Bug Bounty
[Life of a Pentester]

root@bughunter:

whoami?

- Dharmin Suthar
- Cyber Security Analyst & Researcher
- CEH, CEI, CEISH, CPT, CCSE
- Active : Central Bureau of Investigation (CBI)

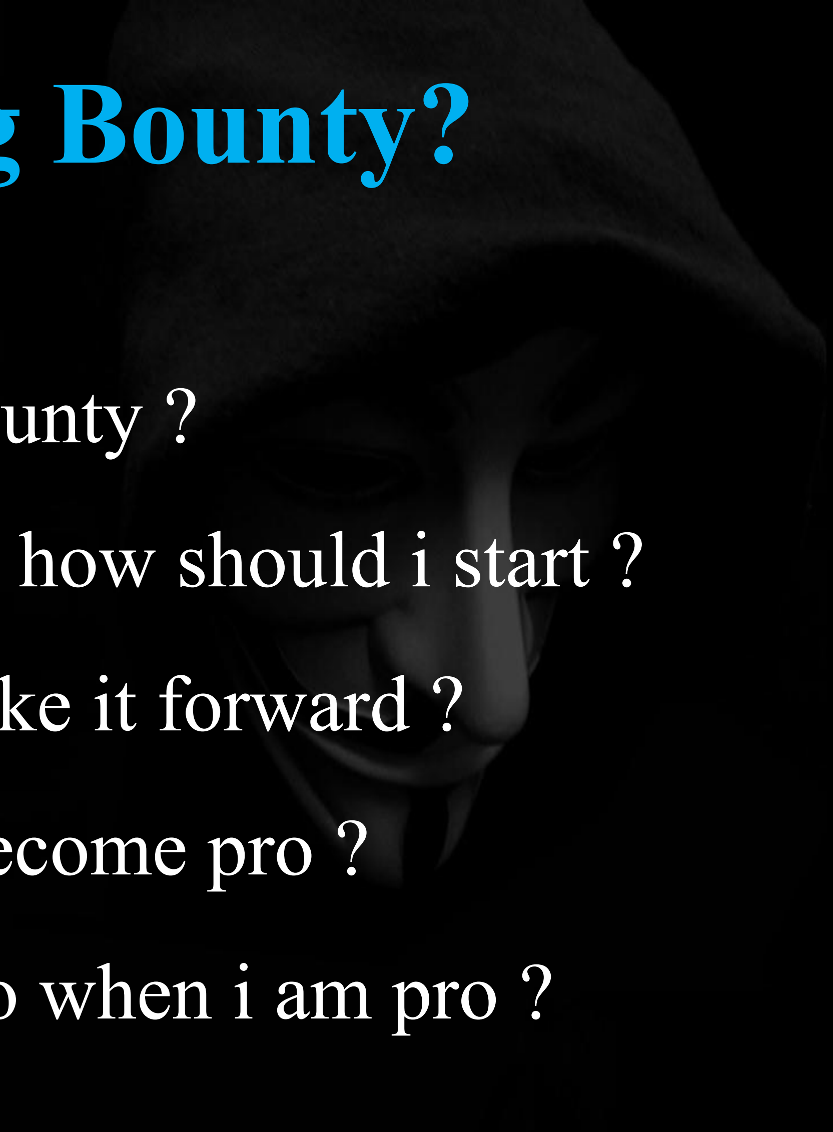
  : Anti Terrorism Squad (ATS)

  : Boston University (Security Researcher)
- Chapter Leader & Partner | 2019 : UK Innovation Department
- Secured : Google, Yahoo, Facebook, Paypal, Microsoft, Nokia, Pusher, Mozilla, etc

Agenda?

- Introduction
- Platforms
- Target
- Attacks
- Tools
- Reports
- Rewards
- Important Things

Bug Bounty?

