

# Journey to the top on bugcrowd

Version 2.0

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





# 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](https://en.oxforddictionaries.com/definition/bug_bounty)*

# Types of bug bounty programs



## Own programs

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





Managed by 3rd  
platform

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

**bugcrowd**

**hackerone**





bugcrowd  
hackerone

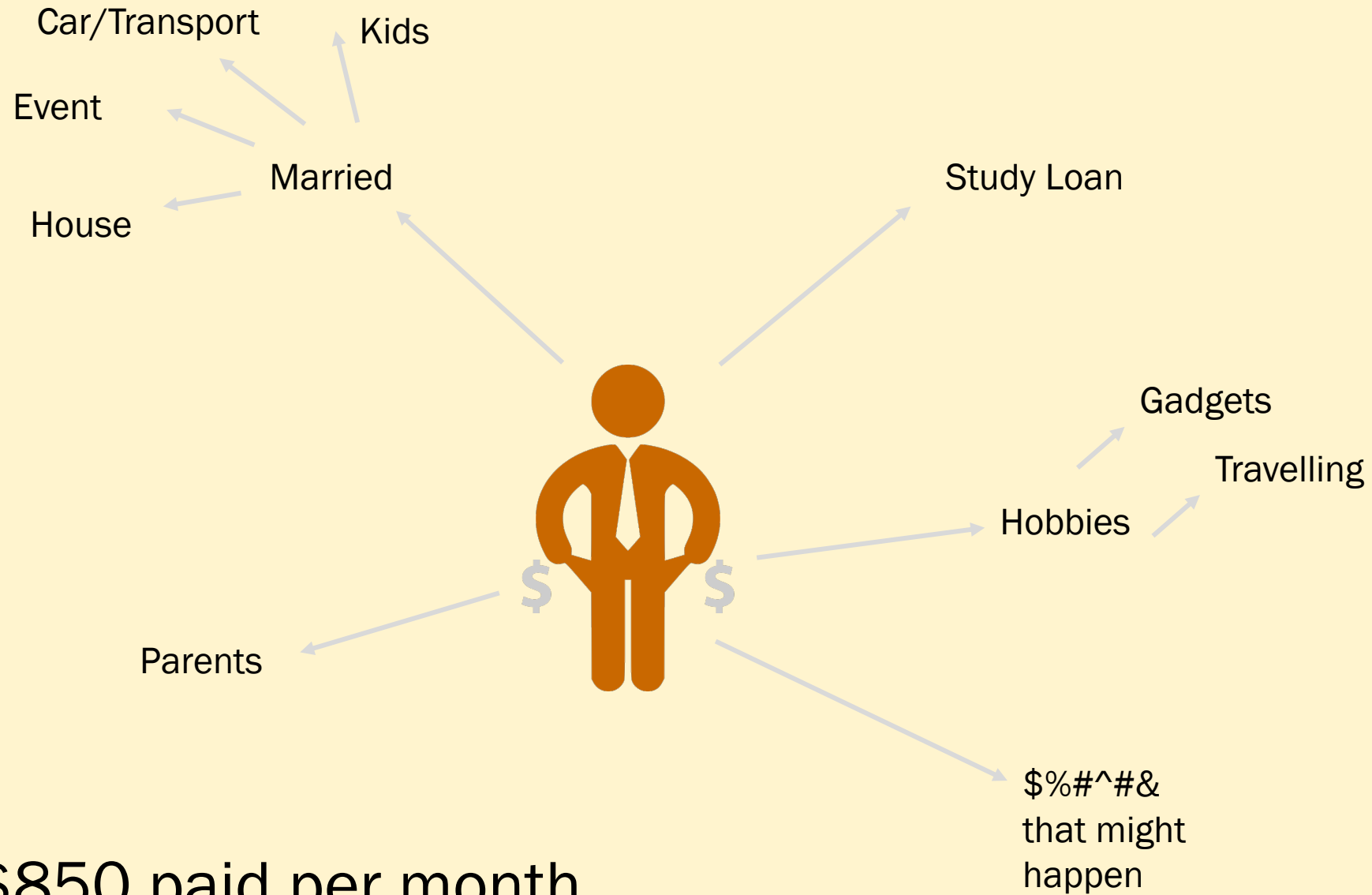


## Self-manage via 3rd party platform

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



# Why bug bounty



~\$850 paid per month

# Hack In The Box 2012

Killing a bounty program, Twice.



