STARTING YOUR BUG HUNTING CAREER NOW

by Jay Turla

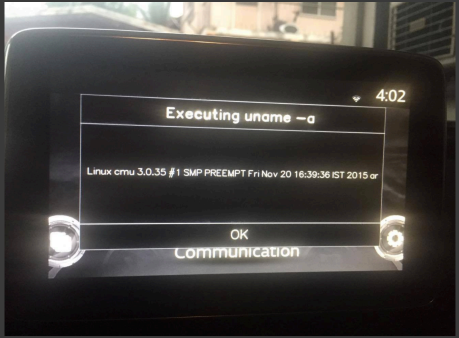
ROOTCON

bugcrowd

AGENDA

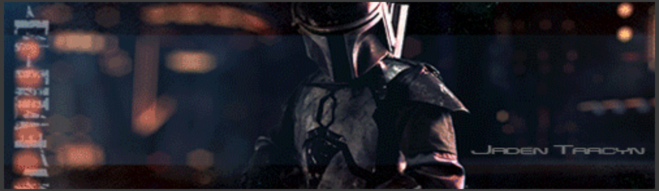
- Whoami
- What is a Bug Bounty or Bug Hunting?
- Some Companies with Bug Bounty Programs
- Bugcrowd Introduction and VRT
- Bug Hunter Methodology
- Sample Issues
- DEMO

WHOAMI



```
4:02
Executing uname –a
Linux cmu 3.0.35 #1 SMP PREEMPT Fri Nov 20 16:39:36 IST 2015 ar
OK
```

- Jay Turla a.k.a The Jetman
- Application Security Engineer @Bugcrowd
- Metasploit Contributor: Host Header Injection Detection, BisonWare BisonFTP Server Buffer Overflow, Zemra Botnet CnC Web Panel Remote Code Execution, etc.
- Twitter : @shipcod3
- ROOTCON Goon
- Former Senior Security Consultant at HP Fortify on Demand



BOUNTY HUNTING?

WANTED
THE NOTORIOUS PYRATE
EZEKIEL BLACKHEART
A BOUNTY OF FIVE HUNDRED POUNDS
WILL BE PAID ON THE PROOF OF
CAPTURE OR DEATH BY HIS MAJESTYS
GOVERNOR IN PORT ROYAL

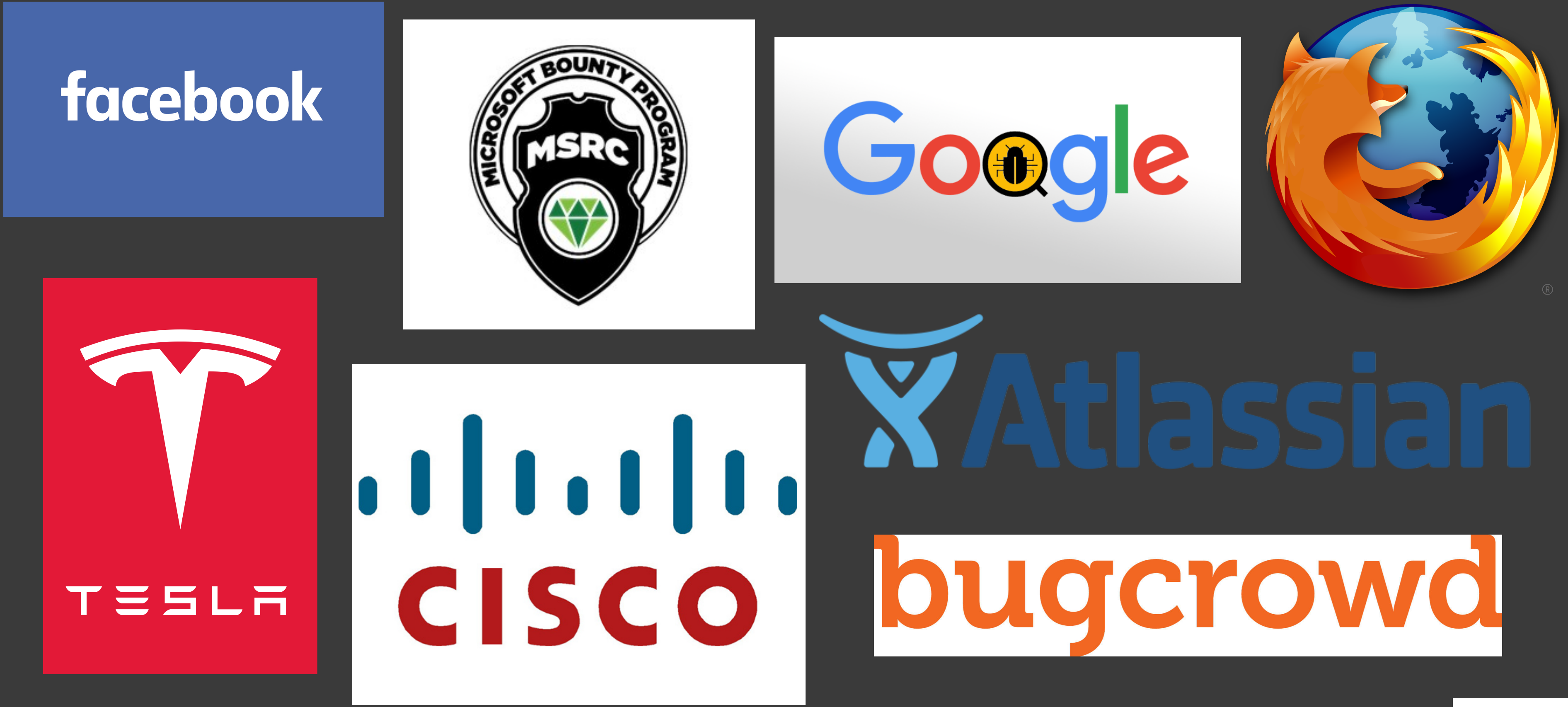
WHAT IS A BUG BOUNTY?
(THINK OF IT AS A COMPETITION)

