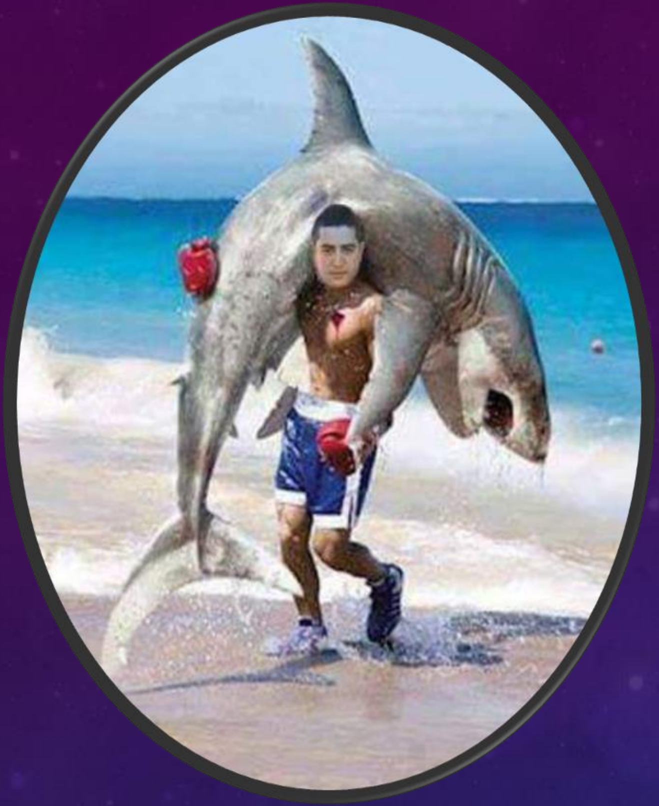
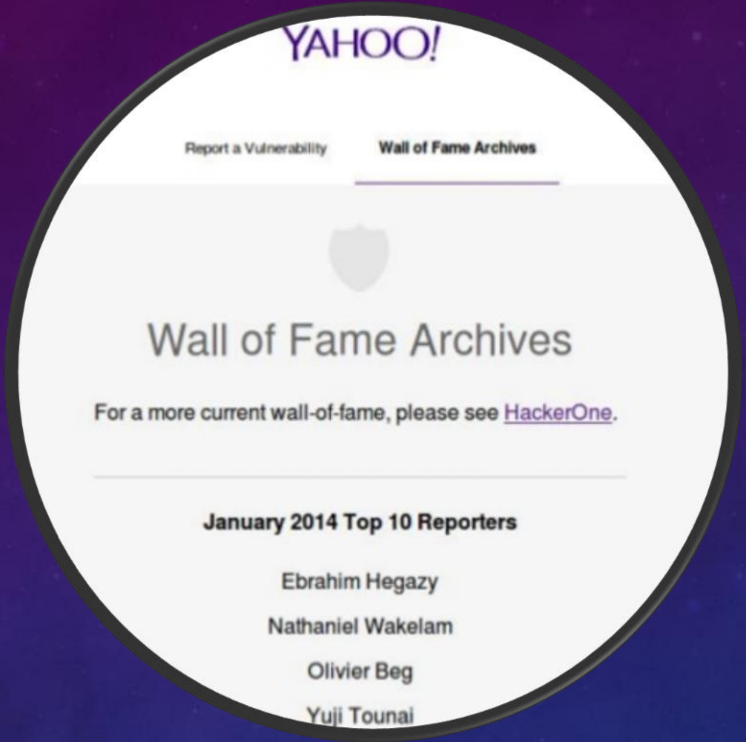
BUG BOUNTY HUNTING

BY EBRAHEM HEGAZY





YAHOO!

Report a Vulnerability | Wall of Fame Archives

Wall of Fame Archives

For a more current wall-of-fame, please see HackerOne.

January 2014 Top 10 Reporters

Ebrahim Hegazy

Nathaniel Wakelam

Olivier Beg

Yuji Tounai

AGENDA

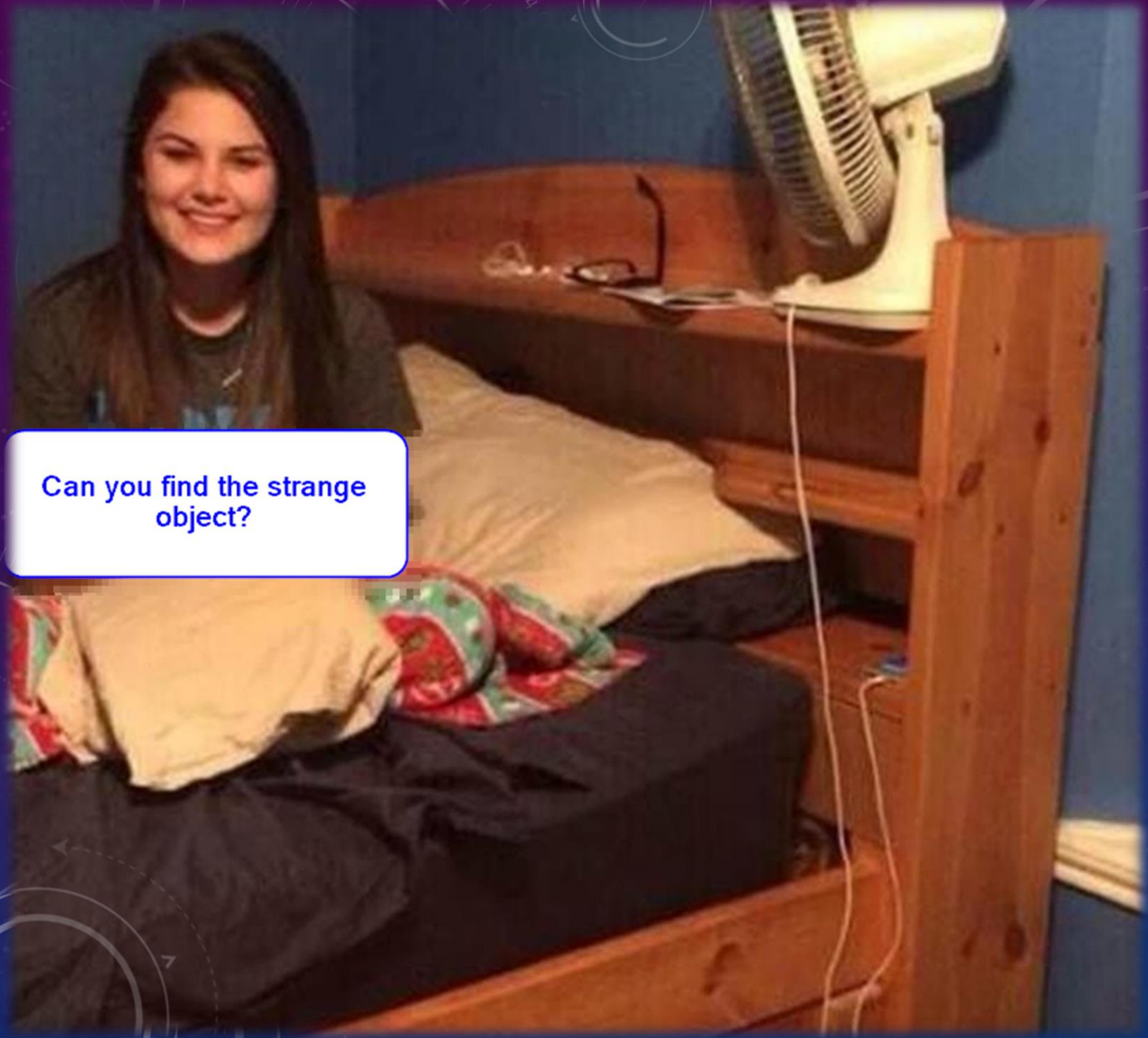
- What are bug bounty programs & why we need it?
- Bug bounty platforms
- How to get started?
- Bug bounty hunting methodology
- Demo on Yahoo and PayPal vulnerabilities
- Resources
- Questions

