பாடல்கள் துணைப்பெற்று வந்ததா இல்லை!!
Bug Bounty
Not just about Making Money !!
Sriram, 24

- Founder & Director of Security, TG Cyberlabs Pvt. Ltd
- Founder, Letshack Foundation
- Chief Security Advisor, 3GIRPS Global Groups
- Bug Bounty Hunter
- Guided more than 25000 students all over India
- Google VRP Security Researcher
What is Bug Bounty da?
This is not a session for existing bug hunters, this is a very basic session how to get into bug hunting
A Vulnerability/bug is a technical issue that results in Data Leakage and cause security issue which could cause damage to both Organization & users.
Bug Bounty is a program offered by organizations, when individuals reported valid security bugs he/she will be rewarded.

On an Average a Bug bounty hunter can earn around $3000/month - INR 2 lakhs approx
send a bug report
A 20yr old researcher found multiple bugs in Apple, which was rewarded $36,000 (INR 27 Lakhs).

A Hacker from China received $800,000 (INR 5.92 crores) from Microsoft. Multiple RCE
Top Bug Bounty Programs

- Google VRP - $1,000,000
- Apple - $1,000,000
- Microsoft - $200,000
- Facebook - $40,000
- Twitter - $20,000
- Snapchat - $35,000

Hackerone, Bugcrowd, Intigriti
Best way to get into Bug Bounty

- Web App Security
- Android/iOS Security

90% of Bug Hunters hunt only on Web targets. So there's a higher chances over Android/iOS targets
Web Security the protective measures and protocols that organizations adopt to protect the organization from cyber criminals and threats that use the web channel.

Apply Security measures on sites to prevent unauthorized access!!
Android/iOS Security

Android/iOS Security where researchers test and build security mechanism on the code to prevent external actors to steal Information of users.
Web Security is a little easier!

- Web Security is easier and resources are all over the internet.
- Android/iOS Security could be trickier and the resources in market is low.
- On Exceptional cases you need to get a Android/iOS device to test the applications which is costlier.
- But the scope and demand is very high in Android.
NO MATTER WHAT, BASICS ARE REALLY IMPORTANT

GET THE BASICS RIGHT
Good understanding of how the Internet works...

• What is a IP
• Learn about protocols (TCP, UDP, ARP...)
• what is a Port
• what is ipv4 & ipv6 - Difference
• What is a Mac address
• OSI Model
• Wireless security basics - Authentication types.
Protocols – IMPORTANT

- FTP – File Transfer Protocol
- TCP – Transmission Control Protocol
- DNS – Domain Name System
- SMTP – Simple Mail Transfer Protocol
- ARP – Address Resolution Protocol
- OCSP – Online Certificate Status Protocol
Learning Networks!

- geeksforgeeks.org
- TCP/IP for Dummies Edition - Book
- cybrary.it
Networking All-In-One Desk Reference For Dummies

9 IN 1

Networking Basics
Building a Network
Network Administration and Security
Troubleshooting and Disaster Planning
TCP/IP and the Internet
Home Networking
Wireless Networking
Windows® 2003 Server Reference
Linux® Reference

Doug Lowe
Operating Systems...

Get used to an Operating system LINUX, UNIX, WINDOWS, ANDROID & IOS

- Get used to CLI - Command Line Interface
- Linux, Windows & mac Administration
Programming

- Python, Ruby, Perl, Java, Bash
- HTML, CSS, Javascript, PHP
- SQL - Structured Query Language
- Develop your programming skills
DUMMIES Edition
What is HTTP & HTTPS
HTTP/1.0 & 1.1

Understanding Data Transfer over the Internet

How Request is sent to the server

How Response is received on your PC
End User

Request

Response

google.com
Web Applications Technologies

- Learning multiple web technologies increases your chances of finding client side and server side bugs
Client Side Scripting/Coding

- HTML - HyperText Markup Language
- Javascript
- Ajax
- Jquery - Javascript Library

Server Side Scripting/Coding

- PHP - Hypertext Preprocessor
- ASP
- Ruby on Rails (Web App Framework)
- Python
Approach !!

- Understanding the scope
- Gather Information about targets
- Right set of tools for right target
- Understanding the Logic
Refer programs for understanding the application even better to find more bugs.

Reading the scope of the program is really important. Programs reject reports which doesn't follow the rules of the program.
Most Important Tool for Web Security

BurpSuite

Burpsuite is a proxy based tool. Burpsuite professional version costs around $399 INR 30,000. Free edition is also available.
OWASP Top 10

- To understand these web security basics, OWASP has some useful guides.
- OWASP has categorized Top 10 vulnerabilities that you should test on Applications.
OWASP Top 10

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross Site Scripting – XSS
- Insecure Deserialization
- Using components with known vulnerabilities
- Insufficient Logging and Monitoring
• You need to practice again and again.
• Patience
• Learn Every Single Day
The Web Application Hacker's Handbook
Finding and Exploiting Security Flaws
Second Edition
Dafydd Stuttard, Marcus Pinto
• Mastering Modern Web Application Penetration Testing
• Hackerone101.com
• Bugcrowd University
Youtube Channel

- Hackersploit
- Live OverFlow
- Hacking Simplified
- IpSec
- John Hammond
- STOK
Websites to get started in Bug Bounty!

- owasp.org
- Geeksforgeeks.org
- Cybrary.it
- portswigger.net
- pentesterLab.com
Reports really matters !!

- Writing a report is really important. It changes the way how the organization handles it.
- Researchers are rewarded little higher for perfectly crafted reports explaining the vulnerability.
- Adding a Video POC will increase the chances are report getting accepted and rewarded.
But this is not enough da Macha !!
Follow me on

@sriram_offcl

@sriramoffcl