Facebook API Breach

Jake Williams (@MalwareJake)
Rendition Infosec
www.rsec.us
@RenditionSec

RENDITION INFOSEC
Cybersecurity by any legal means

Facebook “View As”

- Facebook allows users/developers to see what a profile page looks like from another user’s perspective

How can I see what my profile looks like to other people?

Computer Help Mobile Help Share Article

You can see what your profile looks like to other people by using the **View As** tool.

To use **View As**:

1. Go to your profile and click ••• to the bottom right corner of your cover photo.
2. Click **View As...** in the dropdown menu.
3. You’ll see what your profile looks to the public. To see how your profile appears to a specific person, like a friend or coworker, click **View as Specific Person**, type their name and press enter.

To exit **View As**, click **X** on the banner.

Bug #1 - “View As” must remain “View Only”

- Most features in “View As” mode were actually view only

- One feature that allows users to wish each other “happy birthday” allowed posting of videos while in “View As” mode

> **First:** View As is a privacy feature that lets people see what their own profile looks like to someone else. View As should be a view-only interface. However, for one type of composer (the box that lets you post content to Facebook) — specifically the version that enables people to wish their friends happy birthday — View As incorrectly provided the opportunity to post a video.

Bug #2 – Video uploader access token too privileged

- In order to perform any action on the site, Facebook must first check your access token
- Access tokens should be limited in privilege to prevent abuse
- The access token for the video uploader was significantly overly privileged, giving the token holder full privileges of the Facebook mobile application

Second: A new version of our video uploader (the interface that would be presented as a result of the first bug), introduced in July 2017, incorrectly generated an access token that had the permissions of the Facebook mobile app.

Bug #3 – Video uploader returns the wrong token

- While operating in “View As” mode, the video uploader returned the access token of the user you are impersonating

- The result of this is that attackers who steal the user’s access token can perform any action that the real user can perform through the Facebook mobile application (e.g. almost anything)

> **Third**: When the video uploader appeared as part of View As, it generated the access token not for you as the viewer, but for the user that you were looking up.

Death by a thousand (really three) paper cuts

- Each of these bugs would have been significant on its own
- Combined together, they offered the ability to compromise the account of anyone in your friends list
- Using the stolen access tokens, attackers can pivot to all of their friends, and repeat recursively

Multiple bugs together?! Is this new?

- Using multiple, less consequential bugs together to achieve an impact is not new
- Vulnerability researchers call this exploit chaining
- With exploit chaining, attackers most often use an information disclosure vulnerability (e.g. the access token) in combination with some other flaw to achieve a goal

Third Party Sites

- Third party sites and applications can use Facebook's authentication services instead of building their own proprietary systems

- Once an attacker compromises the access token for a user account, the attacker can impersonate the user on any site or application where the user has authorized Facebook to log in

Can attackers get my password?

- Short answer: No
- Longer answer: Maybe, it depends

- Because of Facebook's security architecture, attackers can't get your password just by having an access token

- Facebook has long contended that it doesn't store plaintext passwords in its systems in any case

Can attackers get my password? (2)

- Third party sites and applications that integrate with Facebook for authentication may not have the same security models
  - Poor security architecture, limited permission boundaries, or bugs may allow attackers to steal much more sensitive information from third party sites using access tokens stolen from Facebook

- The total exposure of this vulnerability is a known unknown
  - We are unlikely to ever know the full potential damage caused by the ~50 million stolen access tokens

How is Facebook investigating this?

- The errant features appear to have been introduced in July 2017
- Depending on the amount of logging data available, there may be no way to track the issue back to the source
  - Facebook has not disclosed the quantity and types of logs available
- Remember that multiple attackers may have independently discovered the same bug

API Logging

- If Facebook has the appropriate logging, they can track where a user's access token was used from and when

- Even if the attacker(s) changed IP addresses frequently while compromising the ~50 million accounts, it is highly unlikely that the stolen attackers consistently used IP addresses in the range that the legitimate users would have

Wait, does everything log?

- According to some recent academic research, probably not
  - https://www.cs.uic.edu/~polakis/papers/sso-usenix18.pdf

- Researchers discovered that when using stolen access tokens (referred to as cookies in their research), logging didn't occur unless the session duration was longer than one hour.