Independent security researchers from all over the world are recruited

Vulnerabilities are found and reported

Rewards are exchanged for reporting vulnerabilities in company applications

SOME COMPANIES THAT HAVE BUG BOUNTY PROGRAMS <3

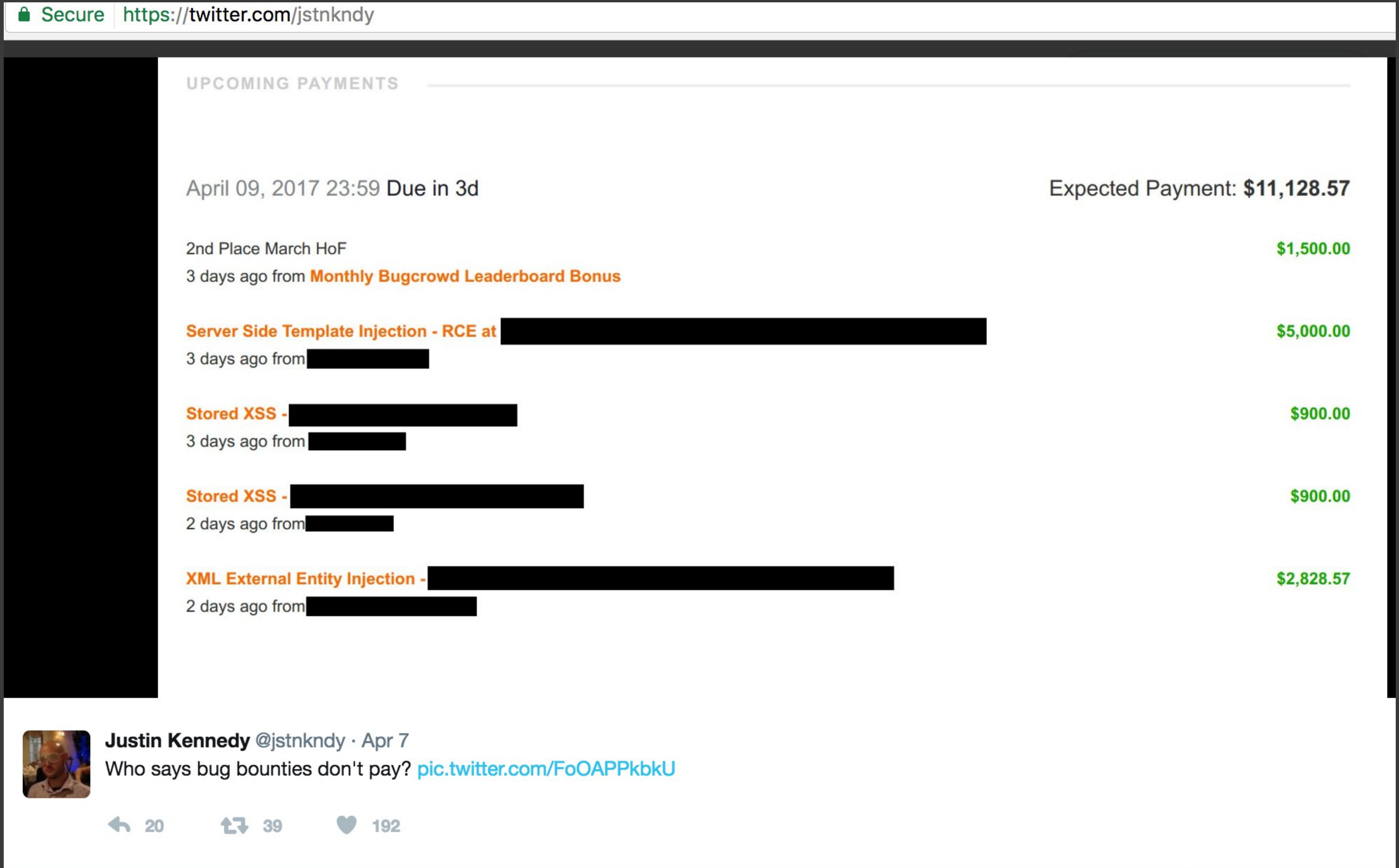


Crowdsourced security platforms like **Bugcrowd** connects organizations to a curated crowd of tens of thousands of researchers from around the world to identify vulnerabilities in their applications, devices, and code—before the bad guys do.

Hack now at https://bugcrowd.com/programs

IS THIS A NEW SCAM? WAIT WHAT?

SHOW ME THE MONEY



Secure https://twitter.com/jstnkndy

UPCOMING PAYMENTS

April 09, 2017 23:59 Due in 3d

Expected Payment: **$11,128.57**

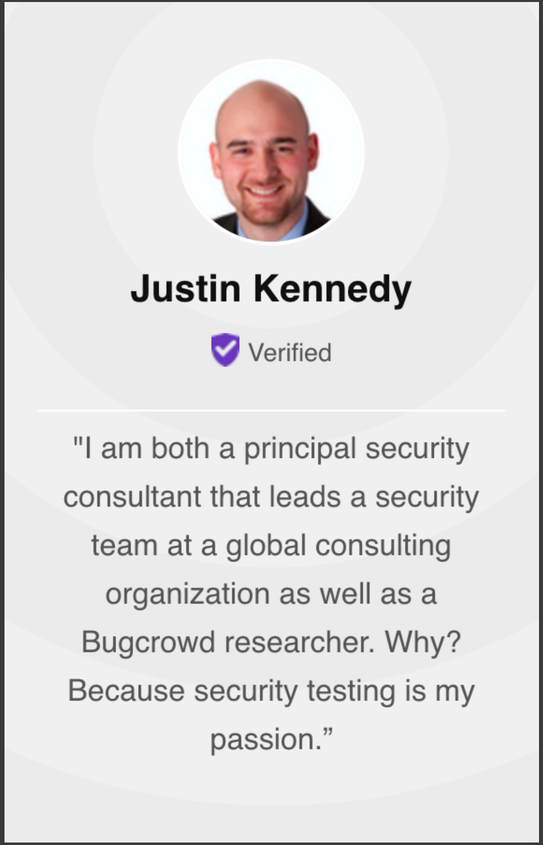
2nd Place March HoF 3 days ago from **Monthly Bugcrowd Leaderboard Bonus**	$1,500.00
Server Side Template Injection - RCE at [redacted] 3 days ago from [redacted]	$5,000.00
Stored XSS - [redacted] 3 days ago from [redacted]	$900.00
Stored XSS - [redacted] 2 days ago from [redacted]	$900.00
XML External Entity Injection - [redacted] 2 days ago from [redacted]	$2,828.57

Justin Kennedy @jstnkndy · Apr 7

Who says bug bounties don't pay? pic.twitter.com/FoOAPPkbkU

↩ 20 🔁 39 ♥ 192

WHO IS THIS GUY?

