웹방어전 풀이

과제	
날짜	@Feb 14, 2021
멘토님	지한별
접속링크	

웹방어전 개요

- 개인별로 서버 및 웹 IDE 제공
  - 은행 홈페이지 컨셉
  - http://141.164.54.190/bob9/
  - http://141.164.54.190:8080/?folder=/var/www/html/bob9/
- 총 14 문제 (서버 사이드 취약점)
- 주어진 사이트에서 취약점 터지는지 직접 시도해보거나
- 웹 IDE에서 소스코드 정적 분석해서 패치 후
- 웹방어전 메인 사이트에서 SLA 체크를 통해 채점
- 취약점이 패치되어서 공격이 안 먹히면 포인트를 취득하는 식
- 14/14 만점

1. 로그인 (SQL Injection)

소스코드

var > www > html > bob9 > logindo.php

```php
<?php
session_start();
include "./dbController.php";
include "./session.php";

$username = $_POST['username'];
$password = hash("sha512", $_POST['password'], false);

$db = new DBController();
$row = $db->db_select("users","name='".$username."'");

$db_password = $row[0]['pass'];

if (isset($password)){
    if ( $db_password === $password ) {
        $_SESSION['username'] = $username;
        echo json_encode(array("msg" => "로그인 성공"));
    }else {
        echo json_encode(array("msg" => "로그인 실패"));
    }
}else{
    echo json_encode(array("msg" => "패스워드를 입력하세요."));
}
?>
```

테스트 구문

1'union(select(1),'pw hash값,' 10000)#

1"union(select(1),"pw hash값," 10000)#

- '만 패치하는 경우 체크
- ' → "

2. 회원가입 (SQL Injection)

소스코드

var > www > html > bob9 > register.php

```php
<?php
include "./dbController.php";

$username = $_POST['username'];
$password = hash("sha512", $_POST['password'], false);

$db = new DBController();
$row = $db->db_select_count("users", "name='".$username."'");

$namecount = (int) $row[0]['_count'];

if($namecount>0) {
    echo json_encode(array("msg" => "이미 존재하는 아이디입니다."));
} else {
    $row = $db->db_insert("users", "name, pass", "'".$username."','".$password."'");
    echo json_encode(array("msg" => "회원가입 완료. 로그인해주세요!"));
}
?>
```

