

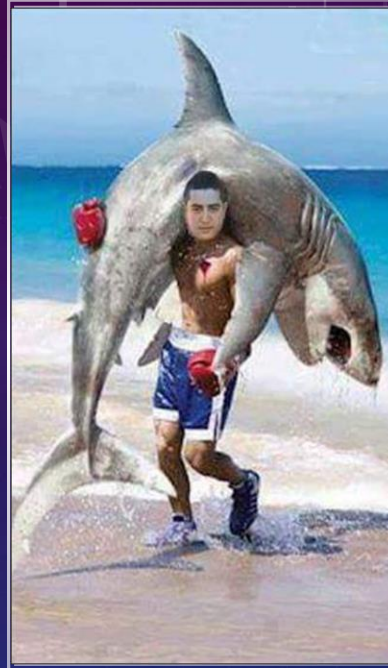
# YOUR ROADMAP TO PENTESTING, BUG HUNTING, AND RED TEAMING

---

BY EBRAHEM HEGAZY







COURSE:~# WHOAMI





# AGENDA

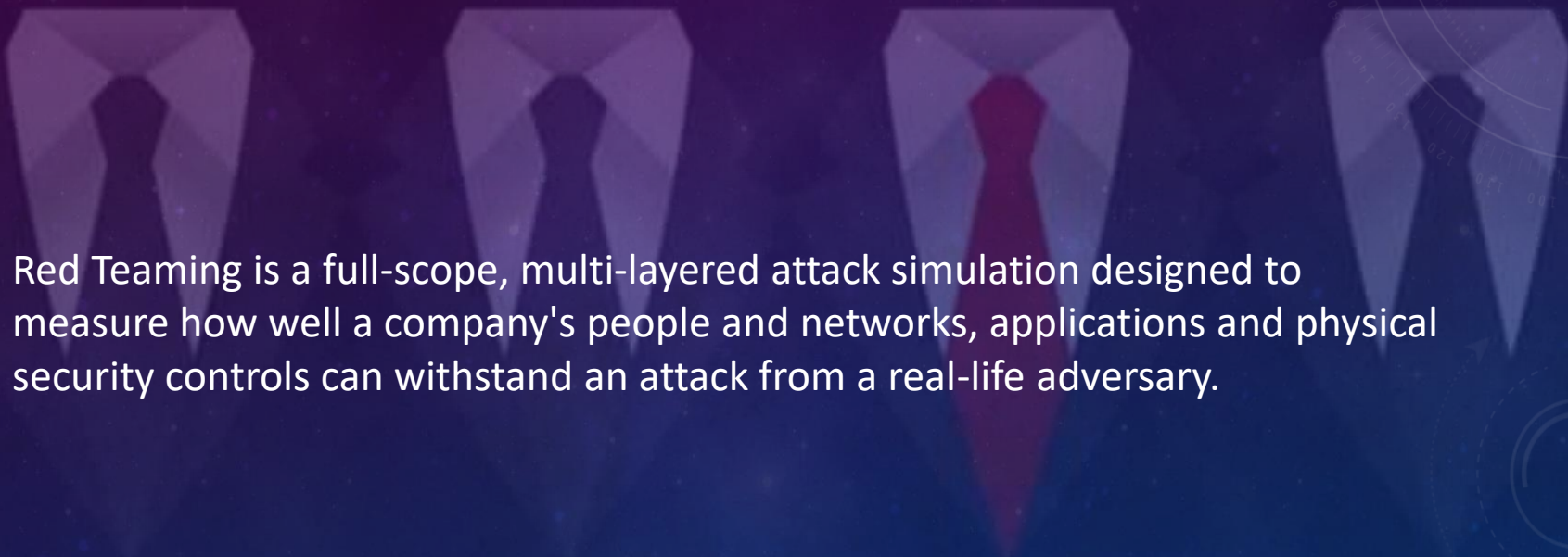
- Pentesting, Bug Bounty hunting, and Red Teaming 101
- RoadMap
- T-Learning model
- MoSCoW technique
- References & contact

# WHAT IS PENTESTING?

Penetration testing (or Pentesting) is a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a defined scope of systems.