> However during our experiments with hijacked cookies we found that no alert is sent to the victim, and *the attacker's session will not show up in the list* unless its duration exceeds one hour. Thus, in practice the victim will never become aware of an attack taking place.

Data available from a stolen access token

Service	Platforms	Attacker	Access	Password	Email	Messages	Locations	Purchases	User Info	Notes
Tinder	iOS	●	full			✓	N/A	N/A	N/A	Messages remain unread when read by the attacker.
InstaMessage	iOS	●	full			✗	N/A	N/A	✓	Does not support simultaneous access from two devices.
Skout	iOS	●	full			✓	N/A	N/A	✓	View favorite users who the victim swiped right.
Hookup	iOS	●⊛	full			✓	✓	N/A	✓	Found workaround for full access via hijacked cookie.
Ovia	iOS	⊛	full			✓	✓	N/A	✓	Pregnancy/health information. Requires IdP password.
Tripadvisor	iOS	●⊛	full		★	✓	✓	✓	✓	Workaround for full access in iOS: re-login using cookie.
Booking.com	iOS | web | Android	●	full		★	N/A	✓	✓	✓	Susceptible to account combination attack.
Foursquare	iOS	●	full		★†	N/A	✓	N/A	✓	Check-in history.
Yelp	iOS	●	full	†		✓	✓	N/A	✓	Check-ins, purchases, saved locations (e.g., home addr.).
Airbnb	iOS	●	full			✓	✓	✓	✓	Access to trip, reservation, and transaction history.
Expedia	iOS	●	full		★	N/A	✓	✓	✓	Passport number, TSA info, flight preferences, payments.
Kayak	iOS	●⊛	partial			N/A	N/A	✓	✓	Email set via SSO; modifiable in IdP until password is set.
Zillow	iOS | web	●	full		★	N/A	✓	N/A	✓	Credit score, home address. Creating password does not require authentication but sends notification.
Uber	iOS	●	full			N/A	✓	✓	✓	Real-time tracking. Email added w/o authentication.
Goodreads	iOS | web	●⊛	full		★	✓	✓	✓	✓	Zip code, DOB. Workaround bypasses RP's password.
ASOS	iOS | web	●	full	★†	★†	N/A	✓	✓	✓	DOB, home address, payment info, orders.

Data available from a stolen access token

Service	Platforms	Attacker	Access	Password	Email	Messages	Locations	Purchases	User Info	Notes
Quora	iOS | web | Android	●	full			✓	N/A	N/A	N/A	Access to private messages.
Shein	iOS	●	full			N/A	✓	✓	✓	Body measurements, orders, payment options, home address. SSO users can not set password.
Teepr Deals	web	●	full	★†	★†	N/A	✓	✓	✓	Access to recent purchases and credits.
Zoosk	iOS	●	full	†	★†	✓	N/A	✓	✓	Phone number, payments. Password reset via attacker's email.
800 Contacts	iOS | web	⊛	full			N/A	N/A	✓	N/A	Requires IdP password.
IMDB	iOS | web	●	full		★	N/A	N/A	N/A	✓	DOB, zipcode, browsing history.
Mediafire	iOS | web	●	full			N/A	N/A	✓	✓	DOB, zipcode. Access to photos and videos. Email only set via SSO and modifiable until the password is set.
4shared	iOS | web	●⊛	full		†	N/A	N/A	N/A	N/A	Cookie does not work in iOS. Access to photos and videos. IdP password required for full access in iOS.
Pinterest	iOS | web	●	full	†	★	✓	✓	✓	N/A	Creating password does not send notification.
The Guardian	iOS | web	●⊛	partial	†	★†	N/A	✓	✓	✓	Creating password does not require authentication and can bypass IdP password requirement.
WashingtonPost	iOS | web	●	full	†		N/A	✓	✓	✓	Email set via SSO. No notification for password creation.

What Facebook hasn't said (yet)

1. How far back do their logs go for access token use?
2. Which 3rd party apps do and do not regularly check for token validity?
3. What would evidence of misuse of access tokens look like? What are they checking?

These aren't just academic questions – answers to these will influence how people update their threat models

Questions?