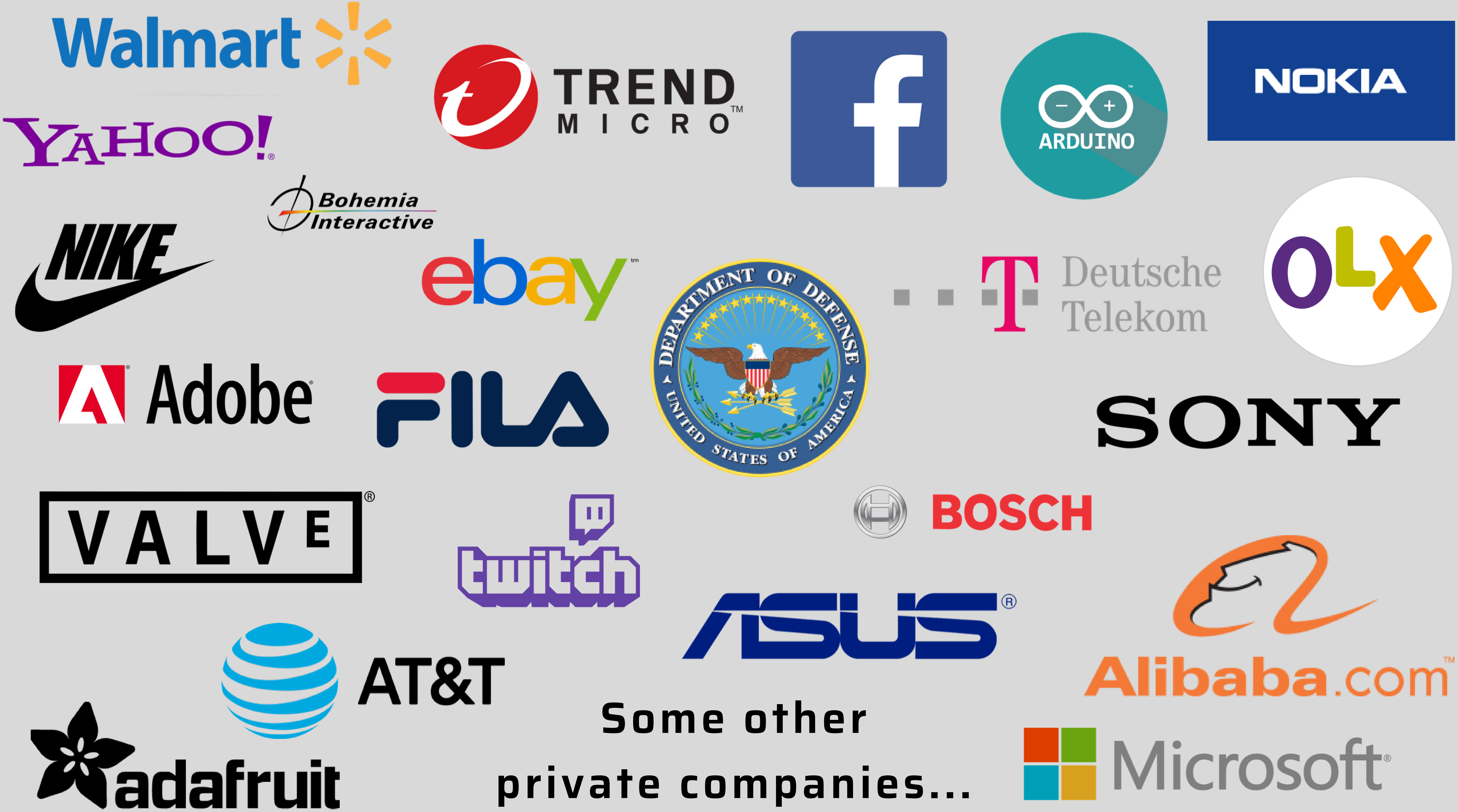
$./gettingstartedinBB

Dan Fabro | 2020

in /0x61underscore

$ cat whoami.txt

- Co-founder & Lead Penetration Tester, Securebites Corp.
- Co-founder, checkmate.ph
- Co-founder, Hackm3
- Core member, BloodHounds :: CTF Team
- Scholar, DOST
- VP, ICpEP.SE - USTP
- 5th-year, CpE
- Part-time Bug Bounty Hunter

