



Pathway to Application Security

By: Harsh Bothra

echo `whoami`



Cyber Security Analyst at Detox Technologies



Bugcrowd Top 150 & MVP Q1



Synack Red Teamer



Author | Speaker | Blogger



Poet



Explorer & Learner

Agenda

AppSec 101

Common Terms

What are security vulnerability

Pathway to Learn Appsec

How to Define Impact

How to Write Good Reports

Methodologies

Future Roadmap

AppSec 101

What is Appsec?

What areas are covered in Appsec?

Is there any difference in Bug Bounties vs AppSec vs Pentesting?

What is current competency of AppSec market?

Is it possible for a beginner to get started into AppSec?

Are there any specific requirements to be into AppSec?

What all prerequisites are a plus to get into AppSec?

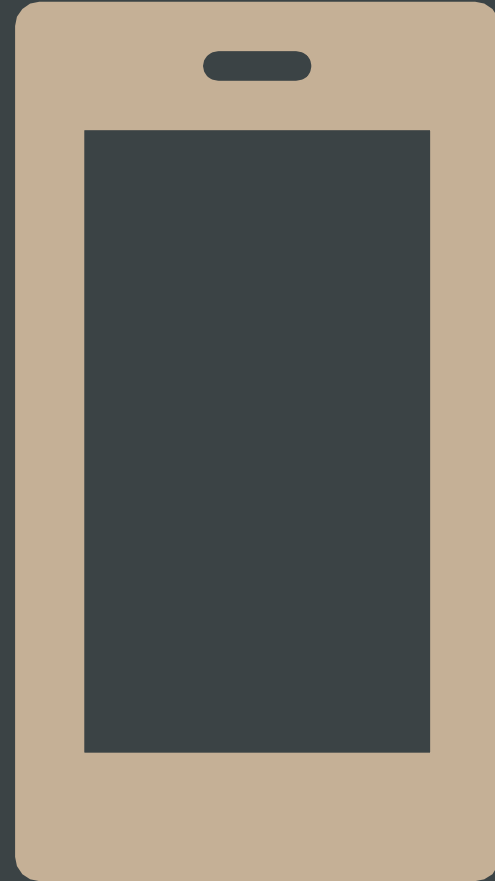
Common Terms

- Vulnerability / Bug
 - Attack Vector
 - Attack Surface
 - Exploit/Exploitation
 - Impact & Severity
 - Issue
 - Pentesting – Manual / Automated
 - Vulnerability Assessment
 - Automation
 - Reconnaissance
 - False Positive/True Positives
 - Chaining Issues
 - Responsible Disclosure
 - Bounty
 - Hall of Fame
 - Red Teaming
 - Blue Teaming
 - Purple Teaming
 - Thick Client
 - Sandbox Environment
- And some others

What are
Security
Vulnerabilities?



Pathway to Learn AppSec



Resources to Follow

- *OWASP TESTING GUIDE - MUST READ*
- *OWASP JUICE SHOP*
- *INFOSEC WRITEUPS on MEDIUM*
- *BUGCROWD LEVELUP TALKS*
- *PENTESTERLABS*
- *WEBSECURITY ACADEMY*
- *PORTSWIGGER RESEARCH BLOG*
- *HACKERONE DISCLOSED TIMELINE*

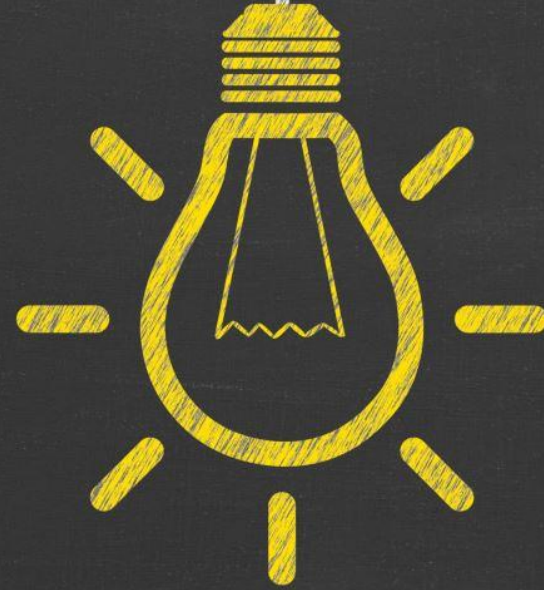
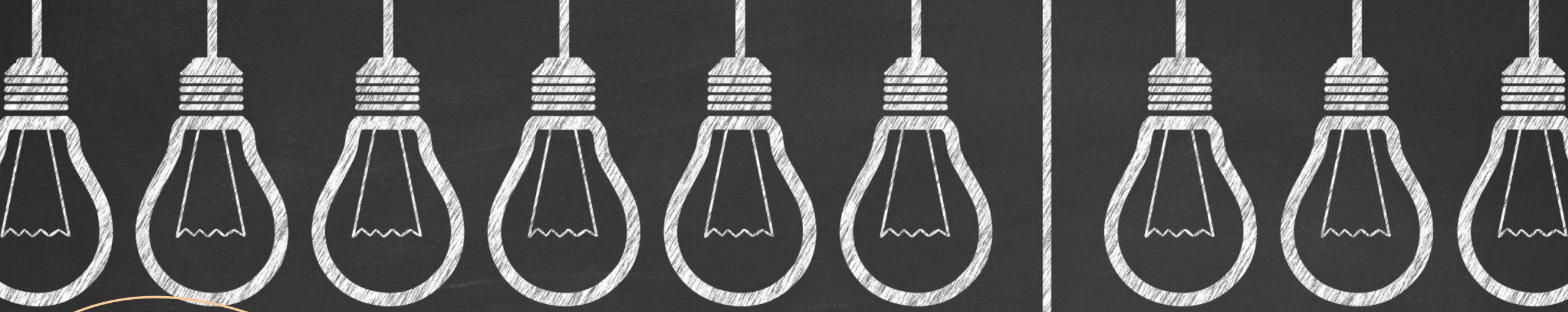
How to Define Impact & Severity

Two Matrices to Define Severity:

- Impact (Three Matrices)
 - Confidentiality
 - Integrity
 - Availability
- Exploitability (Five Matrices)
 - Attack Vector
 - Attack Complexity
 - Privileges Required
 - User Interaction
 - Scope

Writing a Good Report





Methodologies

Learn, Implement & Get Results

Tips


- Learn – Implement – Learn – Implement – Endless Loop
- Never Get too much comfortable with LAB Environment
- Keep on upgrading skills by reading articles
- Grab One Category Issues, Master them, Hunt them and further move to the next category.
- Don't stop if you face duplication or rejection!
- Be active on twitter, lot of good stuff is dropped every day.





FUTURE ROADMAP


Get in Touch at


 Website - <https://harshbothra.tech>

 Twitter - @harshbothra_

 Instagram - @harshbothra_

 Medium - @hbothra22

 LinkedIn - @harshbothra

 Facebook - @hrshbothra

 Email - hbothra22@gmail.com

Thank You ...