Bug Bounty:
A Hunter's Perspective

Miftahul Huq (discord:arpping#5837)

Agenda

01 About me

02 Introduction to BBP

03 Why hunt for bug?

04 Types of bug hunters

05 How to get started

06 Tips for bug hunting

07 Collaboration

08 Reality of bug hunting

~$ Whoami

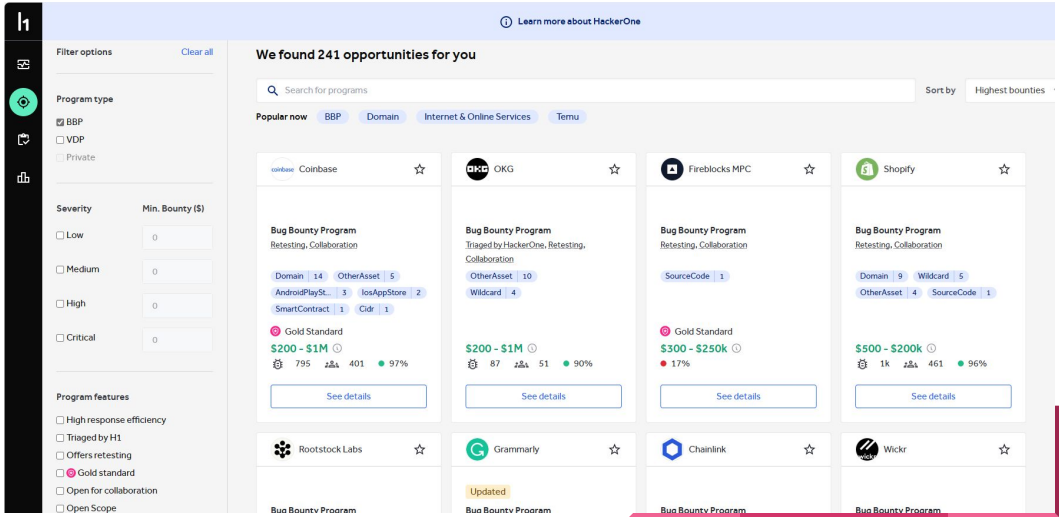
- Miftahul Huq
- 4th yr, BS/MS Cybersecurity Student @ RIT
- Part-time bug hunter (3 months)
- Hobby: videography

What is Bug Bounty Program (BBP)?

- A program where bug bounty hunters earn compensation, or bounty, for revealing security gaps of a company.

- **Types of Bug Bounties:**
  - Web App
  - Mobile App
  - Network infrastructure
  - Hardware
  - API Security

- Hosted via a BBP platform



Top BBP Platforms

Why hunt for bugs?

- Source of income
- Hack legally
- Recognition, prestige, and competition

Types of bug hunters

- All these methods works successfully.

Fully automated and unauthenticated

Fully manual

50/50

0-day all day

How to get started

Just like any other things in life, you just gotta start doing it:

- Create an account on a BBP platform.
- Pick a BBP from a company of your choice.
- Use a hunter’s method to start hunting for bugs.

Learning the basics

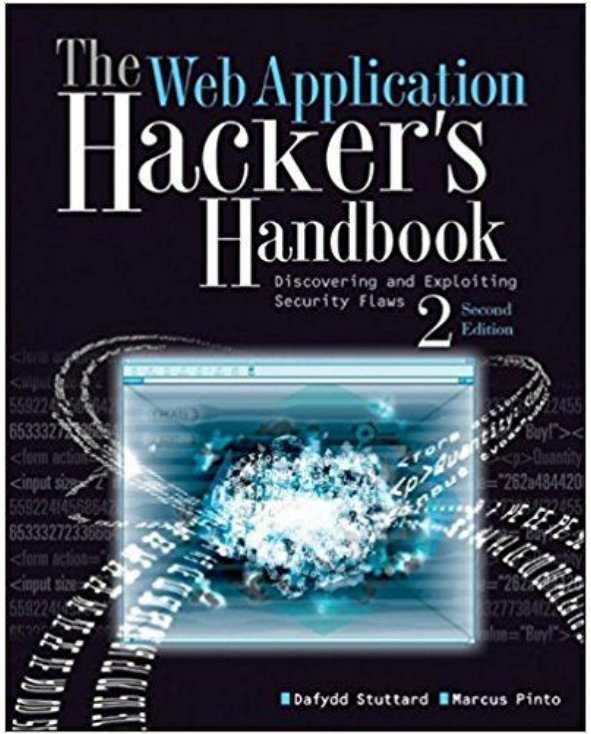
Top platform to learn from:

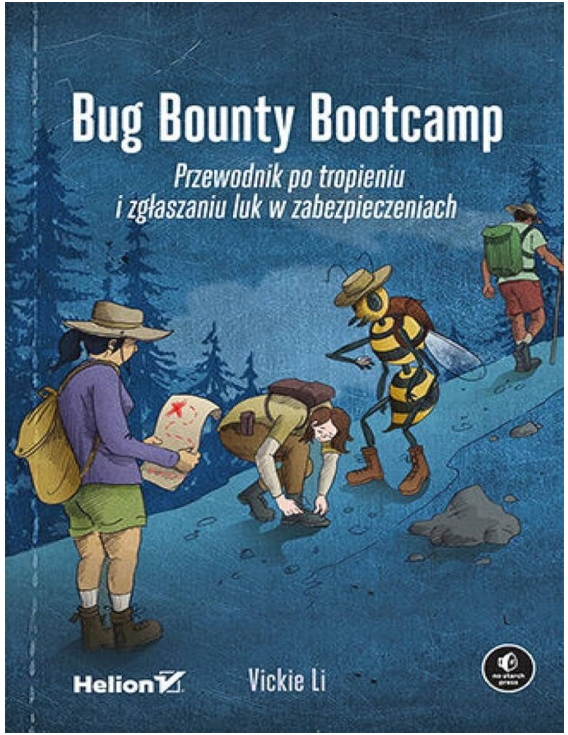
- Hackerone capture the flag
  - Private invitation after completion
- WebSecurity academy (by Portswigger)
- PentesterLab

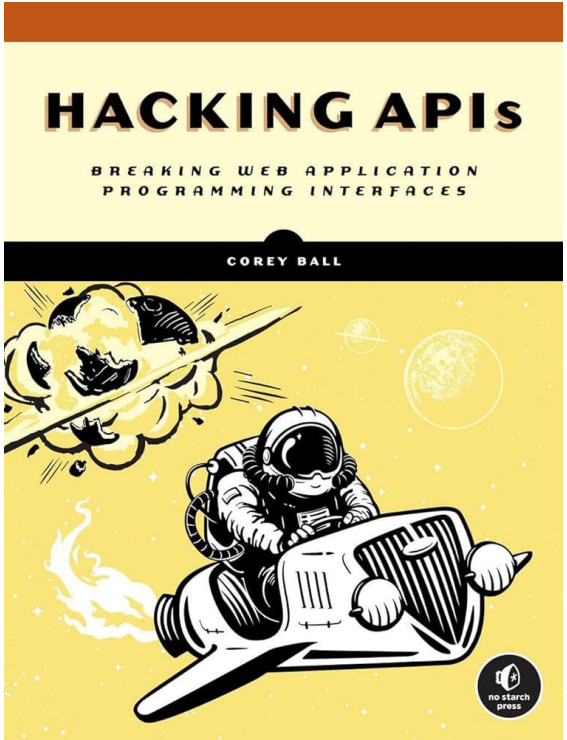
Others:

- HackTheBox
- TryHackMe

Some books to consider are…



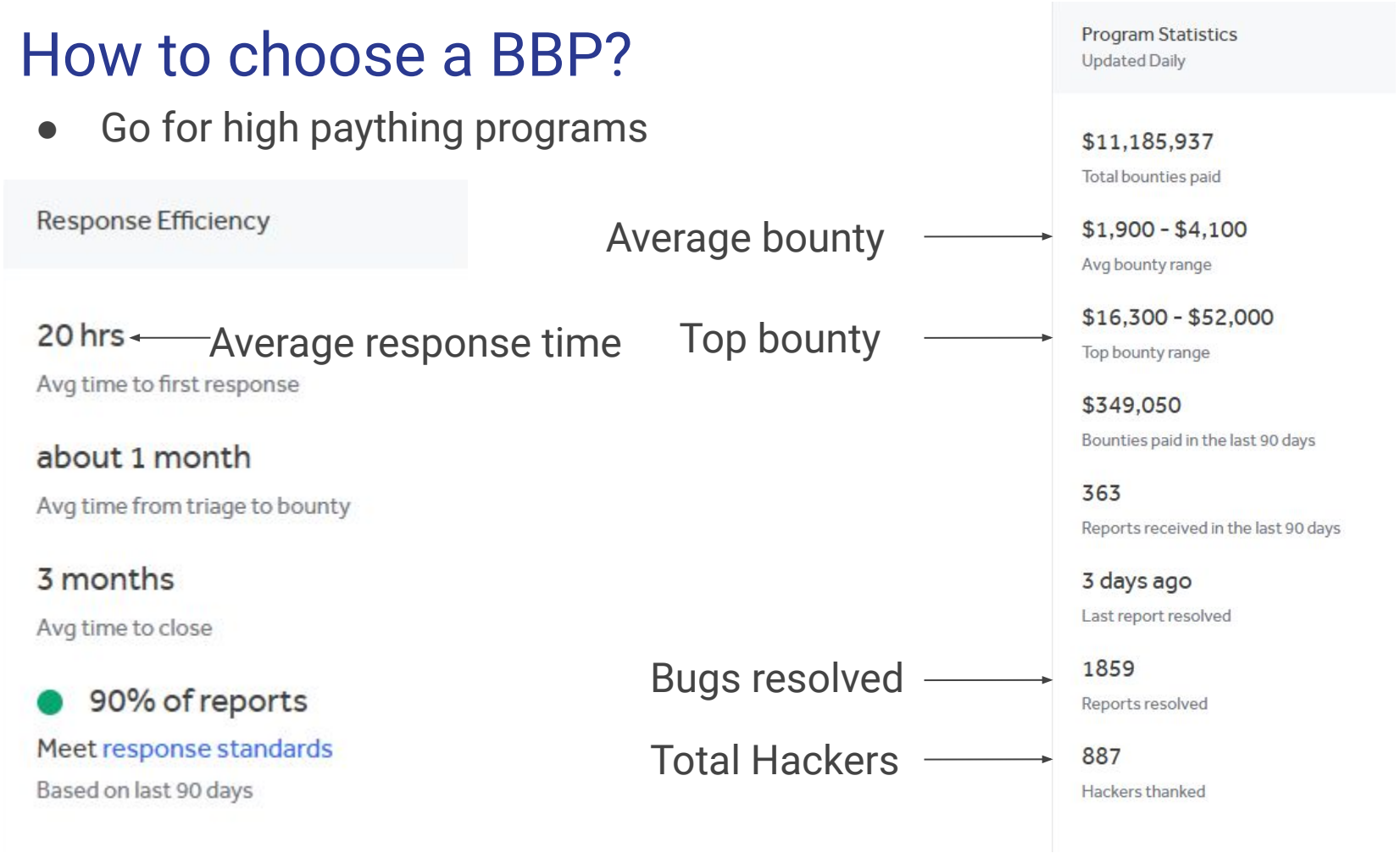




Tips for bug hunting

How to choose a BBP?

