

Forum:[Hack Forums](#)

Thread: [DONT USE SNIP.LY LINKS](#)

Vanderbilt - October 27, 2018, 10:54 pm

Just dont. I got a link like this.

<http://snip.ly/fkrgxk/#https://www.advancedwebranking.com/>

So, instead of giving me a `redir`, it sent me to a frame locked in it, probably like emulating the environment.

I went to the login page, still had the snip.ly part on it, and used the credentials, fakeemail@gmail.com and the password, fakeemail.

It sent a PUT request, not a POST request but with the api, it is almost the same thing. Probably to throw off web browsers or antiviruses

This is the post request for the logging into AWR

```
Code Host: app.advancedwebranking.com  
Origin: https://app.advancedwebranking.com  
Upgrade-Insecure-Requests: 1  
Content-Type: application/x-www-form-urlencoded  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/69.0.3497.100 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Referer: https://app.advancedwebranking.com/signin  
Accept-Encoding: gzip, deflate, br  
Accept-Language: en-US,en;q=0.9  
Cookie: _gcl_aud=1.1.605893394.1540704780; _ga=GA1.2.455764686.1540704780;  
_gid=GA1.2.2121907769.1540704780; _dc_gtm_UA-61715-3=1;  
AWSALB=T9JUwnsD8ROVllygx3wRfT1DYRzgbKBOG5dAllmK8G8Smhqfpm9/hdVbPcpT0895pwIMv  
0EaO0en0QbDX2ciHzZERhECRoVbUphmc23Nn1OCFCHh2t+lo1TLh9ahd;  
csrf_token=RQfuGdU68%2BDGyTNJcBx1bBs45yTIucZzSZVjO43WE3I%3D;  
PHPSESSID=gcd979au4hpsgjbjba3fd95vvs2;  
amplitude_id_87adddfe6b223759ca176b2911430e04advancedwebranking.com=eyJkZXZpY2VJZCI6  
6ljklYzFmMTNiLTU1NDMtNDMyNi04OGFhLTVhOThjMGE1MTY4NlliLCJ1c2VySWQiOm51bGwsl  
m9wdE91dCI6ZmFsc2UsInNlc3Npb25JZCI6MTU0MDcwNTQ0MDg3MiwiibGFzdEV2ZW50VGltZSI6  
MTU0MDcwNTQ0MDg3MiwiXZlbnRJZCI6MCwiaWRlbnpRpZnlJJZCI6MCwic2VxdWVuY2VObW1iZ  
XliOjB9
```

csrf_token=JpWnbN33BRh5KHuYfKrVxy6T7YAF2CiVnUr9cr9vfx8oGxEpZFwFwlkFxtltSjeuw5bz+xPG4L3V41b62fnYNQ==&email=fakeemail@gmail.com&password=fakeemail

Notice how my token was there with my email and pass

This is snip.ly's PUT request

Code Host: snip.ly

Accept: */*
Origin: http://snip.ly
X-CSRFToken: null
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer:
http://snip.ly/render/fkrgxk/?_url=http%3A%2F%2Fsnip.ly%2Ffkrgxk%2F%23https%3A%2F%2Fwww.advancedwebranking.com%2F
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __cfduid=d089565936693cd44dc34e6b4833ab7d31540455838;
sessionid=xuwcw8qaiz7g9rbr2bcfvg41dukq74k1; _ga=GA1.2.1380611076.1540704777;
_gid=GA1.2.1663019132.1540704777; _gat=1

change=page&is_landing_page_transition=false&time_on_page=28

csrf_token=JpWnbN33BRh5KHuYfKrVxy6T7YAF2CiVnUr9cr9vfx8oGxEpZFwFwIkFxtltSjeuw5bz+x
PG4L3V41b62fnYNQ==&email=fakeemail@gmail.com&password=fakeemail
Something is fishy here but i cant put my finger on it. ill just put my email and password there
instead

Zeus - October 30, 2018, 10:12 pm

Thanks for sharing the alert for us!