

Forum:[Hack Forums](#)

Thread: [working CF bypass](#)

sizzuz - June 6, 2016, 5:16 am

I was bored the other day, so it took a closer look at Cloudflares "I am under attack page". While doing so, i stumbled across an interesting header.

Code Refresh: 8;URL=/cdn-cgi//chk_jschl?pass=1465214541.703-WYijW9RVYx

Further investigation showed, that it is not required to solve they javascript challenge at all. Wait the required time, then reload the page with the specified URL from the header and you will get clearance.

I wrote a short script for testing purposes and as proof of concept. As this is probably interesting for others too, i thought i share it:

<http://pastebin.com/chqXentf>

Unluckily i found this, after i was almost done solving the JavaScript with PHP and some funky regex ???

--- Update

Based on my previous findings i created attack scripts.

Usage: <target hostname> <proxy file/nofile> <threads> <time>

e.g.

php ./cfbypass.php <http://www.mydomain.com> proxies.txt 10 60

or if you dont want to use proxies

php ./cfbypass.php <http://www.mydomain.com> nofile 10 60

Version 1 bypasses using the Refresh header

<http://pastebin.com/hW3Qdq5W>

Version 2 bypasses by solving the JS challenge

<http://pastebin.com/aafaNxur>

Alex™ - June 6, 2016, 6:09 am

This is very cool, gonna test it out in a bit and report back.

Conceal - June 6, 2016, 2:29 pm

Looks pretty good, will test it out later. You should have a large array of user agents as one can get blocked, also for proxies you should load them from a text file, pass them through as an array and foreach proxy resend a cURL request and as-well have forking.

I suppose if you're not leaning towards this being an attack script, but good job bud.

HFTetramorph - June 6, 2016, 3:07 pm

Don't worry, if this is anything legit it will be fixed by CloudFlare before the end of the week.

Otherwise, will test it out here in a bit.

Sakuto - June 6, 2016, 3:12 pm

This is really interesting, thanks for your share. Maybe you should post this in a hacking section too, just to get opinion from more qualified users?

CodeBinary - June 6, 2016, 3:17 pm

Is there a way to use this to get an ip?

Sakuto - June 6, 2016, 3:19 pm

(Jun 6, 2016 03:17 PM)Dashy Wrote: [\[CITE\]](#) Is there a way to use this to get an ip?
This have nothing to do with unfortunately.

sizzuz - June 7, 2016, 2:02 am

Thanks for the feedback.

I build a version as attack script. Grab it here:

<http://pastebin.com/hW3Qdq5W>

Usage: <target hostname> <proxy file/nofile> <threads> <time>

e.g.

php ./cfbypass.php <http://www.mydomain.com> proxies.txt 10 60

or if you dont want to use proxies

php ./cfbypass.php <http://www.mydomain.com> nofile 10 60

I would post this in the SST section, but i am not uB3r. Only ub3r are allowed to create new threads there.

Jerry Smith - June 7, 2016, 2:30 am

Honestly OP this is a very generous thing of you to share, as most HF members would've kept this to themselves, or sold it to make profit from it.

Sakuto - June 7, 2016, 3:52 am

Nice share you did there sizuss, the script is a great addition to the current thread and resources. I can post it in the SST section if you want, just PM me.

Alex™ - June 7, 2016, 4:59 pm

(Jun 7, 2016 03:52 AM)Sakuto Wrote: [\[CITE\]](#) Nice share you did there sizuss, the script is a great addition to the current thread and resources. I can post it in the SST section if you want, just PM me. Please fucking don't? This has so many legit uses, it will just get fixed if it gets used for ddos (I can already see OP wrote a script).

Decafe - June 7, 2016, 6:40 pm

(Jun 7, 2016 04:59 PM)Alex™ Wrote: [\[CITE\]](#) Please fucking don't? This has so many legit uses, it will just get fixed if it gets used for ddos (I can already see OP wrote a script).

No, it won't. I released a ddos poc using a different method found [here](#) nearly 9 months ago and cloudflare does not give a single fuck.

HFTetramorph - June 7, 2016, 9:26 pm

Ah yes, I forgot I was going to test this.

After some standard testing of both the scripts, and manually playing with headers the method is correct. However this seems like it may be just a simple logic error on CloudFlare's side. Likely to be easily patched. If anyone is going to implement this I suggest instead implementing Decafe's listed method.

Insane Developer - June 7, 2016, 9:39 pm

This won't work. the pass value is obtained after calculating some maths with JS.

HFTetramorph - June 7, 2016, 9:41 pm

(Jun 7, 2016 09:39 PM)Insane Developer Wrote: [\[CITE\]](#) This won't work. the pass value is obtained after calculating some maths with JS.

Did you even try it for yourself? The pass value is sent before. Then is used to calculate an answer. Returned to a special URL, which then validates a session cookie. The only problem is currently the logic doesn't require the answer and just visiting the special URL is enough to retrieve a session cookie.

sizzuz - June 8, 2016, 1:17 am

Thanks for all the comments.