WHAT ARE BUG BOUNTY PROGRAMS?

When a company starts to offer rewards for security researchers to find vulnerabilities in their infrastructure and applications, under their rules, this is what is so called “Bug Bounty Program”.

Google
facebook
twitter
PayPal
mozill
Mic osoft
Bug Bounty
NOKIA
avast! be free
BARRACUDA NETWORKS
MediaFire

- Yahoo pays a minimum of $50 and up to $15,000
- Google pays a minimum of $100 and up to $20,000
- Facebook pays a minimum of $500 and no max payout
- Github Pays a minimum of $500



WHY DO WE NEED BUG BOUNTY PROGRAMS?

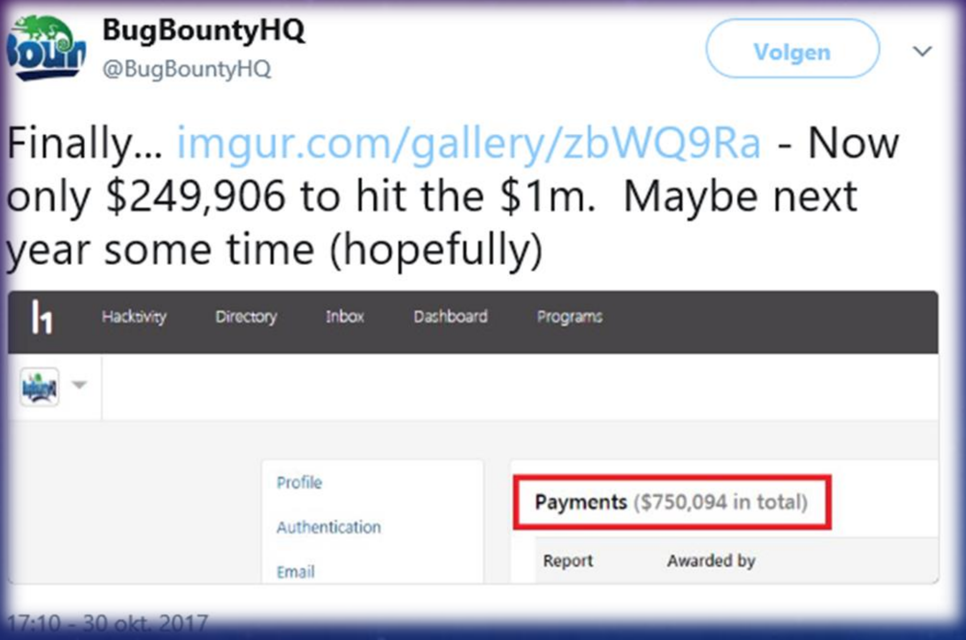
Why do we need Bug Bounty Programs?

As a researcher :

- Ease of getting a job in the industry
- Good opportunity to make $$$$
- Better Experience

As a company:

- Less Security Breaches!
- Better and more secure Apps, Networks etc...
- More researchers from across the world.

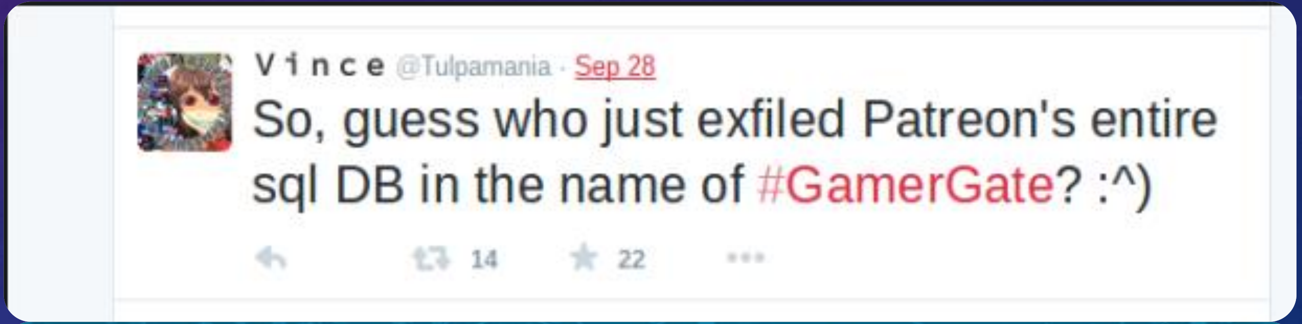


BugBountyHQ
@BugBountyHQ

Finally... imgur.com/gallery/zbWQ9Ra - Now only $249,906 to hit the $1m. Maybe next year some time (hopefully)

Payments ($750,094 in total)