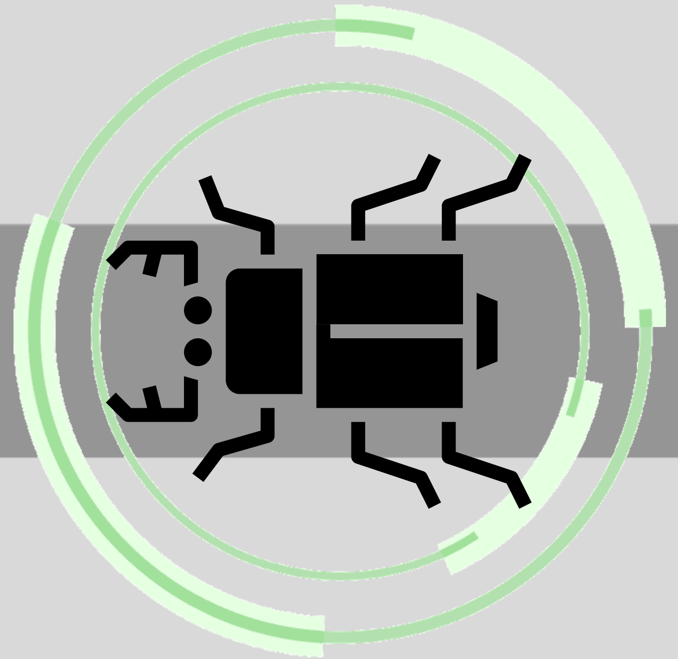


Some other private companies...

✓ **Services**

✓ **Features**

✗



WHY BUG BOUNTY?

For companies:

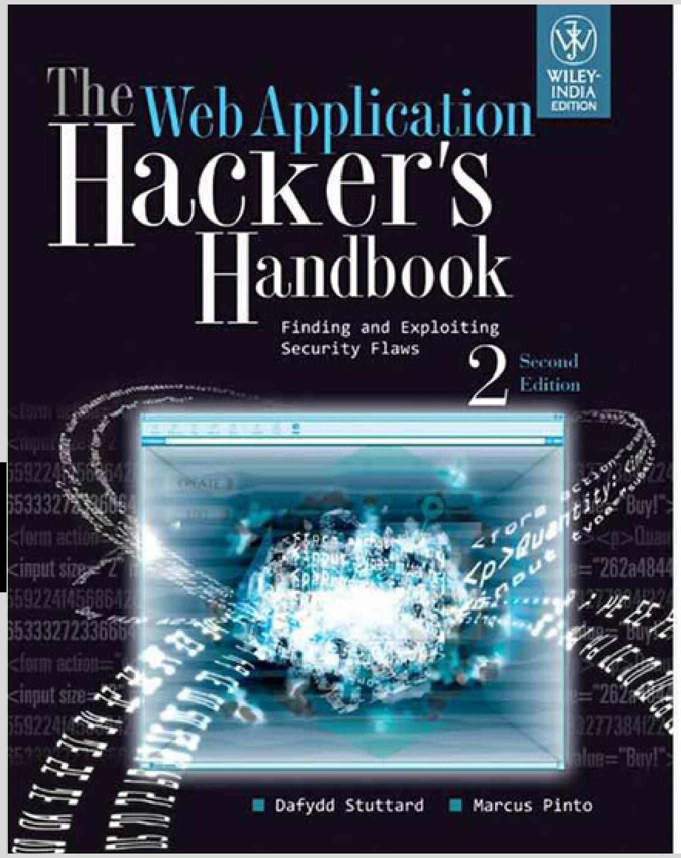
- Less security breaches.
- More better and secure apps.
- Access to thousands of researchers around the world.

