

Forum:[Hack Forums](#)

Thread: [IPlogging using google - revised version discussed with M L T.](#)

Mr. Robot - August 2, 2019, 4:37 pm

Code

```
https://www.google.com/search?q=%48%41%43%4B%46%4F%52%55%4D%53%2E%4E%45%54
&btnI=&Search=cute%20kitten%20photos
```

This looks like it will go to google and/or search for kitten photos. You might be pleasantly surprised that instead you find yourself on Hackforums.

(WIP)

The best way to use this as using an IPlogger website itself wont quite work (afaik) you will buy a domain such as website.com

On the hosting for website.com - add an instant redirect to the google search results like this (save as index.html)

```
Code <!DOCTYPE html>
<html>
  <head>
    <title>HTML Meta Tag</title>
    <meta http-equiv = "refresh" content = "2; url =
http://www.images.google.com/search?q=cute%20kitten%20photos" />
  </head>
  <body>
    <p>ignore me</p>
  </body>
</html>
```

So now when you access your domain you should instantly get redirected to

Code <http://www.images.google.com/search?q=cute%20kitten%20photos>

Then what you would want to do is add an iplogger to the index.html page. This way whenever people access your domain it will log their IP address to a file on your website.

Finally what you would want to do is encode your URL so they can't read it such as
%48%41%43%4B%46%4F%52%55%4D%53%2E%4E%45%54

That string will read as hackforums.net but we will make it your domain. The shorter your domain the smaller the overall URL will look. So for web.com we could use the below link to create the URL.

https://www.w3schools.com/tags/ref_urlencode.asp

```
w = %77
e = %65
b = %62
. = %2E
c = %63
o = %6F
```

m = %6D

Our end string = %77%65%62%2E%63%6F%6D

So now we throw that in our google URL.

Code

<https://www.google.com/search?q=%77%65%62%2E%63%6F%6D&btnI=&Search=cute%20kitten%20photos>

So if we click this link, we will be taken to web.com even though it looks like it should google search cute kitten photos.

<https://www.google.com/search?q=%77%65%62%2E%63%6F%6D&btnI=&Search=cute%20kitten%20photos>

>>If web.com was our own URL with our IPlogger, it would take them to web.com then shoot them back to google search of cute kitten photos without them realizing. This would allow us to log their IP and hope they are none the wiser.

You can check at any time to see if your URL is correct by simply trying to go to

<http://%48%41%43%4B%46%4F%52%55%4D%53%2E%4E%45%54>

Dolippo - August 5, 2019, 2:51 am

Never seen this before !

Very interesting and HQ content. Can be really powerful in some situations.

gogreendv - August 5, 2019, 3:23 am

(Aug 2, 2019 04:37 PM)Mr. Robot Wrote: [\[CITE\]](#) Code

<https://www.google.com/search?q=%48%41%43%4B%46%4F%52%55%4D%53%2E%4E%45%54&btnI=&Search=cute%20kitten%20photos>

This looks like it will go to google and/or search for kitten photos. You might be pleasantly surprised that instead you find yourself on Hackforums.Great! Great! Great!

That's good idea.

Mr. Robot - August 5, 2019, 7:15 am

(Aug 5, 2019 02:51 AM)Dolippo Wrote: [\[CITE\]](#) Never seen this before !

Very interesting and HQ content. Can be really powerful in some situations.

Well hopefully it helps you!

bexpr9 - August 6, 2019, 12:04 am

[q=%48%41%43%4B%46%4F%52%55%4D%53%2E%4E%45%54](http://%48%41%43%4B%46%4F%52%55%4D%53%2E%4E%45%54)

It's good application of the google functions.

Hackers can use it for phishing attacks.

Glory to your wonderful sense!

Mr. Robot - August 7, 2019, 6:10 pm

(Aug 6, 2019 12:04 AM)bexpr9 Wrote: [\[CITE\]](#)
q=%48%41%43%4B%46%4F%52%55%4D%53%2E%4E%45%54

It's good application of the google functions.
Hackers can use it for phishing attacks.
Glory to your wonderful sense!
It can be used for a lot :)

ririki - August 8, 2019, 5:24 am

That's interesting but there is some sort of algorithm.

Some of my websites didn't went through, it went into google search bar instead of re-direct and sometimes it also redirected to completely different website.

Mr. Robot - August 12, 2019, 4:28 pm

(Aug 8, 2019 05:24 AM)ririki Wrote: [\[CITE\]](#) That's interesting but there is some sort of algorithm.

Some of my websites didn't went through, it went into google search bar instead of re-direct and sometimes it also redirected to completely different website.
Were they full URLs with like /index.html or just website.com

wikileaks - August 12, 2019, 4:33 pm

I don't understand this is expected behavior, I was able to do this with twitter and got bountied, but IP Logging with google is worth nothing, it may help an attacker but its still worth nothing fuzzing about.

millions of sites run off google, so an open redirect has to exist either way.

