வணக்கம் நண்பர்களே !!

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

Bug Bounty is a program offered by organizations, when individuals reported valid security bugs he/she will be rewarded.

On a Average a Bug bounty hunter can earn around $3000/month - INR 2 lakhs approx

send a
bug report

#bug_bounty

- 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


mt
#me
mt
#web_security
#android_ios_
security
mt

Web Security

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 !!

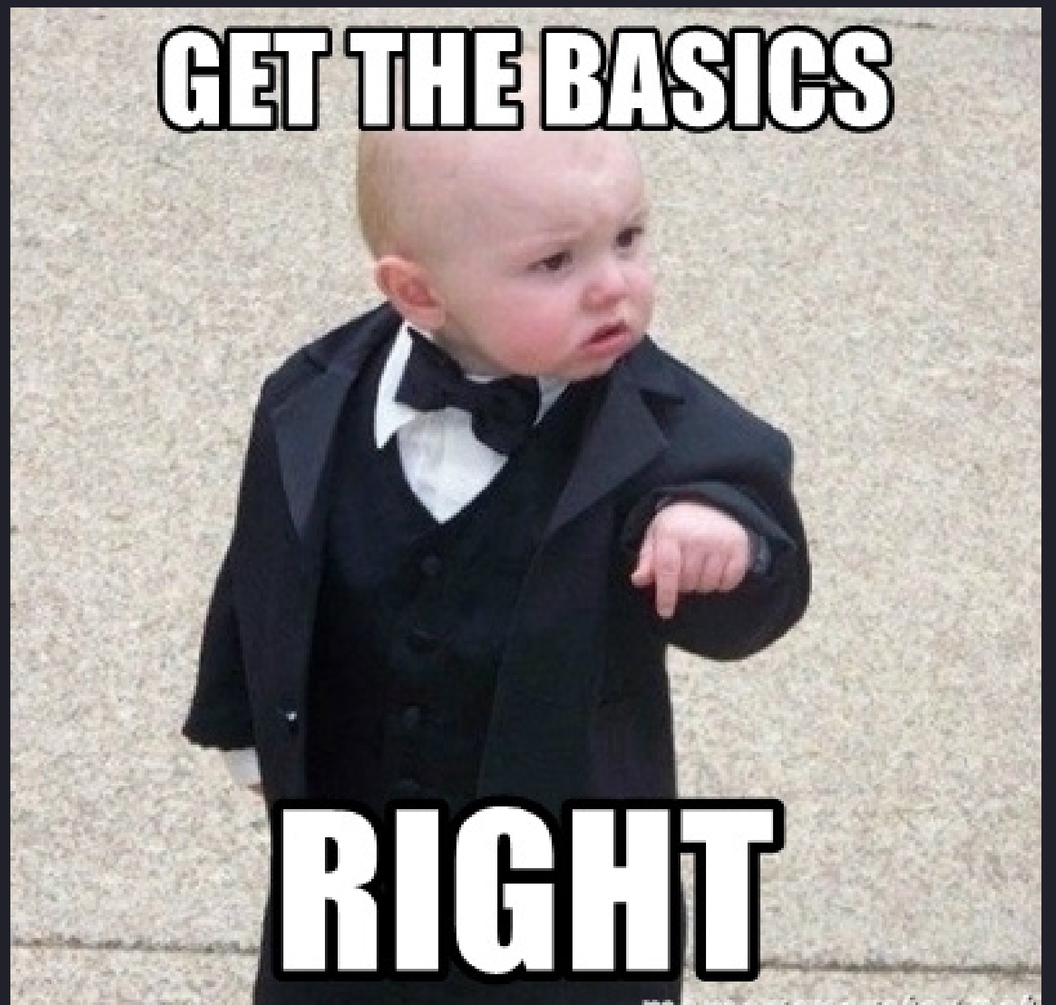
Android/iOS Security

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



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 -XXX

- 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

Nine quick reference guides — one great price!