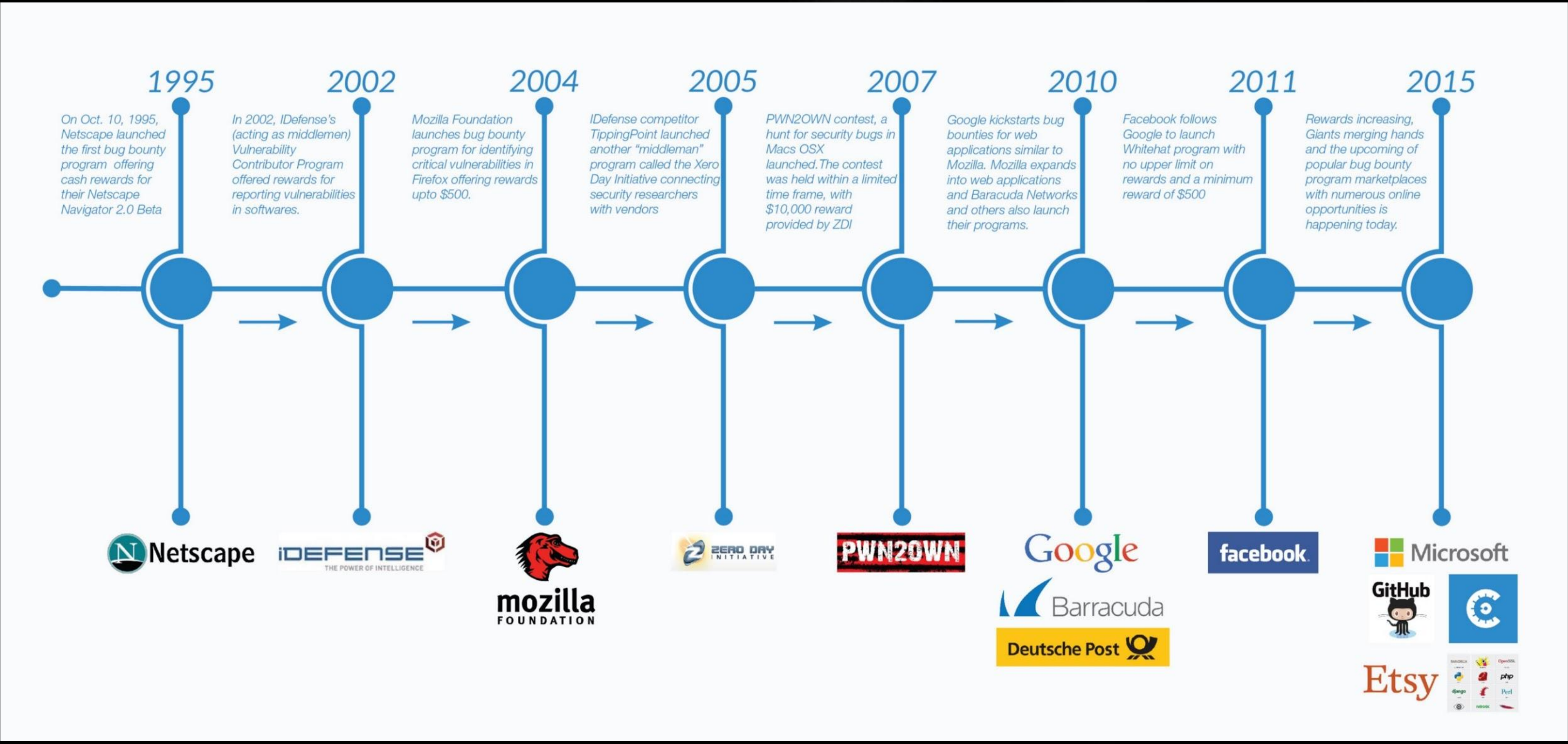


- What is Bug Bounty ?
- I am New Here, how should i start ?
- How should i take it forward ?
- How should i become pro ?
- what should i do when i am pro ?

root@bughunter: What is Bug Bounty ?

- also called as VRP (Vulnerability Reward Program)
- Paying rewards to independent security researchers for finding vulnerabilities in their products.

History?



1995

On Oct. 10, 1995, Netscape launched the first bug bounty program offering cash rewards for their Netscape Navigator 2.0 Beta

2002

In 2002, IDefense's (acting as middlemen) Vulnerability Contributor Program offered rewards for reporting vulnerabilities in softwares.

2004

Mozilla Foundation launches bug bounty program for identifying critical vulnerabilities in Firefox offering rewards upto $500.