By : Itzhak ([Zuk](#)) Avraham; Nir [Goldshlager](#);

05/2012



xss in paypal-shopping.co.uk Bounty/Paypal x

---

 **ahmad**  
to sitesecurity   
attached the POC and my details :)

3<sup>rd</sup> August 2012



4 months  
later



**PayPal Inc sent you \$500.00 USD**

Dear 

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

# Hello Bugcrowd



# Hi folks, meet... **bugcrowd**

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.

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



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. 1<sup>st</sup> 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.



# Leaderboard

SEPTEMBER

ALL TIME

1st	 <b>mongo</b>	<b>17505</b>
2nd	 <b>yappare</b>	<b>8558</b>
3rd	 <b>zseano</b>	<b>6217</b>
4th	 <b>Private user</b>	<b>6169</b>
5th	 <b>mert</b>	<b>5943</b>

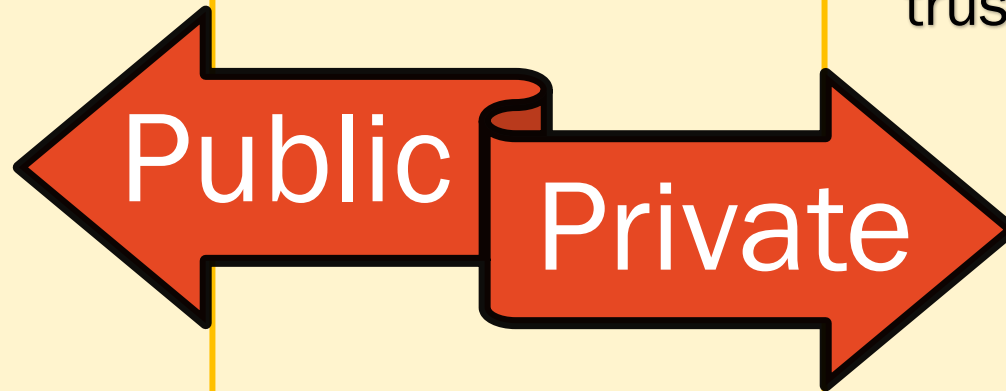
2017!!

- ← A wizard
- ← Normal human being
- ← Talented full-time bughunter from UK
- ← Anonymous
- ← Attack-dev

# 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



# Private Programs in Bugcrowd



## ONGOING

- \$100 - \$1500
- Tested few times
- Long duration
- Multiple targets
- Unknown number of researchers
- Some were a flex program before

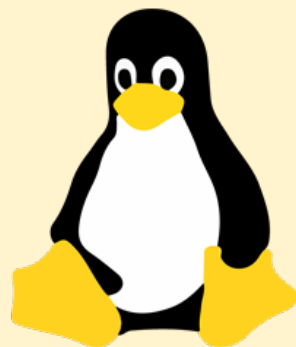
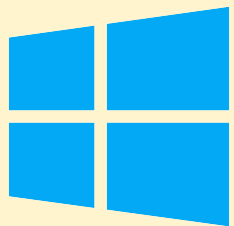


## FLEX

- Pool amount \$10k - \$20k
- Fresh targets
- Short duration
- 1 or 2 targets
- Less than 50 researchers



