HOW TO GET STARTED WITH BUG BOUNTY?

EDIS KONSTANTINI

WHO AM I

- I work as a senior application security engineer at Bugcrowd, the #1 Crowdsourced Cybersecurity Platform.
- I did/sometimes still do bug bounties in my free time.
- My first bug bounty reward was from Offensive Security, on July 12, 2013, a day before my 15th birthday.
- Aside from work stuff, I like hiking and exploring new places. Oh, I also like techno.

WHAT IS THIS TALK ABOUT?

- An introduction to the concept of the Bug Bounty, from a company perspective
- Outline the benefits and potential cons of running a bug bounty program
- Tips and suggestions to the bug hunters


LET'S START WITH THE HISTORY OF BUG BOUNTIES
memegenerator.net

The First "Bugs Bounty" program – 1995

Press Release

https://web.archive.org/web/19970501041756/www101.netscape.com/newsref/pr/newsrelease48.html

NETSCAPE ANNOUNCES "NETSCAPE BUGS BOUNTY" WITH RELEASE OF NETSCAPE NAVIGATOR 2.0 BETA

PROGRAM HARNESSES POWER OF THE INTERNET TO HELP NETSCAPE REFINE BETA VERSIONS AND ENSURE HIGHEST QUALITY SOFTWARE

MOUNTAIN VIEW, Calif. (October 10, 1995) -- Netscape Communications Corporation (NASDAQ: NSCP) today introduced the "Netscape Bugs Bounty", a program that rewards users who help Netscape find and report "bugs" in the beta versions of its recently announced Netscape Navigator 2.0 software. The beta versions of the popular network navigation software are available today for downloading on the Internet for free evaluation.

The contest begins with the beta versions of Netscape Navigator 2.0 -- available for Windows, Macintosh and X Window System operating environments -- that are on the Internet today. As the rules will explain in detail, users who are the first to report a particular bug will be rewarded with various prizes depending on the bug class: users reporting significant security bugs as judged by Netscape will collect a cash prize; users finding any security bugs will win Netscape merchandise; and users finding other serious bugs will be eligible to win a choice of items from the Netscape General Store.

Netscape's beta testing of 2.0 is already underway and providing valuable feedback on the new software. Users who downloaded previous beta versions of the 2.0 software are strongly encouraged to download today's versions, which fix major and minor bugs identified since its initial release -- including security bugs in the pre-release version of the Java language support integrated in 2.0. Netscape is releasing today special beta versions of 2.0 that include Java for users wanting to test it. Because bugs will be reported and fixed on an ongoing basis, Netscape asks users to stay current on the beta version they are using so that the latest software is constantly being refined.

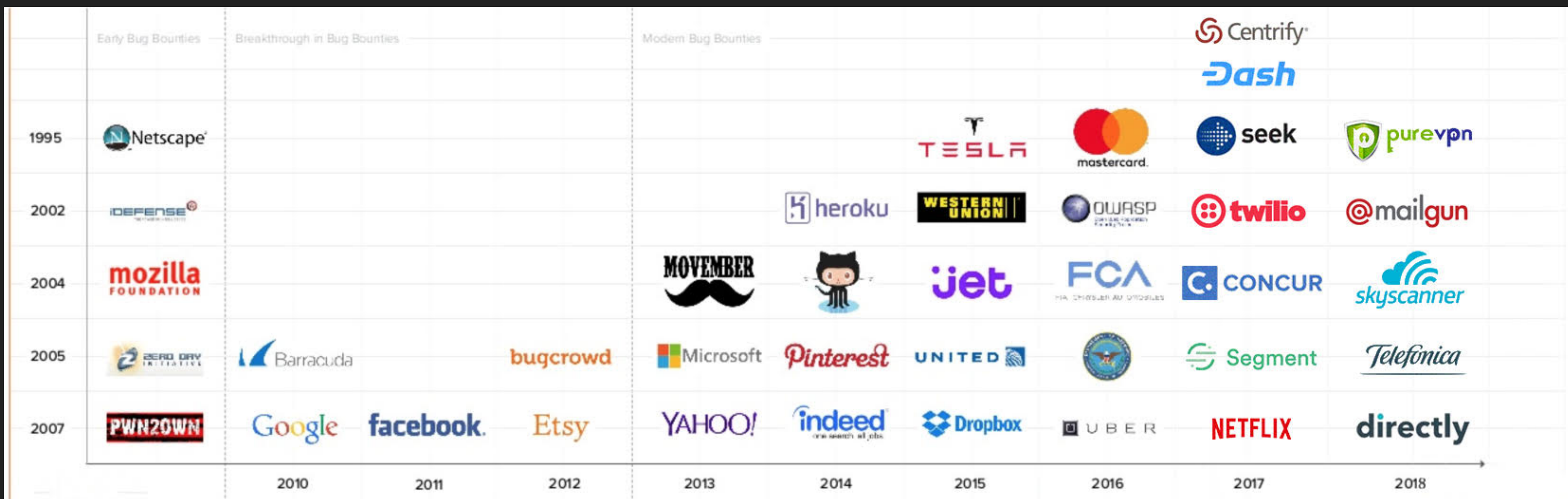
"We are continuing to encourage users to provide feedback on new versions of our software, and the Netscape Bugs Bounty is a natural extension of that process," said Mike Homer, vice president of marketing at Netscape. "By rewarding users for quickly identifying and reporting bugs back to us, this program will encourage an extensive, open review of Netscape Navigator 2.0 and will help us to continue to create products of the highest quality."

