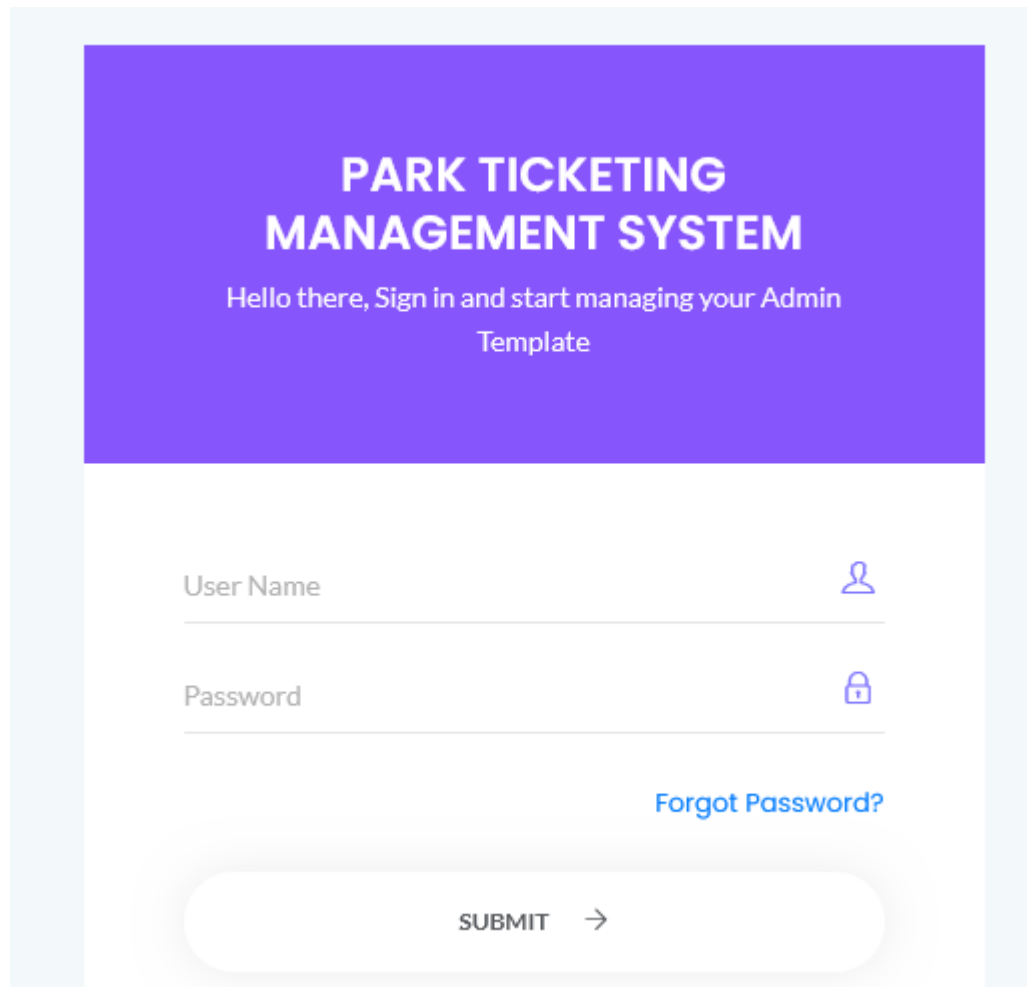



SQL injection vulnerability in “/ptms/index.php” in PHPGurukul Park Ticketing Management System v1.0 allows ATTACKER to execute arbitrary SQL commands via the "login" parameter.


- 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.



