

Forum:[Hack Forums](#)

Thread: [PHPSESSID trouble](#)

Nope.exe - January 28, 2016, 6:21 am

I'm working on making a bot for visitstomoney.com so I can up my profits, but I need to figure out how the phpsessid is generated. I know it's based on IP, but other than that I've learned nothing in my googling that helps.

EDIT: After lots of googling I'm seeing some people saying it's entirely random, some say it's just serialized and some also say it's something to do with php's md5() function. Basically the only thing bugging me is that my bot is returning a bad request error code. Maybe someone will be able to tell me why. Here's the request being sent:

```
std::string request = std::string("GET / HTTP/1.1\r\nHost: ") + host + "\r\nUser-Agent: " + userAgent + "\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.5\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nPHPSESSID: yqvjg72ot96xukxfxgj12so1nq/*randomly generated phpsessid*\r\nDNT: 1\r\nConnection: close\r\n\r\n";
```

user agent i'm testing with is: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:44.0) Gecko/20100101 Firefox/44.0

host i'm using is: <http://VisitsToMoney.com/index.php?refId=755770> //my ref code, that way I can test if it shows up

Also, the X-GC error is: 0.DNS_FAIL.JS-MOBILE-RC-01_183_207_203_8

Fozo - January 28, 2016, 8:56 pm

I can't post links yet sorry:

[github\(dot\)com/php/php-src/blob/d9bfe06194ae8f760cb43a3e7120d0503f327398/ext/session/session.c#L284](https://github.com/php/php-src/blob/d9bfe06194ae8f760cb43a3e7120d0503f327398/ext/session/session.c#L284)

From what I can tell, it's generated with your IP, current server time, and a random number generator.

Nope.exe - January 28, 2016, 9:35 pm

Thanks man, if you want if/when I get my bot working ik give you a free copy xD

That being said, If you're up to it (and you know c/c++) I could use some help. Mostly just with the phpsessid thing but I'm also doing a Web page scraper to get proxies so...

Fozo - January 28, 2016, 11:03 pm

You could just throw a bunch of HTTP HEAD requests at it, capturing the PHPSESSID from the Set-Cookie headers. Example with Code curl (on linux):

```
Code censored@ubuntu:~$ curl VisitsToMoney.com -i -X HEAD
HTTP/1.1 200 OK
Date: Fri, 29 Jan 2016 07:02:56 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
```

Pragma: no-cache

Set-Cookie: PHPSESSID=d6pdrdsl9vrb0b54gs4sfv3j37; path=/

Content-Type: text/html

Using this and some bash, you can generate cookies very quickly:

Spoiler ([Click to View](#))