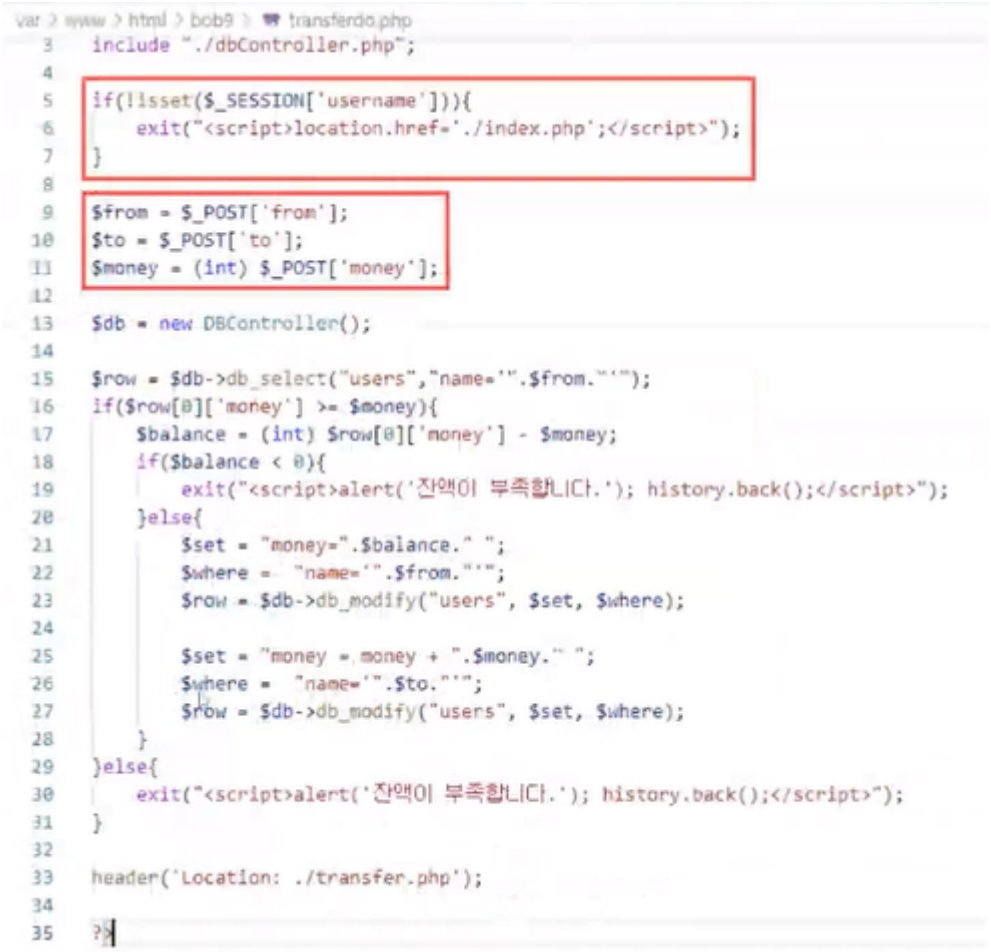
- 회원가입 기능에서 쿼리문 참거짓 판별 가능

테스트 구문

username=1'or(database())='starbank'#

3. 송금하기 (from 값 검증)

소스코드



- from 값 (송금하는 사람) 검증이 없음

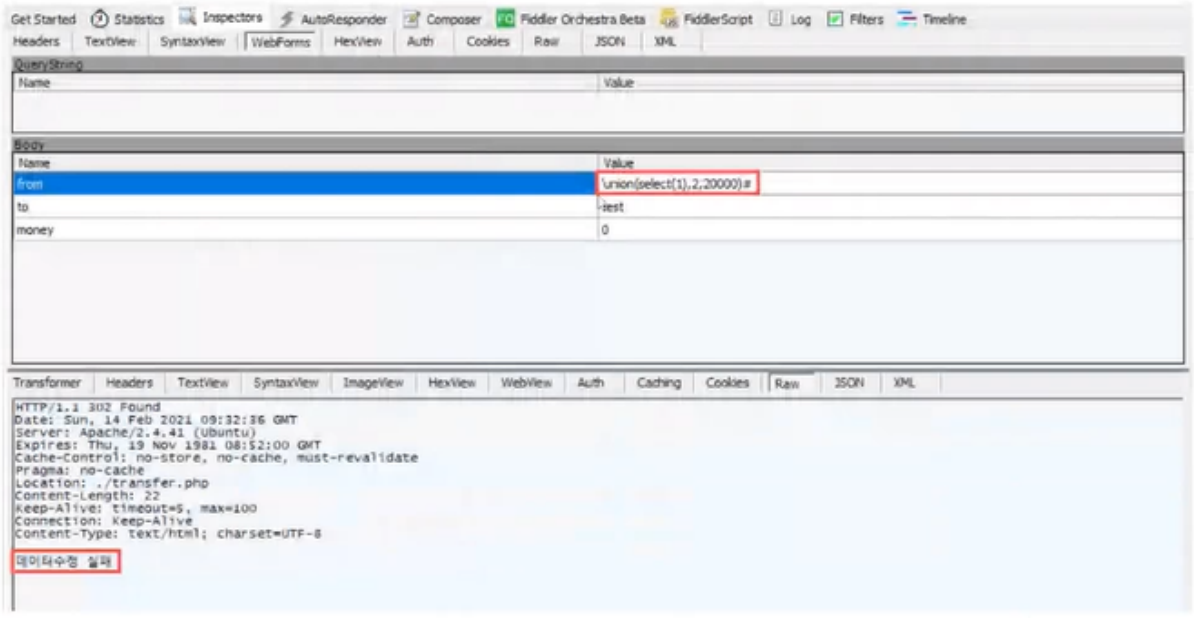
4. 송금하기 (음수 값 체크)

소스코드

```php
include "./dbController.php";

if(!isset($_SESSION['username'])){
    exit("<script>location.href='./index.php';</script>");
}

$from = $_POST['from'];
$to = $_POST['to'];
$money = (int) $_POST['money'];

$db = new DBController();

$row = $db->db_select("users","name='".$from."'");
if($row[0]['money'] >= $money){
    $balance = (int) $row[0]['money'] - $money;
    if($balance < 0){
        exit("<script>alert('잔액이 부족합니다.'); history.back();</script>");
    }else{
        $set = "money=".$balance." ";
        $where = "name='".$from."'";
        $row = $db->db_modify("users", $set, $where);

        $set = "money = money + ".$money." ";
        $where = "name='".$to."'";
        $row = $db->db_modify("users", $set, $where);
    }
}else{
    exit("<script>alert('잔액이 부족합니다.'); history.back();</script>");
}
```