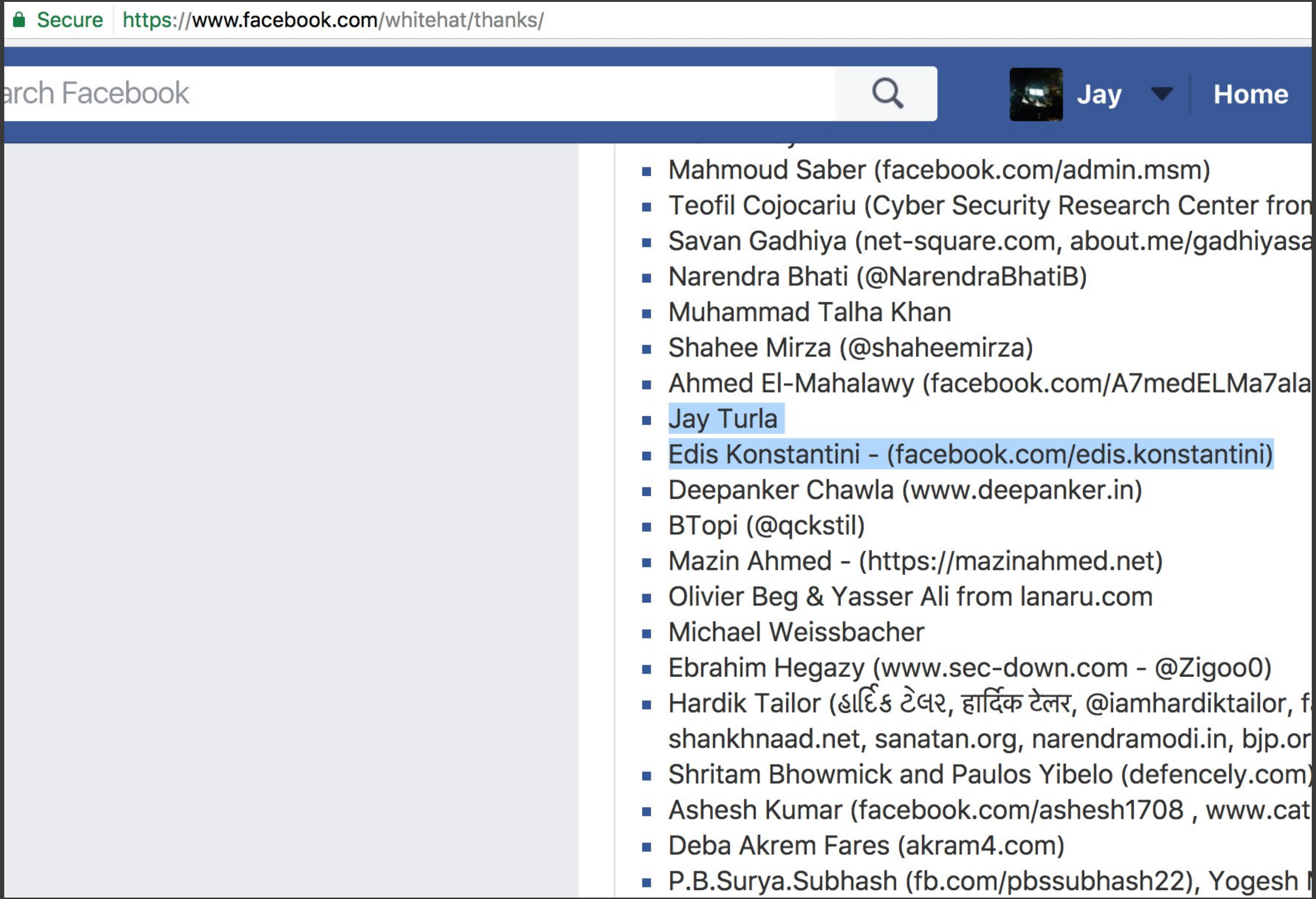


Justin Kennedy

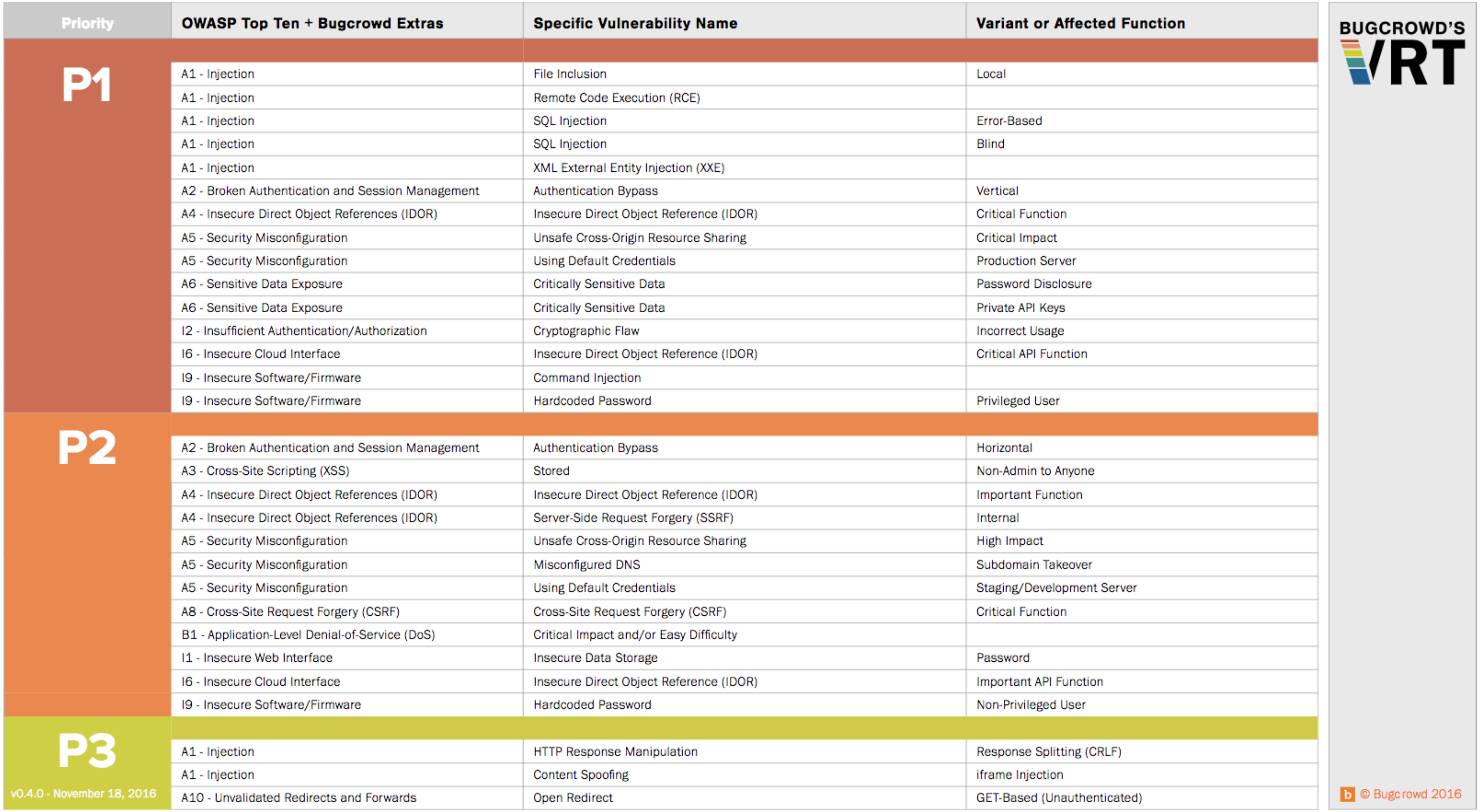
✓ Verified

"I am both a principal security consultant that leads a security team at a global consulting organization as well as a Bugcrowd researcher. Why? Because security testing is my passion."