Networking

ALL-IN-ONE DESK REFERENCE FOR DUMMIES®

2nd Edition

9 BOOKS IN 1

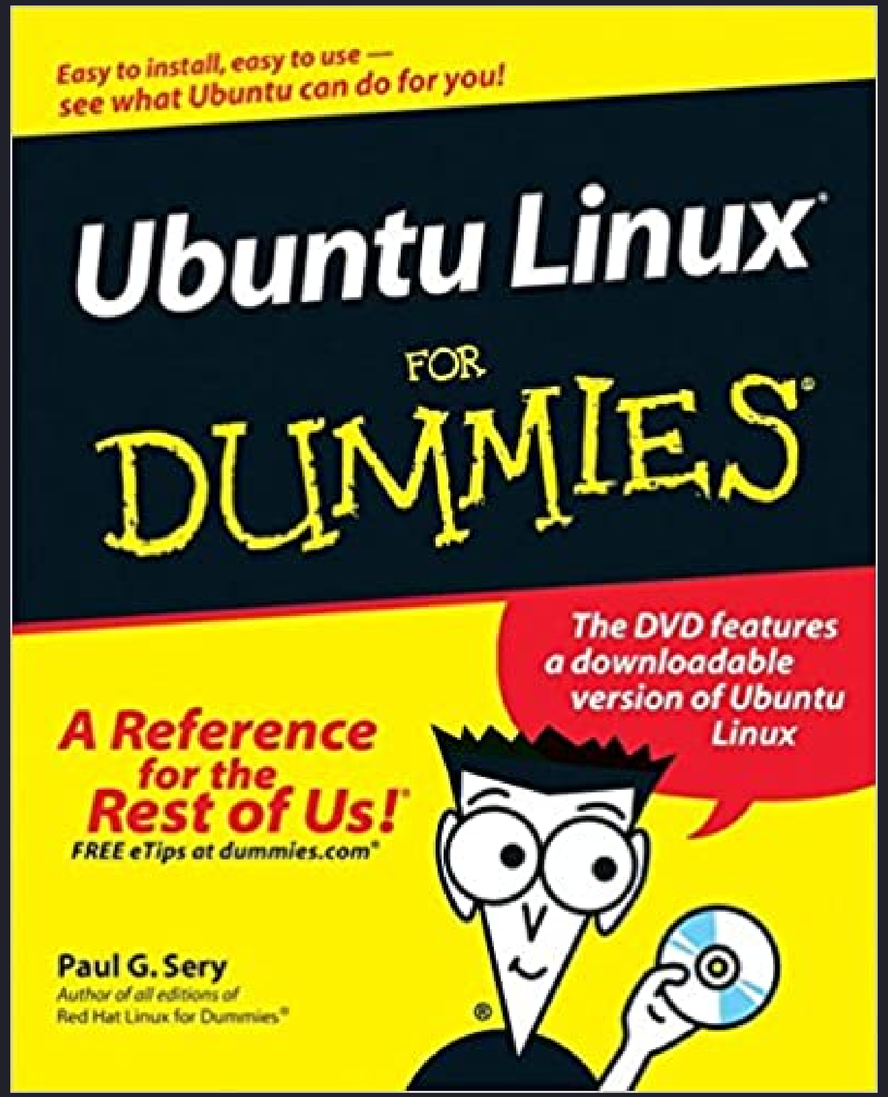
- Networking Basics
- Building a Network
- Network Administration and Security
- Troubleshooting and Disaster Planning
- TCP/IP and the Internet
- Home Networking
- Wireless Networking
- Windows® 2003 Server Reference
- Linux® Reference