2005

IDefense competitor TippingPoint launched another "middleman" program called the Xero Day Initiative connecting security researchers with vendors

2007

PWN2OWN contest, a hunt for security bugs in Macs OSX launched.The contest was held within a limited time frame, with $10,000 reward provided by ZDI

2010

Google kickstarts bug bounties for web applications similar to Mozilla. Mozilla expands into web applications and Baracuda Networks and others also launch their programs.

2011

Facebook follows Google to launch Whitehat program with no upper limit on rewards and a minimum reward of $500

2015

Rewards increasing, Giants merging hands and the upcoming of popular bug bounty program marketplaces with numerous online opportunities is happening today.

root@bughunter:

Process

Target

Information Gathering

Penetration Testing

Report

Platforms

- Facebook, Google, Twitter, Yahoo, PayPal etc.
- Platforms: HackerOne , Bugcrowd, Cobalt, Synack etc.

Target

- Google Trends / Google Dorks
- Pick any company.
- Learn about it thoroughly.
- Its services.
- All subdomains
- All mobile applications.
- Monitor any changes.
- Read Program rules carefully.

Attacks

- XSS - Cross Site Scripting
- SSRF - Server Side Request Forgery
- Cross Site Request Forgery
- Local File Inclusion
- Remote Code Execution
- Information Disclosure
- Sql Injection
- Insecure Direct Object Reference

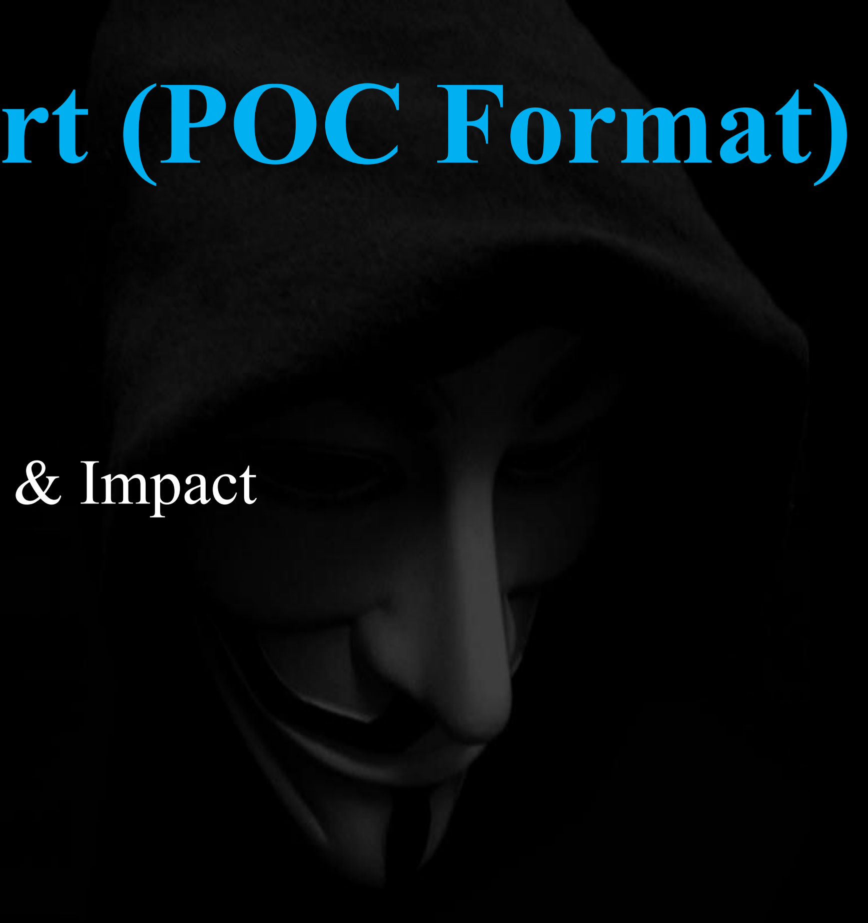
Tools

- BurpSuite
- Acunetix
- Owasp Zap
- Reverse IP Lookup
- Beef
- WPscan / JoomScan
- HackBar (Extension)
- Wfuzz

Report (POC)

- Title
- Description of bug
- Step by step instruction to reproduce the bug
- Screenshot / Videos
- Impact
- Suggestion

