BUG HUNTING TACTICS

Agenda

- Bug Hunting 101
- Bug Hunting Methodologies
- Application Testing Methodology
- Recon Tactics
- Burp Suite Hacks
- Approaches for Client-Side Issues
- Approaches for Server-Side Issues
- Approaches for Logical & Access Control Issues

Bug Hunting 101

For those who are not familiar with Bug Bounties:

- White Hat approach towards Hacking
- Help Organizations in securing their Assets
- In Return, get Rewards.
- Rewards maybe from a Simple “Thanks” to $$$$$
- Legal profession worldwide
- Get good reputation and status
- Multiple Platforms to Get Started
- Big, Lovely Community
- Lots of Support Material Available

Bug Hunting 101
Platforms

- HackerOne
- Intigriti
- Bugcrowd
- Synack
- YesWeHack
- HackenProof
- Cesppa
- Private Programs
- Company Managed Programs (Google, Facebook, Apple, Microsoft, etc.)

Bug Hunting Methodologies

Rule –1: Don’t limit yourself to what you have learnt through tutorials and labs. Real life scenarios are totally different most of the time

Rule –2: Create your own checklist. Make a detailed checklist for every possible test cases that you can perform, and you know.

Rule –3: Keep a track record of everything you test. Often you may return to a program later someday or maybe your payload execute later.

Bug Hunting Methodologies

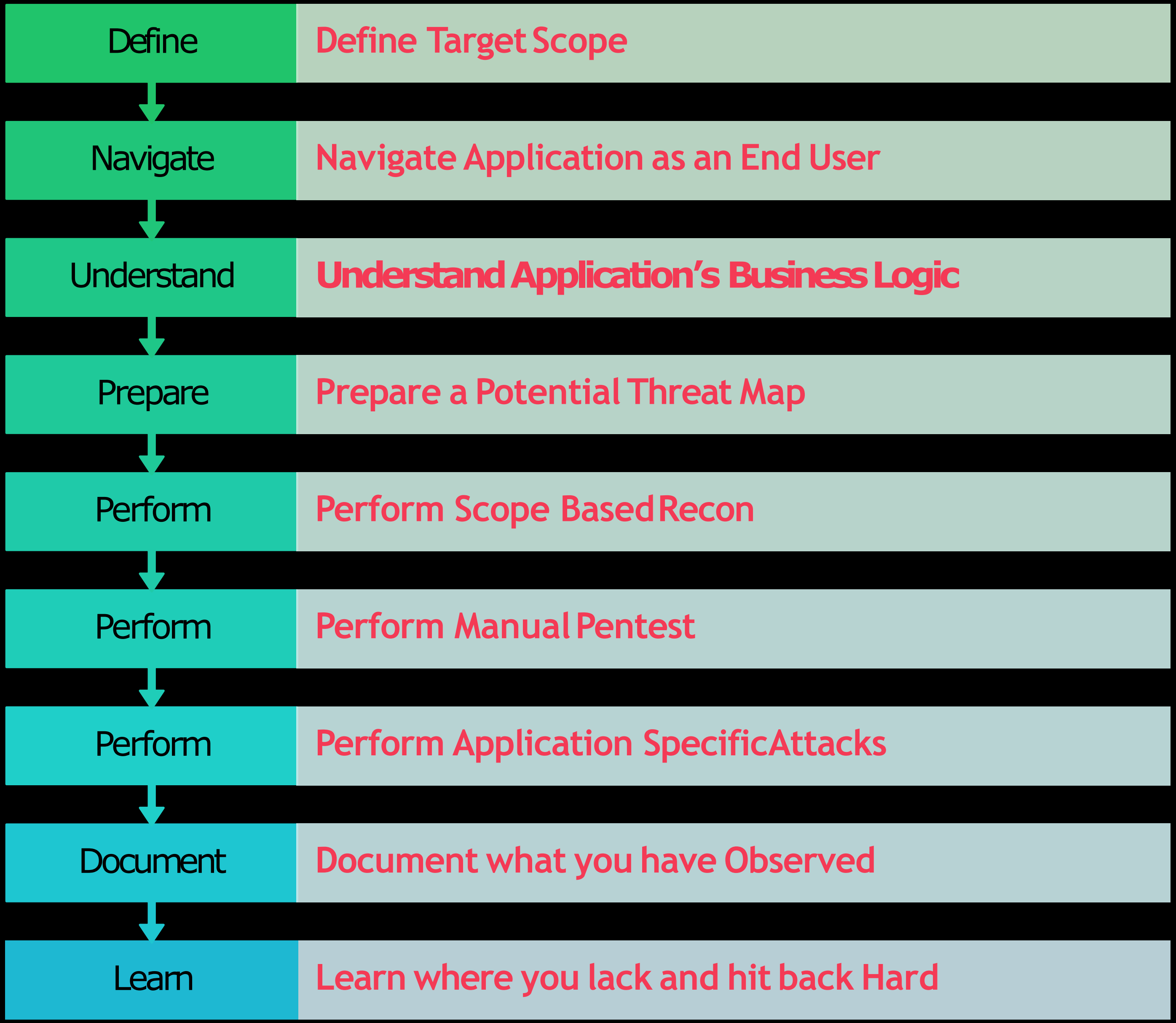
Rule - 4: Track CVEs & Public Exploit Releases. It will help you a lot specially in Network Pentesting.