Netscape Navigator 2.0 is a major new release of Netscape's highly popular navigator for enterprise networks and the Internet. Netscape Navigator 2.0 integrates a full suite of Internet applications -- including electronic mail, threaded discussion groups, and state-of-the-art navigation capabilities -- with advanced features such as rich layout and Live Objects support to give users access to a new generation of live online applications.

Netscape has created two versions of its Netscape Navigator 2.0 beta, available today for downloading from Netscape's home page at . Version b1J for Windows 95, Solaris and IRIX platforms includes Java and is for users who want to participate in the bounty program. Java is a rich new environment that enables a new class of live applications on networks. Users are cautioned that the Java code included is a pre-beta release and may create instability in the user's software. For general users or those on other UNIX environments, Windows 3.1 and Macintosh, Netscape has posted beta versions without Java. After initial testing is complete, future beta versions for all supported platforms will contain Java.

"We are glad to support Netscape in this bounty program," said Eric Schmidt, Chief Technology Officer at Sun. "The Java code is pre-release code and so we expect people to find bugs. This program, along with Sun's extensive beta testing program, will help us to quickly identify and fix any potential vulnerabilities in Java, ensuring a highly secure solution at the time of release."

Timeline of Bug Bounty programs



What we see lately

There's a rapid growth in adoption of the bug bounty programs over the past decade. Every day, more organizations are adopting the Bug Bounty Model. That includes large enterprises as well as small - medium sized enterprises.

Growth

The growing number of organizations across industries adopting bug bounty and vulnerability disclosure programs in the past year has made it clear that the crowdsourced security model is here to stay.

Quality

Bug bounties present significant value comparing to traditional testing methods.