45 Generated in roughly 22 seconds.

Code Set-Cookie: PHPSESSID=db5m30401f97jhl4s6jdrdq5l1; path=/

Set-Cookie: PHPSESSID=sc0kf8cip1nlhdv2f1ubd3u8p0; path=/

Set-Cookie: PHPSESSID=b6590lmc73o0uhleco9kts4i62; path=/

Set-Cookie: PHPSESSID=nl6l39ou571g5v9ejkjee6f37; path=/

Set-Cookie: PHPSESSID=oj391lh6bv0av00uicvhf9kb86; path=/

Set-Cookie: PHPSESSID=cu7v8m48mr5m0tuhg45o5sp9r3; path=/

Set-Cookie: PHPSESSID=dp6qo0nr85f8419ih75oiakjf7; path=/

Set-Cookie: PHPSESSID=5dcdgiu765vgnko0oqd1561l0v2; path=/

Set-Cookie: PHPSESSID=52utb1jcm07mthen886of02324; path=/

Set-Cookie: PHPSESSID=alqpgeeb0l84b7p0j04rkjmbk3; path=/

Set-Cookie: PHPSESSID=q7205eha7393nkncnl85fb2c7; path=/

Set-Cookie: PHPSESSID=1oeaka7543g6o30cj7g4a2nen7; path=/

Set-Cookie: PHPSESSID=tpji1c314ehpv4n6pobj6hluk4; path=/

Set-Cookie: PHPSESSID=jlok3fsd13v508galvd0231sa1; path=/

Set-Cookie: PHPSESSID=ihquskuc4rlo7l3o3j0imfrnf2; path=/

Set-Cookie: PHPSESSID=kkvmd2j40f3l9j800t3dm55f30; path=/

Set-Cookie: PHPSESSID=09g5oet9gd49du0q0qp1sq4fn1; path=/

Set-Cookie: PHPSESSID=un99k0h8jjrbfisbrrld7j17c0; path=/

Set-Cookie: PHPSESSID=v20lt1jed2t5vhstqmi58hlau6; path=/

Set-Cookie: PHPSESSID=l7vqli16j0d9e2aep2hvgs4kc6; path=/

Set-Cookie: PHPSESSID=mqd3kfp9r3fp4utjls2c1fd3f0; path=/

Set-Cookie: PHPSESSID=visl7bu9vjdm9ij6c3vtu8mg0; path=/

Set-Cookie: PHPSESSID=i8u2bhei9ql6c6e2vsmjc0qva2; path=/

Set-Cookie: PHPSESSID=pnid5g6uiocv5camoijsnn3q4; path=/

Set-Cookie: PHPSESSID=adi5gp0med6p2lje51j3cvcvri5; path=/

Set-Cookie: PHPSESSID=c461g23u81t7g6mf6j6p2daih5; path=/

Set-Cookie: PHPSESSID=pp87e4rkc2d95n57kjncss2t54; path=/

Set-Cookie: PHPSESSID=qbetrrf9h6dvemr37s01dap6e5; path=/

Set-Cookie: PHPSESSID=gkvja7to1nnb5vf388qtbdac50; path=/

Set-Cookie: PHPSESSID=pg0a1jb3vaicu8epjjj055kea1; path=/

Set-Cookie: PHPSESSID=k9u2hmok9ukb0k3q98c7rt6pe1; path=/

Set-Cookie: PHPSESSID=1f2vbdao2d73h837k72sq8j9n5; path=/

Set-Cookie: PHPSESSID=f125jdekl1gnj5t4q3k0ukii73; path=/

Set-Cookie: PHPSESSID=9uens1g5vl69rcnjs8akpqo143; path=/

Set-Cookie: PHPSESSID=of2tn0b08fu0vsr955eljavnf6; path=/

Set-Cookie: PHPSESSID=u24tnoi7sgmgf7qhluq0726j90; path=/

Set-Cookie: PHPSESSID=ou7rl6ttbkcpn5i3dctad0hpn5; path=/

Set-Cookie: PHPSESSID=h69vnh3u4iqbqfmh0k516nnas1; path=/

Set-Cookie: PHPSESSID=g2tdjbdp0jhi3k7h06uq7crq35; path=/

Set-Cookie: PHPSESSID=4krbdku60emmgn7kmb0qaskb82; path=/

Set-Cookie: PHPSESSID=v65avib7pihjrckiukhul2j312; path=/

Set-Cookie: PHPSESSID=iguo846qibahm5uurtgbvd0de7; path=/

Set-Cookie: PHPSESSID=lf7lnftl320vv7mfaumo5i07i0; path=/

Set-Cookie: PHPSESSID=7e1lfn2d2jomv4ul2bvff4shl6; path=/

Set-Cookie: PHPSESSID=svrt6mtrakivh969hsqm2sk0j5; path=/

wait, you're getting multiple different phpsessid's but every time that i've used httpfox and checked the data after actually connecting I get the same results. Forgive me for being a noob, but how is curl generating these cookies?

Fozo - January 29, 2016, 1:14 pm

(Jan 29, 2016 10:35 AM)Nope.exe Wrote: [\[CITE\]](#) wait, you're getting multiple different phpsessid's but every time that i've used httpfox and checked the data after actually connecting I get the same results. Forgive me for being a noob, but how is curl generating these cookies?

It's just establishing a new connection to each. On each connection it does not give the server a PHPSESSID cookie, so the server generates a new one. HTTPFox is probably keeping the PHPSESSID cookie and re-using it in each connection.

Nope.exe - January 29, 2016, 1:32 pm

So in my request if I don't send a phpsessid, that should be fine then? And thanks so much for your help man

?lpha - January 29, 2016, 1:35 pm

I assume you are writing this in C++. The thing you are looking for is called a cookie jar.

I am not sure if it's easy to implement something like a cookie jar in C++, maybe look at a higher level language like Python, Java etc.

Fozo - January 29, 2016, 1:55 pm

(Jan 29, 2016 02:32 PM)Nope.exe Wrote: [\[CITE\]](#) So in my request if I don't send a phpsessid, that should be fine then? And thanks so much for your help man

Yeah, it should generate one for you.

I accidentally left my script running last night and have ~110,000 PHPSESSID cookies for that site, lmk if you want them :P

Nope.exe - January 30, 2016, 12:26 am

Well if the request doesn't actually need to have a cookie then I might pass, if not I could just have my bot select one from the file for each visit. What do you think I should do?