17:10 - 30 okt. 2017

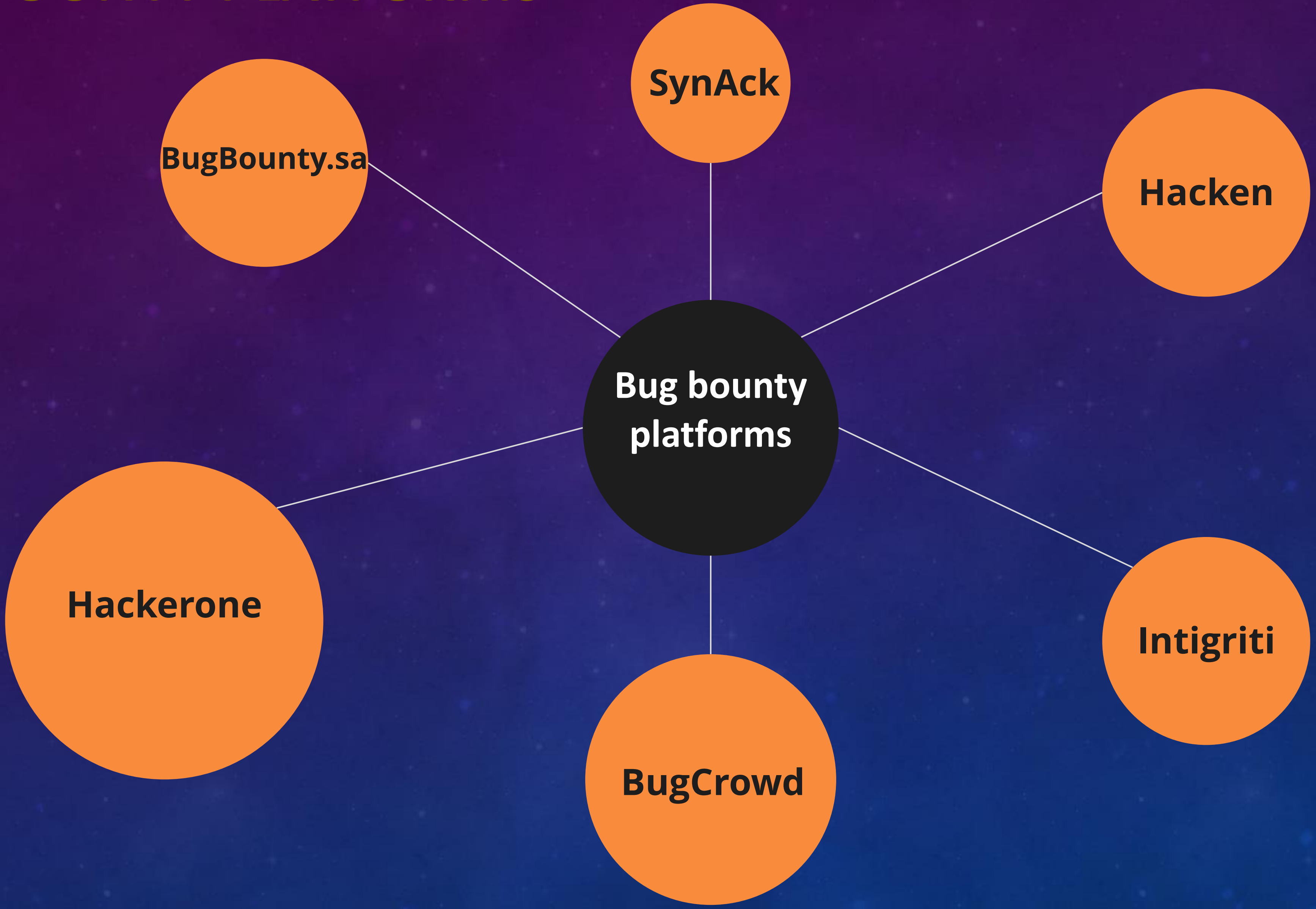


Vince @Tulpamania · Sep 28

So, guess who just exfiled Patreon's entire sql DB in the name of #GamerGate? :^)

'DATA BREACH' DAY
HACKED!
T-Mobile
15 Million
Patreon
2.3 Million
Scottrade
4.6 Million