# Problems..

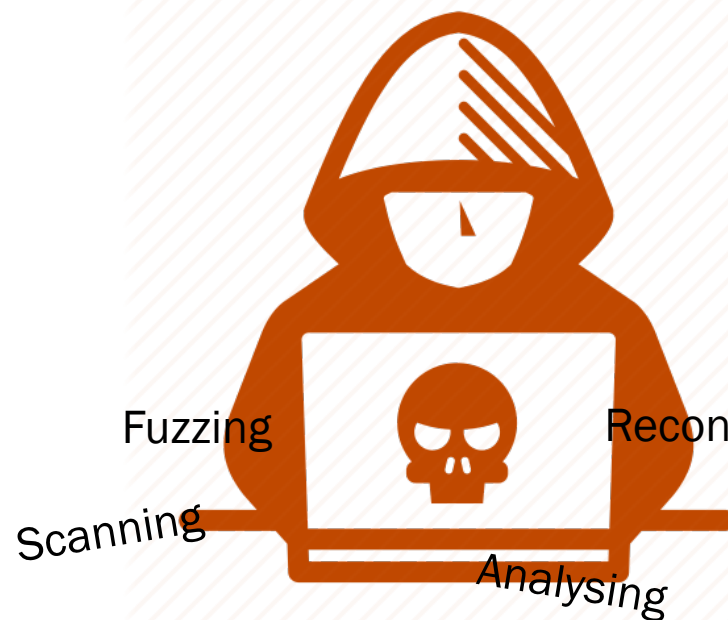
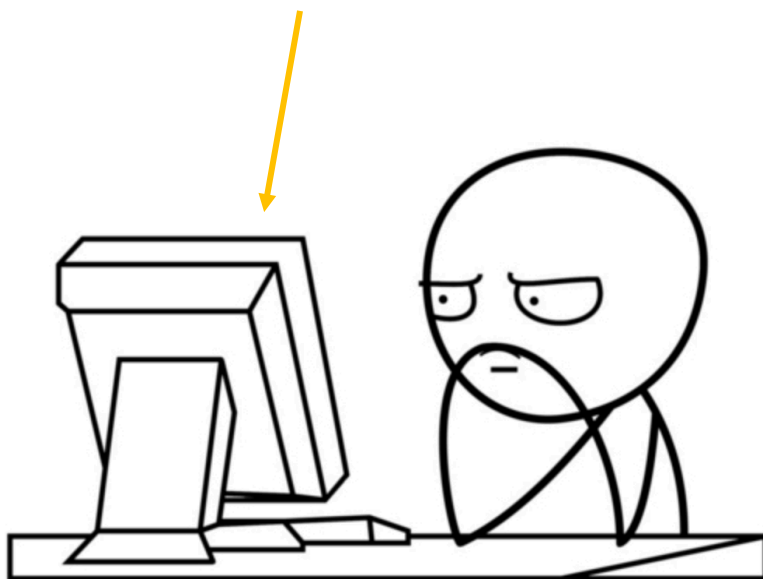


