

Journey to the top on



The untold tales of struggle and pain



- Ahmad Ashraff @yappare
- Origin : Malaysia
- Education : Bachelor of Chemical Engineering
- Experience : +7 years in ITSec industry
- Current : Security Consultant at Aura Information Security
- Hobbies : Backpacking, Watching Animes



About Me



67,100+

Strong researcher community

96

Countries with Bugcrowd researchers

JOIN THE COMMUNITY



yappare

New Zealand

Skiddies. 🐼

ID Verified

Background Checked

All time points

8,558

Current rank

2

About the Presentation

- What is bug bounty program
- Why I started bug hunting
- Problems and troubles – How I encountered them
- Tips and Tricks
- Hope people stop asking me “How many bugs did you found last weekend?”

What is bug bounty program?

A reward offered to a person who identifies an error or vulnerability in a computer program or system.

https://en.oxforddictionaries.com/definition/bug_bounty

How companies manage bug bounty programs

Own programs

- Own platform
- Mature in process
- Great pool of budgets
- Expert security engineers



Self-manage via 3rd party platform

- Standard set by own orgs
- Manage by own team
- Risk/Reward decided by themselves
- Miscommunication can happen



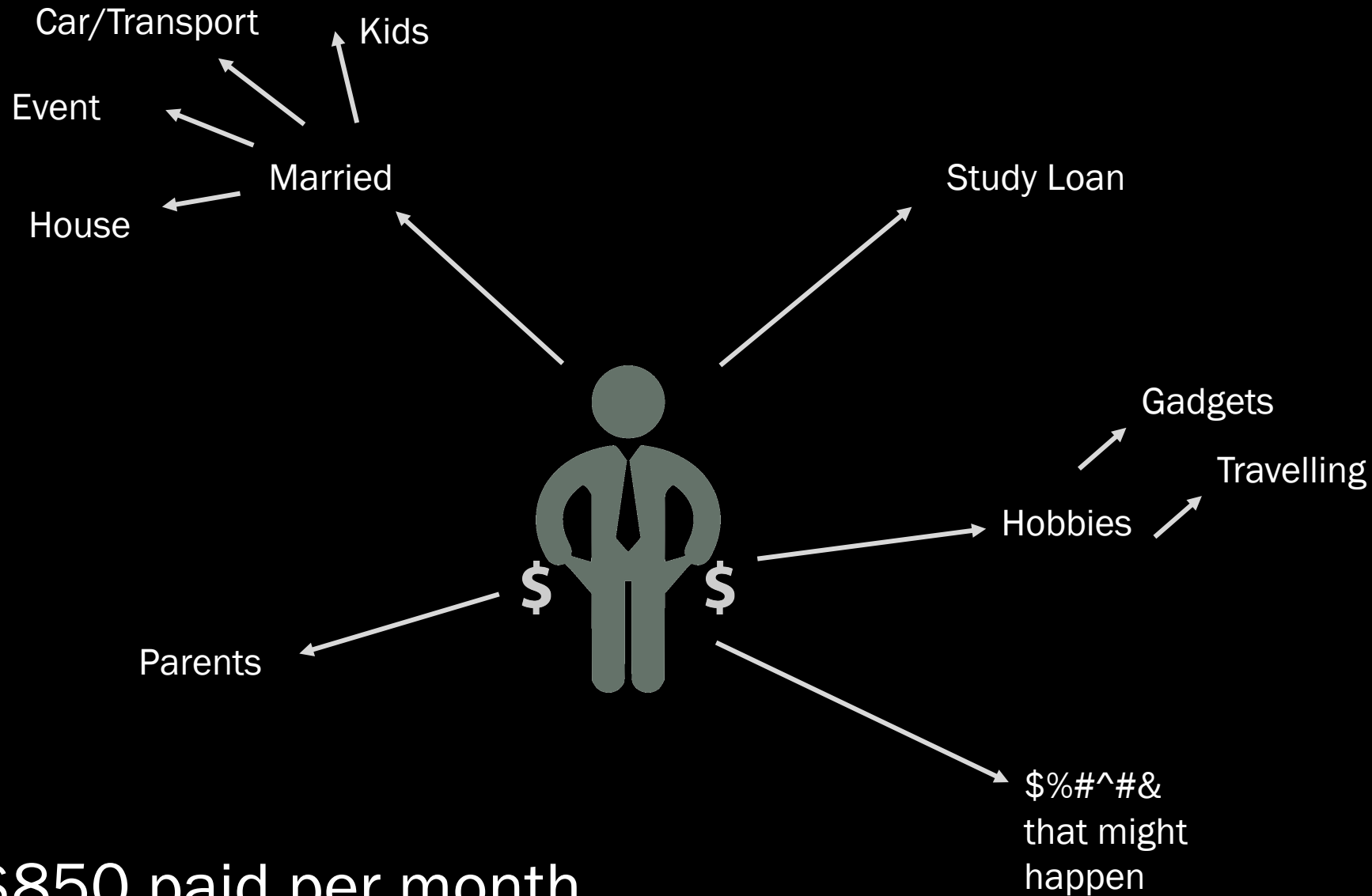
Managed by 3rd platform

- Platform's analyst act as a middle person
- Most of orgs follow the standard provided
- Platform analysts have knowledge

bugcrowd



Why I Started Bug Bounty?



~\$850 paid per month

xss in paypal-shopping.co.uk

Bounty/Paypal x



ahmad

to sitesecurity

attached the POC and my details :)

3rd August 2012



4 months later



PayPal Inc sent you \$500.00 USD

Dear [redacted]

Just thought you'd like to know PayPal Inc sent you \$500.00 USD.

Note from sender, PayPal Inc:

'PayPal Bug Bounty'

1 XSS – Found in less than a day = \$500

Monthly paid = ~\$850

1 XSS in Paypal > Half of monthly paid





Study Loans
Personal Loans
Cars
Credit Cards

»	Bounty/Paypal	PayPal Inc sent you \$250.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$625.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$250.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$375.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$1,975.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$250.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$125.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$50.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$250.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$5,000.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$500.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$250.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$50.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$250.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$500.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$1,500.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$50.00 USD
»	Bounty/Paypal	PayPal Inc sent you \$500.00 USD

11/4/14

5/2/14

5/2/14

8/31/13

6/21/13

4/27/13

4/12/13

4/12/13

4/12/13

4/12/13

3/27/13

3/27/13

3/27/13

3/12/13

2/26/13

2/2/13

1/5/13

12/8/12

It is not just about money

- More knowledge/sharing from other experts
- New techniques
- Better profile
- I'm still at a beginner level

Hi folks, meet...



