What `location.replace(...)` in double square brackets does in a Browser?

Asked 1 year, 4 months ago Modified 1 year, 3 months ago Viewed 34 times

1

I stumbled upon a phishy domain name and I fetched its code via `wget`, and all its underlying JavaScript assets.

I stumbled upon this line of code:

```
[[location.replace("https://suspicious-subdomain.suspicious-domain.com/cart")]]
```

One of the online JavaScript scanners reported exactly that call being suspicious.

I'm trying to understand what are security implications in a call like this in any modern Browser.

The MDN says this about `location.replace`:

> The replace() method of the Location interface replaces the current resource with the one at the provided URL. The difference from the assign() method is that after using replace() the current page will not be saved in session History, meaning the user won't be able to use the back button to navigate to it.

javascript security http-redirect

Share

Improve this question

Follow

edited Sep 8, 2023 at 3:59

pppery

3,784 ●24 ●37 ●50

asked Jul 26, 2023 at 14:34

Zlatan Omerovic

4,097 ●4 ●43 ●70

1 Answer

Sorted by: Highest score (default)

▲
4
▼
✓

This is an array of length one that contains an array of length one that contains the output of `location.replace()`. However, when that is evaluated, the browser location is changed and the rest doesn't matter.

So while this may be a template failure or obfuscation, it will still work. Try it yourself in your Developer Console (aka Browser Console or JavaScript Console; press F12): run `[[location.replace("http://example.com")]]` and you'll find yourself on the IANA's example website.

From a security perspective, this simply facilitates a JS-based redirector, which will fool simpler security web crawlers that only look for HTTP redirects rather than JS. As you noted in the question, this also prevents the user from hitting the Back button, which makes it harder to report the entry page as malicious. (It is not uncommon for malicious redirectors to change their targets as they get blocked, thus alleviating the need to send out new entry pages to potential victims.)

Share

Improve this answer

Follow

edited Sep 7, 2023 at 14:18

answered Jul 26, 2023 at 16:03

Adam Katz

16k ● 5 ● 75 ● 91