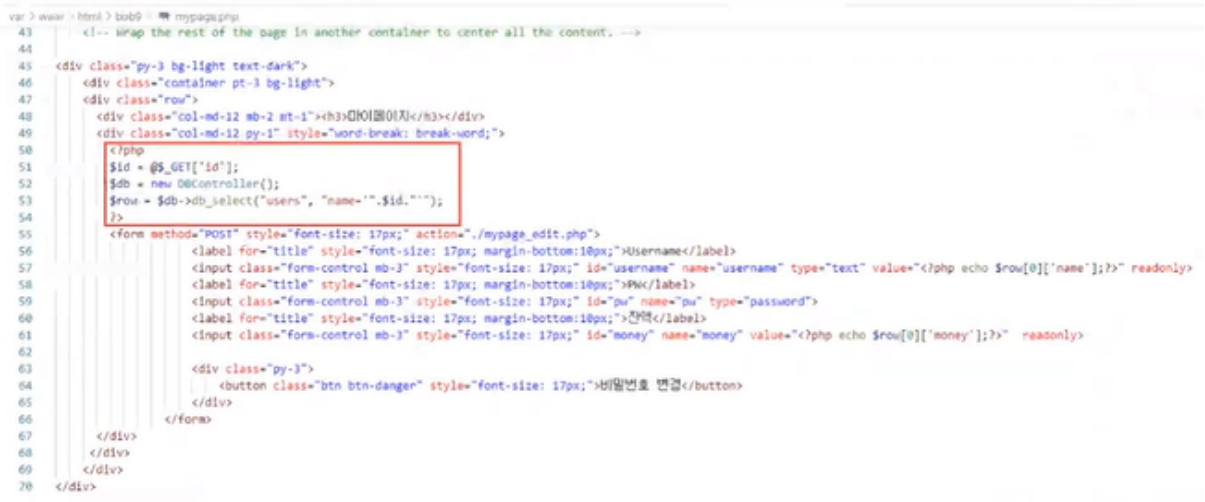
- money 에 음수 값 입력이 가능

5. 송금하기 (Blind SQL Injection)



- from 에서 Blind SQL 인젝션 발생 가능

6. 마이페이지 (SQL Injection)



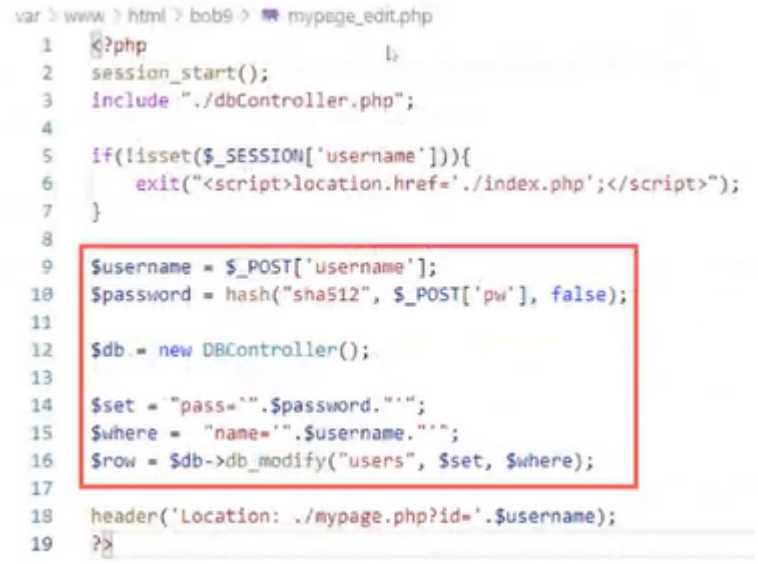
```
var > www > html > bob9 > mypage.php
43    <!-- Wrap the rest of the page in another container to center all the content. -->
44
45  <div class="py-3 bg-light text-dark">
46    <div class="container pt-3 bg-light">
47    <div class="row">
48      <div class="col-md-12 mb-2 mt-1"><h3>마이페이지</h3></div>
49      <div class="col-md-12 py-1" style="word-break: break-word;">
50        <?php
51        $id = @$_GET['id'];
52        $db = new DBController();
53        $row = $db->db_select("users", "name='".$id."'");
54        ?>
55        <form method="POST" style="font-size: 17px;" action="./mypage_edit.php">
56                <label for="title" style="font-size: 17px; margin-bottom:10px;">Username</label>
57                <input class="form-control mb-3" style="font-size: 17px;" id="username" name="username" type="text" value="<?php echo $row[0]['name'];?>" readonly>
58                <label for="title" style="font-size: 17px; margin-bottom:10px;">PW</label>
59                <input class="form-control mb-3" style="font-size: 17px;" id="pw" name="pw" type="password">
60                <label for="title" style="font-size: 17px; margin-bottom:10px;">잔액</label>
61                <input class="form-control mb-3" style="font-size: 17px;" id="money" name="money" value="<?php echo $row[0]['money'];?>"  readonly>
62
63                <div class="py-3">
64                    <button class="btn btn-danger" style="font-size: 17px;">비밀번호 변경</button>
65                </div>
66            </form>
67    </div>
68    </div>
69    </div>
70  </div>
```