# Equipment and Tools

Most programs start at UTC time zone



At work. Doing client's report



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**

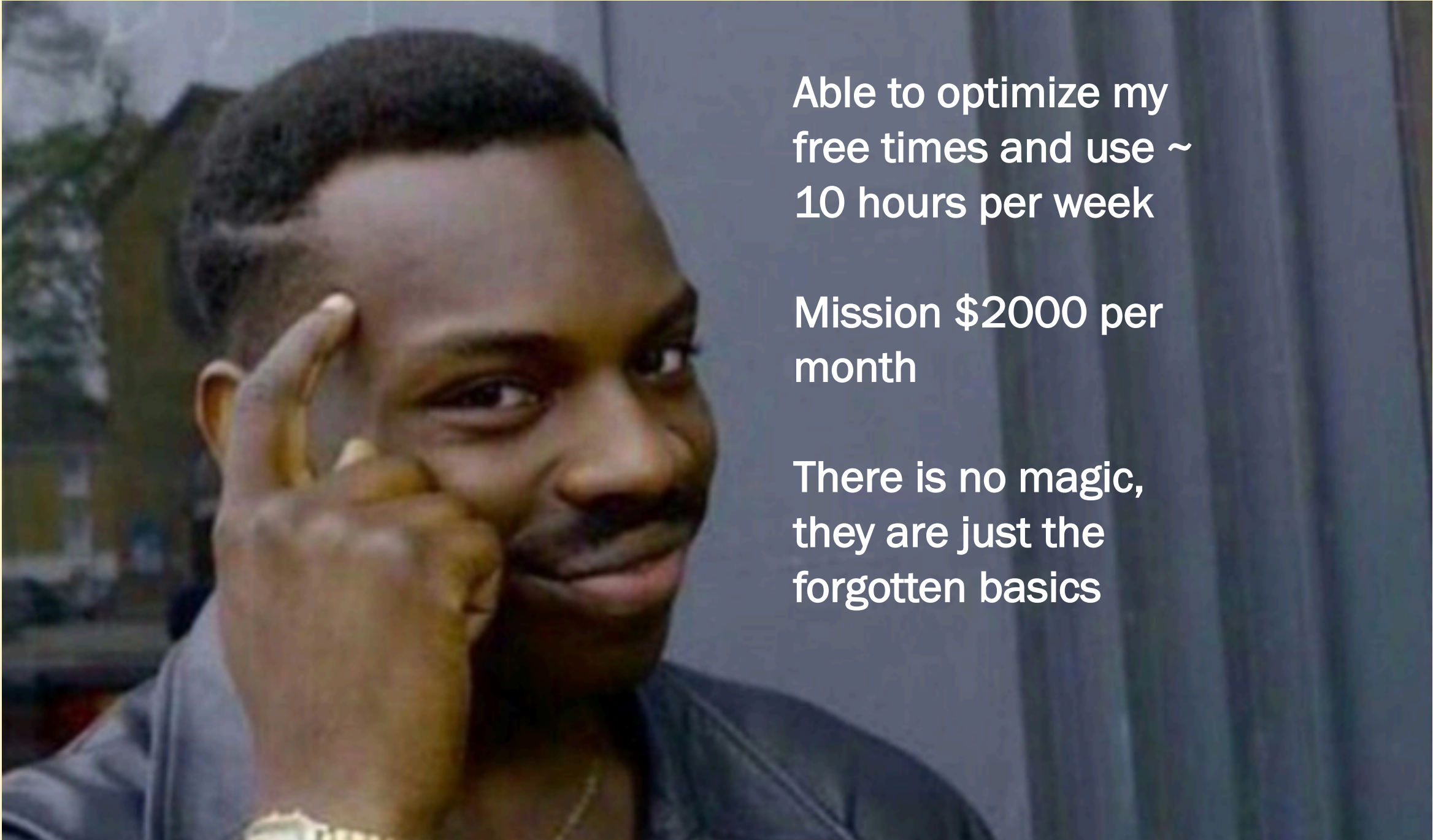
Created 2017-08-22 16:55:54 UTC

55 MINUTES





# Own methodology

A close-up photograph of a Black man with short, dark hair, wearing a black leather jacket. He is looking slightly to the right with a thoughtful expression, pointing his right index finger to his temple. The background is a blurred outdoor setting with a grey wall and some foliage.

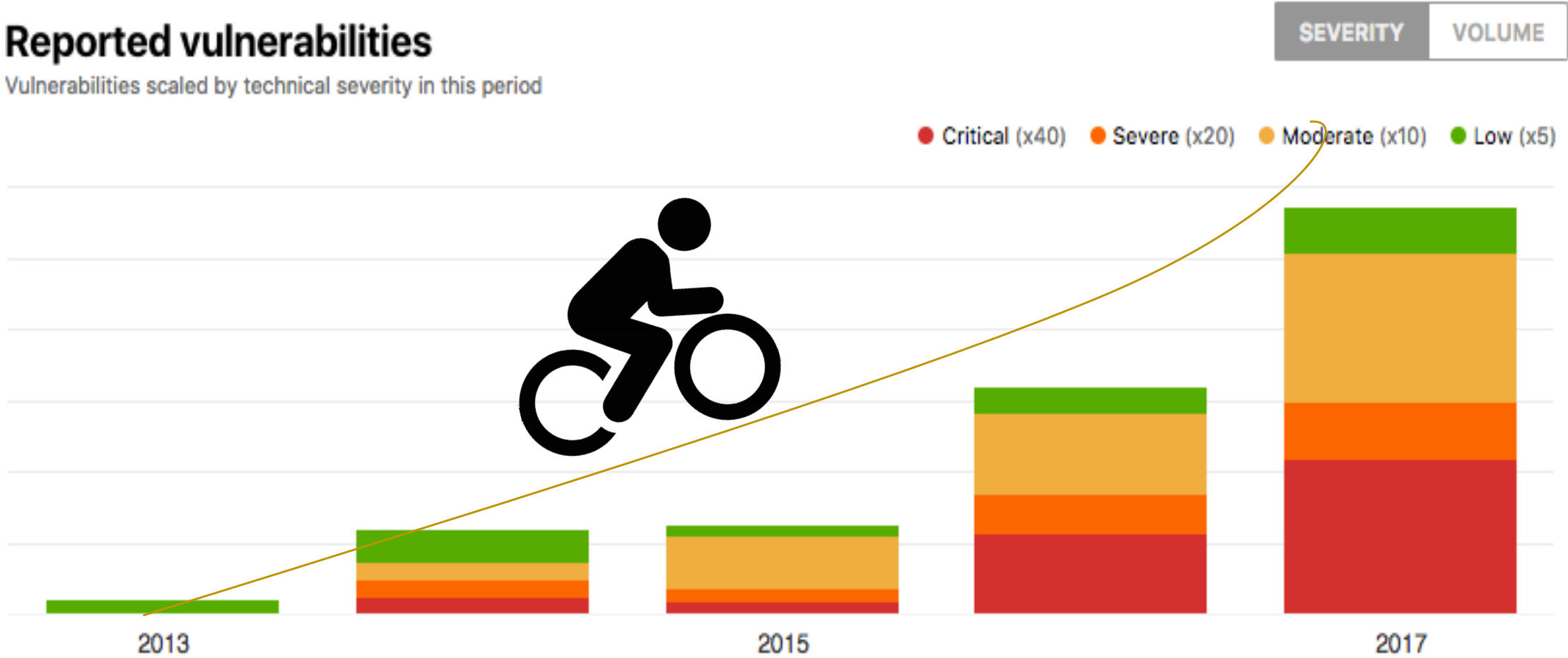
Able to optimize my  
free times and use ~  
10 hours per week