29/11/17

Welcome to the Bugcrowd!

Inbox x

Bounty/Bugcrowd x



casey@bugcrowd.com via formstack.com

1/21/13



Reply



to me



English



Czech

[Translate message](#)

[Turn off for: English](#) x

Thank you!

You submission to join the Bugcrowd has been sent successfully.

Thanks, and welcome to the Bugcrowd! You will now receive notifications of new bug bounty programs to the email address you provided.

Please bear with our slightly clunky email/form-based systems for the time being... We are working away on a platform for managing our ninjas and bounty programs.

Cheers

@[caseyjohnellis](#) and @[sergicles](#) from @[bugcrowd](#)

ps We monitor all of our email addresses and would LOVE to hear from you. If you have comments/questions/concerns/suggestions send them on through.

CHCON 2017

2013!!

SO, ENOUGH PREAMBLE... PLEASE JOIN US IN CONGRATULATING OUR INAUGURAL BUGCROWD TOP 10 FOR 2013:

1. [@bitquark](#)
2. [@yappare](#)
3. [@cyberboy](#)
4. [@jhaddix](#)
5. [@pwndizzle](#)
6. [@eelsivart](#)
7. [@satishb3](#)
8. [@internetwache](#)
9. [@n0x00](#)
10. [@panchocosil](#)



Security at Tesla






Head of Trust and Security at Bugcrowd

Nice work ninjas! We tip our hats to you.

1st	 Private	1158
2nd	 karthickumar	1158
3rd	 baymax	1116

2015. 1st place. Looks good






Early 2016. Still hold the title.

1st	 yappare	2189
2nd	 Mico	1847
3rd	 Bitquark	1739

1st	 mongo	6266
2nd	 Harie_cool	3283
3rd	 Private	3080

Oct 2016 . Started to be a busy
guy. Lost from the radar.

2017!!

Leaderboard			
	SEPTEMBER	ALL TIME	
1st	 mongo	17505	
2nd	 yappare	8558	
3rd	 zseano	6217	
4th	 Private user	6169	
5th	 mert	5943	

← A wizard

← Normal human being

← Talented full-time bughunter from UK

← Anonymous

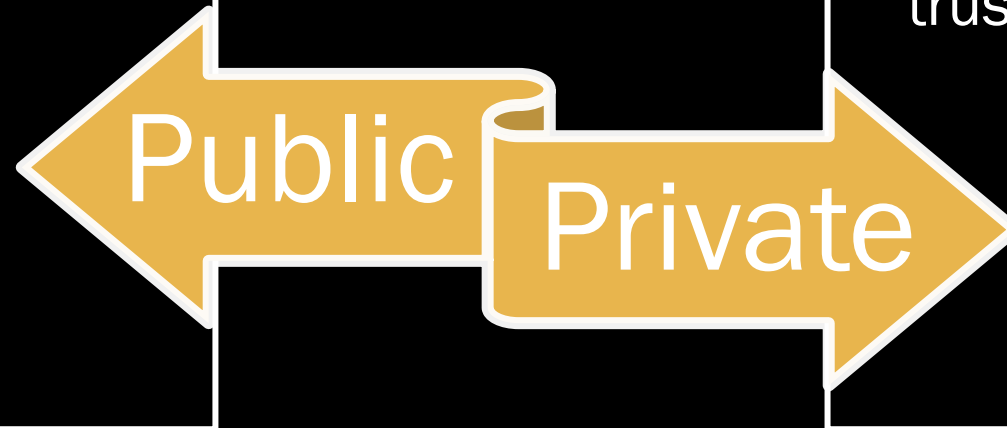
← Attack-dev

<https://bugcrowd.com/leaderboard>

Public VS Private Programs in Bugcrowd

- Can participate once registered
- Kudos/Rewards
- Tested multiple times
- Orgs ready to go to public
- Web,mobile,hardware,API, IOT

- Two types, ongoing & flex (on-demand)
- Kudos/Rewards
- Web,mobile,hardware,API, IOT
- Tested few times or fresh
- Orgs want to be tested by trusted users

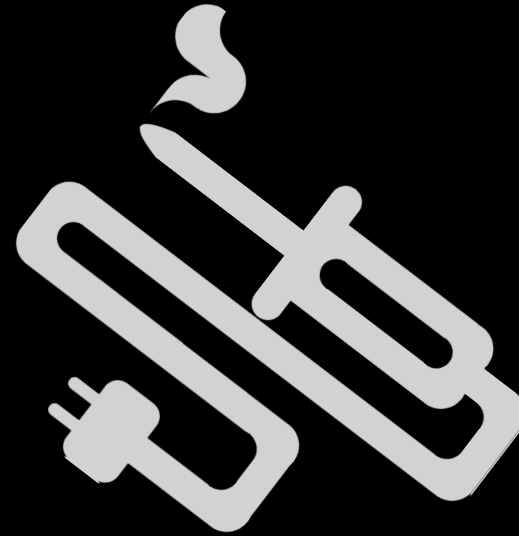
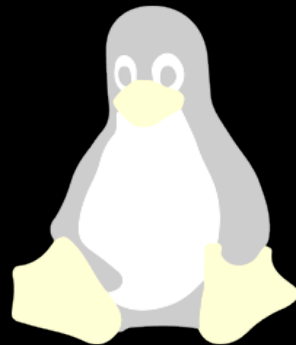
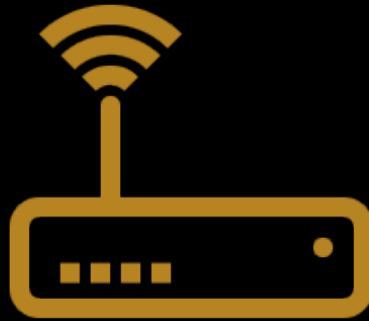
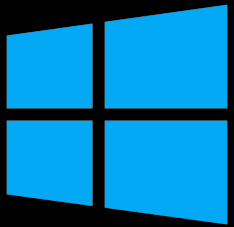




Problems..