# WHAT IS RED TEAMING?



Red Teaming is a full-scope, multi-layered attack simulation designed to measure how well a company's people and networks, applications and physical security controls can withstand an attack from a real-life adversary.

# WHAT IS BUG BOUNTY HUNTING?

Bug bounty hunting is the process of identifying and reporting vulnerabilities in a company defined scope of assets, for which you get rewarded in return.

302		<b>Confidential data of users and limited metadata of programs and reports accessible via GraphQL</b> By yashrs to HackerOne   ● Resolved   Critical   \$20,000.00	
23		<b>Tracking of users on third-party websites using the Twitter cookie, due to a flaw in authenticating image requests</b> By cris-staicu to Twitter   ● Resolved   Medium   \$1,120.00	
19		<b>[dev.twitter.com] XSS and Open Redirect Protection Bypass</b> By bywalks to Twitter   ● Resolved   Medium   \$1,120.00	
31		<b>Privilege Escalation via Keybase Helper (incomplete security fix)</b> By 0xcccc to Keybase   ● Resolved   High   \$3,250.00	
4		<b>Missing CSRF Token On Remove Coupon From Cart</b> By apapedulimu to Starbucks   Duplicate   Low	
27		<b>Open redirect vulnerability in index.php</b> By yoyobabaji to HackerOne   ● Resolved   None	
5		<b>[serve] Access unlisted internal files/folders revealing sensitive information</b> By skyn3t to Node.js third-party modules   ● Resolved   Critical	
259		<b>XSS in steam react chat client</b> By zemnmez to Valve   ● Resolved   Critical   \$7,500.00	disclosed
38		<b>Response program can display "eligible for bounty" in scope area in program policy</b> By kunal94 to HackerOne   ● Resolved   Low   \$500.00	disclosed
18		<b>Missing Protection Mechanism in Mail Servers allows malicious user to use staff.ratelimited.me email could lead to identity theft.</b> By sxw to RATELIMITED   ● Resolved   High	
2		<b>Password Change not notified when changed from settings</b> By karthik87mit to Starbucks   Informative   Medium	



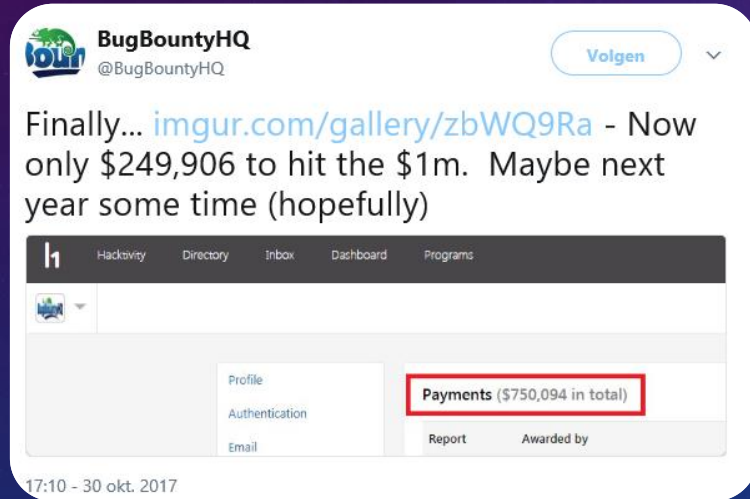
# WHY DO WE NEED BUG BOUNTY PROGRAMS?

## As a researcher :

- Possibility of getting a (better) 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 to research your assets



The screenshot shows the BugBountyHQ profile page on a social media platform. The profile name is BugBountyHQ (@BugBountyHQ) with a blue verified badge. The bio reads: "Finally... [imgur.com/gallery/zbWQ9Ra](https://imgur.com/gallery/zbWQ9Ra) - Now only \$249,906 to hit the \$1m. Maybe next year some time (hopefully)". Below the bio is a navigation bar with links: Hacktivity, Directory, Inbox, Dashboard, and Programs. Under the navigation bar, there is a sidebar with links: Profile, Authentication, and Email. The main content area shows a "Payments" section with a red box around the text "Payments (\$750,094 in total)". Below this, there are links for "Report" and "Awarded by". The date "17:10 - 30 okt. 2017" is visible at the bottom left.



