ABUSING FACEBOOK AND GOOGLE LOGIN

RISKS IN TRUSTING SOCIAL LOGINS

IDO SAFRUTI
PERIMETERX

TOMER COHEN
WIX.COM
ABOUT THE SPEAKERS

Ido Safruti
CTO
perimeterx
@safruti

Tomer Cohen
R&D Security Team Leader
WIX.com
HOW IT ALL STARTED
Sign-up Rate
WHY USE SOCIAL LOGIN
Users like it

- 77% prefer social login*
- Easy
- No passwords
- My details in one trusted place
- Control access level for each app

* WebHostingBuzz 2013
Sites like it

- (Happy users)
- Verified user’s identity
- Easy to implement
- conversions ++
- Simplify registration

**More secure**
- Trust the biggest
- No need to store user’s private data and passwords
- No need to worry about bots and fake accounts (Brute-force / Account creation)
Why we use it
Trust by Proxy

Google
facebook
twitter
GitHub
LinkedIn

SEAL
OF APPROVAL
Login / Authentication

Human or Bot?
So actually...
Account Creation

Unknown time in the past!

Timeline

- LinkedIn
- Google+ (Google)
- Facebook
- Twitter

BIG BANG

O'REILLY' Your Account
And once again...

Human or Bot?
So actually...
WHAT YOU DON’T GET WITH SOCIAL LOGIN

- Secure for the user
- Does not protect the site from compromised users, and automated attacks
- Human verification on creation of social account
  - Create account on your site == social login
DEMO: ABUSING SOCIAL LOGIN:

Use Chrome extension to create account on a 3rd party (uncontrolled) site
Create account with Facebook login

Process user’s parameters

GET access to app

POST grant access

Access to app granted!
Create account with Facebook login

Process user's parameters

Access to app granted!
Create account with Google login

GET access to app in a new tab

Click “Approve access”

Access to app granted!

** for multiple accounts
select an account first...
Create account with Google login

** for multiple accounts select an account first...
Is it a vulnerability!?

“This is a feature that has to do with your browser and is therefore not under Facebook's control. Additionally, exploiting this issue would require physical access and/or heavy social engineering.”

In general all the functionality you describe is functionally allowed in an extension, though it may be against the Chrome Webstore policy and should be removed from there.
CASE STUDY: BOT DISTRIBUTION USING SOCIAL LOGIN
April 2016
Descubre quienes son los que más visitan tu Facebook

¿Cómo funciona?
Usamos una extensión para obetener información sobre las visitas hacia tu perfil, luego la recopilamos mostrándote quienes son los que más han ingresado a tu perfil.

Comenzar

53.169 Personas ya lo han hecho

¿Cuál es el significado de tu nombre? CLICK
Find out who are the most visited your facebook

How does it work?
We use an extension for obtener information about visits to your profile, then collect showing you who are the ones who have entered your profile.

Start

53,169 people already have made

What is the meaning of your name? CLICK
Viad30 Unlocker

Apparemment proposé par Mario Gospartini

Étoiles: 4.5 / 5 (1 avis)

Réseaux sociaux et communication
177 utilisateurs

PRÉSENTATION   AVIS   ASSISTANCE   ARTICLES SIMILAIRES

Compatibilité avec votre appareil

Permet de profiter des avantages d'un compte Viadeo premium

[UPDATE]

* Pop-up qui permet d'activer ou de désactiver la fonctionnalité.
* Accéder directement à la page des visites.
* Faire des recherches rapides
* Mise à jour automatique
* Envoyer des messages à tous les membres

[IMPORTANT]

Signalé un abus

Informations sur la diffusion
Extension-Bot course of action

Inject Code
- To Facebook tabs

Open Wix Frame
- Inside a Facebook page

Sign-up To Wix
- Bypassing bot detection

Publish a New Wix Site
- Redirecting to attack page

Distribute Link
- Among all Facebook friends

Review Extension
- In Google Web Store
Bot Protection? ANYONE??

WHAT THE HELL IS GOING ON HERE?

Google

facebook

Wix.com
"description": "Permet de profiter des avantages d'un compte viadeo premium",
.... },
"manifest_version": 2,
"name": "Viad30 Unlocker",
"permissions": [
  "tabs",
... "http://*/*",
  "https://*/*",
  "cookies",
],
"version": "3.4",
"content_security_policy": "script-src 'self' 'unsafe-eval'; object-src 'self'"}
A Bot’s Life
April 2016

June 2016
Facebook “Tag Me If You Can” Attack

Don't click on that Facebook notification - it could be a VIRUS

NEW malware tags victims in random Facebook comments and status updates from your friends, then infects devices with damaging results.

By MICHAEL MOORE

Facebook 'Comment Tagging Malware' Spreading via Google Chrome

If you receive a Facebook notification regarding a friend tagging you in a comment, be very careful before clicking on the link. It can be a JavaScript malware found targeting users lately!
Facebook “Tag Me If You Can” Attack

Credits: “Facebook Malware – The Missing Piece”, Kaspersky Labs
Who is protecting YOUR site?
Summary

• Social login is great

• Doesn’t work securely out of the box!
  • Secure for the user **
  • Requires careful implementation for your site

• Bot protection is not provided by social login

• Credentials of a human != human
Recommendations

• Track Login / Sign-up rate anomalies

• Watch for weird “origin” and “referer” headers

• Prevent forms from loading inside frames:
  • Use X-FRAME-OPTIONS header
  • Compare top and self
You don’t have to run faster than the bear to get away. You just have to run faster than the guy next to you.

- Jim Butcher -
THANK YOU!

QUESTIONS?

IDO SAFRUTI
PERIMETERX
ido@perimeterx.com
@safruti

TOMER COHEN
WIX.COM
tomerc@wix.com