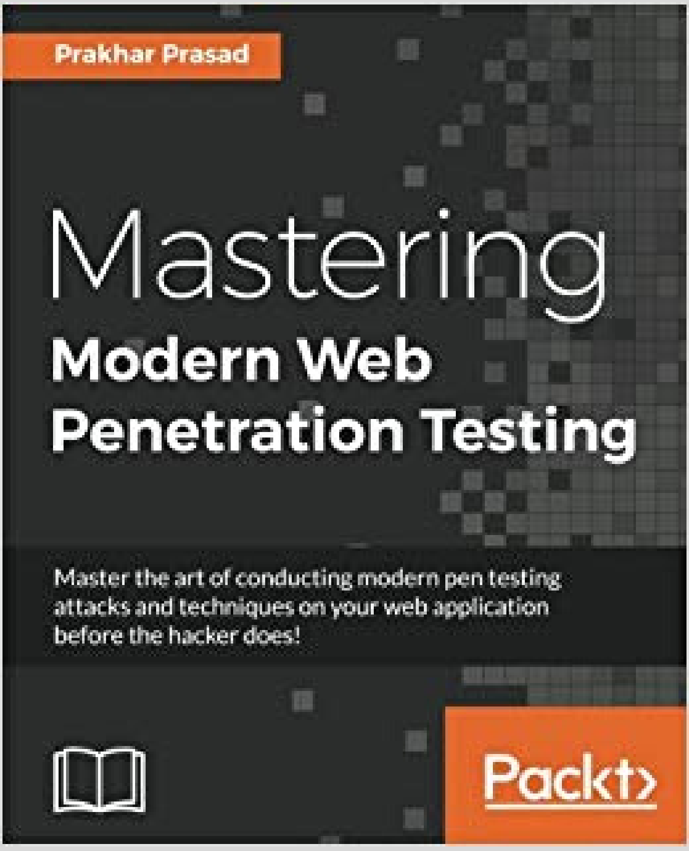
BUG BOUNTY PERKS

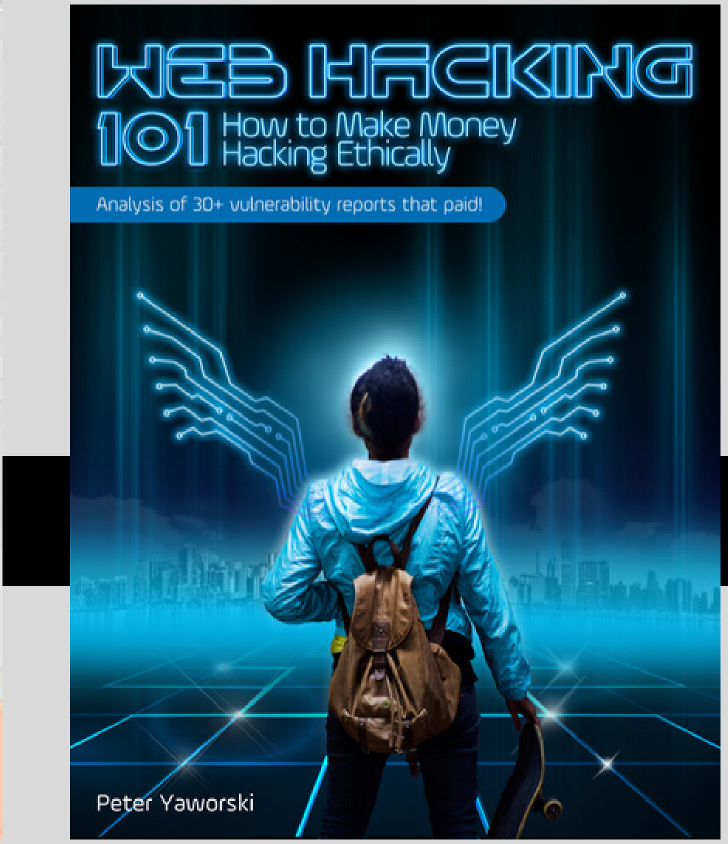
- Connections.
- Free or discounted services from companies.
- Job offer(s).
- Monetary rewards.
- Bragging rights.
- Gain more experience by challenging yourself.

