Knocking Systems for Vulnerabilities & Profit

- Harsh Bothra

Who – Am – I ?

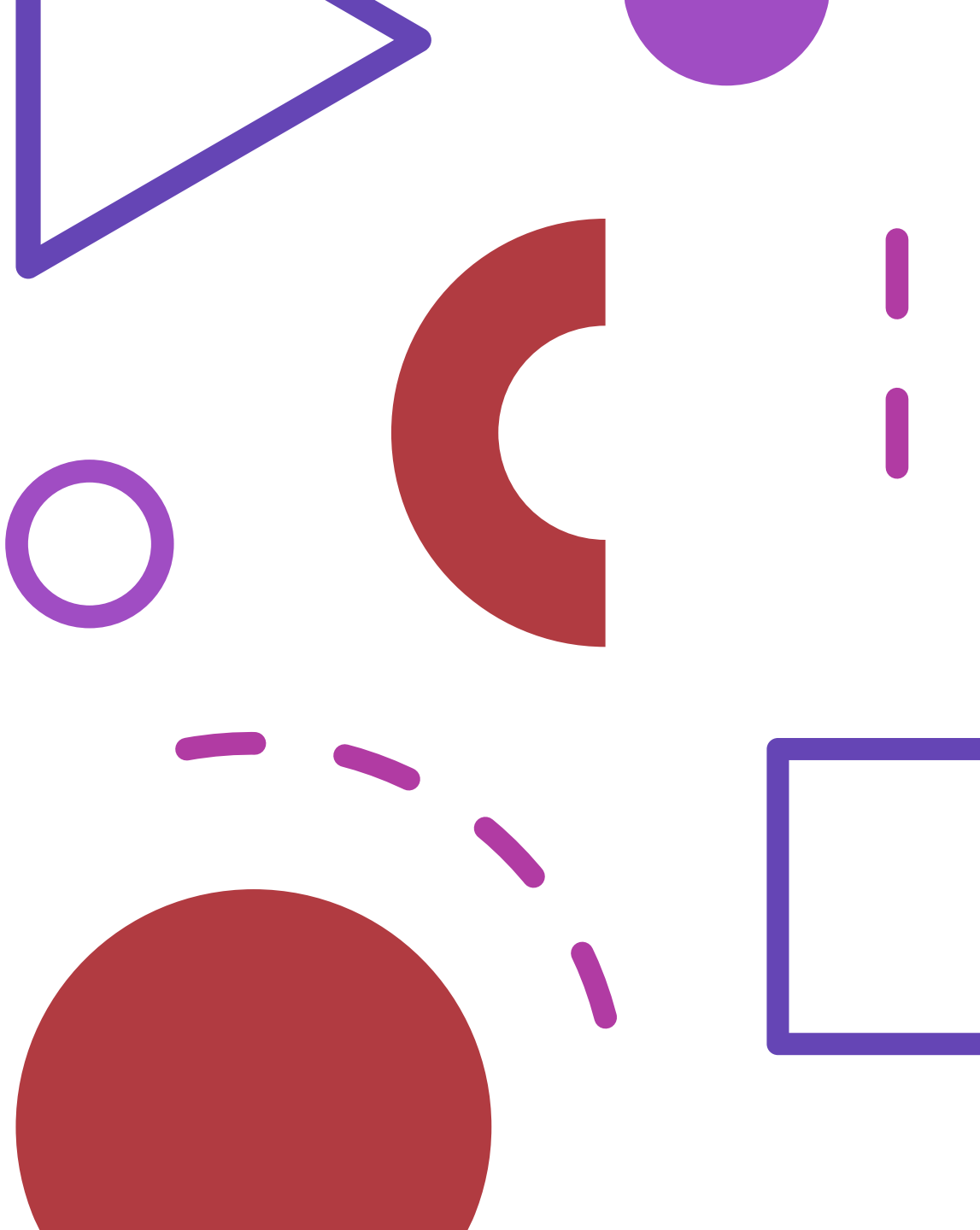
- Security Engineer at Security Innovation
- Bugcrowd Top 200 Researchers – All Time (Ranked 167th Currently)
- Synack Red Team Member
- Author – Hacking: Be a Hacker with Ethics (GoI Recognized)
- Author – Mastering Hacking: The Art of Information Gathering & Scanning
- Blogger
- Occasional Trainer & Speaker
- Poet
- Lifelong Learner

