

Forum:[Hack Forums](#)

Thread: [XSS steal basic auth](#)

Tessaiga88 - April 13, 2021, 11:28 am

<https://medium.com/@agrawalsmart7/steal-csrf-auth-unique-key-header-with-xss-5a54c38d7ec3>

With XML request you can steal response header.

But, what if you want steal REQUEST header like the Authorization from basic auth? Any idea?

Thanks for help

rAmUnDo - April 13, 2021, 9:16 pm

I'm looking to hire and pay well for those who know how to gain root access to sites and extract files ... Paid for each invasion ...

Gee4rce - April 14, 2021, 2:54 pm

(Apr 13, 2021 11:28 AM)Tessaiga88 Wrote: [\[CITE\]](#) But, what if you want steal REQUEST header like the Authorization from basic auth? Any idea?

One idea, "form action hijacking", where you need another vuln like XSS for example, to rewrite the forms "action" destination to a server you own. On there, you want to monitor the incoming requests and filter out the headers of the requests, which will ultimately show you the sent Authbearer.

Maybe CSRF or SSRF vuln could also open doors to this.

Cheers, Gee.

Tessaiga88 - April 15, 2021, 10:56 am

(Apr 14, 2021 02:54 PM)Gee4rce Wrote: [\[CITE\]](#) One idea, "form action hijacking", where you need another vuln like XSS for example, to rewrite the forms "action" destination to a server you own. On there, you want to monitor the incoming requests and filter out the headers of the requests, which will ultimately show you the sent Authbearer.

Maybe CSRF or SSRF vuln could also open doors to this.

Cheers, Gee.

Thanks for reply. Probably not possible for my situation.

I have web site target example 'https://target.com' where 'https://target.com/abc/' is protected by basic auth. But only the /abc/ path. So if you catch headers from another path, you dont get the 'Authorization' header.

Tessaiga88 - April 24, 2021, 3:23 am

up, still looking for a way to get http request header from specific request, starting from XSS vulnerability

Shadow_Cloud - April 27, 2021, 11:35 pm

(Apr 13, 2021 11:28 AM)Tessaiga88 Wrote: [\[CITE\]](#)
<https://medium.com/@agrawalsmart7/steal-csrf-auth-unique-key-header-with-xss-5a54c38d7ec3>

With XML request you can steal response header.

But, what if you want steal REQUEST header like the Authorization from basic auth? Any idea?

Thanks for help

Do you know the tech stack in question here? I remember, although admittedly only vaguely, about an exploit for this by utilizing phpinfo() by accessing the data from PHP_AUTH_USER and PHP_AUTH_PW.

I'm not sure if this is still relevant, I'm talking years ago, but might be worth exploring?

Edit: Obviously I mean making an ajax request to the server that contains phpinfo on it after auth has been done. This would require a lingering phpinfo page on the server, but its actually more common than most people imagine.

Edit2: There might also be a play for a service worker and using fetch >
<https://developer.mozilla.org/en-US/docs/Web/API/Request>

Tessaiga88 - April 30, 2021, 12:37 pm

(Apr 27, 2021 11:35 PM)Shadow_Cloud Wrote: [\[CITE\]](#) Do you know the tech stack in question here? I remember, although admittedly only vaguely, about an exploit for this by utilizing phpinfo() by accessing the data from PHP_AUTH_USER and PHP_AUTH_PW.

I'm not sure if this is still relevant, I'm talking years ago, but might be worth exploring?

Edit: Obviously I mean making an ajax request to the server that contains phpinfo on it after auth has been done. This would require a lingering phpinfo page on the server, but its actually more common than most people imagine.

Edit2: There might also be a play for a service worker and using fetch >
<https://developer.mozilla.org/en-US/docs/Web/API/Request>
Thanks for reply.

Is an asp.net web application, with most pages written in asp classic. Plesk is installed, so php works. But i dont think there is a phpinfo page.

Can you make me an example for service worker?

Tessaiga88 - August 5, 2021, 12:46 pm

After a lot of test, i can says there is no way to steal Request headers with javascript.

<https://developer.mozilla.org/en-US/docs/Web/API/Request/headers>

These API work for setting up headers for a new request. Or get them if you haved assigned one by ".append". You cant read headers assigned by your browser.