CITE\]](#) I still don't get it. Your job is to get that IP address in the first place. What's the point accessing the domain from your computer if your whole point is to get the IP to further attack it? If you already have the IP to put in the hosts file, you've already bypassed CF.

Yes that's right... If u don't know how to get the real IP directly I can teach u, just PM me...

Th3PonyWizard - August 20, 2015, 2:43 am

(Aug 19, 2015 11:56 PM)FFY00 Wrote: [\[CITE\]](#) Yes that's right... If u don't know how to get the real IP directly I can teach u, just PM me...Oh, for me that's not an issue :3

FFY00 - August 20, 2015, 12:10 pm

(Aug 20, 2015 02:43 AM)Th3PonyWizard Wrote: [\[CITE\]](#) Oh, for me that's not an issue :3
Ok, but if you need help in other thing feel free to PM me, i have a very big knowleadge ?

boribari - August 26, 2015, 11:49 am

works maybe for 10% of websites ..