Impact

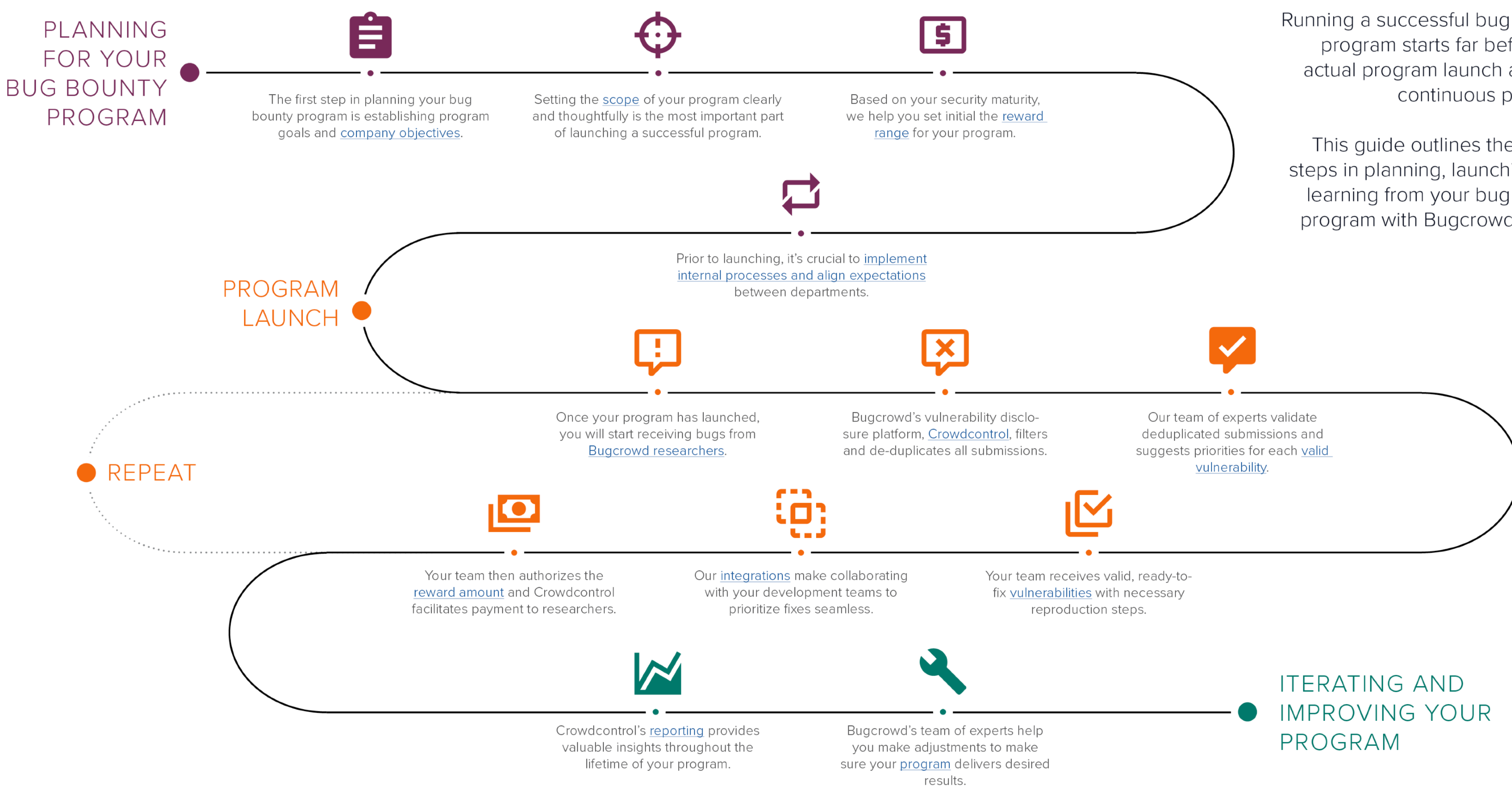
There's been a huge increase of critical vulnerabilities being identified by Bug Bounty programs.

How Bug Bounties Work?

Plan, Launch & Learn: The Bug Bounty Roadmap

Running a successful bug bounty program starts far before the actual program launch and is a continuous process.

This guide outlines the critical steps in planning, launching and learning from your bug bounty program with Bugcrowd's help.