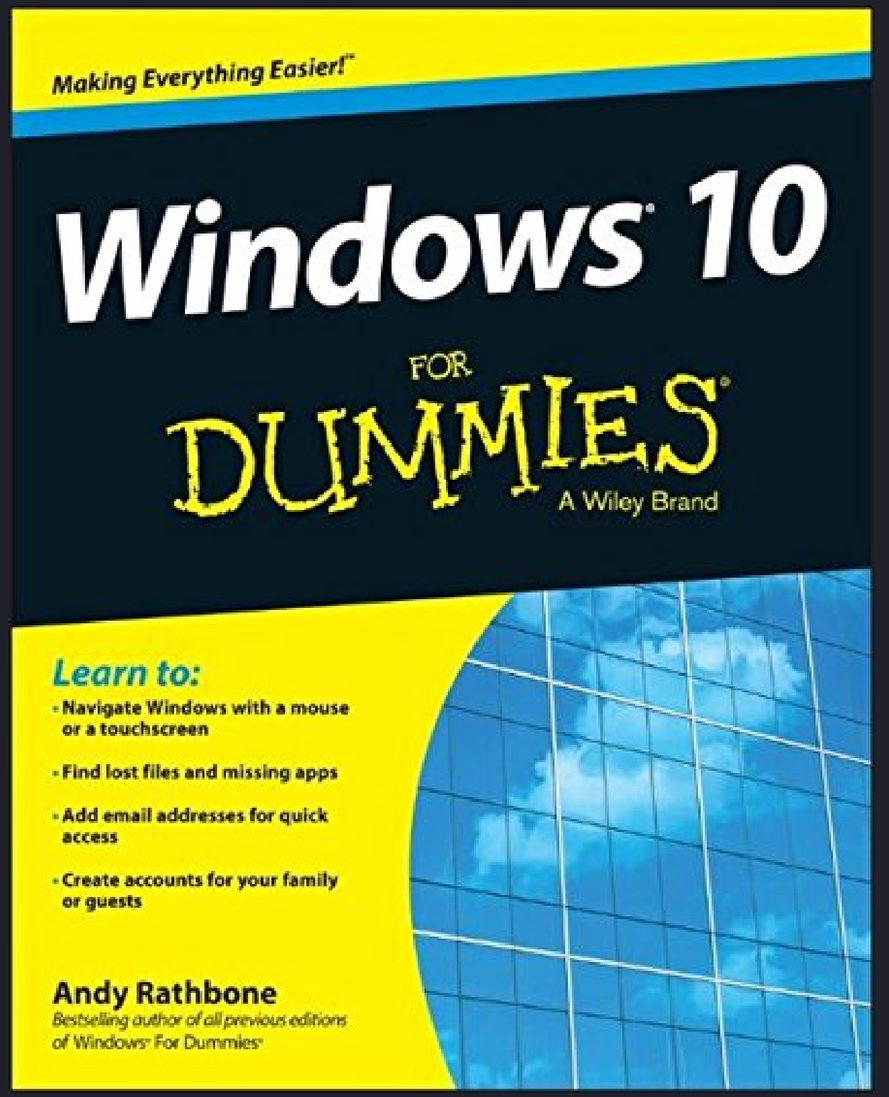
Doug Lowe

Operating Systems...

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

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

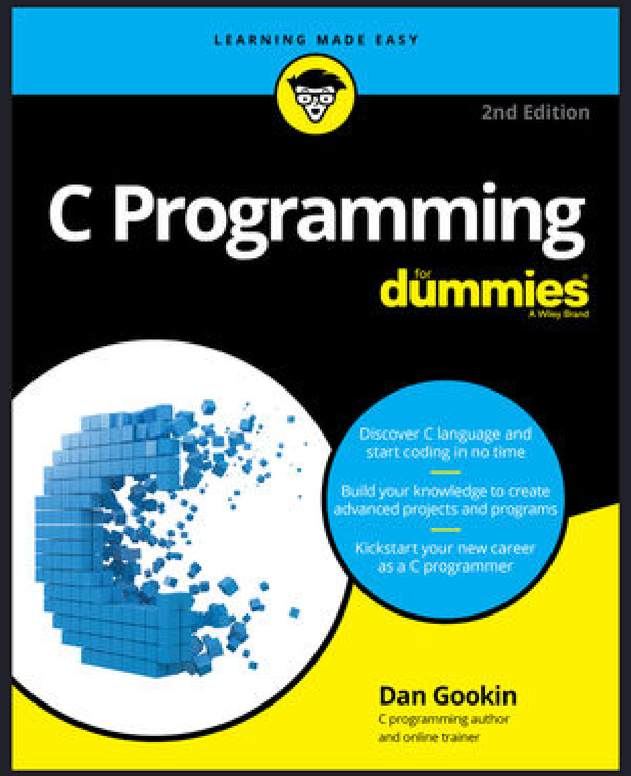

Easy to install, easy to use —
see what Ubuntu can do for you!
Ubuntu Linux
FOR
DUMMIES
The DVD features a downloadable version of Ubuntu Linux
A Reference for the Rest of Us!
FREE eTips at dummies.com
Paul G. Sery
Author of all editions of
Red Hat Linux for Dummies