BUG BOUNTY PLATFORMS



Bug bounty platforms

SynAck

BugBounty.sa

Hacken

Hackerone

Intigriti

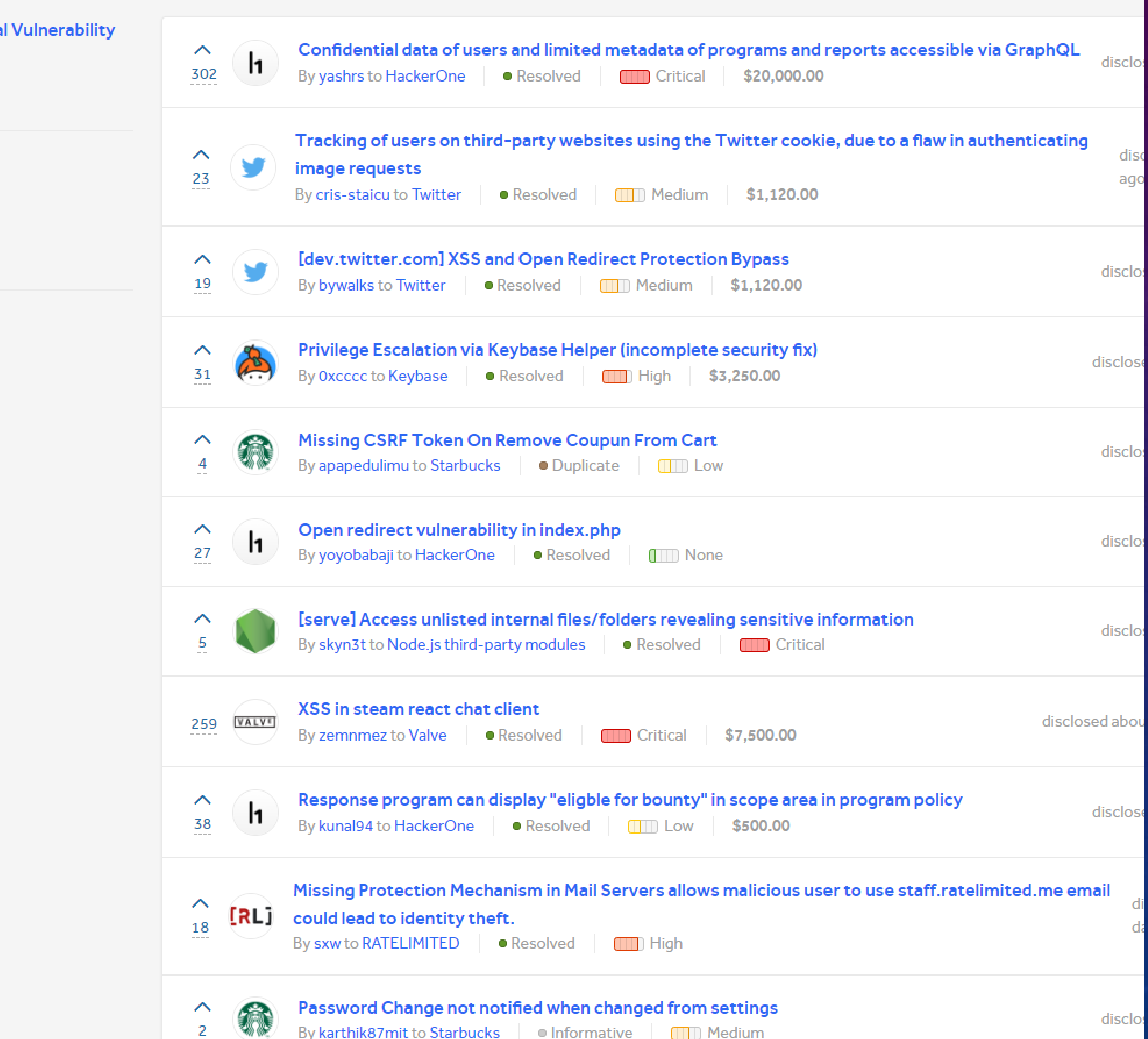
BugCrowd

BUGBOUNTY.SA PLATFORM

Bugbounty.sa is bug bounty hunting platform dedicated for Saudi's.

Largest Saudi's companies are hosted in there, and allows you to research, identify and report security vulnerabilities in their systems.

Monetary rewards varies between 3000 SAR to 50,000 SAR based on the severity.



l Vulnerability

302 Confidential data of users and limited metadata of programs and reports accessible via GraphQL
By yashrs to HackerOne | ● Resolved | Critical | $20,000.00 disclo

23 Tracking of users on third-party websites using the Twitter cookie, due to a flaw in authenticating image requests
By cris-staicu to Twitter | ● Resolved | Medium | $1,120.00 disc ago

19 [dev.twitter.com] XSS and Open Redirect Protection Bypass
By bywalks to Twitter | ● Resolved | Medium | $1,120.00 disclo

31 Privilege Escalation via Keybase Helper (incomplete security fix)
By 0xcccc to Keybase | ● Resolved | High | $3,250.00 disclose

4 Missing CSRF Token On Remove Coupun From Cart
By apapedulimu to Starbucks | ● Duplicate | Low disclo

27 Open redirect vulnerability in index.php
By yoyobabaji to HackerOne | ● Resolved | None disclo

5 [serve] Access unlisted internal files/folders revealing sensitive information
By skyn3t to Node.js third-party modules | ● Resolved | Critical disclo

259 XSS in steam react chat client
By zemnmez to Valve | ● Resolved | Critical | $7,500.00 disclosed abou

38 Response program can display "eligble for bounty" in scope area in program policy
By kunal94 to HackerOne | ● Resolved | Low | $500.00 disclose

18 Missing Protection Mechanism in Mail Servers allows malicious user to use staff.ratelimited.me email could lead to identity theft.
By sxw to RATELIMITED | ● Resolved | High di da

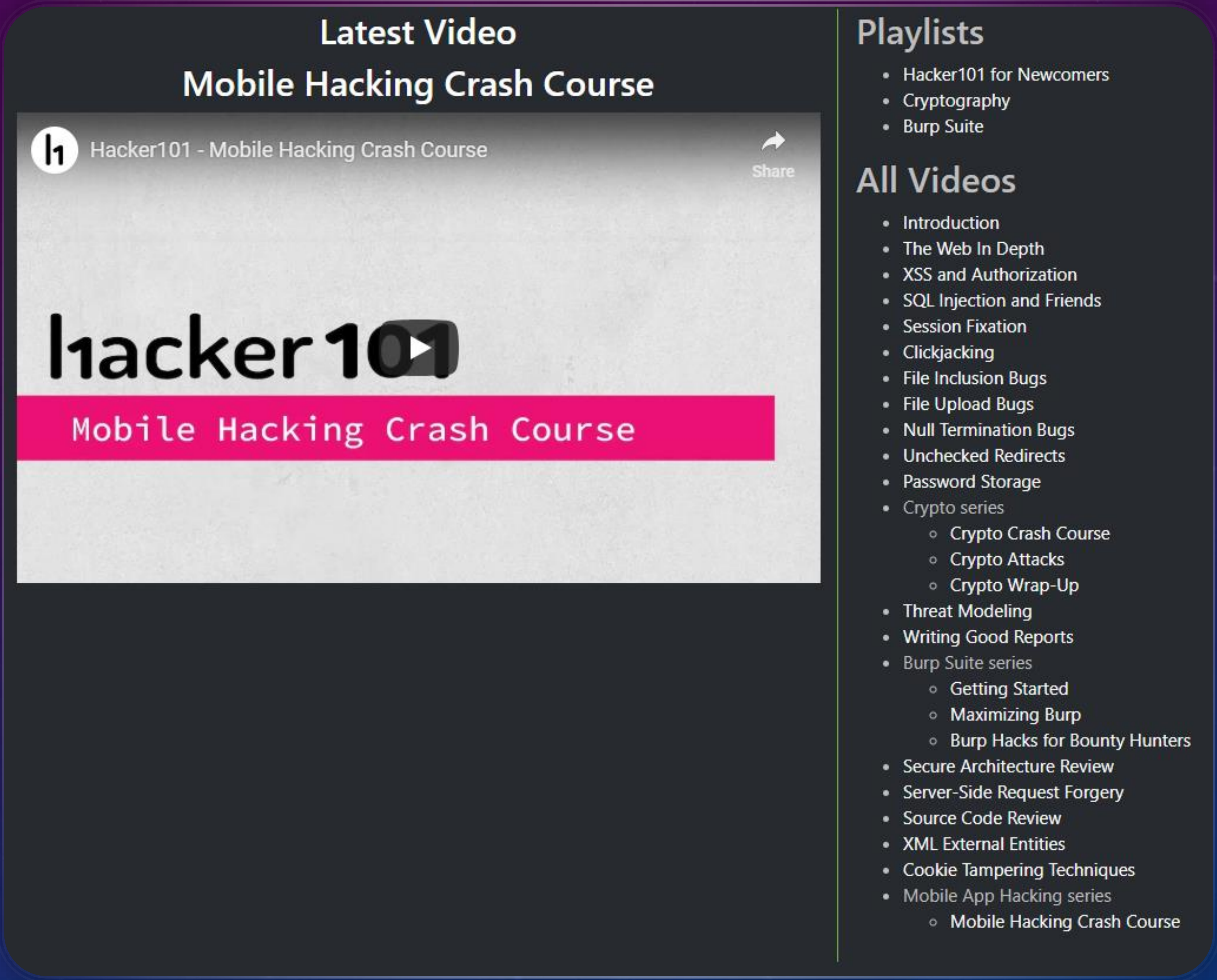
2 Password Change not notified when changed from settings
By karthik87mit to Starbucks | ● Informative | Medium disclo

HOW TO GET STARTED?

There are many resources that could get you started in bug bounty hunting. Such as:

- Web Applications Hackers Handbook
- Pentesting4Arabs on Youtube
- Hacker101.com
- HackerOne.com Hacktivity

HOW TO GET STARTED?



Latest Video

Mobile Hacking Crash Course

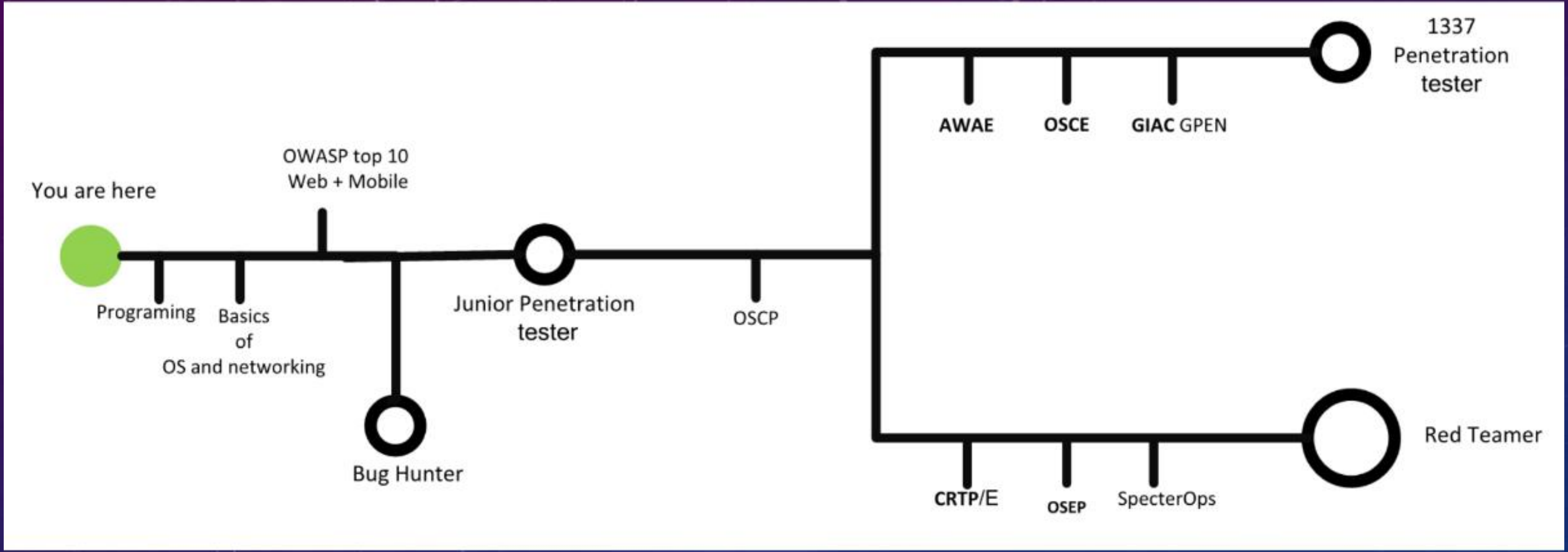
Hacker101 - Mobile Hacking Crash Course
Share
hacker101
Mobile Hacking Crash Course

Playlists

- Hacker101 for Newcomers
- Cryptography
- Burp Suite

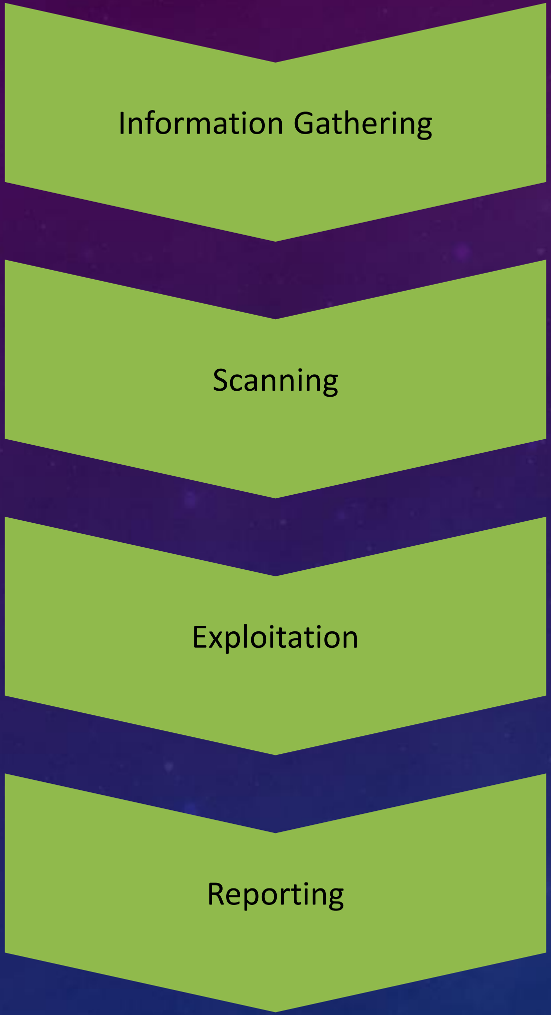
All Videos

- Introduction
- The Web In Depth
- XSS and Authorization
- SQL Injection and Friends
- Session Fixation
- Clickjacking
- File Inclusion Bugs
- File Upload Bugs
- Null Termination Bugs
- Unchecked Redirects
- Password Storage
- Crypto series
  - Crypto Crash Course
  - Crypto Attacks
  - Crypto Wrap-Up
- Threat Modeling
- Writing Good Reports
- Burp Suite series
  - Getting Started
  - Maximizing Burp
  - Burp Hacks for Bounty Hunters
- Secure Architecture Review
- Server-Side Request Forgery
- Source Code Review
- XML External Entities
- Cookie Tampering Techniques
- Mobile App Hacking series
  - Mobile Hacking Crash Course


1337
Penetration
tester
AWAE
OSCE
GIAC GPEN
OWASP top 10
Web + Mobile
You are here
Programing
Basics
of
OS and networking
Junior Penetration
tester
OSCP
Bug Hunter
Red Teamer
CRTP/E
OSEP
SpecterOps

ROADMAP

BUG BOUNTY HUNTING METHODOLOGY



Information Gathering

- Information gathering is always the first step to be performed. Information gathering includes:
  - Collecting as much as possible of sub-domains used by the target in scope
  - Identify the technology used within the applications (i.e. Tomcat, AngularJS, and DBMS)

Scanning

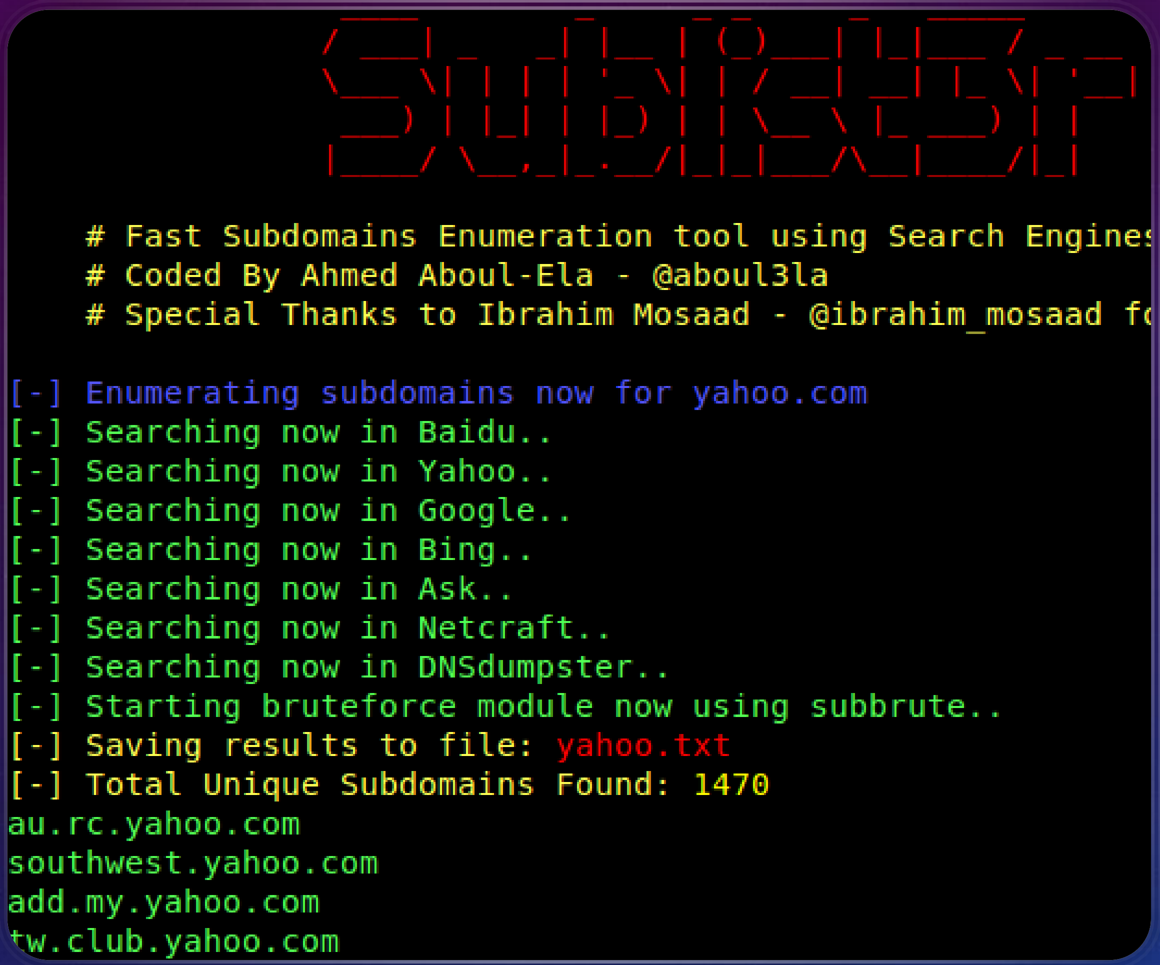
- Scanning stage is used to identify as much information as possible about the identified subdomains and applications. This includes:
  - Port scanning using Nmap, and vulnerability scanning, using BurpSuite scanner.
  - Files and directories brute-forcing, in order to identify backup files, test and development files.

Exploitation

- Once a vulnerability is identified, it is now the time to try to exploit it. When exploiting a vulnerability, make sure to:
  - Never access sensitive data, but only retrieve data sample that could be used as a proof of concept
  - Avoid abusing administrative privileges, if your vulnerability allows for privilege escalation to administrator account

Reporting

- Once you are done with the exploitation stage, and have got a good proof of concept, it is now reporting time. Your report must include:
  - Detailed information about the identified vulnerability
  - How an attacker could exploit it? Are certain privileges required? Or any internet user can exploit it?
  - Proof of concept (i.e. Screenshots)



```
                 ____        _     _ _     _   _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

    # Fast Subdomains Enumeration tool using Search Engines
    # Coded By Ahmed Aboul-Ela - @aboul3la
    # Special Thanks to Ibrahim Mosaad - @ibrahim_mosaad fo

[-] Enumerating subdomains now for yahoo.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Starting bruteforce module now using subbrute..
[-] Saving results to file: yahoo.txt
[-] Total Unique Subdomains Found: 1470
au.rc.yahoo.com
southwest.yahoo.com
add.my.yahoo.com
tw.club.yahoo.com
```

MOST KNOWN TOOLS

BURPSUITE – A proxy tool, and includes vulnerabilities security scanner.

SUBLIST3R – A python script used to collect sub-domains of the target website.

AMASS – An extensive external assets discovery tool

NUCLI: An automated tool to identify vulnerabilities on a large scope. It includes templates for most known vulnerabilities