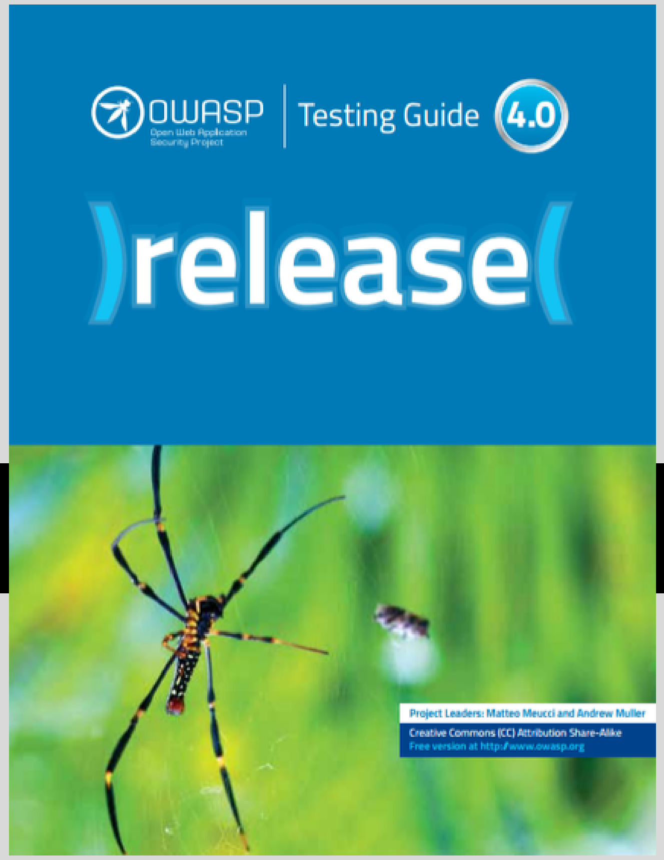
HOW DO I START?

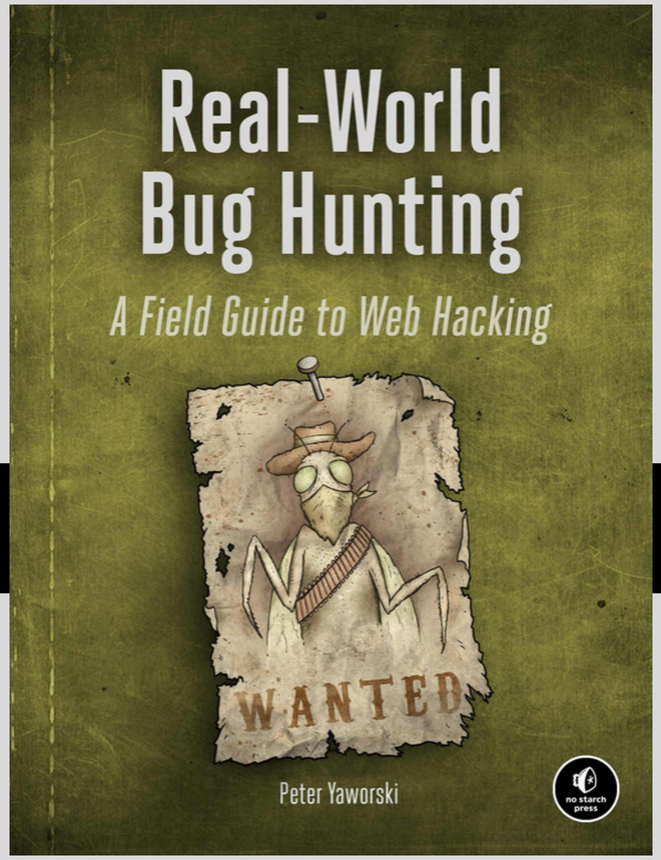
- Learn the basics (Javascript, Web frameworks, etc.)
- Understand the basic web terminologies.
- Do some light reading.
- Join bug bounty communities. Interact.
- hacker101.com / Bugcrowd University / PentesterLab


The Web Application Hacker's Handbook
Finding and Exploiting Security Flaws
2 Second Edition
WILEY-INDIA EDITION
Dafydd Stuttard
Marcus Pinto