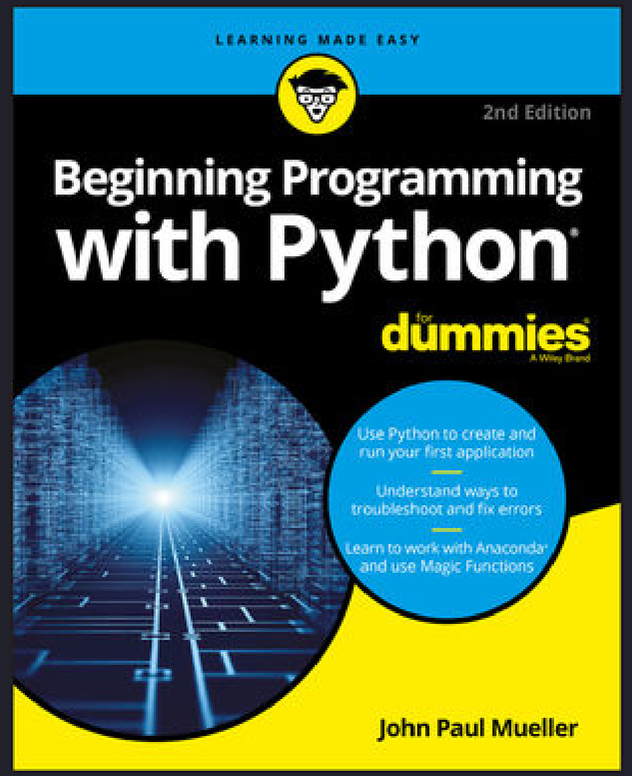

Making Everything Easier!
Windows 10
FOR
DUMMIES
A Wiley Brand
Learn to:
Navigate Windows with a mouse or a touchscreen
Find lost files and missing apps
Add email addresses for quick access
Create accounts for your family or guests
Andy Rathbone
Bestselling author of all previous editions of Windows For Dummies

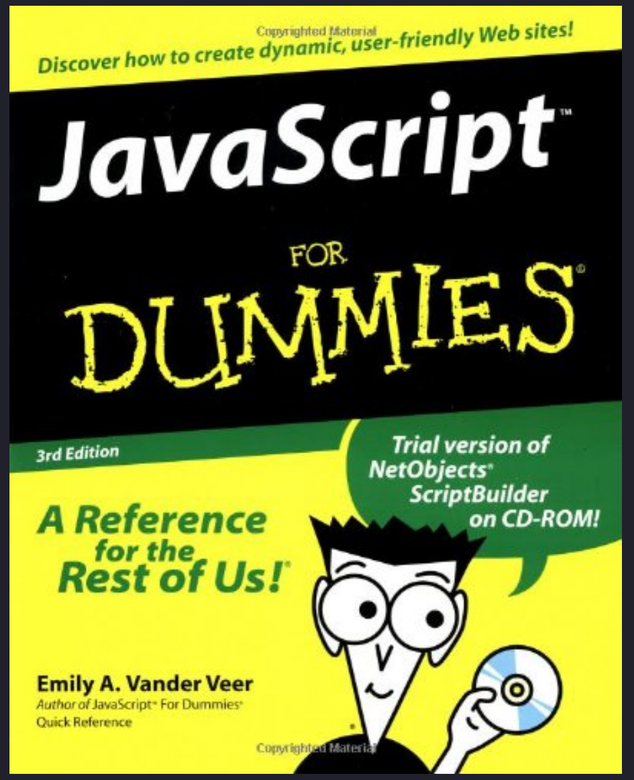
Programming

- 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

Request

End User

google.com

Response

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) >h1
- 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

