

Forum:[Hack Forums](#)

Thread: [XSS in HTTP Header referer](#)

whatadumbass123 - July 30, 2016, 3:42 pm

Parameter Name Referer

Parameter Type HTTP Header

I use tamperdata and create Post data name=Expect and name=Refer

>

In them i put the scriptalert.on.cookie It shows me the sites cookies

Now i want to know Whats the best about getting admin logins? Or users?

Can i do it without sending any links?

Mafius - July 30, 2016, 10:12 pm

To session hijack with non-persistent XSS you MUST send a link.

You'd have to host a page that would redirect the target to the vulnerable page, injecting the session hijack JS into the referer header. I believe this could be accomplished with PHP's header() function.

whatadumbass123 - July 31, 2016, 1:48 am

(Jul 30, 2016 10:12 PM)Mafius Wrote: [\[CITE\]](#) To session hijack with non-persistent XSS you MUST send a link.

You'd have to host a page that would redirect the target to the vulnerable page, injecting the session hijack JS into the referer header. I believe this could be accomplished with PHP's header() function.

My scanner says I can do mitm attacks , even set up mount phising pages? Change pages on the fly?

Mafius - July 31, 2016, 11:32 am

(Jul 31, 2016 01:48 AM)whatadumbass123 Wrote: [\[CITE\]](#) My scanner says I can do mitm attacks , even set up mount phising pages? Change pages on the fly?

After looking into it, it appears browsers handle referer headers all by themselves - so what I suggested isn't actually possible.

MITM attacks could work if you are physically near them.

.trigious - July 31, 2016, 2:40 pm

(Jul 31, 2016 11:32 AM)Mafius Wrote: [\[CITE\]](#) After looking into it, it appears browsers handle referer headers all by themselves - so what I suggested isn't actually possible.

Yes it is. I tried it before. You have to play around with URL rewrites, but it is possible.

Requirement on the vulnerable website is that the Referer needs to be URL decoded before being echo'd. (:

Mafius - July 31, 2016, 3:30 pm

(Jul 31, 2016 02:40 PM)Trigious Wrote: [\[CITE\]](#) Yes it is. I tried it before. You have to play around with URL rewrites, but it is possible.

Requirement on the vulnerable website is that the Referer needs to be URL decoded before being echo'd. (:

Didn't say it wasn't possible, just said what I suggested wasn't the way to do it.

.trigious - August 1, 2016, 12:39 am

(Jul 31, 2016 03:30 PM)Mafius Wrote: [\[CITE\]](#) Didn't say it wasn't possible, just said what I suggested wasn't the way to do it.

Yes, your way is possible.

Since most OSs' will stop you from creating files that are a javascript payload, you will need to simply change the 404 page of your server to a script that will redirect the user to the vuln page.

So:

1. Victim visits evil.com/payload here
2. he gets a 404 error because the file does not actually exist
3. the 404 page redirects the user to the other vuln website
4. the referer now contains the payload, which is url encoded
5. the vulnerable website decodes the Referer and echo's it onto the page
6. XSS

This is very unlikely but possible. (: