Pass the Cookie and Pivot to the Cloud

Disclaimer: Always make sure you have proper authorization before pen testing.

Johann Rehberger
wunderwuzzi23@outlook.com

December 2018

Cookies – Kekse - Biscotti

- **Web Applications & Services use cookies to authenticate users.**

- **Single Key to the Kingdom**
  - If you have the appropriate cookie => Access!
  - 2FA happened already, so that won't protect you

    => probably often more valuable then your password.

- A cookie could be the single key to the "virtual" datacenter of your organization
- A cookie could be the single key to your personal finances, crypto, etc…
- …

So, be aware of the value of cookies, protect and monitor them well!

What is Pass The Cookie?

Pass the Cookie is a post exploitation session hijacking technique.

After compromising a valuable host an adversary steals authentication cookies from browsers and related processes.

The adversary passes the acquired cookies to elevate privileges and pivot from the host to the corresponding cloud service.

This bypasses most multi-factor authentication protocols.

Successfully used during adversarial emulation to achieve mission objective.

Acquiring Cookies, Tools and Techniques

Here are some tools that can be leveraged (there are more):

- **firefox_creds** - Access SQL Lite Database of Firefox
- **Cookie Crimes** - Neat way to grab cookies via headless Chrome
- **ProcDump** - Swiss army knife to dump strings from any process

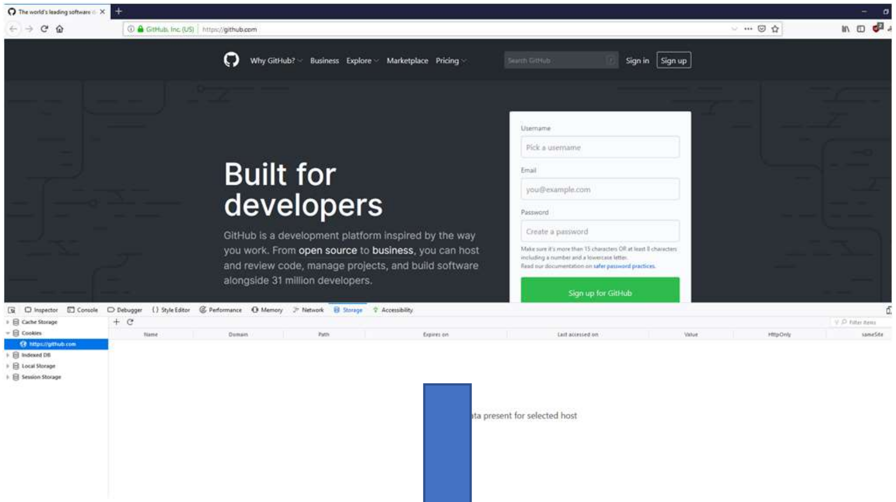
How to Pass the Cookie?

- Leverage default browser features
  E.g. using Developer Console (*document.cookie = “key=value”)* or UI

Disclaimer: Always make sure you have proper authorization before pen testing.

Example – Pass the Cookie

(1) Unauthenticated



The world's leading software

GitHub, Inc. (US) | https://github.com

Why GitHub? Business Explore Marketplace Pricing Search GitHub Sign in Sign up

Built for developers

GitHub is a development platform inspired by the way you work. From **open source** to **business**, you can host and review code, manage projects, and build software alongside 31 million developers.

Username: Pick a username

Email: you@example.com

Password: Create a password

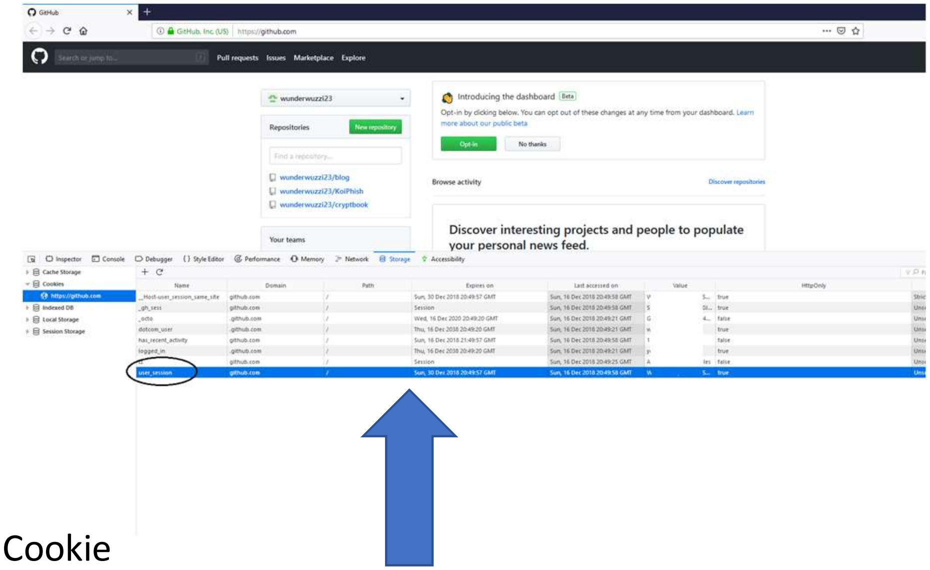
Make sure it's more than 15 characters OR at least 8 characters including a number and a lowercase letter. Read our documentation on safer password practices.

Sign up for GitHub

Name	Domain	Path	Expires on	Last accessed on	Value	HttpOnly	sameSite

ta present for selected host

(3) Refresh => Authenticated!



GitHub

GitHub, Inc. (US) | https://github.com

Search or jump to... Pull requests Issues Marketplace Explore

wunderwuzzi23

Repositories — New repository

Find a repository...

- wunderwuzzi23/blog
- wunderwuzzi23/KoiPhish
- wunderwuzzi23/cryptbook

Your teams

Introducing the dashboard Beta

Opt-in by clicking below. You can opt out of these changes at any time from your dashboard. Learn more about our public beta

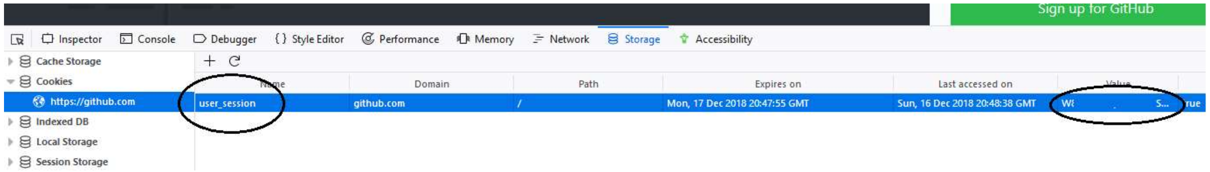
Opt-in | No thanks

Browse activity — Discover repositories

Discover interesting projects and people to populate your personal news feed.

Name	Domain	Path	Expires on	Last accessed on	Value	HttpOnly
__Host-user_session_same_site	github.com	/	Sun, 30 Dec 2018 20:49:57 GMT	Sun, 16 Dec 2018 20:49:58 GMT	V S...	true
_gh_sess	github.com	/	Session	Sun, 16 Dec 2018 20:49:58 GMT	S Dl...	true
_octo	.github.com	/	Wed, 16 Dec 2020 20:49:20 GMT	Sun, 16 Dec 2018 20:49:21 GMT	G 4...	false
dotcom_user	.github.com	/	Thu, 16 Dec 2038 20:49:20 GMT	Sun, 16 Dec 2018 20:49:21 GMT	w	true
has_recent_activity	github.com	/	Sun, 16 Dec 2018 21:49:57 GMT	Sun, 16 Dec 2018 20:49:58 GMT	1	false
logged_in	.github.com	/	Thu, 16 Dec 2038 20:49:20 GMT	Sun, 16 Dec 2018 20:49:21 GMT	y	true
[illegible]	github.com	/	Session	Sun, 16 Dec 2018 20:49:25 GMT	A les	false
user_session	github.com	/	Sun, 30 Dec 2018 20:49:57 GMT	Sun, 16 Dec 2018 20:49:58 GMT	W S...	true

(2) Pass the Cookie



Sign up for GitHub

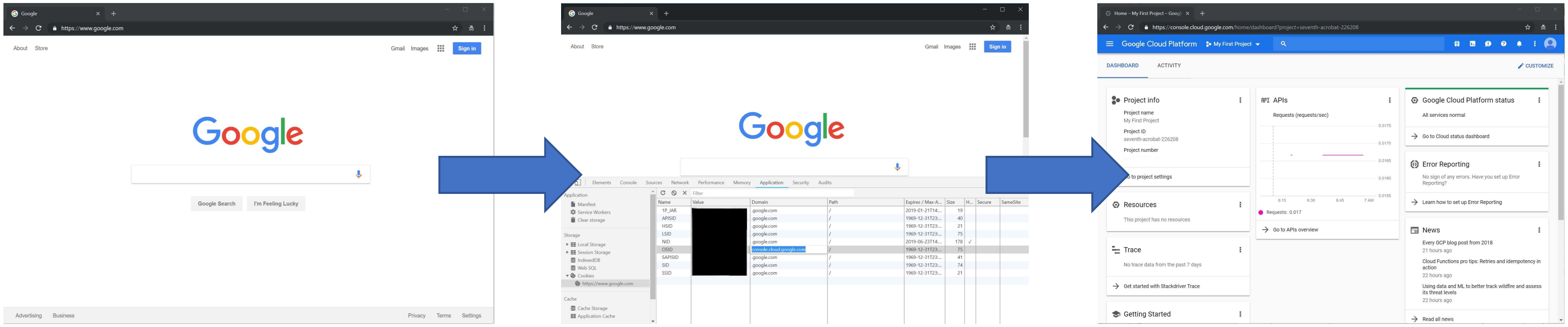
Name	Domain	Path	Expires on	Last accessed on	Value	
user_session	github.com	/	Mon, 17 Dec 2018 20:47:55 GMT	Sun, 16 Dec 2018 20:48:38 GMT	Wl . S...	rue

Disclaimer: Always make sure you have proper authorization before pen testing.

