

Forum:[Hack Forums](#)

Thread: [Is this considered an open redirect?](#)

redlightrouter - February 4, 2017, 10:53 am

Hi all,

On Google Chrome it's possible to redirect yourself from any site to any site, by using the '@' sign.
Example:

<http://google.com@youtube.com> -> goes to youtube.com without any warning, try it.

On Firefox it does give you a warning.

I'm very confused why this isn't patched, but on the other hand, it's Google, if it was a vulnerability it would be patched a while ago.

eggy - February 4, 2017, 1:47 pm

No that's not open redirect....

?Criminal - February 4, 2017, 1:57 pm

Thats intentional design for like logging into sites username:password@domain here but it can be abused theoretically.

anilvac11 - February 4, 2017, 2:44 pm

hmm, weird thing but I don't think this is a big vulnerability

redlightrouter - February 4, 2017, 4:09 pm

(Feb 4, 2017 02:57 PM)?Criminal Wrote: [\[CITE\]](#) Thats intentional design for like logging into sites username:password@domain here but it can be abused theoretically.

Exactly, that's why I don't understand why open redirects are considered vulnerabilities while Google here gives everyone the free pass to do the exact same thing.

You should atleast get a warning before redirecting.

:(' - February 4, 2017, 4:12 pm

you could be spoofed into thinking you're going to a safe site.

e.g google.com@YourPhishingSite.com

of course you can shorten your dodgy link so it looks like <http://google.com@goo.gl/Ah35Ha>

people may think they are going to google by clicking on it.

redlightrouter - February 4, 2017, 4:14 pm

(Feb 4, 2017 02:47 PM)eggy Wrote: [\[CITE\]](#) No that's not open redirect....

You can print out millions of dots, but then explain me why companies are willing to pay hundreds of dollars for something like <http://legitsite.com//evil.com/%2F..> , while <http://legitsite.com@evil.com> does the exact same thing.

I get that the first one is the problem of the company, and the second one pretty much of Google, but that doesn't make the impact less of an issue.

:(- February 4, 2017, 4:14 pm

p.s on safari it works too but I get a warning for phishing before it redirects.

?Criminal - February 4, 2017, 4:23 pm

(Feb 4, 2017 05:09 PM)redlightrouter Wrote: [\[CITE\]](#) Exactly, that's why I don't understand why open redirects are considered vulnerabilities while Google here gives everyone the free pass to do the exact same thing.

You should atleast get a warning before redirecting.

not to google theres a redirect problem with the continue parameter which has been documented for the past 4 years but no one actually abuses it, you would think the DNC hackers would of implemented it into there automated kit. Theres so many different things you can abuse with google and alot of these things aren't important to google but are very useful to attackers.

Ryuga - February 6, 2017, 1:41 pm

Well, this isn't considered a url redirection attack because there's no redirection being done .. It's working as it should?.

[RFC 1738](#), Section 3.1, Common Internet Scheme Syntax (December '94)

Quote://<user>:<password>@<host>:<port>/<url-path>

But, check these out too ..

[RFC 2396](#), Section 3.2.2, Server-based Naming Authority (August '98)

Quote:Some URL schemes use the format "user:password" in the userinfo field. This practice is NOT RECOMMENDED, because the passing of authentication information in clear text (such as URI) has proven to be a security risk in almost every case where it has been used.

[RFC 2616](#), Section 3.2.2, http URL (June '99)

Quote:http_URL = "http:" "/" host [":" port] [abs_path ["?" query]]

So I guess Chrome (and Opera) are just confused on what to do ?, seriously though, I guess they'll stop supporting it soon enough (because of the newer rfc(s)), [IE stopped it in '11](#) or maybe in ['03](#) ?, Safari displays a phishing alert sorta message, Firefox does a head request first and checks whether the site actually requires http basic authentication, if it doesn't, it displays a prompt asking the user to confirm whether he/she actually wants to visit the site.

Chrome stopped supporting it in ['11/'12](#) too, after seeing IE but they apparently began supporting it again, but still, they at least hide/strip the user:pass@, so the users (who don't understand how url works) may know what website they actually are on, Opera doesn't do anything about it, it displays the url as it is.