Mission \$2000 per  
month

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



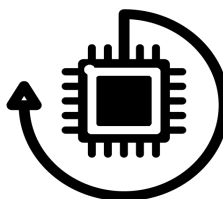
## Web Applications

- Click and view all the things/links/pages
- Focus more on complex programs
- Be a Premium/Developer user



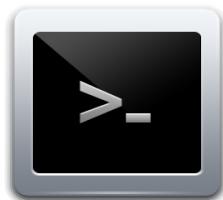
## Mobile Applications

- 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

# Tips 2 – Read and Understand the Program

- Each programs have different objective, different products have different attack surface and impact
  - Restaurant, cars, design, reviews, medical details, subscriptions
- Logic flaw need to be checked



- User's CV.
- Job application
- Draft's job ads



- User's private comments
- Private photo



- User's fitness data
- Health information

## Stationery

From personal notes to professional letters, your correspondence will wow them.



### Design it yourself.

Start from scratch, customise a template, or upload your own logo or complete design.

Business Cards, Flyers & Leaflets, Banners

### Let us help you design it.

We offer a range of design services to help you get exactly what you want.

Design Services

- Common vulnerabilities – XSS, SQLi, etc ✓
- Upload functionalities ✓
- Credit card, personal information, payment bypass ✓
- Authorisation check–No one submitted issue(s) related to own uploaded design/image

[IDOR] Viewing other's uploaded image at  
ate-

UNRESOLVED

\$300 & 10 Kudos Points

Updated 4 months ago | 0 Comments

[IDOR] Viewing other's uploaded image at  
?image\_id=

UNRESOLVED

\$300 & 10 Kudos Points

Updated 4 months ago | 1 Comment

[IDOR] Viewing other's uploaded image at  
ombo.aspx?

UNRESOLVED

\$300 & 10 Kudos Points

Updated 4 months ago | 0 Comments

[IDOR] Submitting Other's Design for Re-design service  
(

RESOLVED

\$900 & 20 Kudos Points

Updated 2 months ago | 3 Comments

[IDOR] View and Share Other's Portfolio  
(

UNRESOLVED

\$300 & 10 Kudos Points

Updated 4 months ago | 7 Comments



## Tips 3 – Risk Matrix Used



### 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 – 40 points + \$1500

P2 – 20 points + \$900

P3 – 10 points + \$300

P4 – 10 points + \$100

P5 – 0 points + \$0



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
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	
P2	Insecure OS/Firmware	Hardcoded Password	Non-Privileged User
P3	Server Security Misconfiguration	Mail Server Misconfiguration	Missing SPF on Email Domain
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
P3	Cross-Site Scripting (XSS)	Reflected	Non-Self