NMAP – A port scanner, and it also includes vulnerability testing scripts

SQLMAP – A tool used to exploit SQL injection vulnerabilities

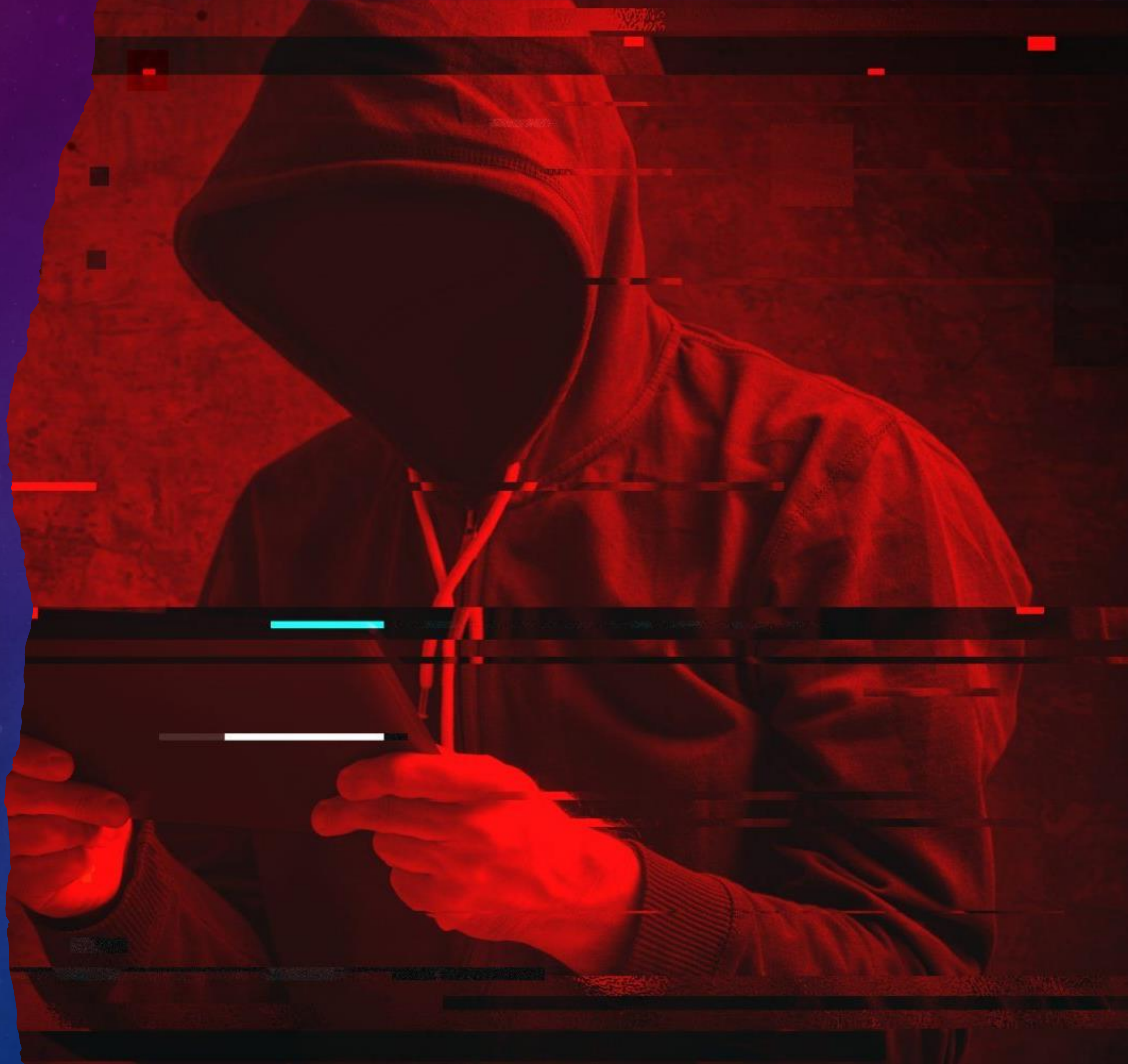
EYEWITNESS – A python tool to take screenshots of large applications sets. It can also perform credentials brute-forcing.

DIRSEARCH – A simple tool to brute-force files and directories names, in order to identify backup and test files.

DIRBUSTER – Similar to DirSearcher.

BROWSER PLUGINS (Flagfox, Wappalyzer)

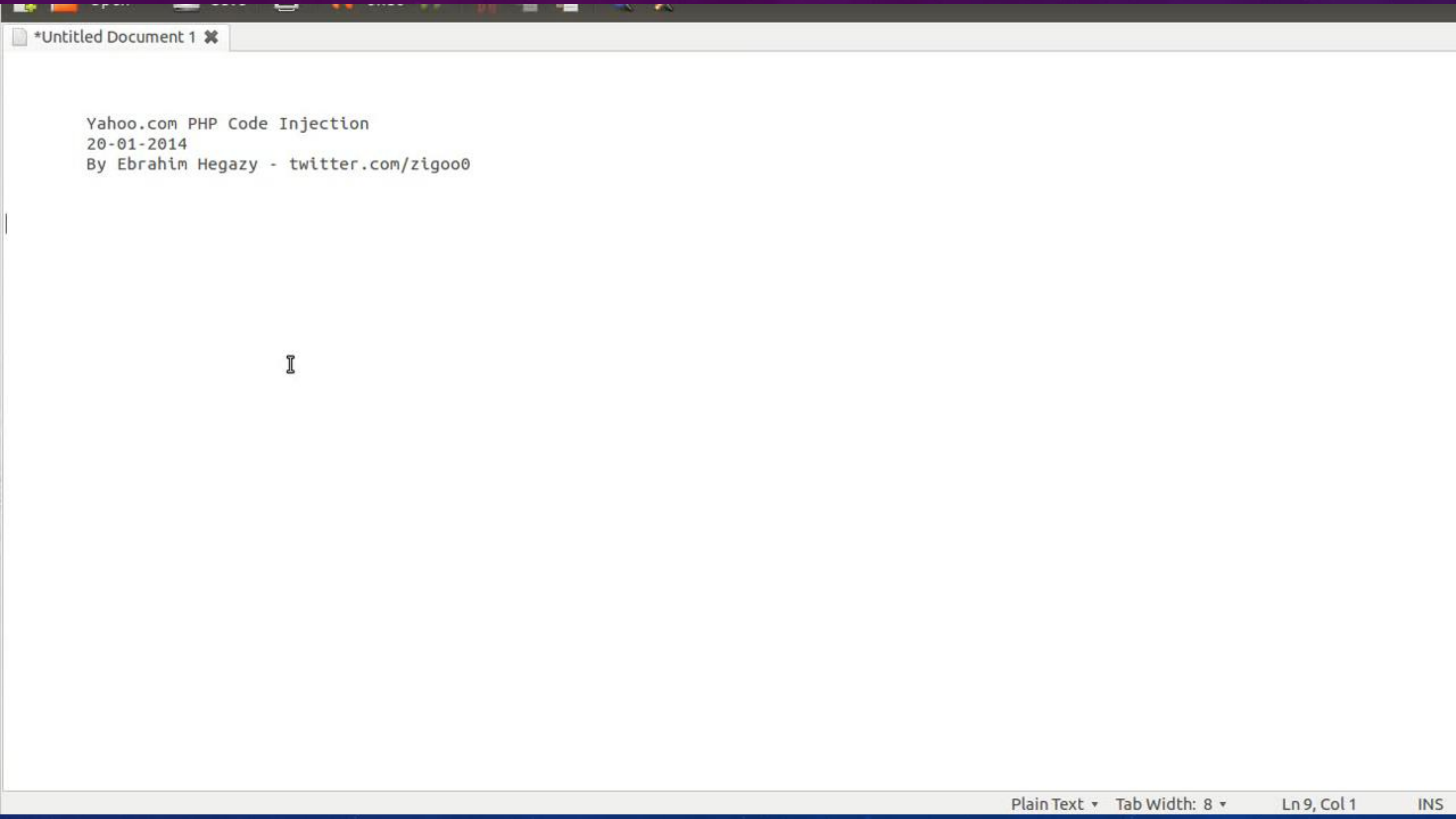
DEMO TIME!