Report (POC Format)

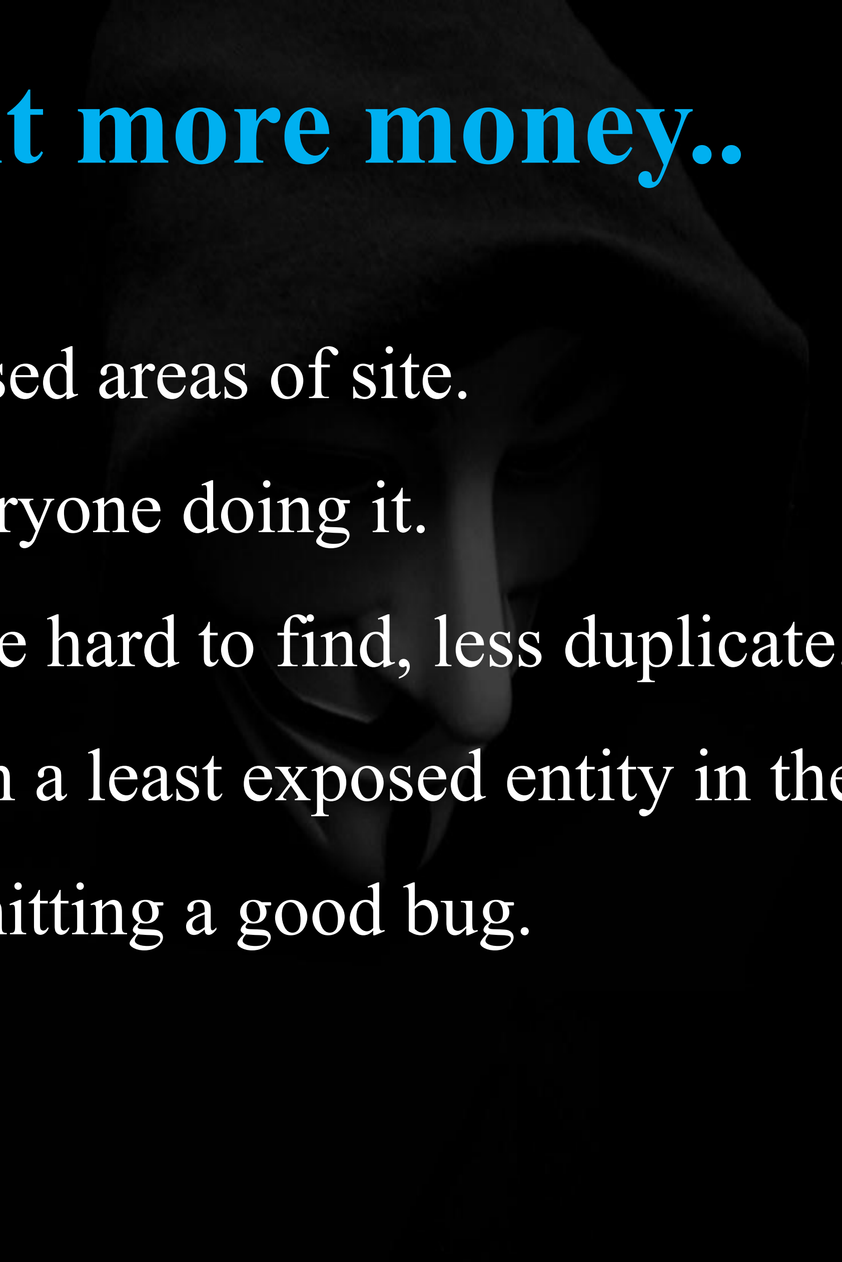


- Vulnerability Name
- Vulnerability Description & Impact
- Vulnerable URL
- Vulnerable Parameter
- Payload Used
- Steps to Reproduce
- How to Fix (Recommandation)
- Proof of Concept(Screenshot)

Rewards

- Money
- Hall Of Fame
- Swag Pack (T-shirt, bag, book)
- Appreciation Letter
- Certificate
- Nothing

root@bughunter: **I want more money..**



- Look out for less exposed areas of site.
- Injection Attacks _ everyone doing it.
- Authorization issues are hard to find, less duplicate.
- Privilege escalations on a least exposed entity in the site have good chances of hitting a good bug.

