

Forum:[Hack Forums](#)

Thread: [Gmail cookie / session hijacking](#)

SIM-5514832 - January 3, 2025, 9:52 am

Yo guys,

currently struggling to get into gmail acc's even tho i have fresh cookies and traffic proxied via the account owners PC, in the past this setup worked for me.

I have seen some posts about Google changing the way they deal with cookies ect, and was wondering what is required these days.

Any help would be greatly appreciated, Thanks!

DramaKing - January 3, 2025, 12:06 pm

As long as the cookies are unencrypted, and the owner doesn't sign out, they should be valid. I've never succeeded at this myself for some reason.

SIM-5514832 - January 3, 2025, 1:26 pm

(Jan 3, 2025 01:06 PM)DramaKing Wrote: [\[CITE\]](#) As long as the cookies are unencrypted, and the owner doesn't sign out, they should be valid. I've never succeeded at this myself for some reason. Yea in theory i dont get why it wont work, i have used remote port debugging dumping and memory dumping (chromekatz) for cookies, so i assume they are good, given then work on other sites also.

But every time i try i get to the page of accounts, all accs are signed out and require to sign in (prompts 2fa) even tho the user has not signed out.

I assume there is some type of device/browser fingerprinting going on, just not sure what exactly :/

DramaKing - January 3, 2025, 1:47 pm

(Jan 3, 2025 02:26 PM)SIM-5514832 Wrote: [\[CITE\]](#) Yea in theory i dont get why it wont work, i have used remote port debugging dumping and memory dumping (chromekatz) for cookies, so i assume they are good, given then work on other sites also.

But every time i try i get to the page of accounts, all accs are signed out and require to sign in (prompts 2fa) even tho the user has not signed out.

I assume there is some type of device/browser fingerprinting going on, just not sure what exactly :/ There must be something in the requests that is different.

stillworking247 - February 25, 2025, 9:15 am

Hi,

It's me, Paris, hit me up (old account stillonline247)

we've lost contact, and i need u asap <3

deathinside - February 25, 2025, 10:55 am

(Jan 3, 2025 02:26 PM)SIM-5514832 Wrote: [\[CITE\]](#) Yea in theory i dont get why it wont work, i have

used remote port debugging dumping and memory dumping (chromekatz) for cookies, so i assume they are good, given then work on other sites also.

But every time i try i get to the page of accounts, all accs are signed out and require to sign in (prompts 2fa) even tho the user has not signed out.

I assume there is some type of device/browser fingerprinting going on, just not sure what exactly :/
Your answer is Chrome Variations Tracking bro. Just Google it you will find out what it is. When you run chrome via obvious; remote debugging or sandbox features, this will be included in your x-variations headers and basically invalidates all of your cookies. I have a better workaround for and I'm developing something better for my workflow but I don't want to publicly disclose the methods and kill it since this kind of forums been actively spied on via white hat intelligence tools

crypteer - February 25, 2025, 11:13 am

Oh Gmail dm me bro om göstersecel
[warn]

•CHESTER• - June 5, 2025, 7:45 am

Did you ever figure this out? I am having the same problem.

Chornaya Magiya - June 5, 2025, 8:09 am

(Jun 5, 2025 07:45 AM)ChesterMolestor Wrote: [\[CITE\]](#) Did you ever figure this out? I am having the same problem.

Cookies is enough, but they rotate every some actions.

So if u get cookie and owner with actual session did some actions that past cookies become not valid.

Bypass for that is to sync latest cookies with chrome browser, then u can re-create whole diff session from cookies u had to chrome profile so u are only one who use that new google chrome profile session and cookies never die ?

•CHESTER• - June 5, 2025, 9:02 am

(Jun 5, 2025 08:09 AM)Chornaya Magiya Wrote: [\[CITE\]](#) Cookies is enough, but they rotate every some actions.

So if u get cookie and owner with actual session did some actions that past cookies become not valid.

Bypass for that is to sync latest cookies with chrome browser, then u can re-create whole diff session from cookies u had to chrome profile so u are only one who use that new google chrome profile session and cookies never die ?

You mentioned that cookies are enough, but in my case, I'm not performing any actions at all. I'm testing with my own cookies. I use PureLogs to extract the cookies while the browser is closed, so no user activity should interfere. Then I recreate the session on another machine, but within half a millisecond of launching it, Google immediately logs me out.

Do you think this could be an issue with PureLogs? Or is it something else?

DramaKing - June 5, 2025, 12:55 pm

(Jun 5, 2025 09:02 AM)ChesterMolestor Wrote: [\[CITE\]](#) You mentioned that cookies are enough, but in my case, I'm not performing any actions at all. I'm testing with my own cookies. I use PureLogs to extract the cookies while the browser is closed, so no user activity should interfere. Then I recreate the session on another machine, but within half a millisecond of launching it, Google immediately

logs me out.

Do you think this could be an issue with PureLogs? Or is it something else?
You shouldn't be able to steal cookies with the browser closed anymore.

Chornaya Magiya - June 8, 2025, 7:05 am

(Jun 5, 2025 09:02 AM)ChesterMolestor Wrote: [\[CITE\]](#) You mentioned that cookies are enough, but in my case, I'm not performing any actions at all. I'm testing with my own cookies. I use PureLogs to extract the cookies while the browser is closed, so no user activity should interfere. Then I recreate the session on another machine, but within half a millisecond of launching it, Google immediately logs me out.

Do you think this could be an issue with PureLogs? Or is it something else?
Stealer fault 100% ?

Simply just export your cookies using "Cookiebro" extension on firefox.
Then on other device import using "Cookiebro" extension on firefox and u will see it works.