Agenda

- Ethical Hacking – 101

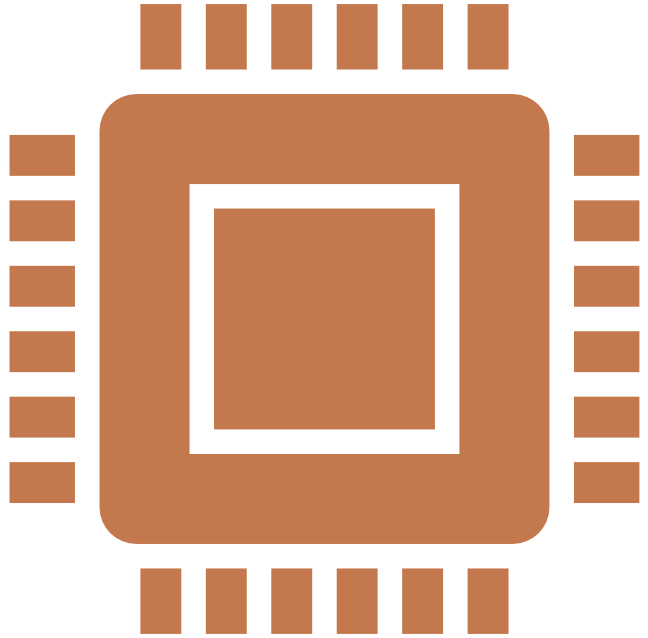
  (Really an Overview)
- Penetration Testing – 101

  (Bit Deep Dive)
- Bug Bounties 101



Ethical Hacking - 101

- What exactly Ethical Hacking is?
- Why do you need Ethical Hackers at first place?
- What you should know about Ethical Hacking?
- How you can start your Journey Towards Ethical Hacking
- Diving into Two Major Career Aspects:
  - Defensive
  - Offensive (<3)



Penetration Testing - 101

This is what we do! This is what I want you to do

Penetration Testing – 101 : Understanding the Game

- What is Penetration Testing?
- How it differs from Ethical Hacking?
- What we need to know before starting into Penetration Testing?

Harsh, are you an idiot? This is so much to know!!

Penetration Testing Cycle

- Reconnaissance
- Enumeration
- Attacking & Exploiting
- Getting Persistence & Lateral Movement
- Pivoting Around the Network
- Reporting !!

What we usually do in penetration testing?

- Start with a Point
- Enumeration the service
- Exploit Something
- Pivot to discover other Points
- Loop Step-1 to Step-4 until done
- Report

Let’s Just discuss some Use Cases based on what we discussed so far

Bug Bounty - 101

When it comes to Bug Bounty, We should talk:

What

Why

When

Where

How

X, Y, Z … of Bug Bounty.

Bug Bounty Ground Rules

My Bug Bounty Methodology

- Select target based upon scope – Wide Scope // Large Application
- RECON -- Watch my talks on Recon to see how I go about Recon
- Do Multiprocessing, While Recon is running, Fire up your Burp Suite and Test for IDORs, Server Side & Client Side Vulns.
- Understand the application logics and read the documents to make sure if you find a business logic, that's valid not an expected behavior.
- Map your Recon with your Testing – Find more hidden endpoints and new assets where others might not have been going/doing
- Report Every Security Issue whether it's a Low or Critical. Sometimes Critical are easy and low are hard to exploit (that's why they are low).
- Learn when stuck//something new is booming the market.
- Take necessary break, chill out!!

//Hack the world//

Tips'o'Tricks

- Recon Tips
- Burp Suite Hacks
- Tips related to various vulnerabilities

Show Time

Let’s have a Tour to my Hacking Arsenal.

Get in Touch at

 Website – https://harshbothra.tech

 Twitter - @harshbothra_

 Instagram - @harshbothra_

 Medium - @hbothra22

 LinkedIn - @harshbothra

 Facebook - @hrshbothra

 Email – hbothra22@gmail.com

Q/A are Welcomed