Bug-Hunting-Day-5

Mar 31, 2019

So, This is summary of my Bug Hunting Diary from Day 2 to Day 5

On day 2 i was confuse, How i start testing such large domains? What tools i must have? Where to start looking for? Does checklist really be helpful?

After looking many tools online i found so many tools on github and all are having own setup.

I used them and messed up with them and I feel lost

So still confuse. Then I ask many of friends about testing a target and using tools and then this is what I learned ->

1. Pick the target from program either public or private or both and find subdomains as much as i can and choose the target which suitable for me. For this focus on tools -> amass,sublister,subbrute,aqatone Best is using all of above as combination like First find subdomains list as all-subdomains-list.txt and then use aquatone on that txt file to grab screenshots.
2. Then from screenshots choose the target which suitable for me like for sqli
3. directory scanning,check for all endpoints

So, Everything is in the dirs,files and Subdomains

Best thing I learned is KISS[Keep It Simple Stupid/Stuff]

So I found following Links very helpful which helped me to clear my confusion

a) https://github.com/ehsahil/recon-my-way

b) https://github.com/S4R1N/BlackBird

c) https://github.com/j3ssie/Osmedeus

d) https://github.com/SolomonSklash/chomp-scan/

e) https://github.com/cak/domained

f) https://pentester.land/cheatsheets/2018/11/14/subdomains-enumeration-cheatsheet.html

sahil blog [recon-my-way] and chomp-scan and cheatsheets by pentester.land I found Most Usefull

Well this all are the recon stuffs. Also I got to know mostly Bug hunters use Burp+Firefox for finding vulnerability

So this is mix of :-

- subdomain scanning
- get all screenshots
- pick subdomain of own choice
- Find all endpoints
- Use Burp+Firefox for vulnerability testing

And all of this is no one time sitting on target Just have to be patience.

Also other thing I got to know is just play with tools untill I become use to of those tools and read their documents and practice over them.

Practicing on Public program in starting for beginners must have GOAL like just learn to recon as much and try to focus one bug at a time and practice on that as much even if We not getting vulnerability in starting but it will help us in future.

All we need is Experience

I will note all Documents of those tools with commands own my own choice in upcoming days.