Learning Source

- https://www.owasp.org/
- https://hackerone.com/blog/what-great-hackers-share/
- https://forum.bugcrowd.com/
- The Hacker’s Handbook
- Proof of Concepts - h1.nobbd.de/
- JavaScript
- Online Tutorials : Cybrary, Udemy, Pluralsight, etc.

Never Ever

- I want money, I don’t care about your policy.
- But, that X company gives money for this.
- I will hack you to the death.
- Don’t use the repeater, I love Burp Scanner, Acunetix.
- I love cookies & session related bugs and version disclosure.
- SQLmap is good only when risk=3

root@bughunter: Have Some Patience

- Duplicate
- Wait for response time
- Forget about submission.
- Learn and find new Bugs
- Find New target.
- Go as deep as possible (Chain attack)
- NEVER Ever run a Scanner.
- Do Manual testing.

root@bughunter:

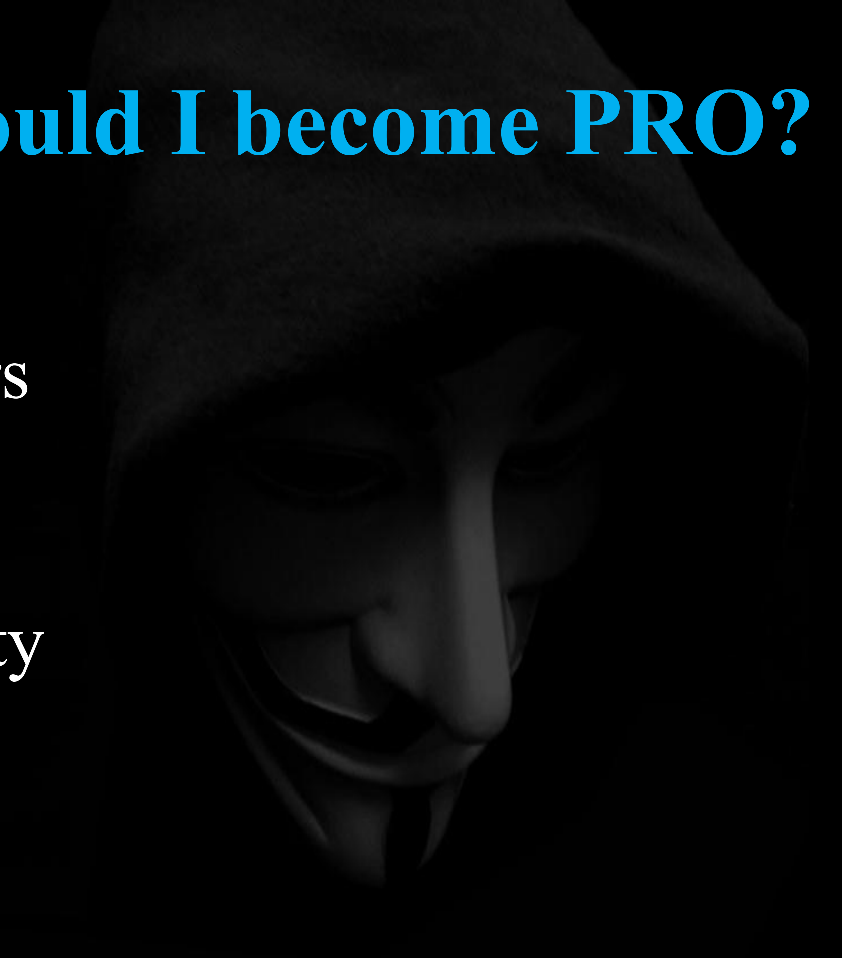
Private Target

- site:ohmylovelywebsite.com –repititive_pages -www -
- forums -answers -discussions
- inurl: src | path | link | url
- Filetype:asp | aspx | jsp | jspa | php
- Intitle: bitcoin | money

Online Tools

- Shodan - Computer Search Engine
- NerdyData - Source Code Search Engine
- Bing: IP Search
- Yandex: Awesome Search Engine

root@bughunter: How should I become PRO?



- Follow Top Researchers
- Read blogs
- Read about vulnerability
- Create your own logics
- Follow twitter