



Unauthenticated SQL Injection ...

Description

Poc

Impact:

Exploitability

Unauthenticated SQL Injection in School Management System

Modified April 6

BUG_Author: EthX0_

Affected Version: [school-management-system \(commit 6](#)

Vendor: <https://github.com/ProjectsAndPrograms>

Software: <https://github.com/ProjectsAndPrograms/school-m>

Vulnerability Files:

- buslocation.php

Description

Unauthenticated SQL Injection (SQLi):

A critical SQL Injection vulnerability exists in the `buslocation.php` file of the School Management System. The application fails to properly sanitize user input before using it in a database query.

Specifically, on line 54 of `student_panel/buslocation.php`, user input is concatenated into the SQL statement: `$sql = "SELECT * FROM bus_location WHERE bus_id='{$_GET['bus_id']}'";`

```

student_panel
├── fetch-data
├── images
├── JS app.js
├── buslocation.php
├── buspanel.php
├── check-fee-rcipt.php
├── database.php
├── exam.php
├── fee-payment.php
├── fetchAttendance.php
└── ...

```

```

49
50
51
52
53
54 $sql = "SELECT * FROM bus_location WHERE bus_id='{$_GET['bus_id']}'";
55
56
57

```