Cool bugs

Not so-cool bugs

Not so-cool bugs

Cool bugs

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

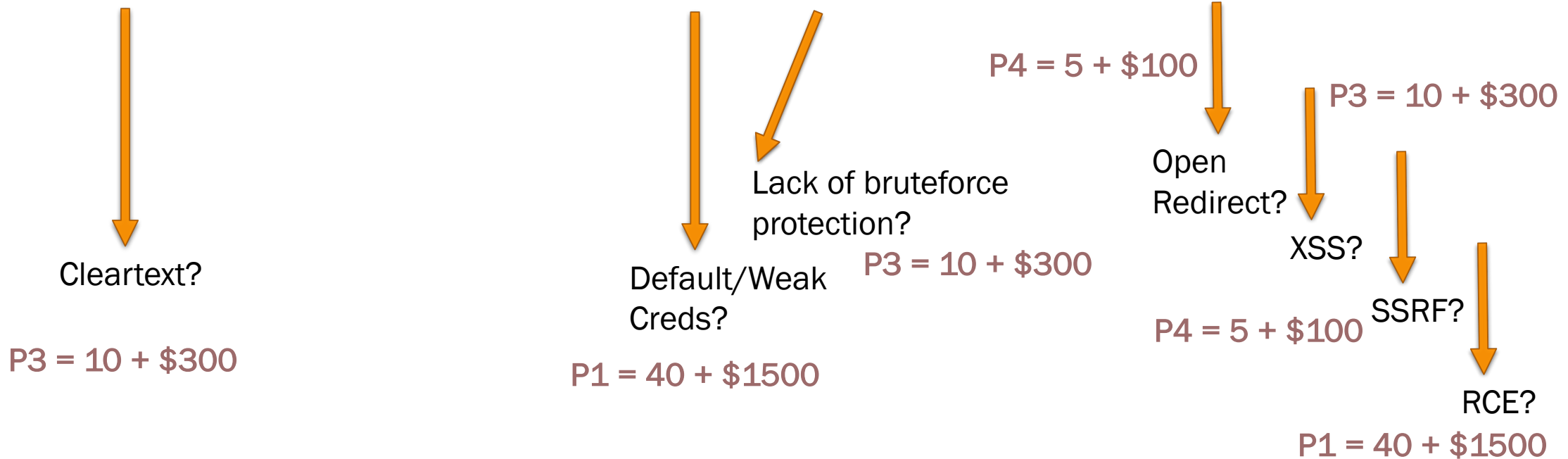
Updated 2 months ago • 0 Comments

Still received the points and rewards



# Tips 4 – Do Not Stop at One Attack

[http://www.brokensites.com/admin/login.php?redirect\\_url=/dashboard](http://www.brokensites.com/admin/login.php?redirect_url=/dashboard)



Total points : 120

Total rewards: \$4100

### RFXSS on returnUrl

SEEK

Updated 4 months ago | 0 Comments

RESOLVED

\$300 & 10 Kudos Points

### Open Redirection bypass on returnUrl

SEEK

Updated 6 months ago | 4 Comments

DUPLICATE

1 Kudos Points

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



**SYNTAXERROR**

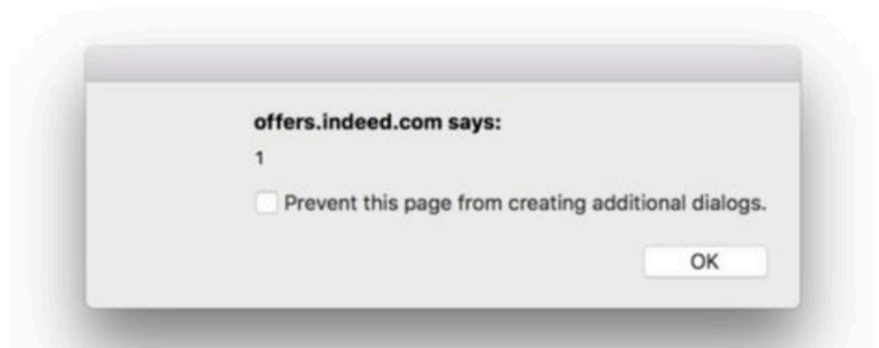
@SYNTAXERRORBA

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 5 – 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



ESIDES WELLINGTON NEW ZEALAND



»	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] changed the state of Bypassing Administraton page on mobile. [redacted]

~\$11,000





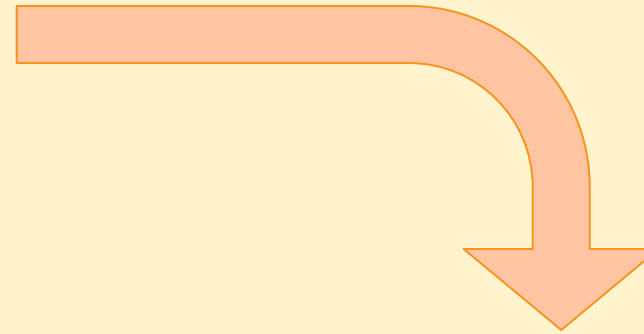
# Tips 6 – Be Friend with JS Files

Time consuming, but it is worth

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

ms/scripts/scripts.6aa7edd2.js

```
debug || HrefUtilService.getQueryVariable(' debug ')) {  
  dUrl += '&debug=true';  
  
  += '#/login';  
  cation.href = reloadUrl;  
  [REDACTED]  
  
  .showPDMPModal();  
  
  k = function onPDMPClick() {  
    ce.showPDMPModal();  
  
    ionicView.afterEnter', function () {  
      angular  
      ant('ServerSideConfig', {supportEmail:[REDACTED].com', [REDACTED]lewareUrl:'https://[REDACTED]m', DebugUsername:[REDACTED], DebugPassword:'!Welcome
```