Rule - 5: Be Lazy & Automate Stuff. Automate repetitive tasks, write small scripts that do your job while you focus on manual approach.

Rule - 6: Say no to Automated Vulnerability Scanners. They miss a lot of security issues and are not reliable. They are a helping hand not a replacement.

Rule - 7: Always be active to learn, apply & Experiment. Spend time on your target and you will see results eventually.

Application Testing Methodology



Define	Define Target Scope
Navigate	Navigate Application as an End User
Understand	**Understand Application's Business Logic**
Prepare	Prepare a Potential Threat Map
Perform	Perform Scope Based Recon
Perform	Perform Manual Pentest
Perform	Perform Application SpecificAttacks
Document	Document what you have Observed
Learn	Learn where you lack and hit back Hard

Potential Threat Mapping

Navigate Application Thoroughly

List All Components & Functionalities

Prepare Theoretical Attack Scenarios for each Functionality

Create possible C.I.A. & C.R.U.D. based Impact Scenarios

Export Potential Test Cases in a Check List format

Verify all these test cases while you perform Assessment

Manual Testing Approach

- Keep Vulnerability Standards such as OWASP TOP 10, OWASPASVS & SANS TOP Risks in mind while performing pentest
- Under the application workflows
- Figure out various possible workflows of the same features
- Try to break the application flow –This is where Business Logics exists
- Understand what technologies are being used by the application
- Perform technology specific attacks
- Try to find out bypasses for evading filters
- Try to perform testing for every single vulnerabilities
- Do not rely upon Automated Scanner Tools
- Learn, Research & Hack Again