DEMO 1 – YAHOO REMOTE CODE EXECUTION VULNERABILITY

One of the Yahoo applications was vulnerable to remote code execution (RCE) due to passing user input to eval() function.

What could go wrong?

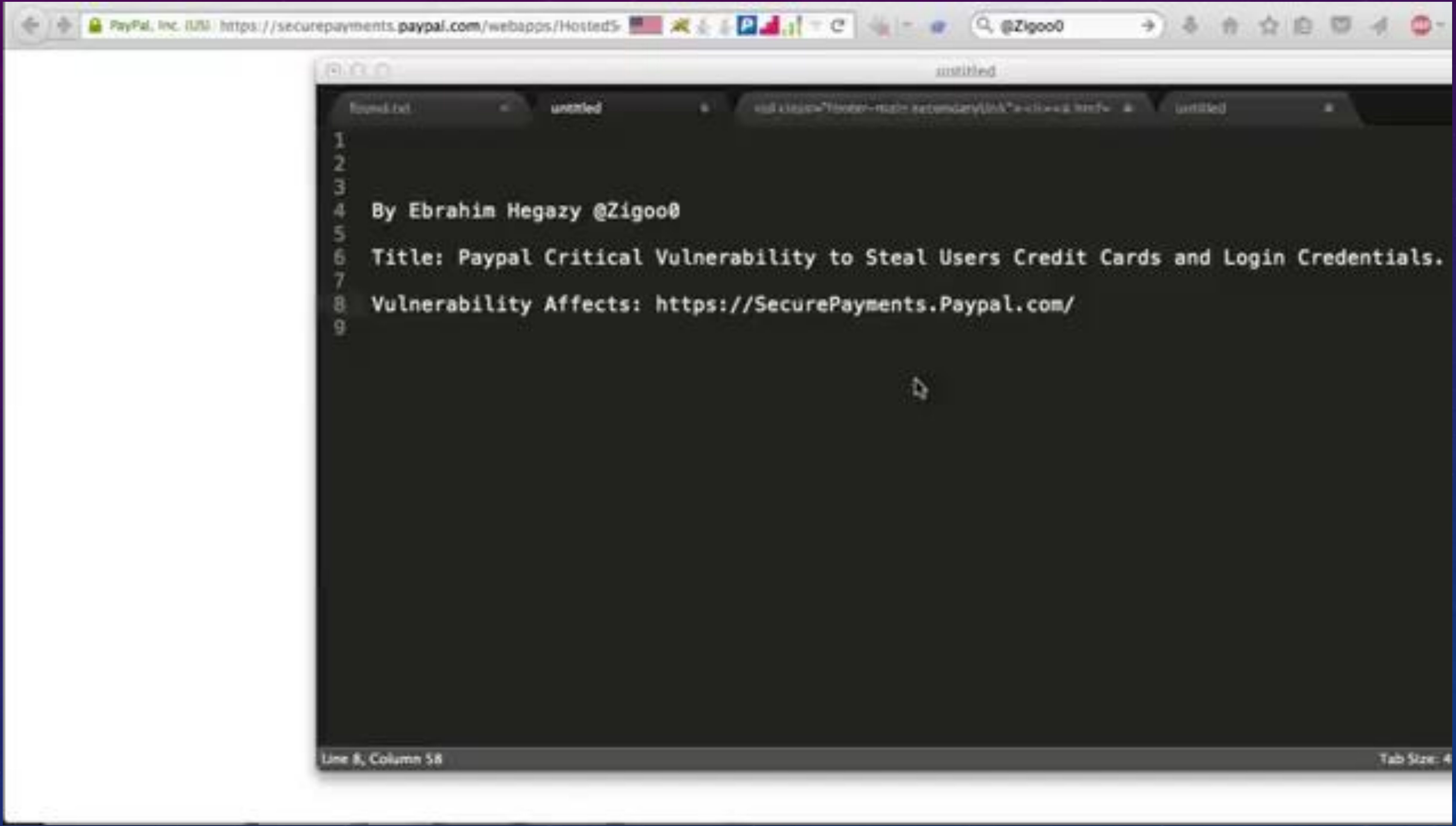


```
Yahoo.com PHP Code Injection
20-01-2014
By Ebrahim Hegazy - twitter.com/zigoo0
```

DEMO 2 – PAYPAL STORED CROSS-SITE SCRIPTING (XSS)

Stored XSS occurs when a web application gathers input from a user which might be malicious, and then stores that input in a data store for later use. The input that is stored is not correctly filtered.

As a consequence, the malicious data will appear to be part of the web site and run within the user’s browser under the privileges of the web application.


PayPal, Inc. (US) https://securepayments.paypal.com/webapps/HostedS
@Zigoo0
untitled
untitled
Line 8, Column 58
Tab Size: 4

By Ebrahim Hegazy @Zigoo0

Title: Paypal Critical Vulnerability to Steal Users Credit Cards and Login Credentials.

Vulnerability Affects: https://SecurePayments.Paypal.com/

USEFUL RESOURCES

Your Roadmap to Bugbounty Hunting, Pentesting and Red Teaming:
https://www.youtube.com/watch?v=f3hP49LGoik

Pentesting4Arabs Course:
https://www.youtube.com/watch?v=BjfCWSFmIFI&list=PLv7cogHXoVhXvHPzIl1dWtBiYUAL8baHj

HackerOne Hacktivity
https://hackerone.com/hacktivity

BugCrowd bug hunters methodology
https://www.bugcrowd.com/about/blog/topic/bug-hunter-methodology/

Bug Bounty Cheat Sheet
https://github.com/EdOverflow/bugbounty-cheatsheet

Awesome Bug Bounty List
https://github.com/djadmin/awesome-bug-bounty

Bug Bounty Reference
https://github.com/ngalongc/bug-bounty-reference

QUESTIONS?

STAY IN TOUCH!

- https://www.twitter.com/zigoo0
- https://www.sec-down.com
- https://www.youtube.com/zigoo0