password 57 of

View source > find .js > analyse

```
}  
function setSelectShop(cityName, shopSelectId, Shopid) {  
  $.ajax({  
    url: "/clues/getShopsList",  
    data: { "cityName": encodeURIComponent(cityName) },  
    cache: false,  
    type: "post",  
    dataType: "json",  
    success: function (data) {  
      $("#" + shopSelectId).html("<option va  
      if(data.Data != null && data.Data.leng  
        for(var i = 0; i < data.Data.lengt  
          $("#" + shopSelectId).append("  
        }  
      }  
    }  
    if(Shopid) {  
      get default(G("shop id"), Shopid, "select one");
```

MSSQL Injection at https://www.[REDACTED]clues/getCitysLi[REDACTED]  
Updated on 09/21/2017

P1 Resolved

<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!

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



*Check  
on  
another  
JS*

## Photo Storage

Photo Uploader

Upload Log

Browse

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.

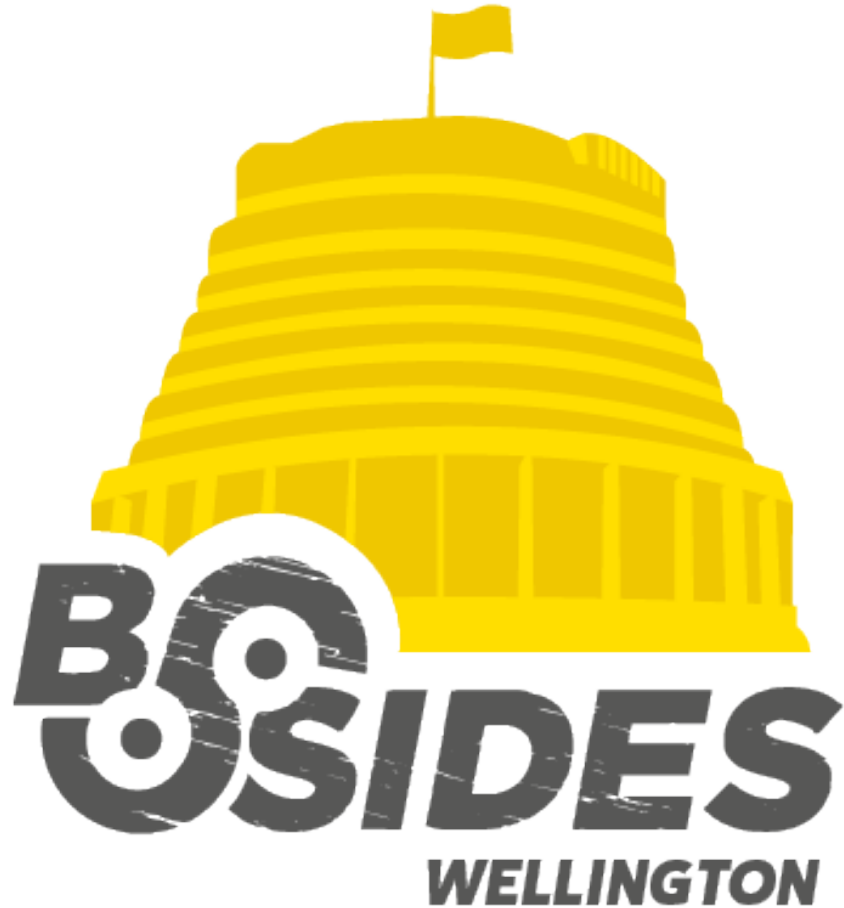


I don't participate.

# 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/BufaloWill/oxml\\_xxe](https://github.com/BufaloWill/oxml_xxe)
- JS Parser
  - <https://github.com/zseano/JS-Scan>
  - <https://github.com/nahamsec/JSParser>





Thank you to

- **BSIDES WELLINGTON**
- **Aura Information Security**
- **BugCrowd**
- **Bug hunters all over the world**
- **BurpSuite Pro**