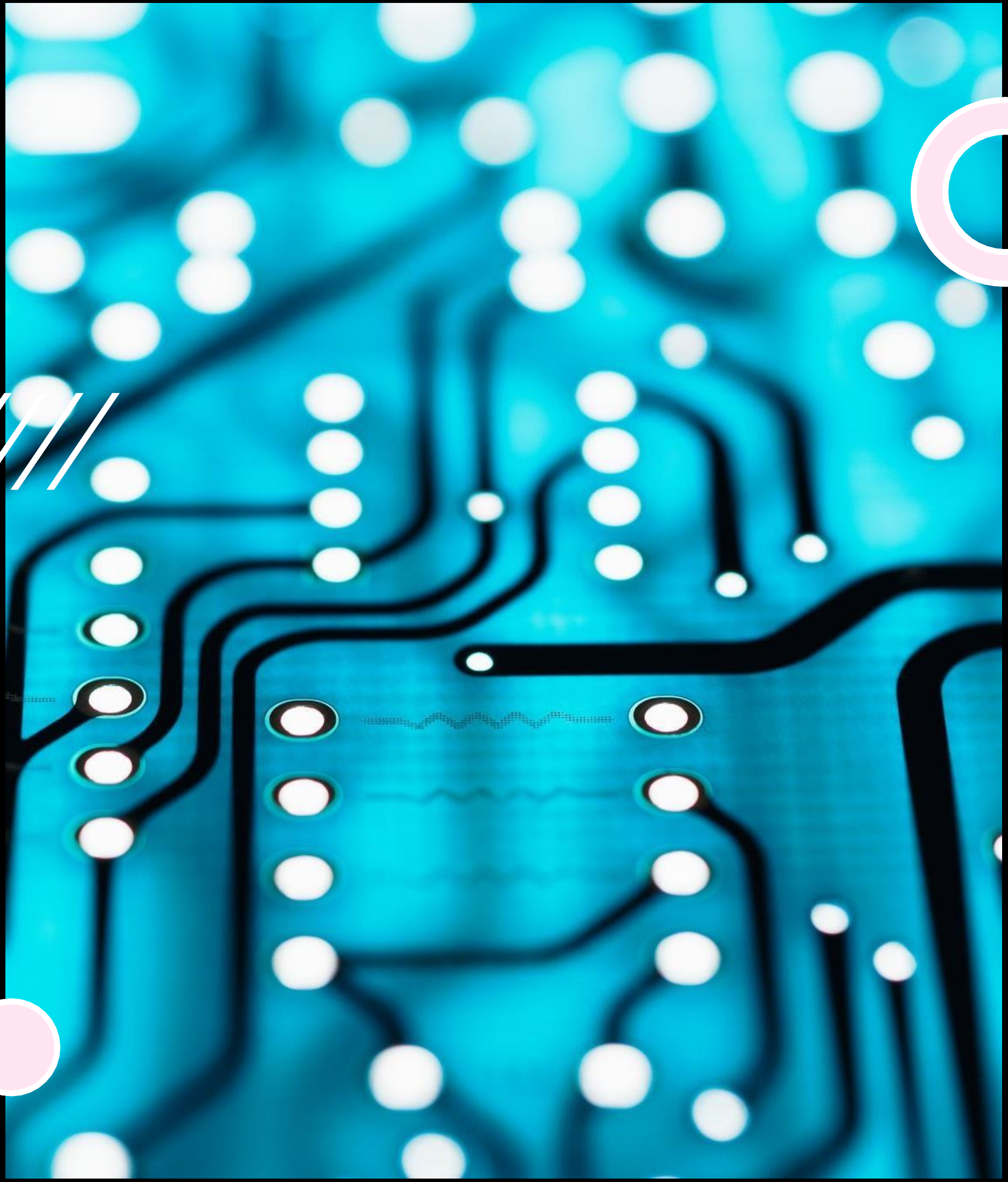
Scope Based Recon

- Scope Based Recon is a simply methodology to divide How to Perform when a specific set of Scope is Provided.
- Scopes are divided into three categories:
  - Small Scope
  - Medium Scope
  - Large Scope
- Why Scope Based Recon?
  - Saves a lot of time
  - You know what exactly to look for
  - You can easily automate your recon workflow
  - Less-chance to submit Out-of-Scope Issues
  - Just like other security methodologies enables you perform a better Recon

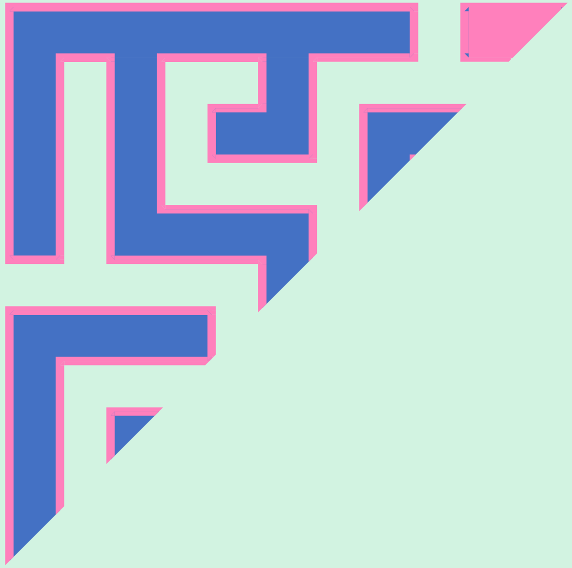
Burp Suite Hacks

- Advance Scope Controls
- Important Extensions
- Testing Access Control Issues
- Fuzzing with Burp Suite
- Introduction to Burp Macros
- Other Interesting Options