YOU CAN BE A HERO



- Mahmoud Saber (facebook.com/admin.msm)
- Teofil Cojocariu (Cyber Security Research Center fron
- Savan Gadhiya (net-square.com, about.me/gadhiyasa
- Narendra Bhati (@NarendraBhatiB)
- Muhammad Talha Khan
- Shahee Mirza (@shaheemirza)
- Ahmed El-Mahalawy (facebook.com/A7medELMa7ala
- Jay Turla
- Edis Konstantini - (facebook.com/edis.konstantini)
- Deepanker Chawla (www.deepanker.in)
- BTopi (@qckstil)
- Mazin Ahmed - (https://mazinahmed.net)
- Olivier Beg & Yasser Ali from lanaru.com
- Michael Weissbacher
- Ebrahim Hegazy (www.sec-down.com - @Zigoo0)
- Hardik Tailor (હાર્દિક ટેલર, हार्दिक टेलर, @iamhardiktailor, f shankhnaad.net, sanatan.org, narendramodi.in, bjp.or
- Shritam Bhowmick and Paulos Yibelo (defencely.com)
- Ashesh Kumar (facebook.com/ashesh1708 , www.cat
- Deba Akrem Fares (akram4.com)
- P.B.Surya.Subhash (fb.com/pbssubhash22), Yogesh I



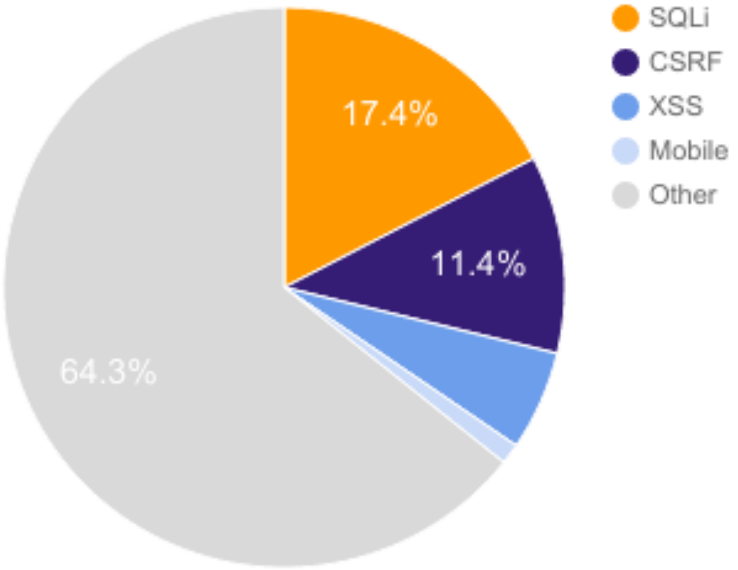
Priority	OWASP Top Ten + Bugcrowd Extras	Specific Vulnerability Name	Variant or Affected Function
P1	A1 - Injection	File Inclusion	Local
	A1 - Injection	Remote Code Execution (RCE)	
	A1 - Injection	SQL Injection	Error-Based
	A1 - Injection	SQL Injection	Blind
	A1 - Injection	XML External Entity Injection (XXE)	
	A2 - Broken Authentication and Session Management	Authentication Bypass	Vertical
	A4 - Insecure Direct Object References (IDOR)	Insecure Direct Object Reference (IDOR)	Critical Function
	A5 - Security Misconfiguration	Unsafe Cross-Origin Resource Sharing	Critical Impact
	A5 - Security Misconfiguration	Using Default Credentials	Production Server
	A6 - Sensitive Data Exposure	Critically Sensitive Data	Password Disclosure
	A6 - Sensitive Data Exposure	Critically Sensitive Data	Private API Keys
	I2 - Insufficient Authentication/Authorization	Cryptographic Flaw	Incorrect Usage
	I6 - Insecure Cloud Interface	Insecure Direct Object Reference (IDOR)	Critical API Function
	I9 - Insecure Software/Firmware	Command Injection	
	I9 - Insecure Software/Firmware	Hardcoded Password	Privileged User
P2	A2 - Broken Authentication and Session Management	Authentication Bypass	Horizontal
	A3 - Cross-Site Scripting (XSS)	Stored	Non-Admin to Anyone
	A4 - Insecure Direct Object References (IDOR)	Insecure Direct Object Reference (IDOR)	Important Function
	A4 - Insecure Direct Object References (IDOR)	Server-Side Request Forgery (SSRF)	Internal
	A5 - Security Misconfiguration	Unsafe Cross-Origin Resource Sharing	High Impact
	A5 - Security Misconfiguration	Misconfigured DNS	Subdomain Takeover
	A5 - Security Misconfiguration	Using Default Credentials	Staging/Development Server
	A8 - Cross-Site Request Forgery (CSRF)	Cross-Site Request Forgery (CSRF)	Critical Function
	B1 - Application-Level Denial-of-Service (DoS)	Critical Impact and/or Easy Difficulty	
	I1 - Insecure Web Interface	Insecure Data Storage	Password
	I6 - Insecure Cloud Interface	Insecure Direct Object Reference (IDOR)	Important API Function
	I9 - Insecure Software/Firmware	Hardcoded Password	Non-Privileged User
P3	A1 - Injection	HTTP Response Manipulation	Response Splitting (CRLF)
	A1 - Injection	Content Spoofing	iframe Injection
v0.4.0 - November 18, 2016	A10 - Unvalidated Redirects and Forwards	Open Redirect	GET-Based (Unauthenticated)