**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--

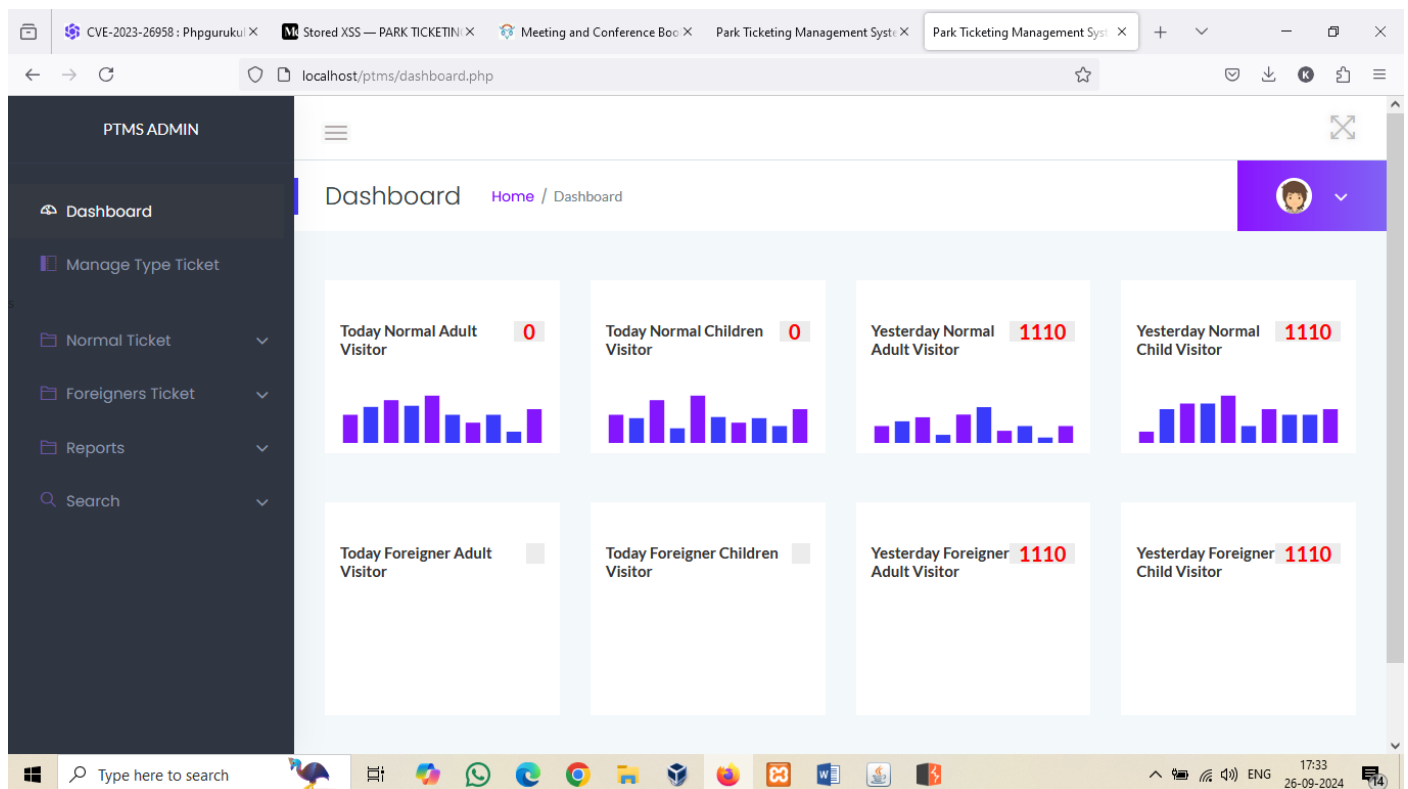
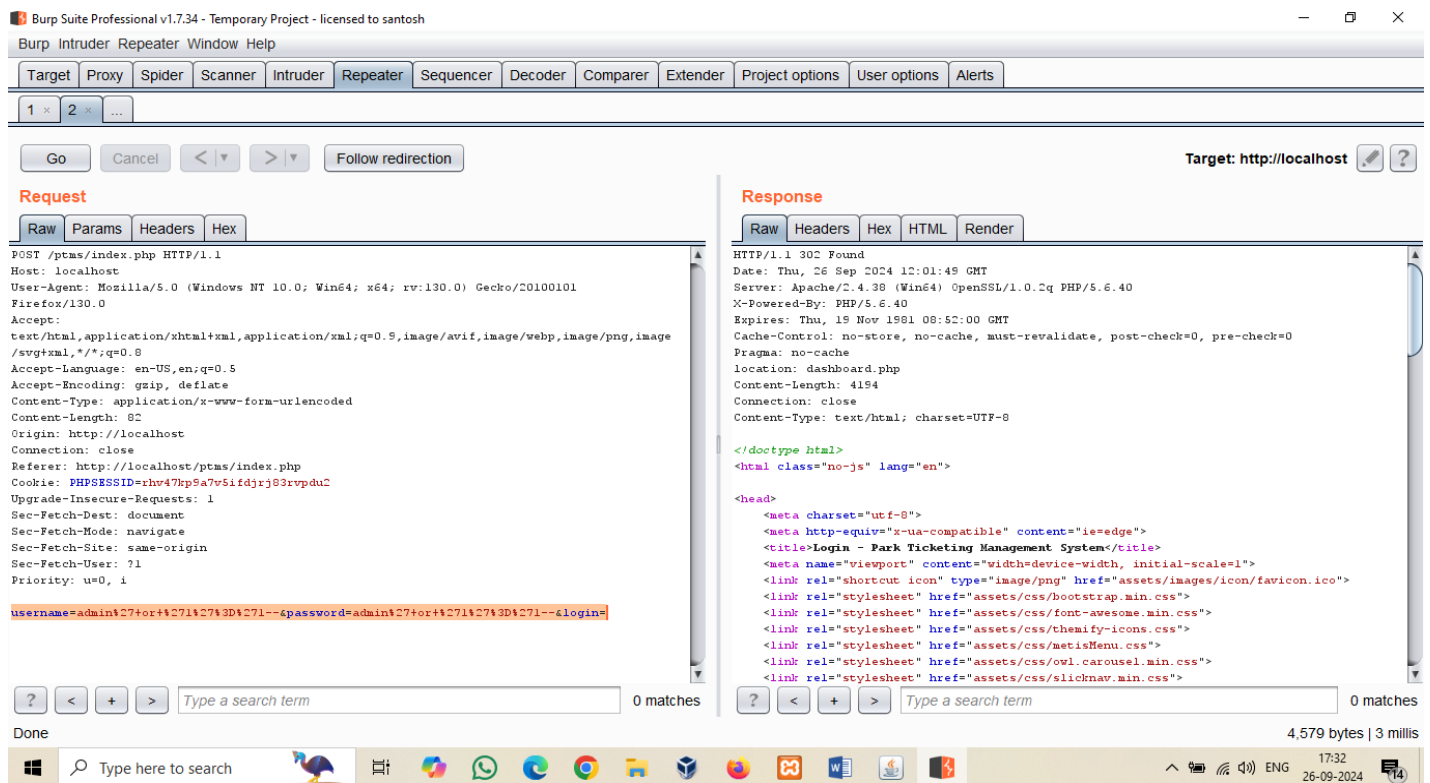
Password

●●●●●●●●●●●●●●●●

[Forgot Password?](#)

SUBMIT →

2. Enter any random value and click "Reset" button. Intercept the request in BurpSuite  
And send repeater.



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

[SQL Injection | OWASP Foundation](#)