Open Web Application
Security Project

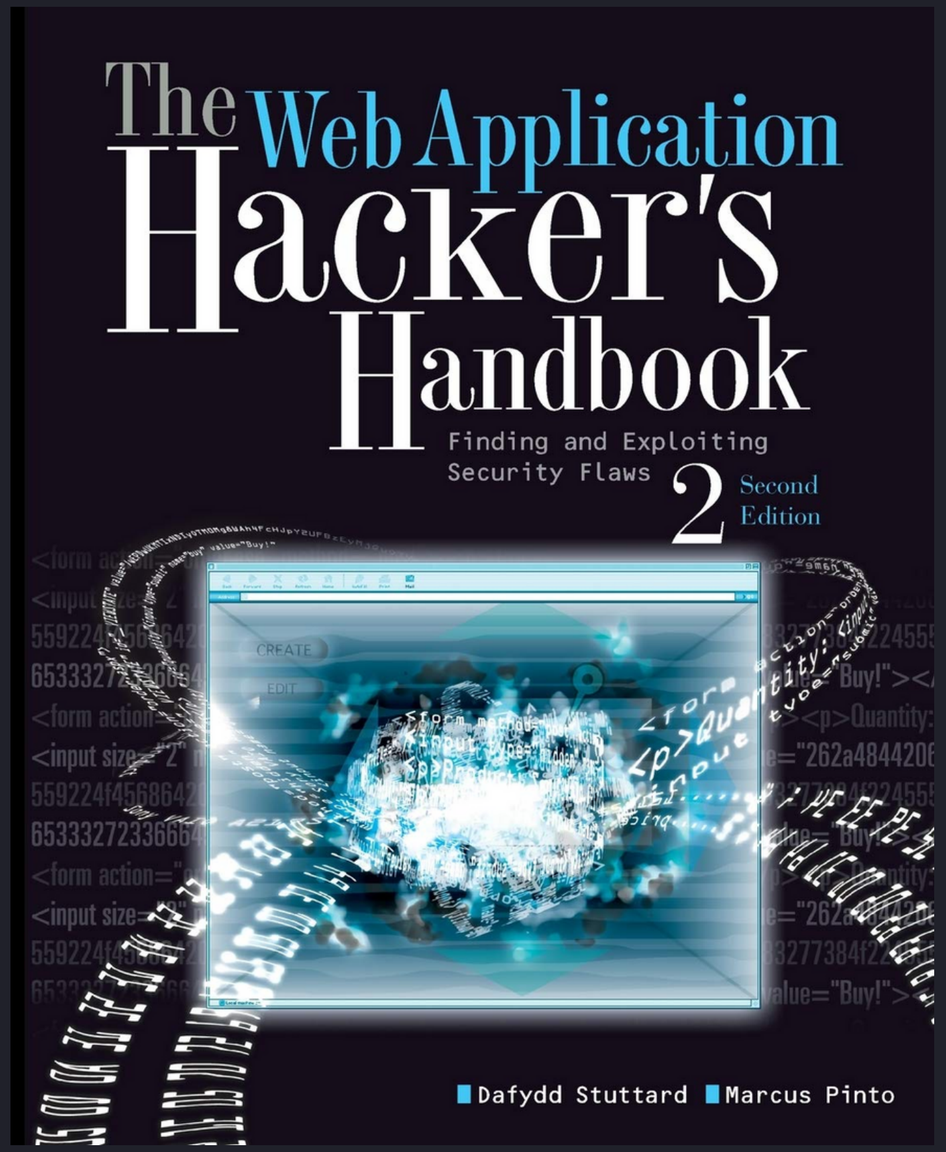
OWASP Top 10

- To understand these web security basics, OWASP has some useful guides.
- OWASP has categorized Top 10 vulnerabiltites 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

- Mastering Modern Web Application Penetration Testing
- Hackerone101.com
- Bugcrowd University

Youtube Channel

- Hackersploit
- Live OverFlow
- Hacking Simplified
- IppSec
- 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

யாமறிந்த மொழிகளிலே
தமிழ்மொழிபோல்
இனிதாவது எங்கும்
காணோம்.

-பாரதியார்