- 마이페이지의 id 값에서 SQLi 발생

테스트 구문

id=222%27union(select(database()),2,user())%23

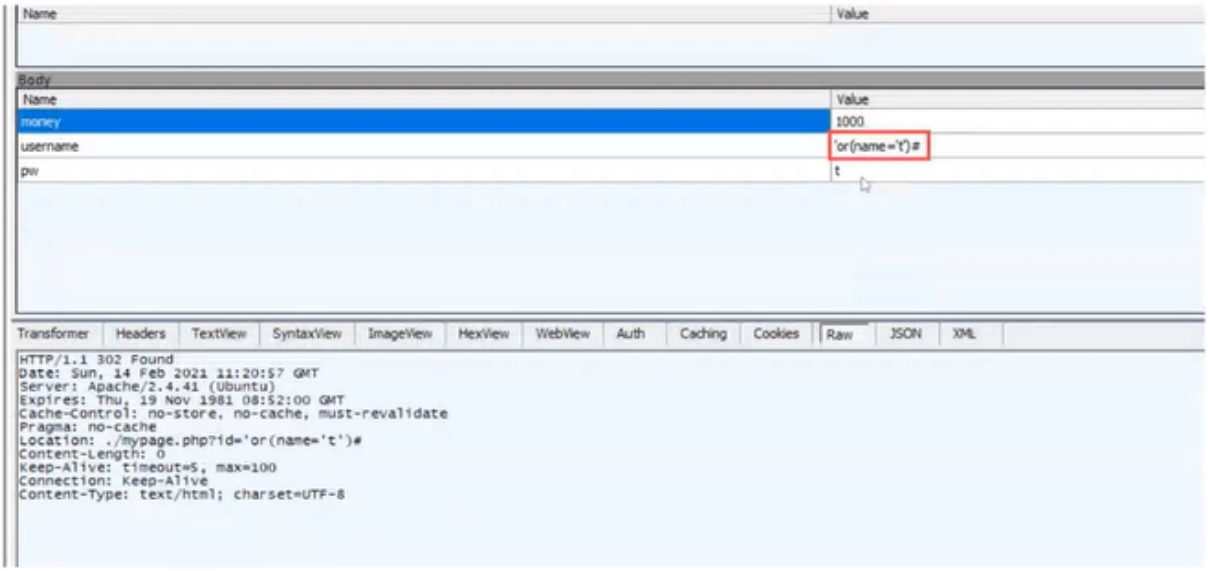
7. mypage_edit (타 회원 정보 수정)



