

# Forum:[Hack Forums](#)

Thread: [Easily bypass Cloudflare protection on any site](#)

m077 - January 9, 2022, 4:54 am

Commonly, web resources are currently using Cloudflare DNS as their WAF. This interferes with penetration testing by blocking certain requests and gives us false information about the actual state of security for the web application.

In this tutorial, I'll show how easy it is to bypass most hosts that are using Cloudflare as their WAF.

So first of all, you'll need to git clone this repository locally:

Code `git clone https://github.com/m0rtem/CloudFail`

Afterwards we execute commands as follows:

Code `cd CloudFail`

`pip3 install -r requirements.txt`

`python3 cloudfail.py -t yourtarget.com`

After a brief amount of time, the resulting output should be something as follows:

Code [14:17:54] Fetching initial information from: yourtarget.com...

[14:17:54] Server IP: 172.x.195.y

[14:17:54] Testing if yourtarget.com is on the Cloudflare network...

[14:17:54] yourtarget.com is part of the Cloudflare network!

[14:17:54] Testing for misconfigured DNS using dnsdumpster...

[14:17:57] [FOUND:HOST] yourtarget.com 104.21.92.146 CLOUDFLARENETunknown unknown

[14:17:57] [FOUND:HOST] www.yourtarget.com 172.67.195.52 CLOUDFLARENETUnited States United States

[14:17:57] [FOUND:HOST] mail.yourtarget.com 144.x.y.24 HETZNER-ASGermany Germany

[14:17:57] [FOUND:DNS] cleo.ns.cloudflare.com. 108.162.193.89 CLOUDFLARENETUnited States United States

[14:17:57] [FOUND:DNS] joan.ns.cloudflare.com. 108.162.192.173 CLOUDFLARENETUnited States United States

[14:17:57] [FOUND:MX] 144.x.139.y HETZNER-ASGermany 10 mail.yourtarget.com.

[14:17:57] [FOUND:MX] 144.x.139.y HETZNER-ASGermany 20 cs111.thewebmen.com.

[14:17:57] Scanning crimeflare database...

[14:17:58] [FOUND:IP] 144.x.224.y

[14:17:58] Scanning 11219 subdomains (subdomains.txt), please wait...

[14:21:44] [FOUND:SUBDOMAIN] mail.yourtarget.com IP: 144.x.139.y HTTP: 200

[14:22:03] [FOUND:SUBDOMAIN] new.yourtarget.com IP: 144.x.139.y HTTP: 200

As you can see, there is one result from crimeflare database and one similar IP pointing to Hetzner-AS. Next we have to do is modify our hosts file:

\*n?x based systems:

Code `sudo vi /etc/hostsWindows:`

For simplicity I suggest using <https://hostsfileeditor.com/>

Now add two records to the file:

Code `144.x.224.y yourtarget.com`

`144.x.224.y www.yourtarget.com`

Now verify that "ping yourtarget.com" responds to the IP address you've set in the hosts file. If it doesn't, check for errors (in the Windows program, you have to check both boxes on the left side

and press Save).

If it does, open your browser in Incognito mode and visit the site — if it opens the site itself, congratulations — CloudFlare is bypassed. If it doesn't, change IP to a different one (144.x.139.y in this case) and repeat until it does.

Congratulations, you have now bypassed the WAF and can test the web application without any obstructions.