Mr. Robot - August 12, 2019, 4:37 pm

(Aug 12, 2019 04:33 PM)wikileaks Wrote: [\[CITE\]](#) I don't understand this is expected behavior, I was able to do this with twitter and got bountied, but IP Logging with google is worth nothing, it may help an attacker but its still worth nothing fuzzing about.

millions of sites run off google, so an open redirect has to exist either way.
When there are new exploits out for the newest versions of browsers, this type of attack can be used to infect people by going google > website > google without a visitor noticing.
Quickly allowing you to hack them.
While there are numerous redirects and while this is expected behavior, it has many use cases - using google on certain websites that only trust google links is another example.
The same way steam was exploiting users by trusting some links.

duplex - August 12, 2019, 4:40 pm

This is pretty amazing, wow

wikileaks - August 12, 2019, 4:42 pm

(Aug 12, 2019 04:37 PM)Mr. Robot Wrote: [\[CITE\]](#) When there are new exploits out for the newest versions of browsers, this type of attack can be used to infect people by going google > website > google without a visitor noticing.
Quickly allowing you to hack them.
While there are numerous redirects and while this is expected behavior, it has many use cases - using google on certain websites that only trust google links is another example.

The same way steam was exploiting users by trusting some links.
Yes but Steam is much smaller than google, but you can't infect people with this without UI.
I found something similar with zendesk where I was able to download any file I wanted but it still required a click of a button.

This is helpful but useless, plus at this point google is at the top when it comes to spreading through this method :P
I like the bug but you wont do much.

ririki - August 12, 2019, 4:43 pm

(Aug 12, 2019 04:28 PM)Mr. Robot Wrote: [\[CITE\]](#) Were they full URLs with like /index.html or just website.com
Mainly just website.com

For example HaveFriday.com and I was sent to HaveFun.org -- HaveFriday was not registered domain.

Then I also tried Website.net and instead of redirecting me, it searched it over google.

Then I also tried random words and it re-directs me to random websites.

<https://www.google.com/search?q=%48%55%53%4B%2E%4F%4D&btnI=&Search=cute%48%55%53%4B%2E%4F%4D> = HUSKY.COM and it was redirect to <https://huskrestaurant.com/>

Mr. Robot - August 12, 2019, 4:54 pm

(Aug 12, 2019 04:42 PM)wikileaks Wrote: [\[CITE\]](#) Yes but Steam is much smaller than google, but you can't infect people with this without UI.

I found something similar with zendesk where I was able to download any file I wanted but it still required a click of a button.

This is helpful but useless, plus at this point google is at the top when it comes to spreading through this method :P

I like the bug but you wont do much.

What? Of course you can infect people without user interaction? Let me guess, you heard JDBs are no longer a thing and just assume browser exploits don't exist nor come out weekly.

(Aug 12, 2019 04:43 PM)ririki Wrote: [\[CITE\]](#) Mainly just website.com

For example HaveFriday.com and I was sent to HaveFun.org -- HaveFriday was not registered domain.

Then I also tried Website.net and instead of redirecting me, it searched it over google.

Then I also tried random words and it re-directs me to random websites.

<https://www.google.com/search?q=%48%55%53%4B%2E%4F%4D&btnI=&Search=cute%48%55%53%4B%2E%4F%4D> = HUSKY.COM and it was redirect to <https://huskrestaurant.com/>

Try this one.

Code

<https://www.google.com/search?q=%68%75%73%6B%79%2E%63%6F%6D&btnI=&Search=cute>

ririki - August 12, 2019, 5:00 pm

(Aug 12, 2019 04:54 PM)Mr. Robot Wrote: [\[CITE\]](#) Try this one.

Code

<https://www.google.com/search?q=%68%75%73%6B%79%2E%63%6F%6D&btnI=&Search=cute>

Yeah, looks like it's working.

I only used capital letters, it might have been the thing.

Mr. Robot - August 12, 2019, 5:01 pm

(Aug 12, 2019 05:00 PM)ririki Wrote: [\[CITE\]](#) Yeah, looks like it's working.

I only used capital letters, it might have been the thing.
No problem my dude.

Mr. Robot - *August 31, 2019, 2:48 pm*

Still useful to this day. Awesome fun.

wonderlust90 - *October 13, 2019, 1:27 pm*

(Aug 31, 2019 02:48 PM)Mr. Robot Wrote: [\[CITE\]](#) Still useful to this day. Awesome fun.
Not working anymore. Now google shows redirect notice.

Redirect Notice

The previous page is sending you to [https://www.\\$WEBSITE.com/](https://www.$WEBSITE.com/).

If you do not want to visit that page, you can return to the previous page.