The screenshot shows a tweet by Vince @Tulpamania dated Sep 28. The tweet text is: "So, guess who just exfiltrated Patreon's entire sql DB in the name of #GamerGate? :^)". The tweet has 14 retweets and 22 likes.



The graphic is titled "DATA BREACH' DAY HACKED!" and lists three companies with their user counts:

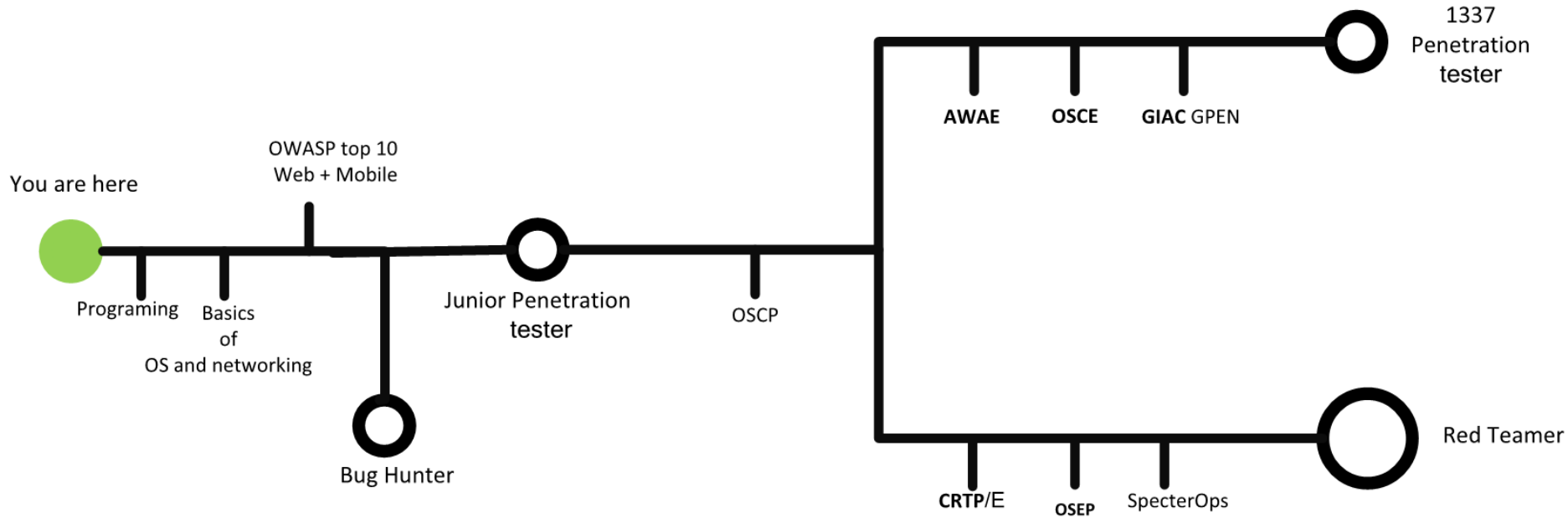
Company	User Count
T-Mobile	15 Million
Patreon	2.3 Million
Scottrade	4.6 Million

The background is a dark teal color. On the left side, there are several concentric circular patterns with dashed lines and arrows, resembling a compass or a radar screen. A large circular scale with numerical markings from 140 to 260 is visible. A path of four glowing green circles is connected by a dashed line, starting from the left and moving towards the right. At the bottom center, there is a cluster of small, glowing white dots arranged in a circular pattern.

# ROADMAP



انا كنت مفكر انه  
كورس واحد  
هذاكره  
والبس بعدها  
الجاكت  
أبوظعبوط!