BUGCROWD'S VRT

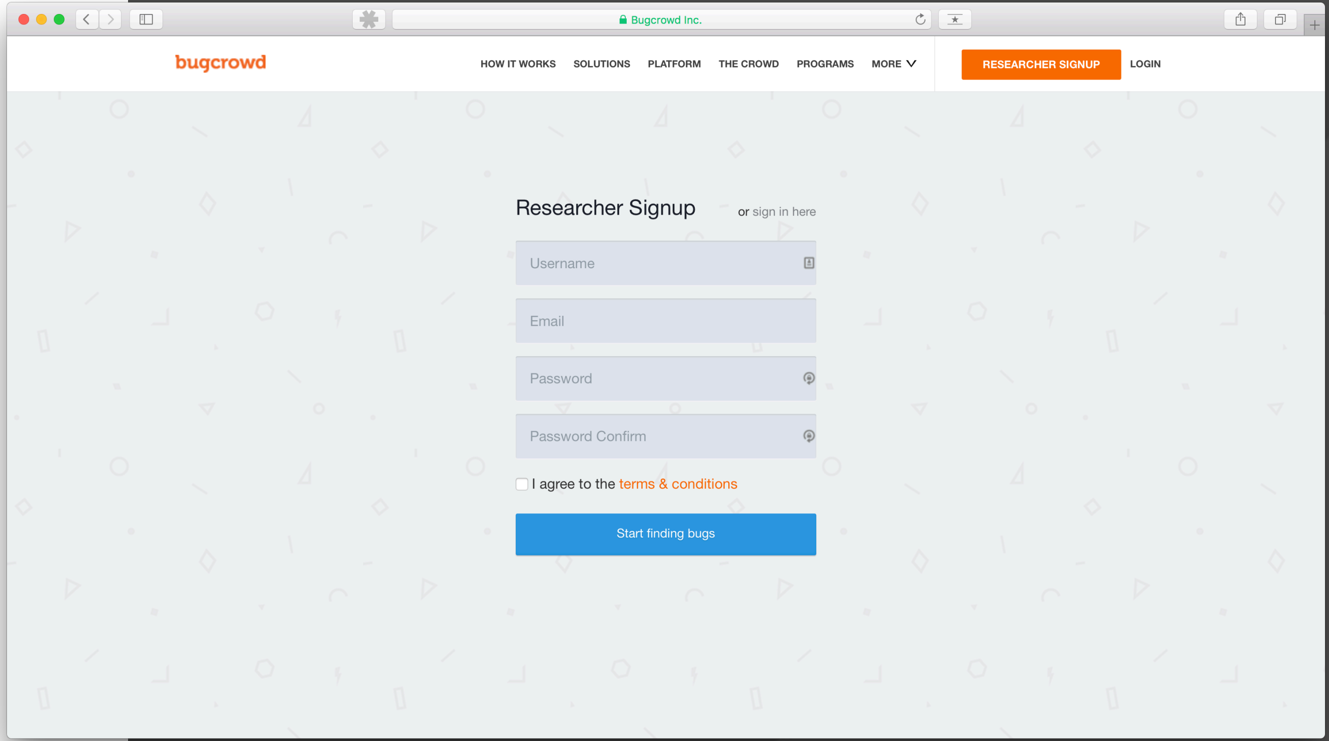
BUG TYPE AND PRIORITY

In 2016, a critical issue was reported every...

13 HRS



EASY SIGNUP



Researcher Signup

or sign in here

Username

Email

Password

Password Confirm

□ I agree to the terms & conditions

Start finding bugs

BUG HUNTER METHODOLOGIES

METHODOLOGY FOR BUG HUNTING
JASON HADDIX

- https://github.com/jhaddix/tbhm
- Video & Slides
- https://bugcrowd.com/resources/how-to-shot-web-by-jason-haddix

METHODOLOGY FOR BUG HUNTING ON NEW BOUNTIES

BRETT BUERHAUS

- Review the scope
- Perform reconnaissance to find valid targets
- Scan against discovered targets to gather additional information
- Review all of the services and applications
- Fuzz for errors and to expose vulnerabilities
- Attack vulnerabilities to build proof-of-concepts

OTHER GOOD RESOURCES

- Awesome Hacking: https://github.com/Hack-with-Github/Awesome-Hacking
- The Web Application Hacker’s Handbook
- OWASP: https://www.owasp.org/index.php/Main_Page
- HPE Security Fortify Taxonomy: https://vulncat.hpefod.com/en
- DEF CON Archives: https://defcon.org/html/links/dc-archives.html
- ROOTCON Archives: https://www.rootcon.org/xml/archives/events
- SecLists Project: https://github.com/danielmiessler/SecLists

PRACTICING YOUR SKILLS

VIRTUAL MACHINES AND VULNERABLE WEB APPS

- EASY TO SETUP

- vulnhub.com - materials (mostly VMs you can play with) that allows anyone to gain practical 'hands-on' experience in digital security, computer software & network administration.
- Damn Vulnerable Web Application - http://www.dvwa.co.uk/
- OWASP Mutillidae - https://www.owasp.org/index.php/OWASP_Mutillidae_2_Project
- bWAPP - http://www.itsecgames.com/
- OWASP Broken Web Applications Project - https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

ONLINE PLAYGROUND

-NO NEED TO SET IT UP

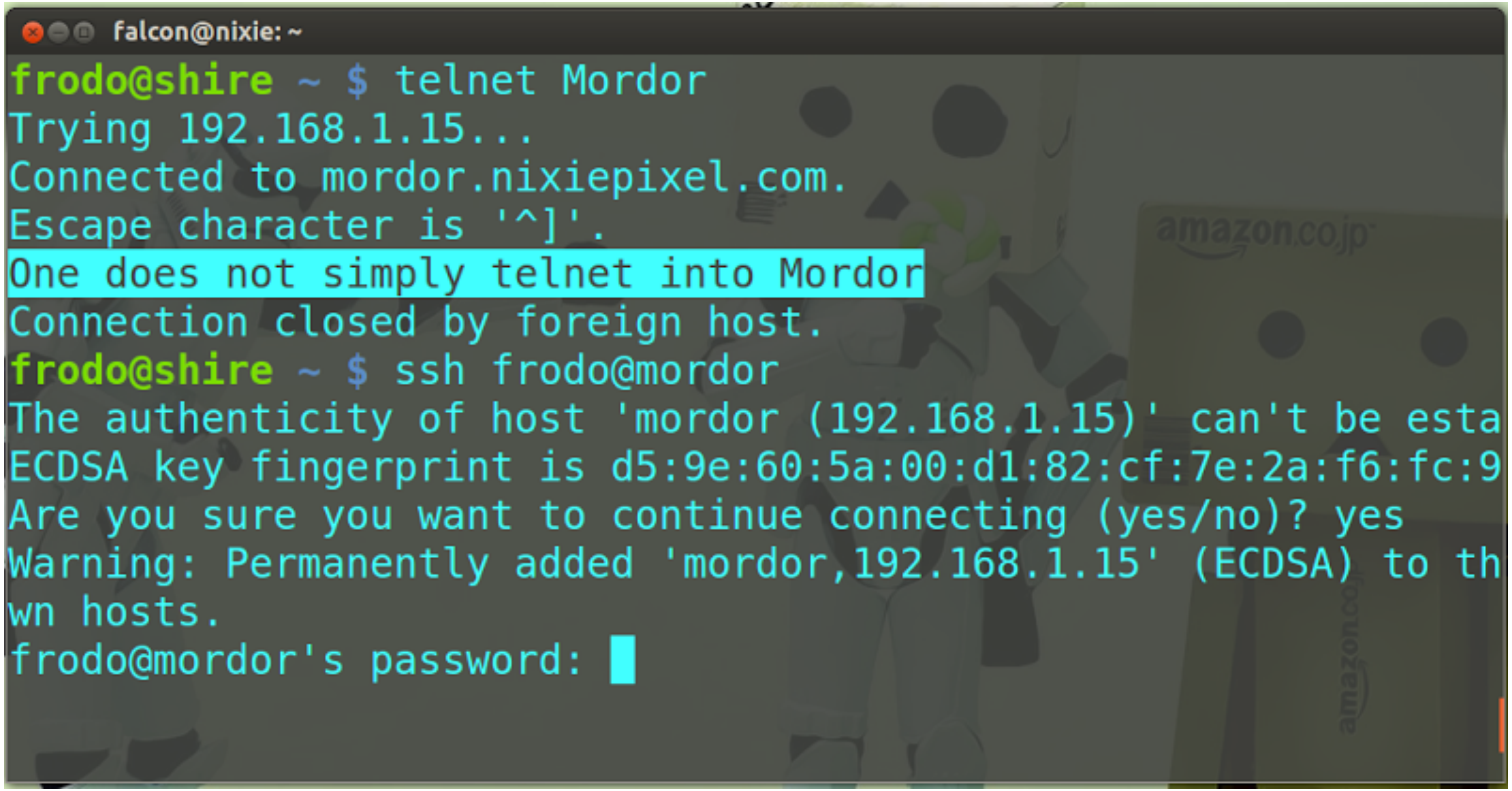
- http://flaws.cloud/ - series of levels you'll learn about common mistakes and gotchas when using Amazon Web Services (AWS)
- n00bs CTF Labs - http://ctf.infosecinstitute.com/index.php
- Google XSS Challenge- https://xss-game.appspot.com/
- Zero Web App - http://zero.webappsecurity.com/
- CTF365 - https://ctf365.com/
- Demo Testfire - http://demo.testfire.net/