What you need to know before starting a bug bounty program

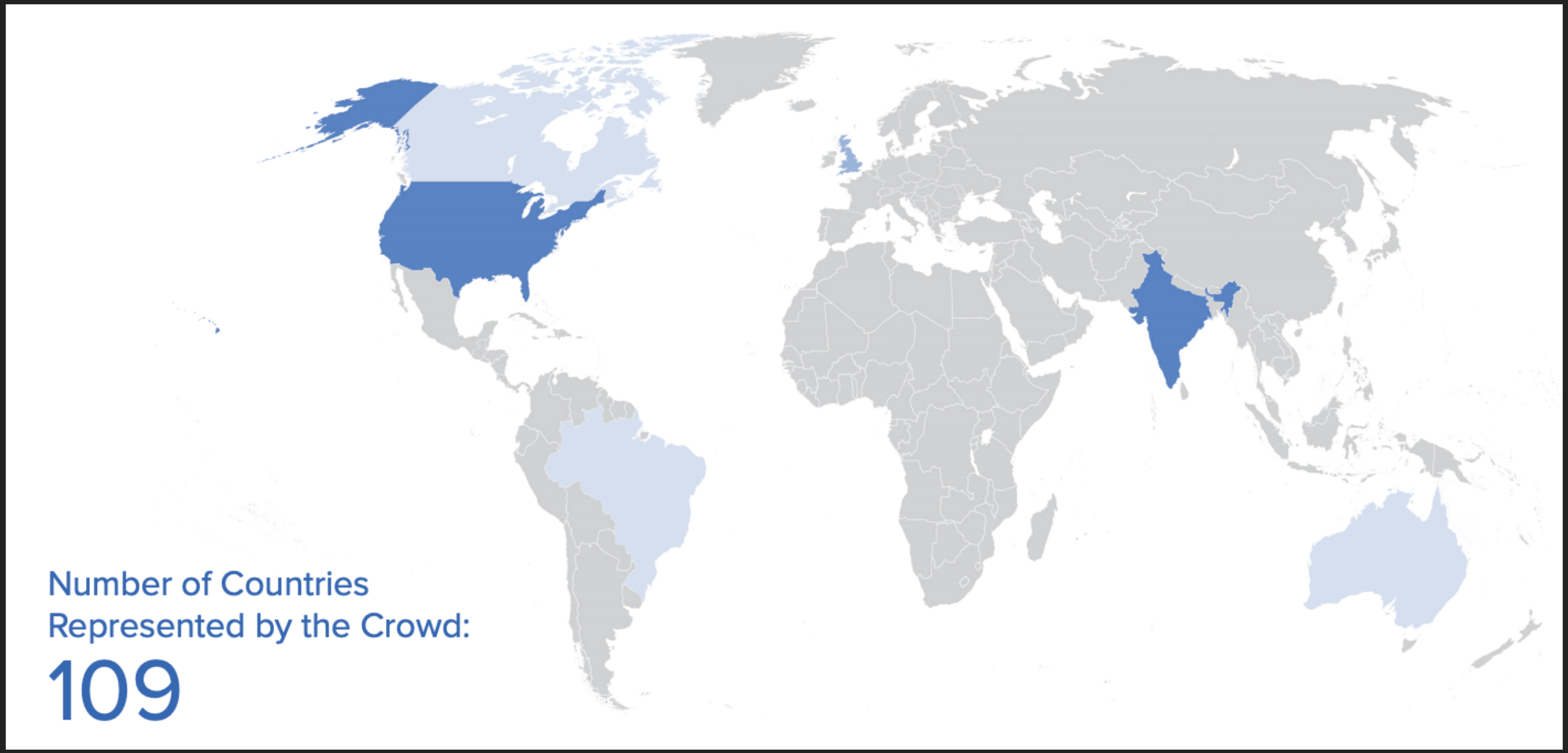
- **Scope** - *.example.com
- **Focus** - payment processing
- **Exclusions** - 3rd party sites
- **Organization-wide awareness**
- **Environment** - prod vs staging
- **Access** - shared credentials or self signup
- **Decide** - Private or Public?

POST LAUNCH - THINGS YOU NEED TO KNOW AFTER LAUNCHING A PROGRAM

- Commitment
- Communication
- Reports
- Define a Vulnerability Rating Taxonomy VRT

WHO ARE THE BUG HUNTERS?

- All over the world
- All levels of experience
- Passionate about security
- All ages
- Like to challenge
- To make internet more secure!



Source: Bugcrowd's State of Bug Bounty 2018 Report

SOME TIPS AND SUGGESTIONS TO THE BUG HUNTERS

- **Read. Learn. Practice**. Because practice makes it perfect!
  As most of the bug bounty programs are related to web targets, the “The Web Application Hacker’s Handbook” is a must-read book that I suggest to everyone.
- **Sharing is caring**! This is the motto of many well known researchers that like to share vulnerabilities they find, and their methodology, so make sure to read blog posts of other hackers.
- **Check online materials** . Watch tutorials and videos related to hacking.
  Bug Bounty Hunting Methodology v3 – Jason Haddix is a great example.
- **Be patient**. Because, it will take time to find the first valid bug. Don’t be disappointed. Duplicates are everywhere!

- **Approaching a target**: Let's assume that the program has a large scope (*.example.com), don't waste your time on main site if you are late to the party as chances are low that you'll find anything in the main site(as everyone probably went over it so many times).
- **Recon**: Start to perform reconnaissance to find subdomains.
  Find subdomains through various tools like Sublist3r etc.
- Use Nmap, as it will certainly help to find hosts running on non-standard ports that may be vulnerable to critical issues.
  - Review the services and ports found by recon. Check for the infrastructure of the application. Try to understand how they handle sessions/authentication, check for CSRF (whether if they have some protection for it, i.e csrf token), test for IDOR's. Take a look at how they filter input versus encoding etc.
- If you get stuck at some point, ask for help. The bug bounty community helps each other, but before asking, make sure you check all the possibilities to resolve it.

The value of writing good submission

- Keep the description short and simple
- Show full proof-of-concept
- Explain the potential impact
- Don’t add video unless it has some good music in background
- Provide remediation advice

Thanks y'all!

Questions?