Prakhar Prasad
Mastering Modern Web Penetration Testing
Master the art of conducting modern pen testing attacks and techniques on your web application before the hacker does!
Packt>

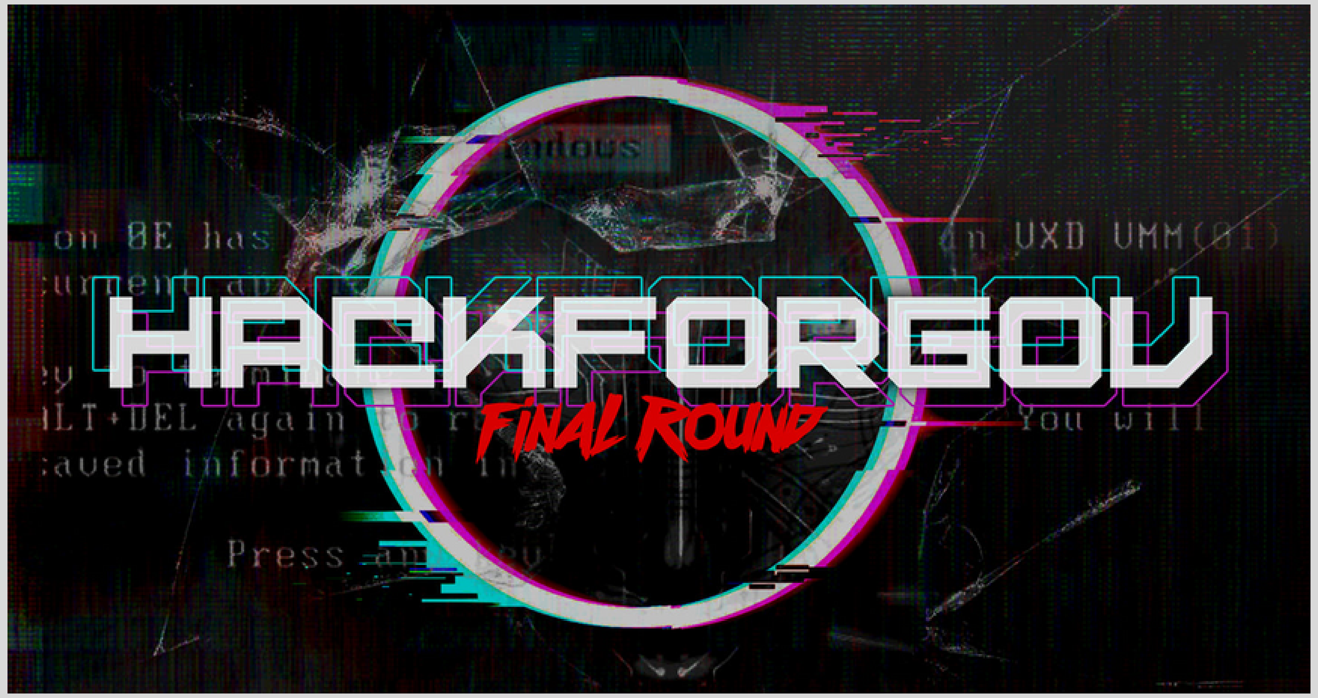

WEB HACKING 101
How to Make Money Hacking Ethically
Analysis of 30+ vulnerability reports that paid!
Peter Yaworski





CTF (Capture the Flag)

CTF (Capture the Flag)



© J Igdon

© J Igdon

DO I NEED TO INVEST SOME MONEY?

HOW SHOULD I KNOW IT'S TIME FOR ME TO START?

WILL I GO TO PRISON IF EVER I BROKE AN INSTITUTION'S PRODUCTION SITE?

WHEN DOING BUG BOUNTY...

