

Forum:[Hack Forums](#)

Thread: [Testing Site - Cloudflare Origin IP Grabbed - How To Bypass Origin IP Block?](#)

GR305 - July 30, 2020, 8:11 am

I was able to capture the origin IP of a site I'm testing and was wondering if it is possible to use the origin IP that cloudflare uses as the main IP of said website to test for vulnerabilities? It blocks it from being used as an HTTP link.

AeroBotPro - July 30, 2020, 8:34 am

Considering that Cloudflare hosts many sites behind 1 IP, they take measures to make sure this doesn't happen.

You will get Error 1003: Direct IP access not allowed. You need to be redirected from the domain for CF to work properly.

Moving forward:

Check out censys[.]io.

Enter your target's domain (or search in title or text like google) and you will be surprised how many back ends are exposed due to misconfigs when setting up/transferring sites :)

GR305 - July 30, 2020, 6:21 pm

(Jul 30, 2020 08:34 AM)AeroBotPro Wrote: [\[CITE\]](#) Considering that Cloudflare hosts many sites behind 1 IP, they take measures to make sure this doesn't happen.

You will geterror 1003: Direct IP access not allowed. You need to be redirected from the domain for CF to work properly.

Moving forward:

Check out censys[.]io.

Enter your target's domain (or search in title or text like google) and you will be surprised how many back ends are exposed due to misconfigs when setting up/transferring sites :)

Thanks so much for the information! Any place I can learn more about this? I'm currently reading "the web application hackers handbook"

AeroBotPro - August 1, 2020, 8:52 am

(Jul 30, 2020 06:21 PM)GR305 Wrote: [\[CITE\]](#) Thanks so much for the information! Any place I can learn more about this? I'm currently reading "the web application hackers handbook"

Absolutely, glad I could help! I don't have many resources on this, I guess this would be considered a "dorking" technique, for further research's sake ?

KeySender - August 15, 2020, 12:55 pm

<https://www.mycyber.tools/>

niqscann - October 11, 2020, 3:31 am

nmap also works if admin is idiot.

you can chk google for nmap cloudflare bypass commands

NeverMore - October 11, 2020, 5:16 am

if you can Bypass cloudflare WAF , you dont need to get the original IP to hack site,

this is how cloudflare WAF works : <https://www.cloudflare.com/waf/>

and this is some bypassing ways for it :

<https://blog.detectify.com/2019/07/31/bypassing-cloudflare-waf-with-the-origin-server-ip-address/>
<https://medium.com/bugbountywriteup/bypass-cloudflare-waf-to-pwned-application-2c9e4f862319>
<https://enciphers.com/bypassing-cloudflare-waf-to-get-more-vulnerabilities/>

feel free to ask me about anything for bypassing it,

Carb0n - October 26, 2020, 6:37 pm

(Oct 11, 2020 05:16 AM)invo12 Wrote: [\[CITE\]](#) if you can Bypass cloudflare WAF , you dont need to get the original IP to hack site,

this is how cloudflare WAF works : <https://www.cloudflare.com/waf/>

and this is some bypassing ways for it :

<https://blog.detectify.com/2019/07/31/bypassing-cloudflare-waf-with-the-origin-server-ip-address/>
<https://medium.com/bugbountywriteup/bypass-cloudflare-waf-to-pwned-application-2c9e4f862319>
<https://enciphers.com/bypassing-cloudflare-waf-to-get-more-vulnerabilities/>

feel free to ask me about anything for bypassing it,
Well, would you be able to do it?

Phil Swift 47 - October 27, 2020, 12:13 am

(Jul 30, 2020 08:34 AM)AeroBotPro Wrote: [\[CITE\]](#) Considering that Cloudflare hosts many sites behind 1 IP, they take measures to make sure this doesn't happen.

You will get error 1003: Direct IP access not allowed. You need to be redirected from the domain for CF to work properly.

Moving forward:

Check out censys[.]io.

Enter your target's domain (or search in title or text like google) and you will be surprised how many back ends are exposed due to misconfigs when setting up/transferring sites :)

This is true and if one could look at hosting history one may be able to find the host from a date before cloudflare was enabled.... I pulled 3 Websites today that were hosted behind cloudflare however 2-3 years ago the weren't using cloud flare and I found the server.... I also found from whois that one was on namescheap domain services.

A lot of tools.... I may edit this for the direct link to the website.

(Jul 30, 2020 08:11 AM)GR305 Wrote: [\[CITE\]](#) I was able to capture the origin IP of a site I'm testing and was wondering if it is possible to use the origin IP that cloudflare uses as the main IP of said website to test for vulnerabilities? It blocks it from being used as an HTTP link.

Here this a free and paid for service but works amazing, you can pull History of the website's hosting and DNS allowing you to gather some info.... Maybe check some registrar DBs of the non cloud flare domains or sub domains.

<https://securitytrails.com/domain/>

