Bug Hunting Topic

RECON & TIPS ABOUT EASY CRITICAL/HIGH BUGS

About Me

- Orwa Atiyat From Jordan
- Full Time Bug Hunter
- Ranked As 59th Full Rank On Bugcrowd Platform
- Ranked As 6th On P1 Warrior On Bugcrowd
- 160+ Critical Bugs On Bugcrowd
- 50+ Critical/high Bugs On H1
- 5 Critical/high Bugs On Facebook
- 2 Critical/high bugs On Google
- Owned CVE-2022-21500 & CVE-2022-21567

Collect Domains

Crt.sh – Securitytrails

https://ultimatedomains.com/extract-domains.php

https://github.com/Cyber-Guy1/domainCollector

Collect Subdomain [Amass]

amass enum -passive -norecursive -noalts -d domain -o subdomain.txt

amass enum -passive -norecursive -noalts -df domains.txt -o sub-domains.txt

Scan Ports

https://github.com/projectdiscovery/naabu

Filter Subdomain List To Live

cat subs.txt | httpx -o live.txt

cat subs.txt | httpx -t 60 -nc -p top-ports -o live.txt

Collect Endpoints

https://web.archive.org/cdx/search/cdx?url=*.XXX&fl=original&collapse=urlkey

dorking over bing

[theres a lot of sources about google & waybackurls]

Github Searching For Leaked Credentials

Shodan Searching
ssl:"X" 200
Ssl.cert.subject.CN:"X" 200

Explain Critical Easy Bugs To Find…..

Great Enumerations Scripts
https://github.com/six2dez/reconftw
https://github.com/yogeshojha/rengine
https://github.com/iamthefrogy/frogy
https://github.com/Cyber-Guy1/Subdomainer

Tips….

- https://twitter.com/GodfatherOrwa
- https://bugcrowd.com/orwagodfather
- https://hackerone.com/mr-hakhak?type=user

- Thanks….