



Bug Hunting Methodology

Become a Successful
Bug Bounty Hunter



METHODOLOGY

This is my methodology to uncover most bugs in applications. This is not technical but more a mind map.



METHODOLOGY

Tools:

- Burp Suite
- Chrome Developer Tools
- Firefox / Chrome Browser



METHODOLOGY

- Read the scope
- Understand the scope
- Digest scope
- Take notes
- Visualize in diagrams
- **UNDERSTAND THE APPLICATION**



METHODOLOGY

- Read the scope
- Understand the scope
- Digest scope
- Take notes
- Visualize in diagrams
- **UNDERSTAND THE APPLICATION**



METHODOLOGY

1. Public Info / XSS / Open Redirect / SSRF, Tokens

- Search Google, GitHub etc.
- Test every parameter for XSS
- Follow the XSS methodology chapter
- Analyze source code, inspect DOM and Java Script files to find redirects, URL inputs etc.



METHODOLOGY

2. Direct pages you can navigate to

These are pages you can directly navigate to from the browser. Pages which are not being accessed by AJAX / Fetch / XHR requests or hidden links. Note them down! Try with different privilege levels if you can



METHODOLOGY

3. The secondary pages

These are pages visible from a Fetch/XHR request or a hidden links. Note them down! Try with different privilege levels if you can



METHODOLOGY

4. The connections between these pages

How do these direct and indirect pages communicate? What's the relation between them? Note them down! Try with different privilege levels if you can



METHODOLOGY

5. Identify feature you already may have testing ideas on

Identify all functions for unauthenticated users, authenticated users, admins etc.

Registration, Login, Password Reset, Contact, Password change, profile change, book/buy something, search, track, cancel, delete, modify etc.



METHODOLOGY

6. Quick wins

- Public info available?
- Any parameters with IDs like `php?q=560720`
- Bypass for invitation code?
- Can fewer privilege account access admin functions? etc.
- Can unauthenticated users call admin functions? etc.
- Replace complex IDs with simple ID
- Any Parameters for redirection? Open Redirect? > XSS, SSRF?
- How to appear in insert functions on admin / privileged pages?
- View / edit things of someone else?



Thank You!

Become a Successful
Bug Bounty Hunter