As i had the version, which actually solves the challenge, almost done, i gave it the last touches. Here you go:

<http://pastebin.com/aafaNxur>

I would appreciate some feedback on this.

Insane Developer - June 8, 2016, 3:02 am

(Jun 7, 2016 09:41 PM)BinaryEvolved Wrote: [\[CITE\]](#) Did you even try it for yourself? The pass value is sent before. Then is used to calculate an answer. Returned to a special URL, which then validates a session cookie. The only problem is currently the logic doesn't require the answer and just visiting the special URL is enough to retrieve a session cookie.

ok u guess im wrong. Was on a phone, gunna look at it now.

sizzuz - June 8, 2016, 3:58 am

(Jun 8, 2016 03:02 AM)Insane Developer Wrote: [\[CITE\]](#) ok u guess im wrong. Was on a phone, gunna look at it now.

Actually it is possible to test this in a very easy way.

1. Disable JavaScript in your browser (i am using Firefox)
2. Visit a website, which has CF UAM enabled
3. You will see a message, that you need to enable JavaScript
4. Just wait..
5. You will notice, page reloads and you will get clearance.

While doing so, you can watch the requests and headers in the console.

This happens due to the Refresh header. No need to complete any challenge, just follow Refresh header after time x.

I am almost sure, that CF added this at some point on purpose for situations, where the JS challenge fails due to disabled JS or JS error.

Afaik curl, wget etc dont follow a Refresh header, it is not like a 301 or 302 redirect. And to be honest i haven't seen this before.

stackoverflowin - June 8, 2016, 4:25 pm

I looked into this a month ago and honestly never caught on this, great solution.

debug - June 8, 2016, 4:36 pm

Great work. I converted it to C# and it's working very nicely ;)

Sakuto - June 9, 2016, 6:39 am

(Jun 8, 2016 04:36 PM)debug Wrote: [\[CITE\]](#) Great work. I converted it to C# and it's working very nicely ;)

Mind sharing your code?

debug - June 9, 2016, 7:34 am

(Jun 9, 2016 06:39 AM)Sakuto Wrote: [\[CITE\]](#) Mind sharing your code?I'll consider releasing it, I just don't want it to be skidded. Pretty brave of OP to release honestly.

debug - June 9, 2016, 10:14 am

(Jun 9, 2016 10:09 AM)Yani Wrote: [\[CITE\]](#) Well, I'm all for opensourcing, but:

1. Make request to CF enabled website
2. Look for this header
3. Wait 8 seconds
4. Visit link in header
5. Done

There's not really any source to be posted lolI know, it's very simple process. I'd just hate to see it abused.

HFTetramorph - June 9, 2016, 6:35 pm

(Jun 9, 2016 10:14 AM)debug Wrote: [\[CITE\]](#) I know, it's very simple process. I'd just hate to see it abused.

I am just waiting for CloudFlare to fix what should be a simple logic error somewhere in a few lines of code.. CloudFlare has stated in the past that their IUAM page once mass bypassed would just be rewritten to be harder.

In fact for the longest time CloudFlare just has javascript compute a simple math question like $2+2=4$ and send back the answer. It worked for so long because most didn't bother to check how it worked..

<https://blog.cloudflare.com/when-the-bad-guys-name-malware-after-you-you/>

stackoverflowin - June 10, 2016, 5:19 am

(Jun 9, 2016 06:35 PM)BinaryEvolved Wrote: [\[CITE\]](#) I am just waiting for CloudFlare to fix what should be a simple logic error somewhere in a few lines of code.. CloudFlare has stated in the past that their IUAM page once mass bypassed would just be rewritten to be harder.

In fact for the longest time CloudFlare just has javascript compute a simple math question like $2+2=4$ and send back the answer. It worked for so long because most didn't bother to check how it worked..

<https://blog.cloudflare.com/when-the-bad-guys-name-malware-after-you-you/>

You actually reported it to them? Are you a fucking spastic?

Decafe - June 10, 2016, 11:34 pm

(Jun 8, 2016 01:17 AM)sizzuz Wrote: [\[CITE\]](#) Thanks for all the comments.

As i had the version, which actually solves the challenge, almost done, i gave it the last touches. Here you go:

<http://pastebin.com/aafaNxur>

I would appreciate some feedback on this.

> eval

> barf

(Jun 9, 2016 06:35 PM)BinaryEvolved Wrote: [\[CITE\]](#) I am just waiting for CloudFlare to fix what should be a simple logic error somewhere in a few lines of code.. CloudFlare has stated in the past that their IUAM page once mass bypassed would just be rewritten to be harder.

In fact for the longest time CloudFlare just has javascript compute a simple math question like

2+2=4 and send back the answer. It worked for so long because most didn't bother to check how it worked..

<https://blog.cloudflare.com/when-the-bad-guys-name-malware-after-you-you/>

> 14 Feb 2013

Cloudflare stopped caring. They told me they were fixing it over a year ago and nothing has happened, they simply do not care.