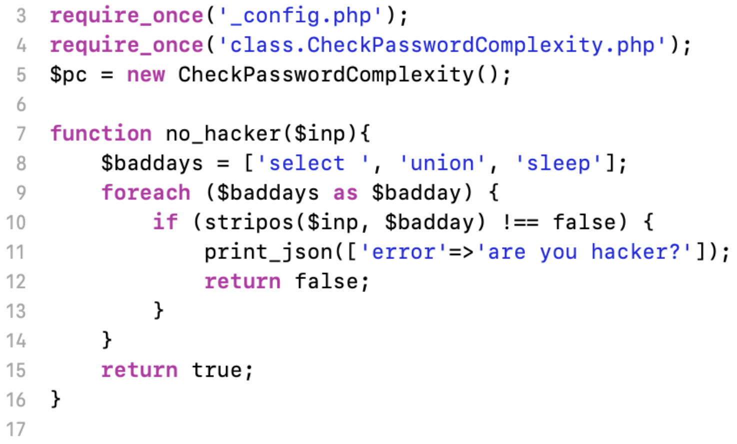
Instruction:

“The developer launch a website for student to register and login to gain access. You are now work under security department in faculty of ICT, Mahidol university. Your job is to check the vulnerability of this website.”

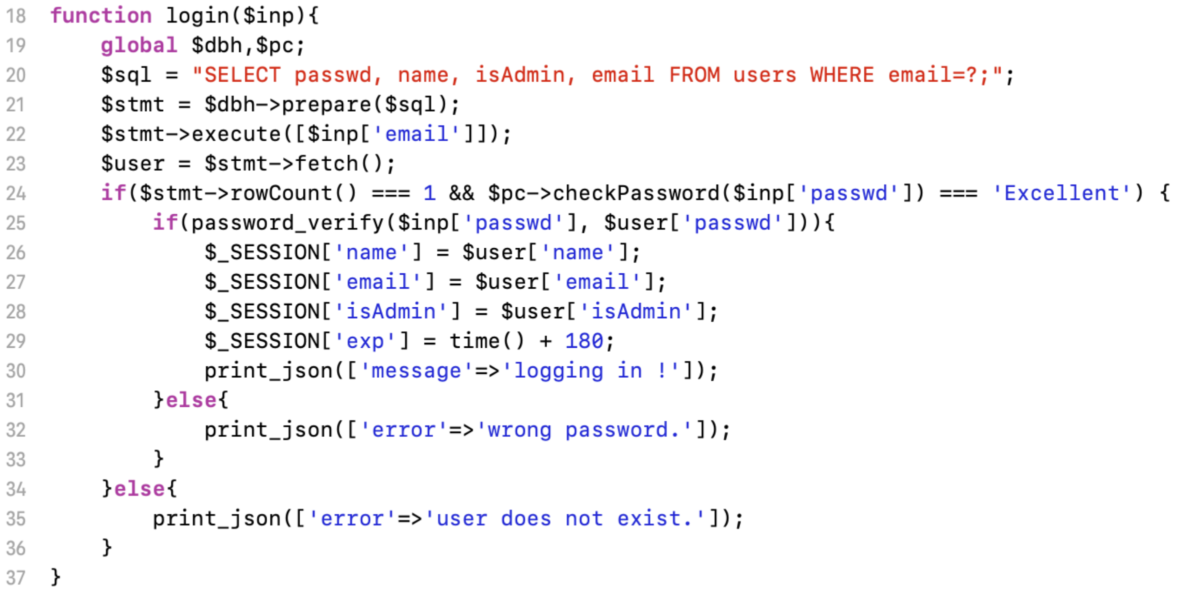
Hint:	You have to work with 1 file which is index.php

index.php



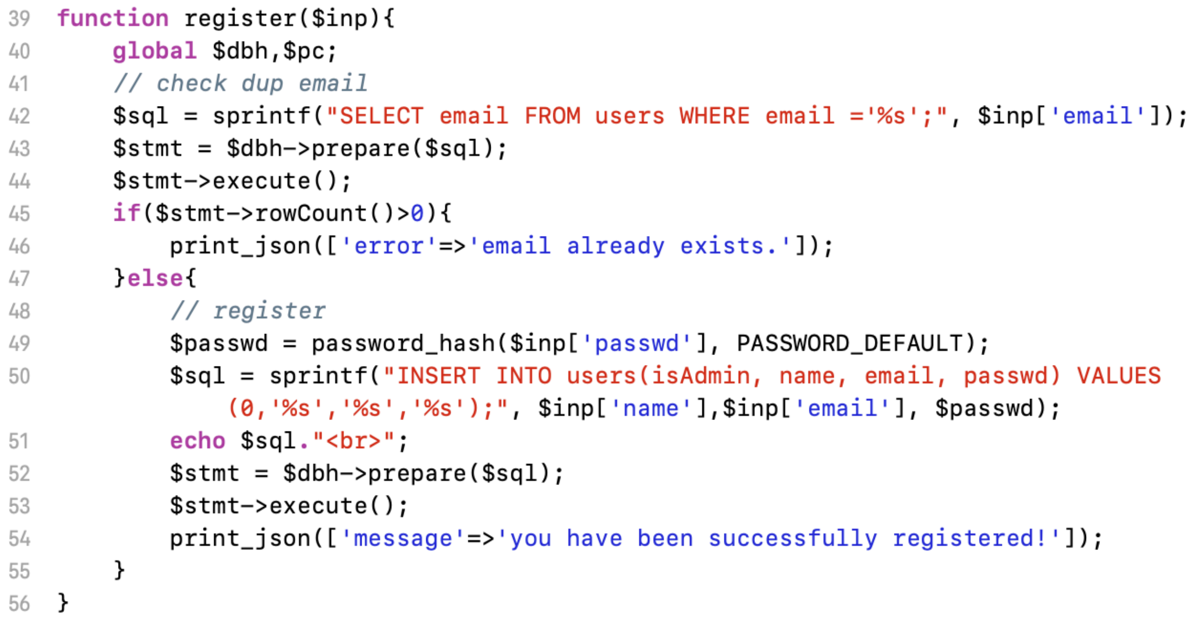
```
 3  require_once('_config.php');
 4  require_once('class.CheckPasswordComplexity.php');
 5  $pc = new CheckPasswordComplexity();
 6
 7  function no_hacker($inp){
 8      $baddays = ['select ', 'union', 'sleep'];
 9      foreach ($baddays as $badday) {
10          if (stripos($inp, $badday) !== false) {
11              print_json(['error'=>'are you hacker?']);
12              return false;
13          }
14      }
15      return true;
16  }
17
```