Problems

Equipment and Tools



You have been invited to participate in a private
\$12,500.00 On-Demand Program!

15 researchers have been invited to a program starting
Tuesday, August 22 2017 at 16:00 UTC and ending
Tuesday, September 05 2017 at 16:00 UTC

- Tough competition. Experts everywhere
- Fast and Furious. Really fast. Need to avoid duplicate submission

Submission is a duplicate of:

Open Redirect [next] - <http://com/account/login>

Created 2017-08-22 16:04:39 UTC

8 5 MINUTES

ic

Submission is a duplicate of:

Stored XSS [chart_name] - charts

Created 2017-08-22 16:29:04 UTC

6! 30 MINUTES

9ca

Submission is a duplicate of:

Stored XSS [chart_description] - charts

Created 2017-08-22 16:55:54 UTC

55 MINUTES



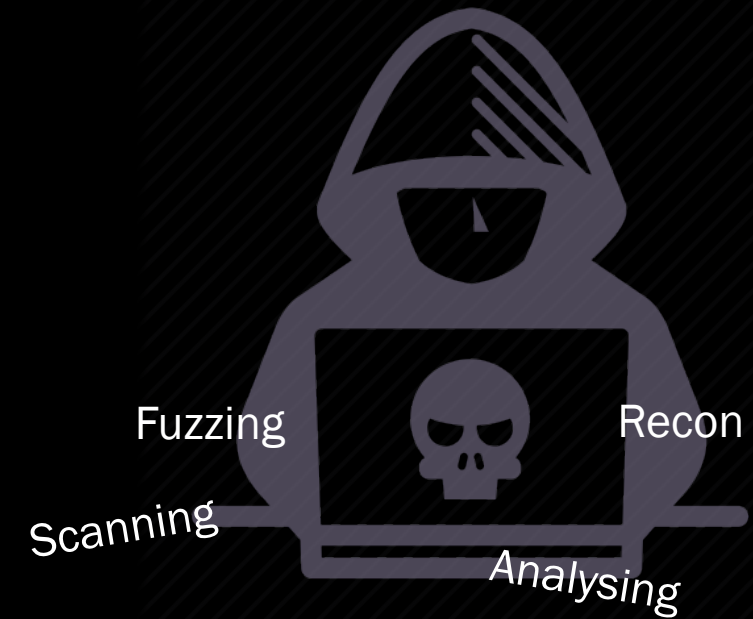
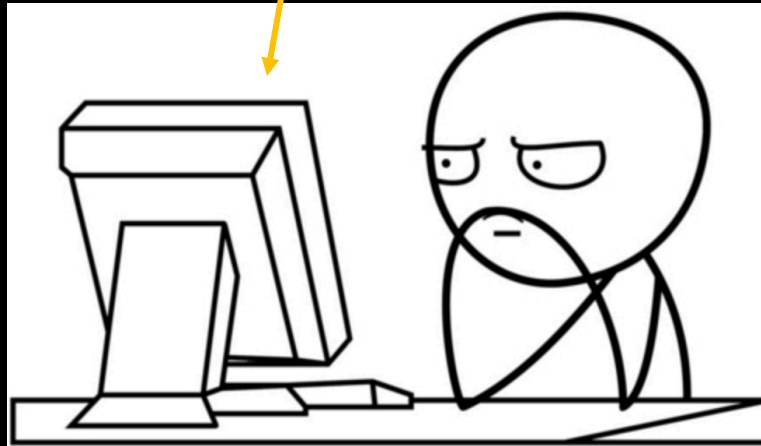
Problems

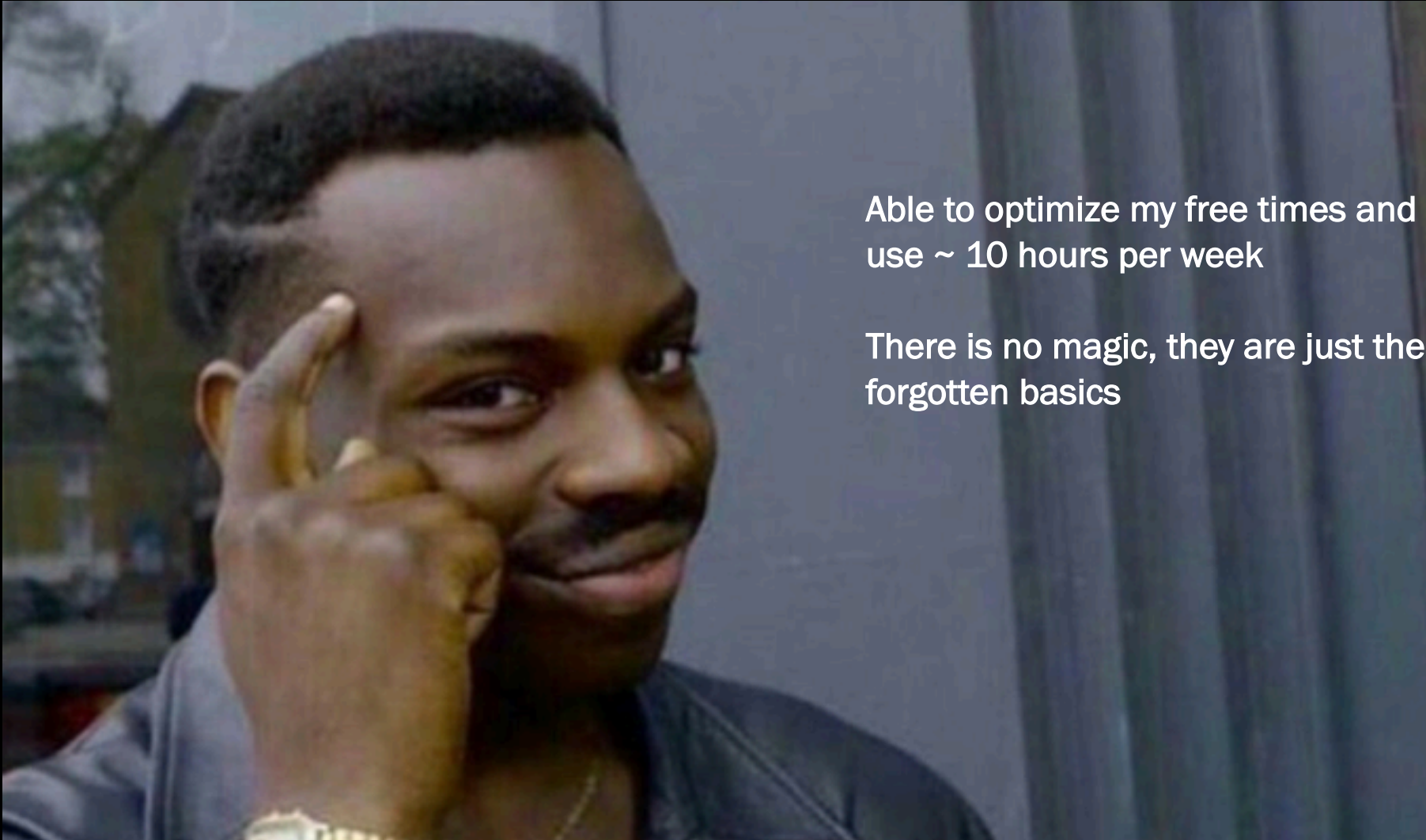
Most programs start at **UTC time zone**