- Don't threaten company employees
- Don't beg for money/reward
- Don't compare two different programs
- Respect the institution's decisions
- Read the program rules
- Respect other researchers
- ALWAYS BE HUMBLE AND BE PATIENT.

bugbountystarterpack_

LOADING

bugbountystarterpack_

1.) BURP Suite Community Edition or Professional, Fiddler (installed with Yamagata extensions), or OWASP Zed Attack Proxy Project

bugbountystarterpack_

2.) Recon tools.

bugbountystarterpack_

3.) Hella bunch of payloads.

bugbountystarterpack_

Practice makes perfect. Thus, try:

- BWapp [http://www.itsecgames.com/]
- WebGoat [https://github.com/WebGoat/]
- HackTheBox [https://www.hackthebox.eu]
- Mutillidae
- DVWA (http://www.dvwa.co.uk/)
- OWASP Juice Shop

bugbountystarterpack_

Targets? Find one on:

1.) Secuna [https://secuna.io]

2.) HackerOne [https://www.hackerone.com]

3.) Bugcrowd [https://www.bugcrowd.com]

4.) Intigriti [https://www.intigriti.com]

5.) Hackenproof [https://hackenproof.com]

6.) OpenBugBounty [https://openbugbounty.org]

7.) Synack [https://www.synack.com]

8.) Zerocopter [https://zerocopter.com]

9.) BountyFactory [https://bountyfactory.io]

10.)inurl:/responsible-disclosure

report_

LOADING

report_

PARTS:

- Contact Details (Name, Email address, Link)
- Description
- Vulnerable URL
- Step-by-Step instructions
- Proof-of-Concept (Screenshots, Video, Code)
- Impact
- Suggested Mitigation

