menevarad007 / **CVE-2026-37749** Public

Code Issues Pull requests Actions Projects Security and quality Insights

.. 1 Branch 0 Tags Go to file Go to file Code

menevarad007 Update CVE assignment date in README 366533f · 53 minutes ago

README.md	Update CVE assignment date in …	53 minutes ago
exploit.py	Exploit for SQLi authentication by…	yesterday

README

CVE-2026-37749 — CodeAstro Simple Attendance Management System 1.0 - SQL Injection

Details

Field	Info
CVE ID	CVE-2026-37749
Type	SQL Injection → Authentication Bypass
Severity	Critical (CVSSv3: 9.8)
Vendor	CodeAstro
Product	Simple Attendance Management System
Version	1.0
Discoverer	Varad AP Mene
Date	2026-04-16
CWE	CWE-89

Description

A SQL Injection vulnerability exists in CodeAstro Simple Attendance Management System v1.0 in the login form of index.php. The username POST parameter is concatenated directly into a MySQL query without sanitization or use of prepared statements. An unauthenticated remote attacker can bypass authentication and gain administrative access by submitting a crafted SQL payload in the username field.

Affected Product: Simple Attendance Management System v1.0 **Vendor:** CodeAstro **Affected File:** index.php **Parameter:** username (POST) **Payload:** admin'-- - **CVE:** CVE-2026-37749 **CWE:** CWE-89 **CVSSv3:** 9.8 Critical (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Product Description

Simple Attendance Management System 1.0 is a PHP/MySQL web application published by CodeAstro used to manage student attendance records in schools and colleges.

Vendor URL: https://codeastro.com/simple-attendance-management-system-in-php-with-source-code/

Vulnerable File

index.php — Login form

Vulnerable Code

```
// index.php - Line 23
$query = "SELECT * FROM admin WHERE username='$username' AND password='$password'";
$result = mysql_query($query);
```

Raw $_POST data used directly — no escaping, no prepared statements.

Proof of Concept

Step 1 — Go to login page: http://target/attendance/index.php

Step 2 — Enter these credentials: Username: admin'-- - Password: anything Type: admin

Step 3 — Click Login Result: Admin panel access granted without valid credentials!

Impact

- Authentication bypass without valid credentials
- Full admin access to all attendance records
- Data exposure and manipulation
- **No authentication required** — exploitable by anyone

Remediation

```php
$stmt = $mysqli->prepare("SELECT * FROM admin WHERE username=? AND password=?");
$stmt->bind_param("ss", $username, $password);
$stmt->execute();
$result = $stmt->get_result();
```

Timeline

Date	Event
2026-03-24	Vulnerability discovered
2026-03-24	Reported to MITRE
2026-04-16	CVE-2026-37749 assigned
2026-04-16	Public disclosure
2026-04-16	MITRE notified about publication
2026-04-16	Vendor notified via CodeAstro contact form
2026-04-16	Submitted to Exploit-DB

References

- https://codeastro.com/simple-attendance-management-system-in-php-with-source-code/

Discoverer

Varad AP Mene

Releases

No releases published

Packages

No packages published

Contributors 1

menevarad007 Varad Mene

Languages

- **Python** 100.0%