Me in NZST.

At work. Doing host review



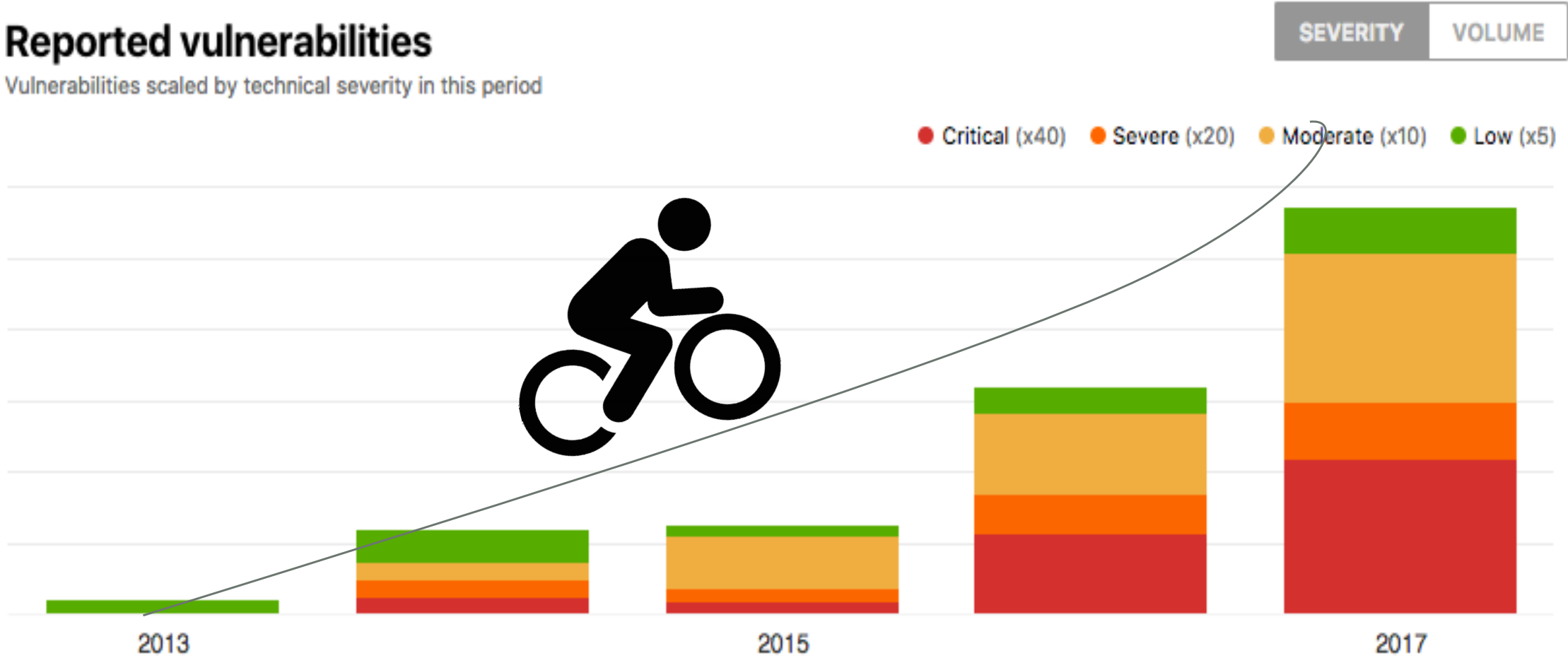


Able to optimize my free times and
use ~ 10 hours per week

There is no magic, they are just the
forgotten basics

Reported vulnerabilities

Vulnerabilities scaled by technical severity in this period



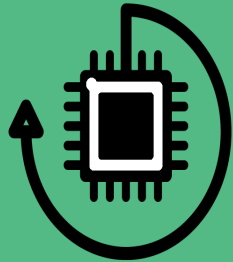
Tips 1 – Focus on less participants

29/11/17



Mobile Applications

- Windows < iOS < Android
- Cert Pinning



IoT/Device

- Specific device need to be purchased
- Need knowledge, tools



Scripts/Binary

- Dev knowledge, binary exploitation
- Fuzzing technique

Preparing
is a mess

CHCON 2017

Tips 1 – Focus on less participants



Reverse recon

Wide targets -
automated+manual

Old or No Reward
programs

Complex setup - AWS account,
premium, developer, OS
dependent

Reverse recon

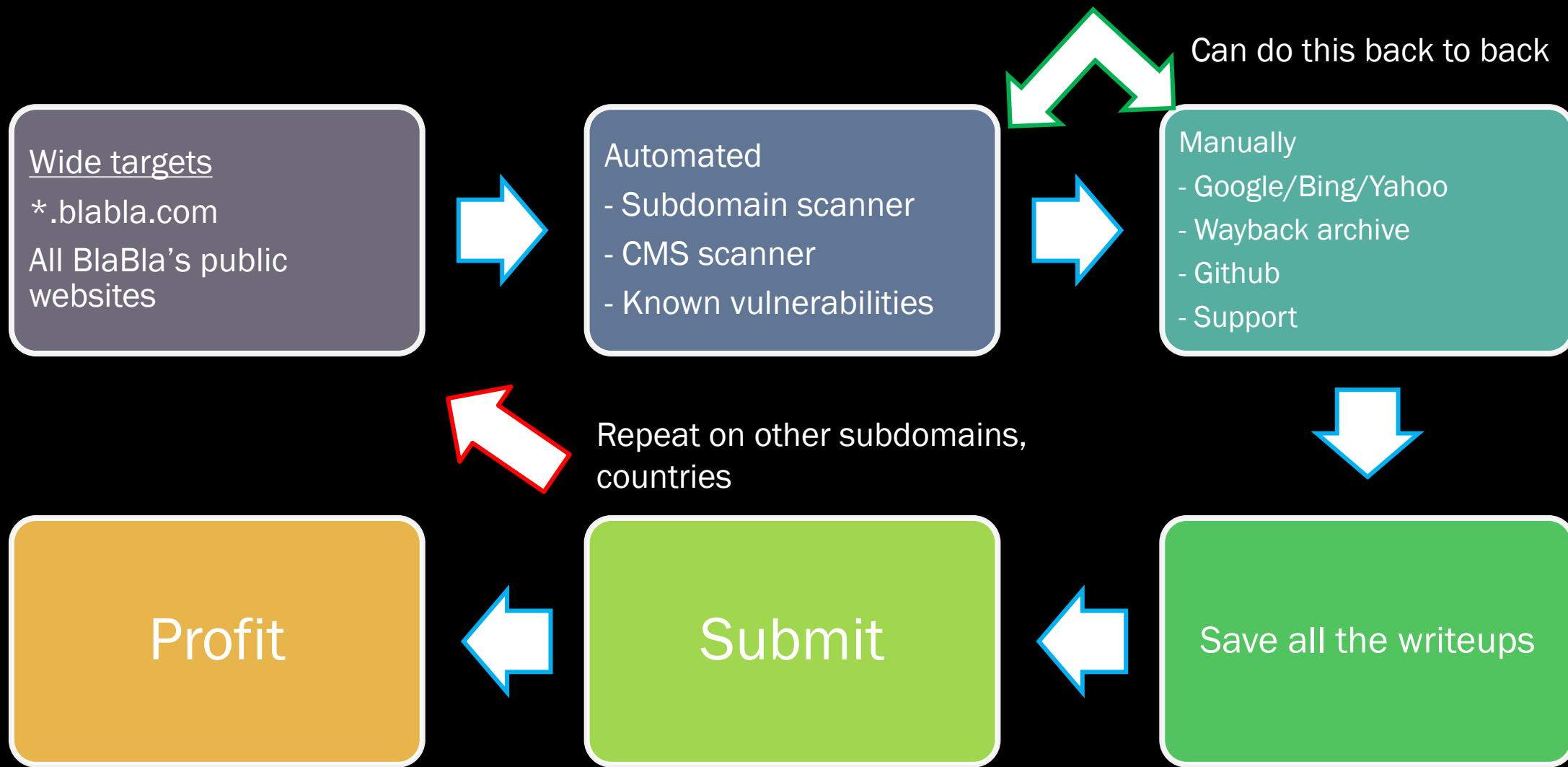
IF the provided in scope is/are **production sites**

- Check on their dev/staging/qa environment
- Check on their Github
- Check on their old sites through wayback archive

IF the provided in scope is/are **staging/testing/dev/qa** sites

- Check on their production environment
- Check on their old sites of the production through wayback archive
- Check on their support/issues website

Good in
discovery
path/modules/
features



