Listing

Challenges

- **HTTP - Directory indexin :** https://www.root-me.org/en/Challenges/Web-Server/HTTP-Directory-indexing

  use dirsearch || dirbuster

Notes

Gobuster

-x php,txt,html,htm --> specify file extenstions

gobuster dir -u http://10.10.10.163 -w <dirbuster medium> -x php -o gobusterout

gobuster dir -u http://10.10.10.163 -w <dirbuster medium> -x php -o gobusterout
gobuster dir -u http://3.21.186.210:3002/-w <dirbuster medium> -x php,html -o gobusterout

gobuster on results if 301 ?

Dirb

dirb http://10.10.10.6 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt | tee dirbmedium

dirb http://10.10.10.168:8080/ -w /usr/share/wordlists/dirb/small.txt | tee dirbSmall.txt

dirb http://10.10.10.171 -w /usr/share/wordlists/dirb/Big.txt | tee dirbBig.txt

dirb http://10.10.10.171 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o dirbout -X php,js,py

DirSearch

Inside /opt/dirsearch

https://github.com/maurosoria/dirsearch

python3 dirsearch.py -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -e php -f -t 20 -u http://bank.htb > /root/htb/bank/dirsearch

To download all files in a webpage :

Wget -r http://bank.htb/balance-transfer/

Another way is using burp pro
Add folder to scope in target tab
Right click : Spider this branch
Filter by : regex —> negative search