SOME ISSUES YOU CAN REPORT NOW

things to ponder about security issues that are easy to spot

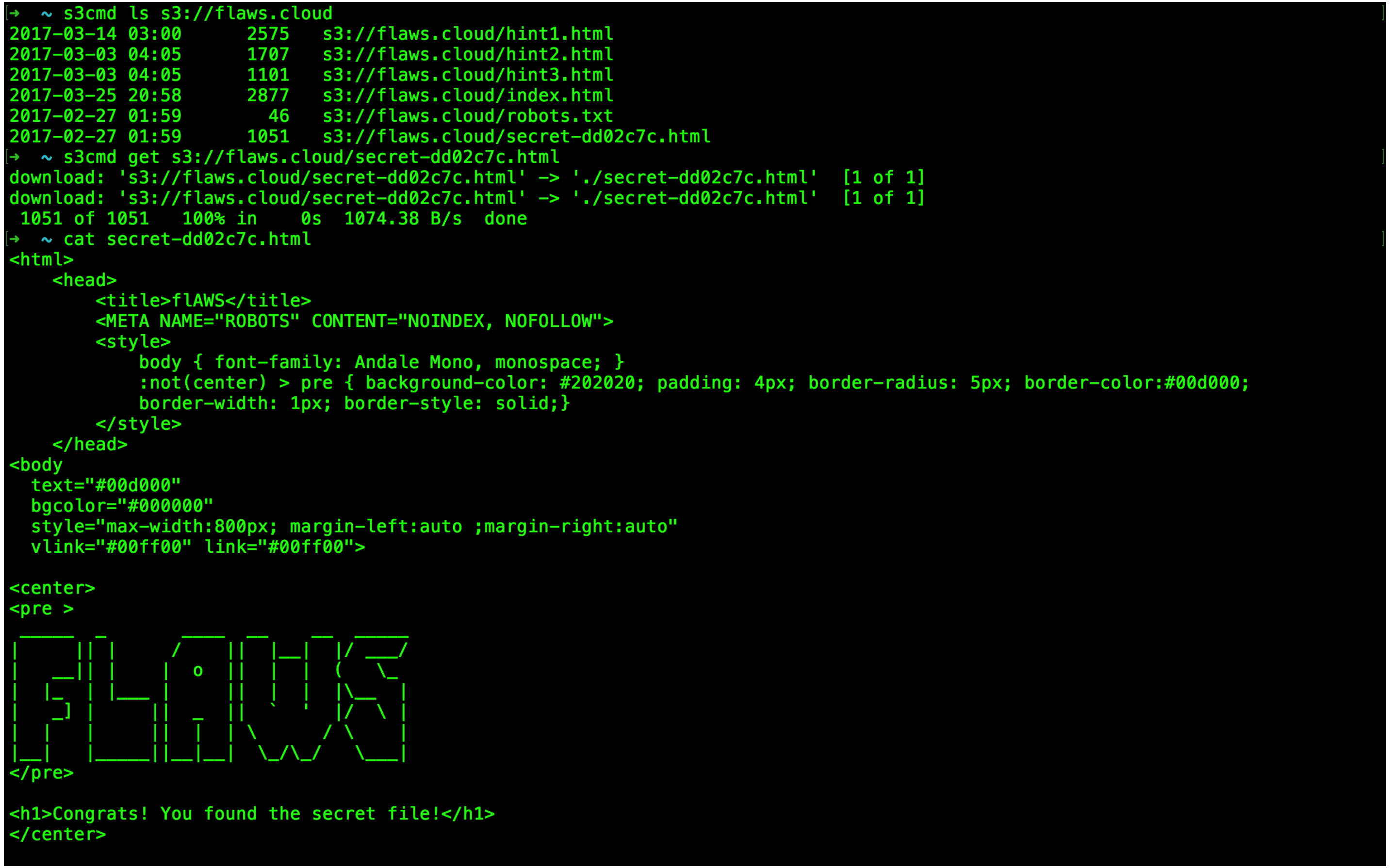
SESSION NOT INVALIDATED AFTER LOGOUT, PASSWORD RESET, PASSWORD CHANGE

TELNET ENABLED (CREDENTIALS REQUIRED)



```
frodo@shire ~ $ telnet Mordor
Trying 192.168.1.15...
Connected to mordor.nixiepixel.com.
Escape character is '^]'.
One does not simply telnet into Mordor
Connection closed by foreign host.
frodo@shire ~ $ ssh frodo@mordor
The authenticity of host 'mordor (192.168.1.15)' can't be esta
ECDSA key fingerprint is d5:9e:60:5a:00:d1:82:cf:7e:2a:f6:fc:9
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mordor,192.168.1.15' (ECDSA) to th
wn hosts.
frodo@mordor's password: 
```