AQUATONE



aquatone-discover

aquatone-takeover

aquatone-scan

aquatone-gather

- Threat Crowd.
- Certificate Search (crt.sh)
- Censys
- Shodan
- Riddler
- PassiveTotal
- Netcraft
- HackerTarget
- Google Transparency Report
- DNSDB
- VirusTotal
- Dictionary

Find misconfigured DNS setup

Port scan on common web server ports

Access the discovered web ports and provide headers information plus screenshot

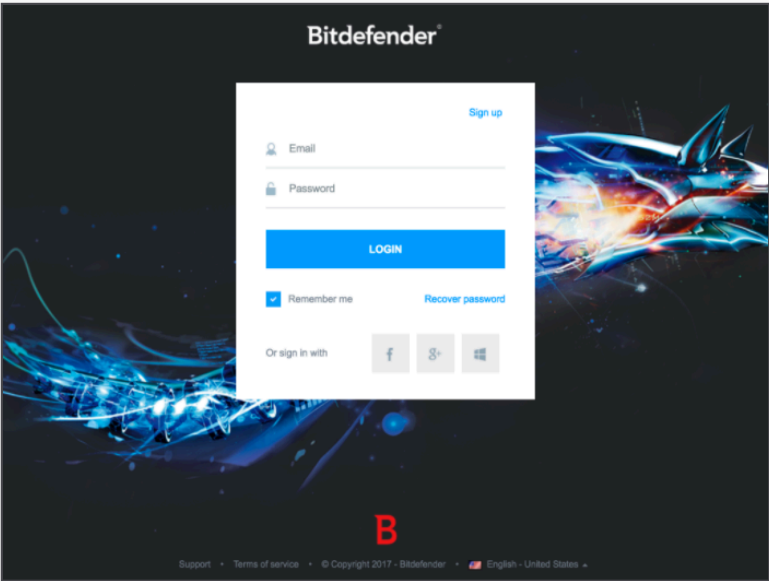
81.161.59.50	naas.bitdefender.net
50.97.42.198	ngx1.wdc1.vdc.bitdefender.net
88.198.155.42	ngx2.hzn.vdc.bitdefender.net
54.246.127.51	ngx2.irl.vdc.bitdefender.net
50.97.42.209	ngx2.wdc1.vdc.bitdefender.net
178.33.61.83	nimbus-db1.rb2.vdc.bitdefender.net
178.33.61.114	nimbus-ep1.rb2.vdc.bitdefender.net
178.33.60.188	nimbus-ep2.rb2.vdc.bitdefender.net
52.198.191.94	nimbus.bitdefender.net
81.161.59.54	nis.bitdefender.net
195.189.155.129	ns02.adn.buh.vdc.bitdefender.net
195.189.155.129	ns02.buh.bitdefender.net
81.161.59.33	oem-login.bitdefender.net
37.59.67.148	oem.rb2.ovh.vdc.bitdefender.net
37.59.67.148	oem.rb2.vdc.bitdefender.net
37.59.67.150	oemcloud.bitdefender.net
81.161.59.166	orangenimbus-02.bbu.gts.bitdefender.net
91.199.104.144	orangenimbus.bbu.dsd.bitdefender.net
91.199.104.143	orangesecurity.bbu.dsd.bitdefender.net