- Go for high paything programs



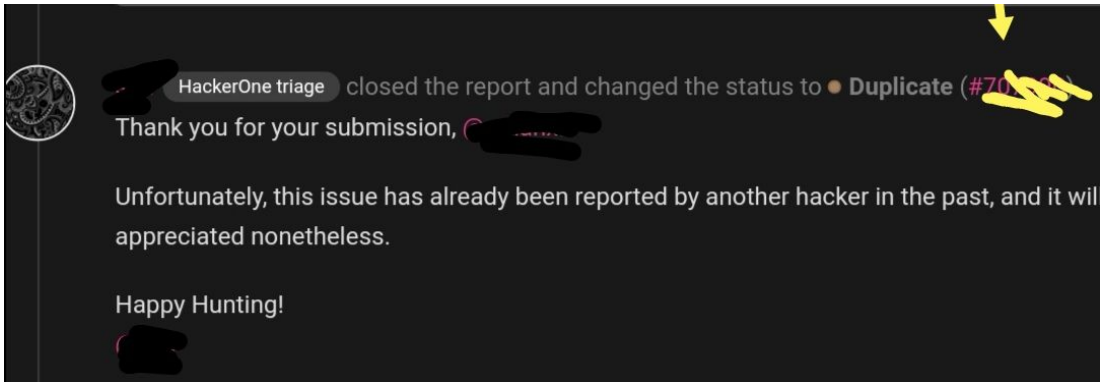
Go big or go home!

- Focus on high severity security vulnerabilities:

P1 - Critical	P2 - High
❖ Remote Code Execution (RCE) ❖ SQL Injection (SQLi) ❖ Server-Side Request Forgery (SSRF) ❖ Authentication Bypass ❖ Disclosure of Secrets ❖ Command Injection	❖ Stored XSS ❖ Admin privilege escalation ❖ OAuth misconfiguration ❖ Sensitive information disclosure ❖ Insecure Direct Object Reference (IDOR)

Why?

- Avoid duplicates and related frustration
- High bounty or reward
- Quick resolution by the company



Go above and beyond

- Create accounts
- Subscribe to paid plans
- Complete any setup complexity
- Order hardware devices
- Read the documentation
- etc…

Security Impact

- More impact means higher bounty

XSS - Hijacking user's session token ✓

vs

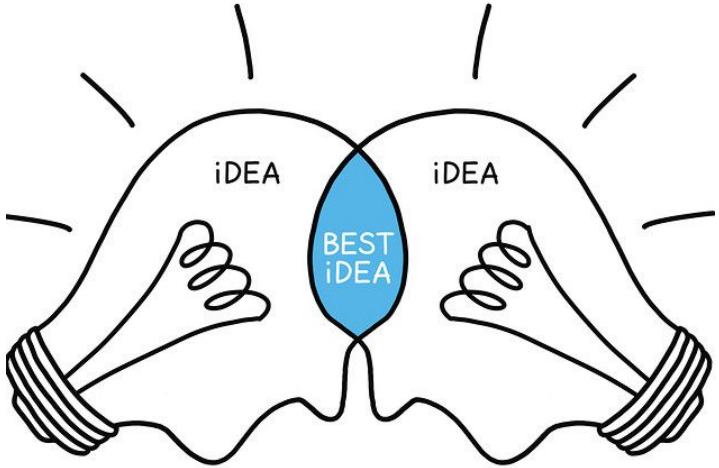
XSS - SImple alert popup ✗

Other tips

- Automate reconnaissance or information gathering
- Automation should not replace manual testing
- Chain vulnerabilities for higher impact
- Save the low hanging fruits for future chain attack

Collaboration

- Find higher impact bugs
- Different skill set
- Get help if your stuck
- Upfront agreement on bounty or resources
- BBP platforms helps with bounty split and collab



Reality of bug hunting

- Requires time, consistency, persistence and patience.
- Depending on the person, it might be steep learning curve.
- Drain mental health, and affect physical health if you don’t exercise.

Recommendation

- Have a set time when you can do bug hunting
- Take regular breaks
- Eat healthy
- Exercise
- Sleep

References

- HackerOne. “What Are Bug Bounties and How Do They Work?” *HackerOne*, 25 Mar. 2024, www.hackerone.com/vulnerability-management/what-are-bug-bounties-how-do-they-work-examples.
- https://hackerone.com/paypal
- HackerOne. “Quality Reports.” *HackerOne Help Center*, 14 Apr. 2024, docs.hackerone.com/en/articles/8475116-quality-reports.
- Nahamsec. “How to Pick Your Targets // How to Bug Bounty.” *YouTube*, YouTube, 27 Feb. 2023, www.youtube.com/watch?v=vbXpRHcKIr0

Any Questions or Comments?