MISCONFIGURED S3 BUCKETS

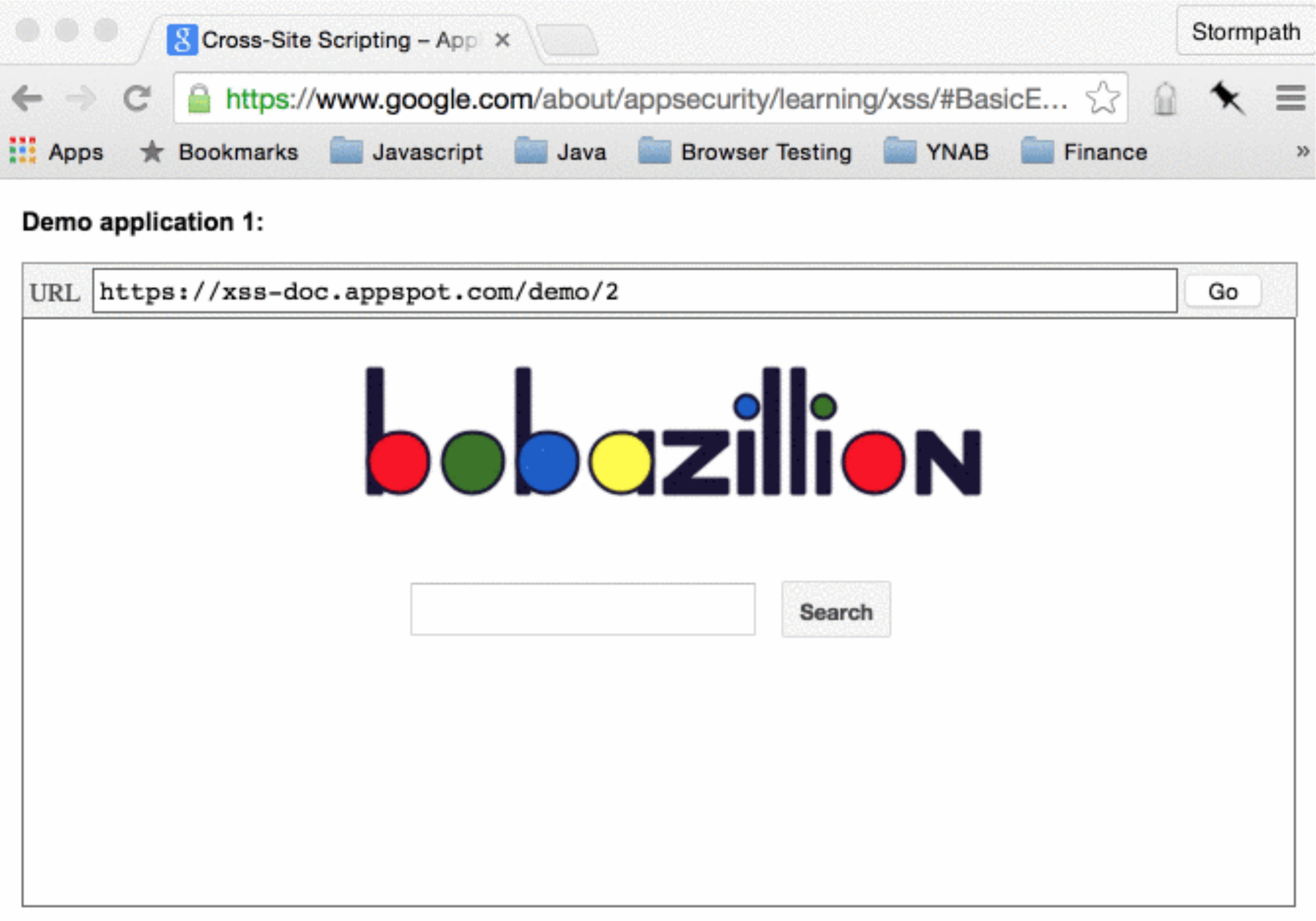


```
➜  ~ s3cmd ls s3://flaws.cloud
2017-03-14 03:00      2575   s3://flaws.cloud/hint1.html
2017-03-03 04:05      1707   s3://flaws.cloud/hint2.html
2017-03-03 04:05      1101   s3://flaws.cloud/hint3.html
2017-03-25 20:58      2877   s3://flaws.cloud/index.html
2017-02-27 01:59        46   s3://flaws.cloud/robots.txt
2017-02-27 01:59      1051   s3://flaws.cloud/secret-dd02c7c.html
➜  ~ s3cmd get s3://flaws.cloud/secret-dd02c7c.html
download: 's3://flaws.cloud/secret-dd02c7c.html' -> './secret-dd02c7c.html'  [1 of 1]
download: 's3://flaws.cloud/secret-dd02c7c.html' -> './secret-dd02c7c.html'  [1 of 1]
 1051 of 1051   100% in    0s  1074.38 B/s  done
➜  ~ cat secret-dd02c7c.html
<html>
    <head>
        <title>flAWS</title>
        <META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW">
        <style>
            body { font-family: Andale Mono, monospace; }
            :not(center) > pre { background-color: #202020; padding: 4px; border-radius: 5px; border-color:#00d000;
            border-width: 1px; border-style: solid;}
        </style>
    </head>
<body
  text="#00d000"
  bgcolor="#000000"
  style="max-width:800px; margin-left:auto ;margin-right:auto"
  vlink="#00ff00" link="#00ff00">

<center>
<pre >
 _____  _       ____  __    __  _____
|     || |     /    ||  |__|  |/ ___/
|   __|| |    |  o  ||  |  |  (   \_
|  |_  | |___ |     ||  |  |  |\__  |
|   _] |     ||  _  ||  `  '  |/  \ |
|  |   |     ||  |  | \      / \    |
|__|   |_____||__|__|  \_/\_/   \___|
</pre>

<h1>Congrats! You found the secret file!</h1>
</center>
```

