HACKTHEBOX

ATTACKING WEB APPLICATIONS WITH FFUF

CHEAT SHEET

Ffuf

Command	Description
`ffuf -h`	ffuf help
`ffuf -w wordlist.txt:FUZZ -u http://SERVER_IP:PORT/FUZZ`	Directory Fuzzing
`ffuf -w wordlist.txt:FUZZ -u http://SERVER_IP:PORT/indexFUZZ`	Extension Fuzzing
`ffuf -w wordlist.txt:FUZZ -u http://SERVER_IP:PORT/blog/FUZZ.php`	Page Fuzzing
`ffuf -w wordlist.txt:FUZZ -u http://SERVER_IP:PORT/FUZZ -recursion -recursion-depth 1 -e .php -v`	Recursive Fuzzing
`ffuf -w wordlist.txt:FUZZ -u https://FUZZ.hackthebox.eu/`	Sub-domain Fuzzing
`ffuf -w wordlist.txt:FUZZ -u http://academy.htb:PORT/ -H 'Host: FUZZ.academy.htb' -fs xxx`	VHost Fuzzing
`ffuf -w wordlist.txt:FUZZ -u http://admin.academy.htb:PORT/admin/admin.php?FUZZ=key -fs xxx`	Parameter Fuzzing - GET

Command	Description
`ffuf -w wordlist.txt:FUZZ -u http://admin.academy.htb:PORT/admin/admin.php -X POST -d 'FUZZ=key' -H 'Content-Type: application/x-www-form-urlencoded' -fs xxx`	Parameter Fuzzing - POST
`ffuf -w ids.txt:FUZZ -u http://admin.academy.htb:PORT/admin/admin.php -X POST -d 'id=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs xxx`	Value Fuzzing

Wordlists

Command	Description
`/opt/useful/seclists/Discovery/Web-Content/directory-list-2.3-small.txt`	Directory/Page Wordlist
`/opt/useful/seclists/Discovery/Web-Content/web-extensions.txt`	Extensions Wordlist
`/opt/useful/seclists/Discovery/DNS/subdomains-top1million-5000.txt`	Domain Wordlist
`/opt/useful/seclists/Discovery/Web-Content/burp-parameter-names.txt`	Parameters Wordlist

Misc

Command	Description
`sudo sh -c 'echo "SERVER_IP academy.htb" >> /etc/hosts'`	Add DNS entry
`for i in $(seq 1 1000); do echo $i >> ids.txt; done`	Create Sequence Wordlist
`curl http://admin.academy.htb:PORT/admin/admin.php -X POST -d 'id=key' -H 'Content-Type: application/x-www-form-urlencoded'`	curl w/ POST