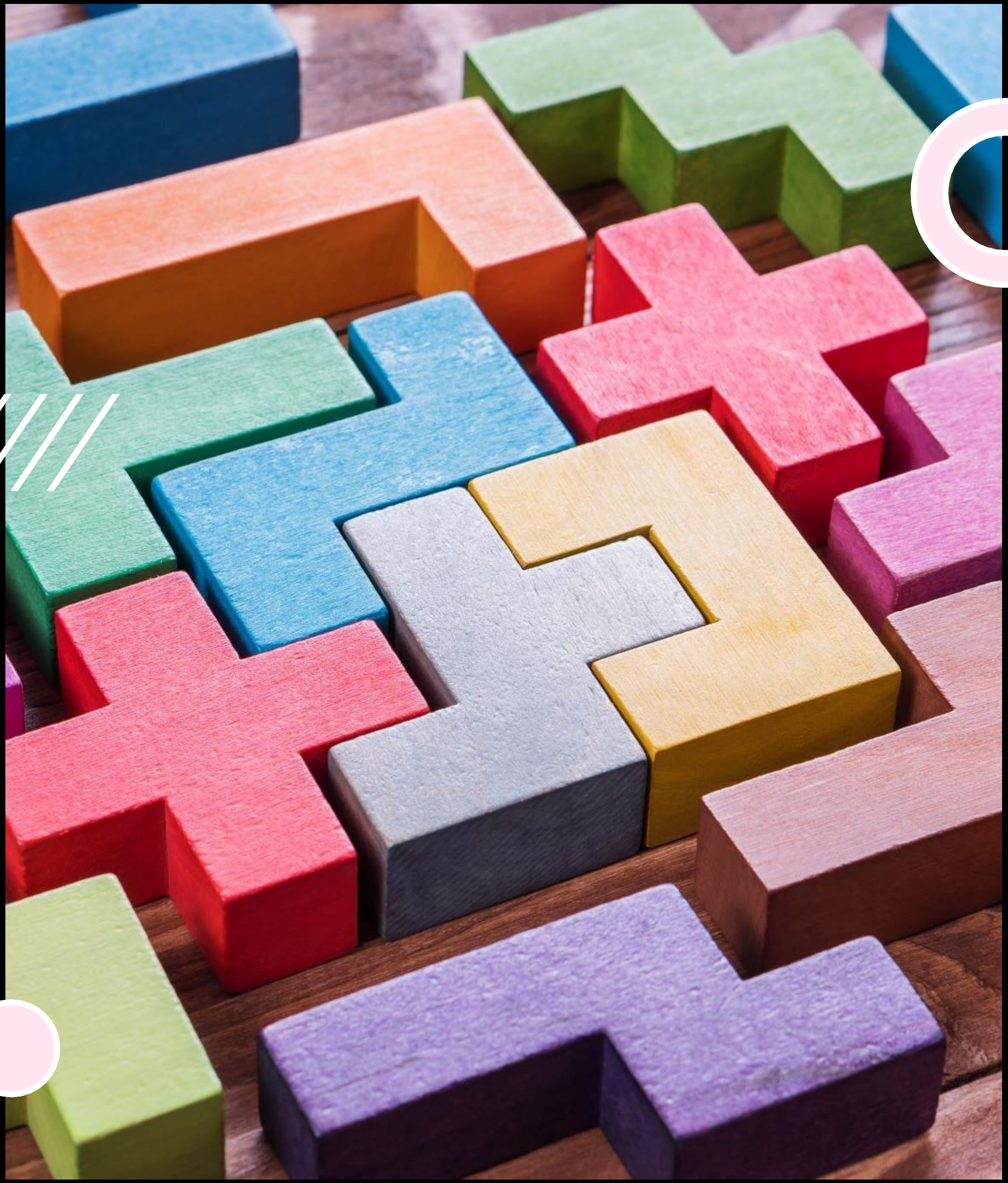
APPROACHES FOR SERVER-SIDE ISSUES



APPROACHES FOR CLIENT-SIDE ISSUES



APPROACHES FOR BUSINESS LOGIC ISSUES



THANKS...