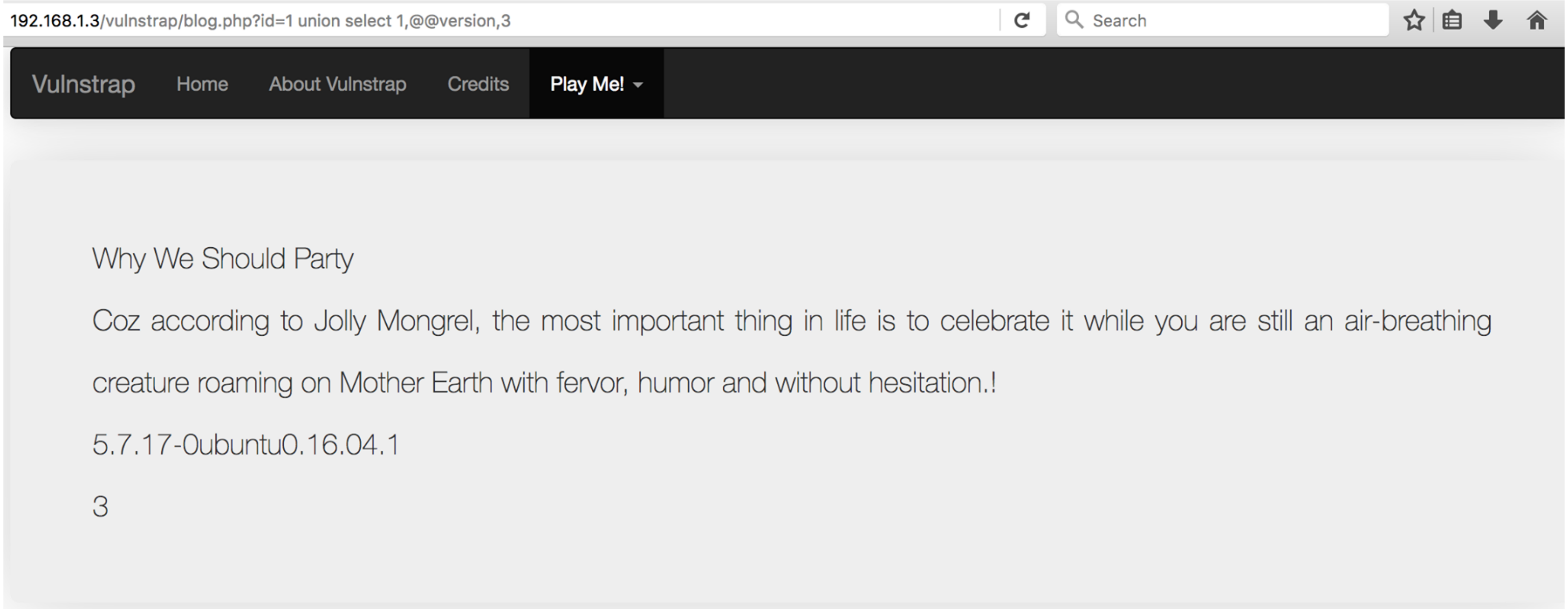
XSS (CROSS-SITE SCRIPTING)


Cross-Site Scripting – App
Stormpath
https://www.google.com/about/appsecurity/learning/xss/#BasicE...
Apps
Bookmarks
Javascript
Java
Browser Testing
YNAB
Finance

Demo application 1:

URL https://xss-doc.appspot.com/demo/2 Go

SQL INJECTION



```
192.168.1.3/vulnstrap/blog.php?id=1 union select 1,@@version,3
```

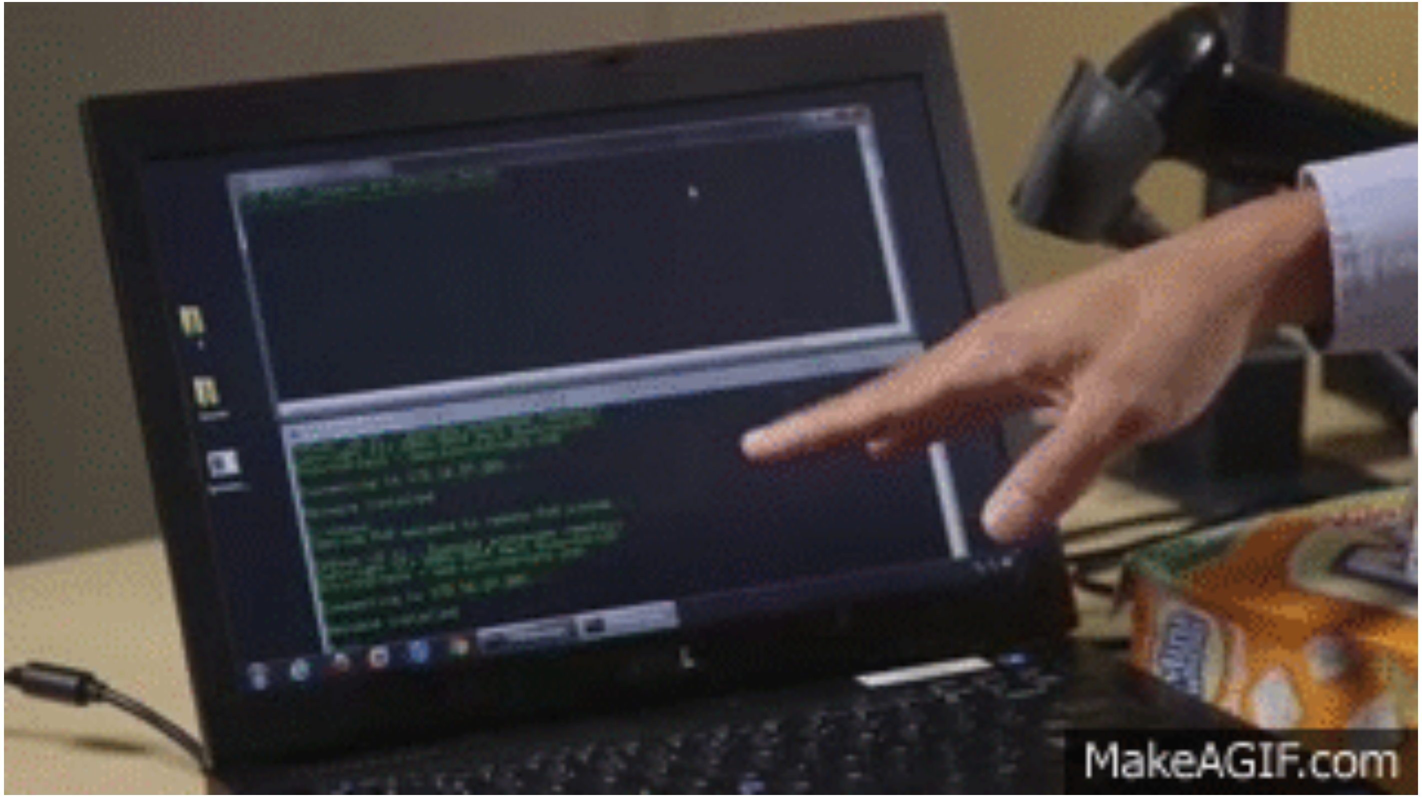
Why We Should Party

Coz according to Jolly Mongrel, the most important thing in life is to celebrate it while you are still an air-breathing creature roaming on Mother Earth with fervor, humor and without hesitation.!

5.7.17-0ubuntu0.16.04.1

3

LET'S HAVE SOME DEMO



QUESTIONS?