On no_hacker function, the bad word space will be check with an input in order to avoid some SQL injection attack.



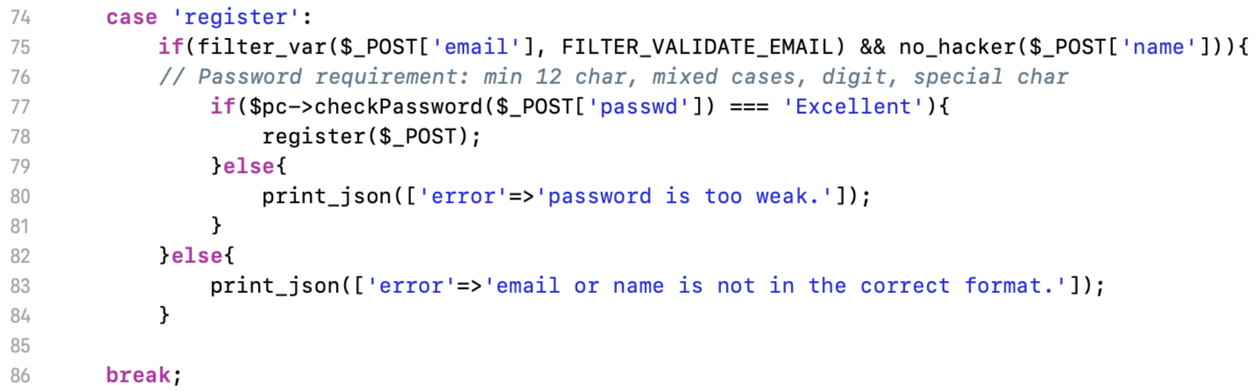
```
18  function login($inp){
19      global $dbh,$pc;
20      $sql = "SELECT passwd, name, isAdmin, email FROM users WHERE email=?;";
21      $stmt = $dbh->prepare($sql);
22      $stmt->execute([$inp['email']]);
23      $user = $stmt->fetch();
24      if($stmt->rowCount() === 1 && $pc->checkPassword($inp['passwd']) === 'Excellent') {
25          if(password_verify($inp['passwd'], $user['passwd'])){
26              $_SESSION['name'] = $user['name'];
27              $_SESSION['email'] = $user['email'];
28              $_SESSION['isAdmin'] = $user['isAdmin'];
29              $_SESSION['exp'] = time() + 180;
30              print_json(['message'=>'logging in !']);
31          }else{
32              print_json(['error'=>'wrong password.']);
33          }
34      }else{
35          print_json(['error'=>'user does not exist.']);
36      }
37  }
```

On function login, the user have to login with email and password which will be check with database inside server. Then, the session will keep information to show on next page. [Line: 26 - 30]



```
39  function register($inp){
40      global $dbh,$pc;
41      // check dup email
42      $sql = sprintf("SELECT email FROM users WHERE email ='%s';", $inp['email']);
43      $stmt = $dbh->prepare($sql);
44      $stmt->execute();
45      if($stmt->rowCount()>0){
46          print_json(['error'=>'email already exists.']);
47      }else{
48          // register
49          $passwd = password_hash($inp['passwd'], PASSWORD_DEFAULT);
50          $sql = sprintf("INSERT INTO users(isAdmin, name, email, passwd) VALUES
                (0,'%s','%s','%s');", $inp['name'],$inp['email'], $passwd);
51          echo $sql."<br>";
52          $stmt = $dbh->prepare($sql);
53          $stmt->execute();
54          print_json(['message'=>'you have been successfully registered!']);
55      }
56  }
```

On function register, user have to register with name, email, and password. The query will be executed here for inserting a new user account. The password will be hash with Blowfish-Encryption (a hashing function). [Line:49]



```
74      case 'register':
75          if(filter_var($_POST['email'], FILTER_VALIDATE_EMAIL) && no_hacker($_POST['name'])){
76          // Password requirement: min 12 char, mixed cases, digit, special char
77              if($pc->checkPassword($_POST['passwd']) === 'Excellent'){
78                  register($_POST);
79              }else{
80                  print_json(['error'=>'password is too weak.']);
81              }
82          }else{
83              print_json(['error'=>'email or name is not in the correct format.']);
84          }
85
86      break;
```

On switch case 'register', the email and input is validated with filter_var() function and no_hacker() function. [Line:75]

Some Helping Tools:
- https://dev.mysql.com/doc/refman/8.0/en/insert.html
- https://bcrypt-generator.com/