discovery

scanning

gathering

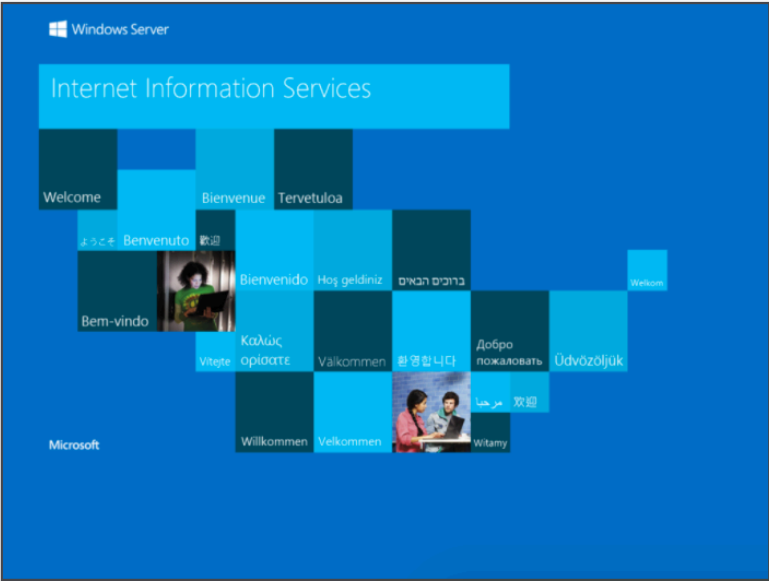
443/tcp	81.161.59.75	beta.mdm-ios.bitdefender.net
80/tcp	81.161.59.46	beta.nimbus.bitdefender.net
80/tcp	88.99.61.43	upgr-midgress-09.fra.htz.bitdefender.net
443/tcp	46.4.81.5	upgr-midgress-10.fra.htz.bitdefender.net
80/tcp	159.8.234.71	www-any.ams3.slr.bitdefender.net
443/tcp	37.59.67.146	cldmon.rb2.vdc.bitdefender.net, labs.rb2.ovh
80/tcp	88.198.13.39	upgr-midgress-02.fra.htz.bitdefender.net
443/tcp	136.243.104.171	0upmidg.cdn.bitdefender.net, upgr-midgress-14
80/tcp	54.89.56.163	csamazon.bitdefender.net
443/tcp	81.161.59.59	download.bitdefender.net, flow.bitdefender.net
443/tcp	88.99.61.43	upgr-midgress-09.fra.htz.bitdefender.net
80/tcp	195.189.155.159	myacc.bbu.gts.bitdefender.net
443/tcp	52.198.191.94	nimbus.bitdefender.net
80/tcp	52.214.200.142	hq.nimbus.bitdefender.net
443/tcp	78.46.80.140	upgr-midgress-11.fra.htz.bitdefender.net
80/tcp	81.161.59.75	beta.mdm-ios.bitdefender.net
80/tcp	81.161.59.50	naas.bitdefender.net
443/tcp	35.156.23.48	elb-fra-amz.nimbus.bitdefender.net



<http://forum.rbx2.vdc.bitdefender.net/>

[source code](#) | [headers](#) | [screenshot](#)

200 OK	
Cf-Ray	39cc1fd55eed1914-AKL
Content-Length	188
Content-Type	text/html
Date	Mon, 11 Sep 2017 16:50:09 GMT
Server	cloudflare-nginx
Set-Cookie	__cfduid=d8af4b5d1d68d4d9878656a9630ba4af21505148
Status	200
Strict-Transport-Security	max-age=63072000; includeSubdomains; preload
X-Content-Type-Options	nosniff
X-Frame-Options	SAMEORIGIN



<https://hive1.wdc1.vdc.bitdefender.net/>

[source code](#) | [headers](#) | [screenshot](#)

200 OK	
Accept-Ranges	bytes
Content-Length	701
Content-Type	text/html
Date	Mon, 11 Sep 2017 16:48:40 GMT
Etag	"3f89ba42ebcbd11:0"
Last-Modified	Tue, 21 Jun 2016 18:32:26 GMT
Server	Microsoft-IIS/8.5

Tips 2 – Risk Matrix Used

P1 – 40 points + \$1500

P2 – 20 points + \$900

P3 – 10 points + \$300

P4 – 10 points + \$100

P5 – 0 points + \$0



Bugcrowd's Vulnerability Rating Taxonomy

Bugcrowd's VRT is a resource outlining Bugcrowd's baseline priority rating, including certain edge cases, for vulnerabilities that we often see.

P1	Insecure OS/Firmware	Hardcoded Password	Privileged User	
P1	Broken Cryptography	Cryptographic Flaw	Incorrect Usage	
P2	Server Security Misconfiguration	Using Default Credentials	Staging/Development Server	
P2	Server Security Misconfiguration	Misconfigured DNS	Subdomain Takeover	
P2	Cross-Site Scripting (XSS)	Stored	Non-Admin to Anyone	Cool bugs
P2	Missing Function Level Access Control	Server-Side Request Forgery (SSRF)	Internal	
P2	Cross-Site Request Forgery (CSRF)	Applicaton-Wide		
P2	Application-Level Denial-of-Service (DoS)	Critical Impact and/or Easy Difficulty		Not so-cool bugs
P2	Insecure OS/Firmware	Hardcoded Password	Non-Privileged User	
P3	Server Security Misconfiguration	Mail Server Misconfiguration	Missing SPF on Email Domain	Not so-cool bugs
P3	Server Security Misconfiguration	Mail Server Misconfiguration	Email Spoofable Via Third-Party API Misconfiguration	
P3	Server Security Misconfiguration	No Rate Limiting on Form	Login	
P3	Server-Side Injection	HTTP Response Manipulation	Response Splitting (CRLF)	
P3	Server-Side Injection	Content Spoofing	iframe Injection	
P3	Broken Authentication and Session Management	Weak Login Function	Over HTTP	
P3	Broken Authentication and Session Management	Session Fixation		
P3	Sensitive Data Exposure	EXIF Geolocation Data Not Stripped From Uploaded Images	Automatic User Enumeration	
P3	Cross-Site Scripting (XSS)	Stored	Admin to Anyone	Cool bugs
P3	Cross-Site Scripting (XSS)	Reflected	Non-Self	