bbh_burnout_

LOADING

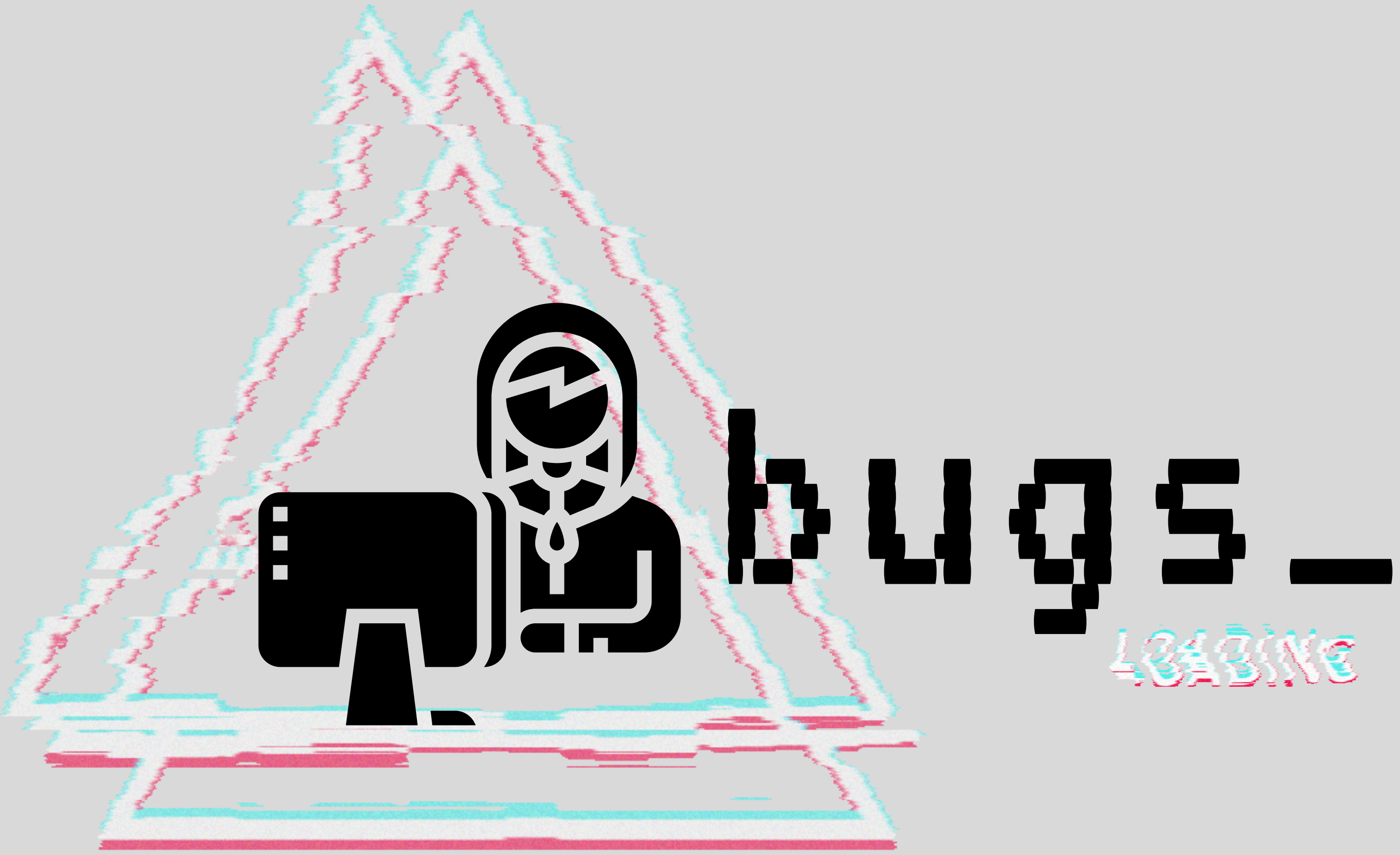
bbh_burnout_

- Dupes
- Expectations
- Long time to triage/payout
- Lack of focus
- Overwhelmed by the community

WARNING

bbh_burnout_

- Organize.
- Rest.
- Don't be a douchebag.


bugs_
LOADING

bugs_

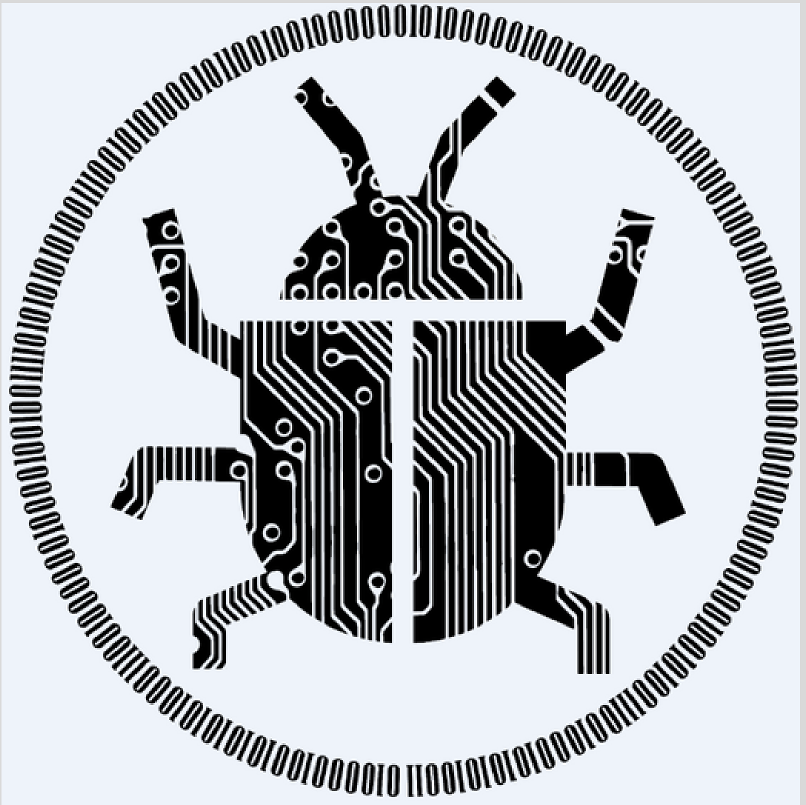
- CSRF
- Security Misconfiguration
- XSS (Stored, DOM, Reflected)
- Account Takeover
- SQL Injection
- XXE Injection
- Application DOS
- IDORs
- Information Leakage

Many more...

LEARN
MORE

quick_demo

LOADING



/BloodHoundsPH

/hackm3.ph

/bugbountyph

discord.gg/2A7ttrG

thanks!