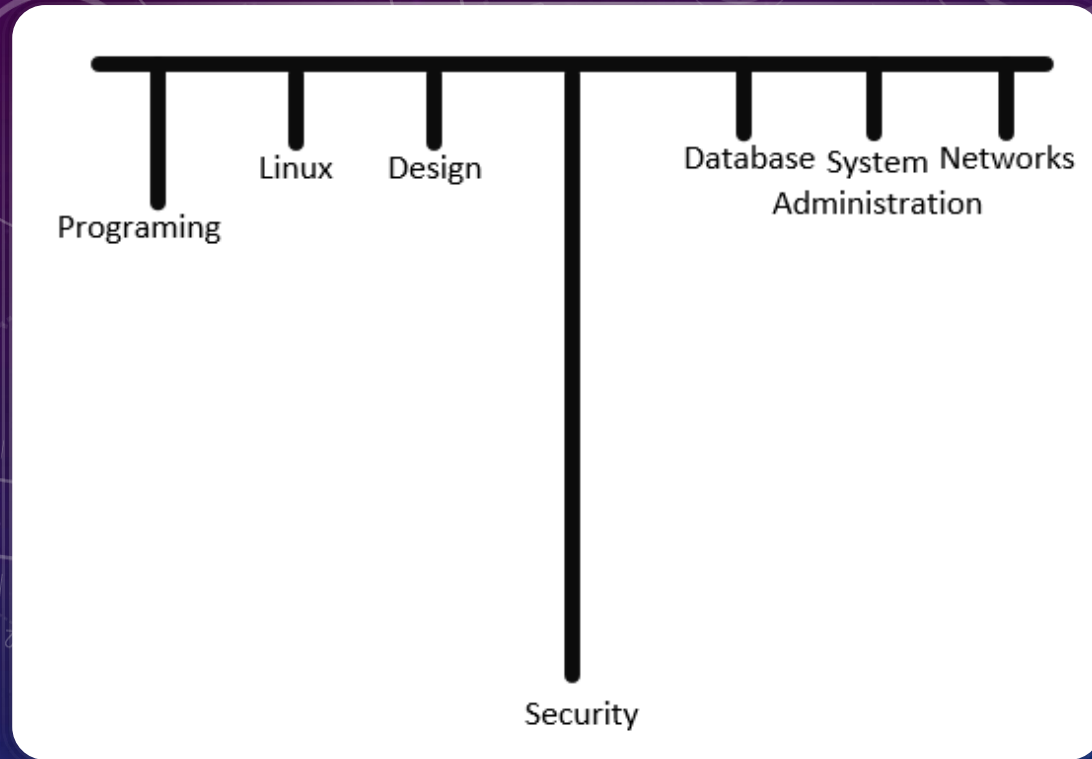


# ROADMAP



# هنتعلم کل ده ازاي؟





# T-LEARNING MODEL



# MOSCOW TECHNIQUE

MoSCoW prioritization, also known as the MoSCoW method or MoSCoW analysis, is a prioritization technique for managing tasks/project. But it could also be used to prioritize anything.

HTML

HTML5

CSS

JavaScript

PHP from XYZ

PHP from ABC

OOP

MYSQL


Oracle

MSSQL

How to write Secure code

Networking

Cisco CCNA

Must	Should	Could	Won't
PHP from XYZ MYSQL  (Ctrl) ▾	<u>JavaScript</u> HTML CSS OOP	PHP from ABC	



ANY  
QUESTIONS  
?

# REFERENCES

- Intro to 13 InfoSec jobs - <https://www.youtube.com/watch?v=fzkHCqCJ0as>
- MoSCoW technique - <https://www.youtube.com/watch?v=wRF9dAo7-W8>
- Youtube course - <https://www.youtube.com/user/Zigoo0>
- Facebook group for questions - <https://www.facebook.com/groups/pentesting4arabs/>
- The Bug Hunter's Methodology v4 - <https://www.youtube.com/watch?v=p4Jglu1mcel>
- Courses Links:
  - Web Security Academy: <https://portswigger.net/web-security>
  - CyberTalents: <https://cybertalents.com/>
  - RootMe: <https://www.root-me.org/en/Challenges/>
  - OSEP: <https://www.offensive-security.com/pen300-osep/>
  - SpecterOps course: <https://specterops.io/how-we-help/training-offerings/adversary-tactics-red-team-operations>

# CONTACT ME

[Twitter.com/zigoo0](https://twitter.com/zigoo0)

[Facebook.com/zigoo.eg](https://facebook.com/zigoo.eg)