Cleartext Password Submission at http://www

Updated 13 days ago • 5 Comments

ost

Resolved

10 points

Cleartext Password Submission at http://

Updated 4 months ago • 0 Comments

Unresolved

10 points

Cleartext Password Submission at http://

Updated 3 months ago • 0 Comments

n.php

Unresolved

10 points

Still a P3 risk.
Still received the same points

Cleartext Password Submission at

Updated a month ago • 0 Comments

Unresolved

10 points

Cleartext Password SUBmission at http://wwwdev.

Updated 5 days ago • 1 Comment

do

Unresolved

10 points

Cleartext password submission at http://www.

Updated 4 days ago • 0 Comments

Unresolved

10 points



Lack of Bruteforce Protection on Login Page at

Unresolved

\$300 & 10 points

Updated 3 months ago • 2 Comments

No Rate Limiting on Admin's Login page at https://b.../logon.aspx

Unresolved

\$300 & 10 points

Updated 7 months ago • 0 Comments

Lack of Password Rate Limiting on Server's Administrator Login at https://...

Unresolved

10 points

Updated 17 days ago • 0 Comments

Lack of Rate Limiting in Request for Quote

Unresolved

\$154.63 & 5 points

Updated 2 months ago • 0 Comments

Lack of Rate Limiting in Sending Notifications

Unresolved

\$154.63 & 5 points

Updated 2 months ago • 0 Comments

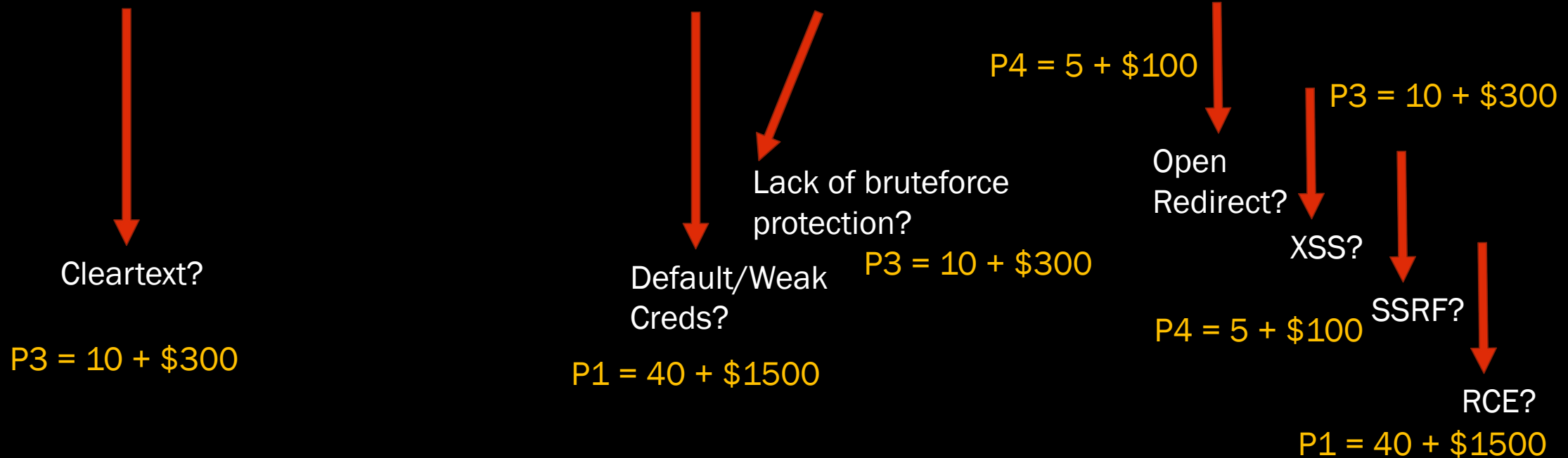
Still received the points and rewards



Tips 3 – Do Not Stop at One Attack

29/11/17

http://www.brokensites.com/admin/login.php?redirect_url=/dashboard



Total points : 120

Total rewards: \$4100

CHCON 2017

RFXSS on returnUrl <input type="text"/> Updated 4 months ago 0 Comments	RESOLVED	\$300 & 10 Kudos Points
Open Redirection bypass on returnUrl <input type="text"/> Updated 6 months ago 1 Comments	DUPLICATE	1 Kudos Points

Same parameter, same program, different time of submission, different attacks, 1 dupe, 1 valid. 😊



SYNTAXERROR

@SYNTAXERRORBA

Following



I just published “Reflective XSS and Open Redirect on [Indeed.com](#) subdomain”

...m/directcontent.html?target=javascript:alert(1)



Airbnb – Chaining Third-Party Open Redirect into Server-Side Request Forgery (SSRF) via LivePerson Chat

Author: Brett Buerhaus

March 9, 2017 bbuerhaus [airbnb](#), [hackerone](#), [livechat](#), [liveperson](#), [ssrf](#), [web](#)

Tips 4 – Mobile View

29/11/17



- Redirected to main page
- Forbidden
- No Access

m.website.com
mobile.website.com
touch.website.com
www.website.com/m/
www.website.com/mobile



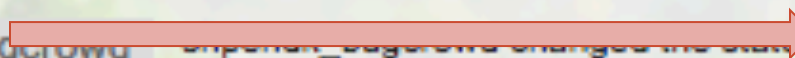
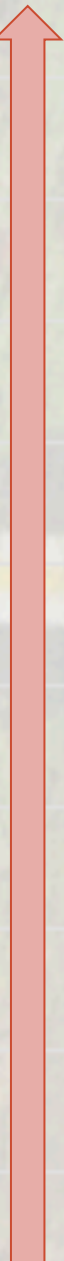
- Redirected to mobile page
- New session cookies?
- More features
- More user inputs
- Lack of security checks



