superhacker

Challenge

```
$flag1 = "[REDACTED]";
$flag2 = "[REDACTED]";
if(array_key_exists("username",$_REQUEST)){
    $link = mysqli_connect('localhost','challenge','[REDACTED]');
    $uName = $_REQUEST['username'];
    $pass = $_REQUEST['password'];

    mysqli_select_db($link,'toPwn');
    $statement = "SELECT * FROM users WHERE username = '$uName' AND password = '$pass'";
    $res = mysqli_query($link,$statement);
    if(array_key_exists("iamahacker",$_GET)){
        echo "$flag1 ";
        if(array_key_exists("debug",$_GET)){
            echo "$statement ";
        }
        if(mysqli_num_rows($res) > 0){
            echo "$flag2" ;
        }
    }else{
        echo 'nope!';
    }
    mysqli_close($link);
```

In the given source code, we can see that there are hard coded authentication variables.
One of which is a value 'iamhacker'.
This variable is also obtained via a $_GET request.
This is worth noting because it signals we can pass values to this server via the URL as this is how this type of request is passed.

It also appears that the server is not checking for a valid username and password before printing the first flag.
Because the source code is a running PHP script, we pass a variable via the URL with a preceding ? character and appending a & character between consecutive variables.
With these facts, we can pass any username and any password alongside setting the 'iamahacker' value to be true.

Solution

The created payload included all three variables:

http://ctf.hackucf.org:4001/index.php/?username=hacker&password=hacker&iamahacker=TRUE

After rendering the URL we get the flag:
flag{r3

Unfortunately, I could not get the second flag because the SQL database has been disconnected.