Anatomy of a Cloud Breach

A cookie might be the single key to your companies “virtual datacenter”.

- Attacker stole cookies of a GCP user.
- Navigates to root domain. Observe that we are unauthenticated.
- Pass the Cookies using the browser user interface
- Refresh the browser and observe being logged in, then browse to GCP.



https://www.google.com

Name	Value	Domain	Path	Expires / Max-A...	Size	H...	Secure	SameSite
1P_JAR	[redacted]	.google.com	/	2019-01-21T14:...	19			
APISID	[redacted]	.google.com	/	1969-12-31T23:...	40			
HSID	[redacted]	.google.com	/	1969-12-31T23:...	21			
LSID	[redacted]	.google.com	/	1969-12-31T23:...	75			
NID	[redacted]	.google.com	/	2019-06-23T14:...	178	✓		
OSID	[redacted]	console.cloud.google.com	/	1969-12-31T23:...	75			
SAPISID	[redacted]	.google.com	/	1969-12-31T23:...	41			
SID	[redacted]	.google.com	/	1969-12-31T23:...	74			
SSID	[redacted]	.google.com	/	1969-12-31T23:...	21			

https://console.cloud.google.com/home/dashboard?project=seventh-acrobat-226208

Project name: My First Project

Project ID: seventh-acrobat-226208

Project number

Home – My First Project – Googl
Google Cloud Platform
My First Project
DASHBOARD
ACTIVITY
CUSTOMIZE
Project info
to project settings
Resources
This project has no resources
Trace
No trace data from the past 7 days
Get started with Stackdriver Trace
Getting Started
APIs
Requests (requests/sec)
0.0175
0.0170
0.0165
0.0160
0.0155
6:15
6:30
6:45
7 AM
Requests: 0.017
Go to APIs overview
Google Cloud Platform status
All services normal
Go to Cloud status dashboard
Error Reporting
No sign of any errors. Have you set up Error Reporting?
Learn how to set up Error Reporting
News
Every GCP blog post from 2018
21 hours ago
Cloud Functions pro tips: Retries and idempotency in action
22 hours ago
Using data and ML to better track wildfire and assess its threat levels
22 hours ago
Read all news

Disclaimer: Always make sure you have proper authorization before pen testing.

Pass the Cookie - Cheat Sheet

Application	Cookie Name	Domain	Notes
Amazon Web Services	aws-userInfo aws-creds	.amazon.com	https://console.aws.amazon.com
Google Cloud Platform	OSID, HSID, SID, SSID APISID, SAPISID, LSID	.google.com	https://console.cloud.google.com Set OSID on console.cloud.google.com, Others on .google.com
Microsoft Online	ESTSAUTHPERSISTENT	.microsoftonline.com	
Facebook for Work	c_user xs	.facebook.com	Also works for regular Facebook
OneLogin	sub_session_onelogin.com	.onelogin.com	
GitHub	user_session	.github.com	
Hotmail, Calendar	RPSSecAuth	.live.com	
Gmail	OSID, HSID, SID, SSID APISID, SAPISID, LSID	.google.com	https://mail.google.com For basic mail first 4 are enough.

https://wunderwuzzi23.github.io/blog/passthecookie.html#CheatSheet

Disclaimer: Always make sure you have proper authorization before pen testing.

Detections

When it comes to detections a few things come to mind:

- Monitor for **applications that perform process dumps**
- Monitor for **access anomalies of cookie storage locations, databases,**..
- Monitor for **unusual activity on critical web assets** (like cloud provider management consoles, etc,…)
- Monitor for **login anomalies** (location, time, unusual access patterns)
- **Leverage features that cloud providers offer**! (Threat Detection,...)
- **Perform adversarial emulations in your organization to test detection capabilities**.
- …

Mitigations

- **Regularly delete cookies**, so they get removed from your machine
- Delete session cookies as well
- **Be the only Administrator on your own machine**
- **Browse sensitive/high value sites from isolated machines**
  - ➢Accessing your companies AWS account with admin privileges from a regular dev box is not a good idea
  - ➢Don’t use your work computer for personal things (do you trust your Administrators)
- **Separation of duties.**
- **Leverage features that cloud providers offer**! (IAM, RBAC, Firewall, Threat Detection,…)
- Require further authentication proof for sensitive operations
- Requiring client side certificates makes it more difficult to pass the cookie

Thanks!

Contact

wunderwuzzi23@outlook.com

Relevant Resources:

- https://wunderwuzzi23.github.io/blog/passthecookie.html
- https://www.owasp.org/index.php/Session_hijacking_attack