CHCON 2017

»	Inbox	Bounty/Bugcrowd	[redacted] rewarded SQLi on https://mobile.[redacted] airlines...
»	Inbox	Bounty/Bugcrowd	shpendk_bugcrowd changed the state of SQLi on https://mobile.[redacted]n/managea...
»	Inbox	Bounty/Bugcrowd	[redacted] rewarded Excessively RXSS in mobile [redacted]n/*/.php/[xss]
»	Inbox	Bounty/Bugcrowd	shpendk_bugcrowd changed the state of Excessively RXSS in mobile [redacted]n/*/*...
»	Inbox	Bounty/Bugcrowd	[redacted] rewarded Missing CSRF Prevention on Whole Administration page at ...
»	Inbox	Bounty/Bugcrowd	shpendk_bugcrowd changed the state of Missing CSRF Prevention on Whole Administration p...
»	Inbox	Bounty/Bugcrowd	[redacted] rewarded SQLi on https://mobile.[redacted] aircraft...
»	Inbox	Bounty/Bugcrowd	shpendk_bugcrowd changed the state of SQLi on https://mobile.[redacted]agea...
»	Inbox	Bounty/Bugcrowd	[redacted] rewarded SQL Injection on https://mobile.[redacted]w/manag...
»	Inbox	Bounty/Bugcrowd	shpendk_bugcrowd changed the state of SQL Injection on https://mobile.[redacted]...
»	Inbox	Bounty/Bugcrowd	[redacted] rewarded Bypassing Administraton page on mobile.[redacted]
»	Inbox	Bounty/Bugcrowd	[redacted] rewarded Bypassing Administraton page on mobile.[redacted]

~\$11,000



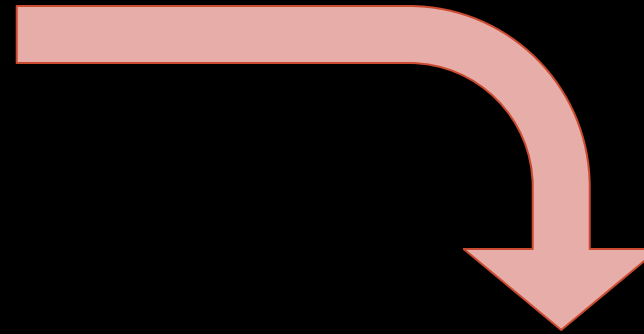
Tips 5 – Be Friend with JS Files

Time consuming, but it is worth your effort

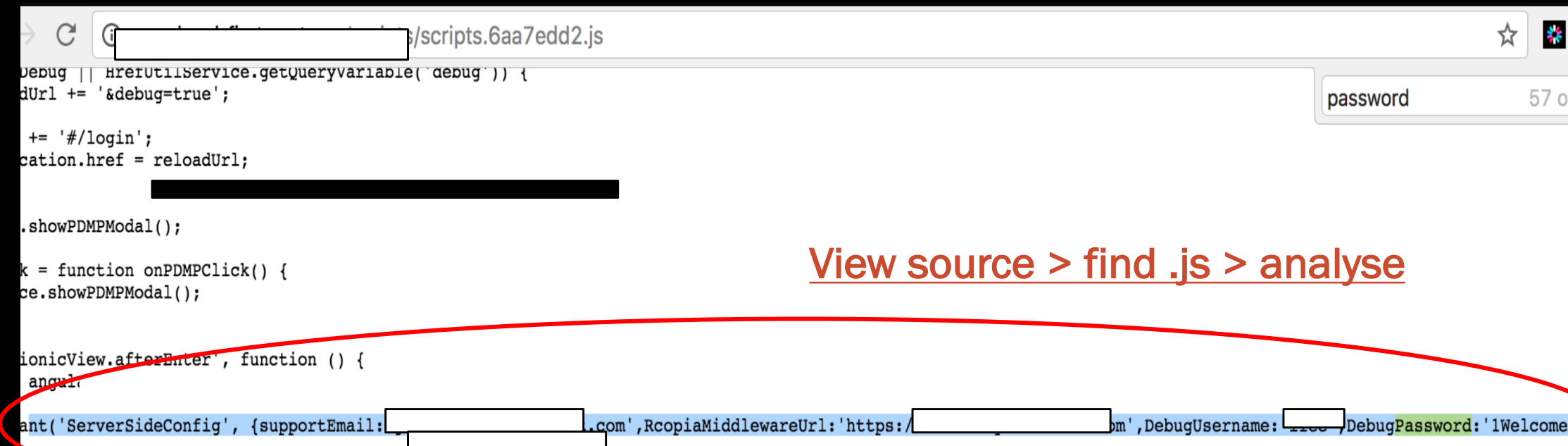
Filter by file extension

☒ Show only:

☐ Hide:



- Locate another .js files
- Locate path/files that not in crawled results
- Locate admin's features/action
- Hardcoded credentials
- Backup/Github/Dev sites
- Method of encryption



<https://bountysite.com/admin/dashboard?redirect=/>



Check on login.js

<https://bountysite.com/admin/dashboard/js/login.js>

Not authorized to view this page.

Please try a different page or request permission from your manager. Thanks!



Check
on
another
JS

<https://bountysite.com/admin/dashboard/photography/loginx>

Photo Storage

Photo Uploader

Upload Log

Browse

Unit: Select A Unit

P1 = 40 + \$1000

Tips X – Out of Scope

Some of the programs have a number of out of scope issues that they don't want to see.



I don't participate.

List of tools

- Burp Suite Pro
- Recon tools
 - Aquatone - <https://github.com/michenriksen/aquatone>
 - Spiderfoot - <http://www.spiderfoot.net/>
 - Enumall - <https://github.com/jhaddix/domain>
 - Sublist3r - <https://github.com/aboul3la/Sublist3r>
- Scanning tools
 - WPScan - <https://wpscan.org/>
 - Droopescan - <https://github.com/droope/droopescan>
 - SQLMap - <http://sqlmap.org/>
 - OXML_XXE- https://github.com/BuffaloWill/oxml_xxe
- JS Parser
 - <https://github.com/zseano/JS-Scan>
 - <https://github.com/nahamsec/JSParser>





Thank you to

- Christchurch Conference 2017
- Aura Information Security
- BugCrowd
- Bug hunters all over the world
- BurpSuite Pro