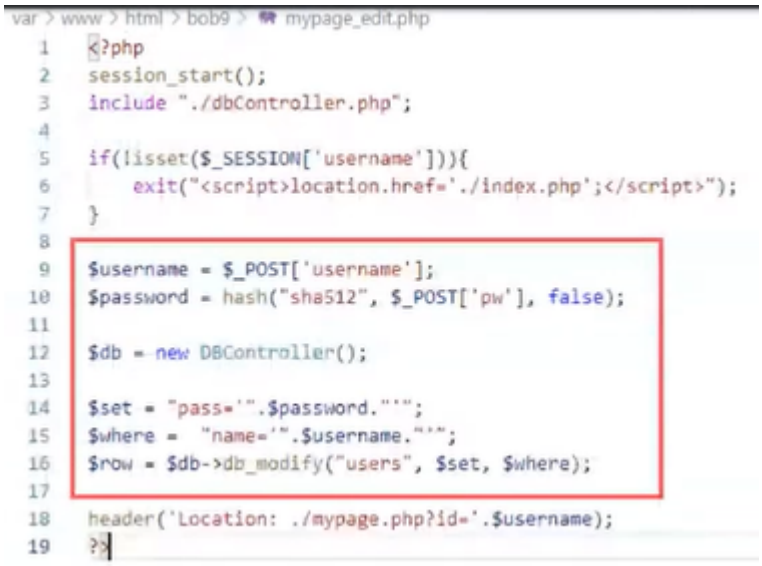
```
var > www > html > bob9 > mypage_edit.php
1   <?php
2   session_start();
3   include "./dbController.php";
4
5   if(!isset($_SESSION['username'])){
6       exit("<script>location.href='./index.php';</script>");
7   }
8
9   $username = $_POST['username'];
10  $password = hash("sha512", $_POST['pw'], false);
11
12  $db = new DBController();
13
14  $set = "pass='".$password."'";
15  $where =  "name='".$username."'";
16  $row = $db->db_modify("users", $set, $where);
17
18  header('Location: ./mypage.php?id='.$username);
19  ?>
```

- id 파라미터 변조 후 비밀번호 검증

8. mypage_edit (SQL Injection)



소스코드



- 마이페이지에서 타 회원 비밀번호 변경

username='or(name='t')#

pw=t(변경할 비밀번호)

$where="name'or(name='t')#"

9. 1:1 문의 게시판 (SQL Injection)

소스코드

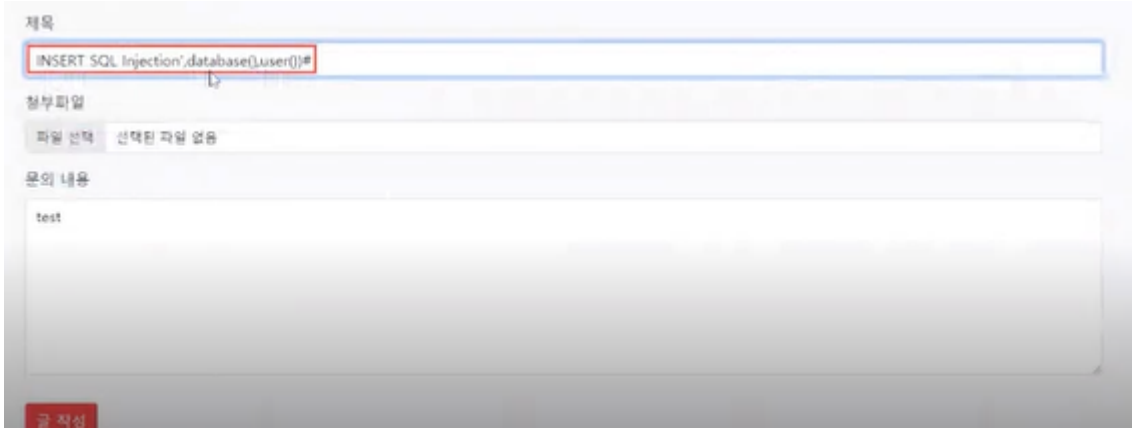
```
var > www > html > bob8 > board_read.php
35          </a>
36        </div>
37
38
39        <!-- Marketing messaging and featurettes
40        ================================================== -->
41        <!-- Wrap the rest of the page in another container to center all the content. -->
42  <?php
43      $no = $_GET['no'];
44      $db = new DBController();
45      $row = $db->db_select("board", "name='".$_SESSION['username']."' and no=".$no);
46      foreach ($row as $table) {
47          $title = $table['title'];
48          $date = $table['write_time'];
49          $contents = $table['contents'];
50          $upload_file_name = $table['upload_file_name'];
51          $comments = $table['comments'];
52      }
53      if(!isset($upload_file_name)){
54          $upload_file_name = "없음";
55      }else { }
56  ?>
```

- no 파라미터에서 SQLi 가능

테스트 구문

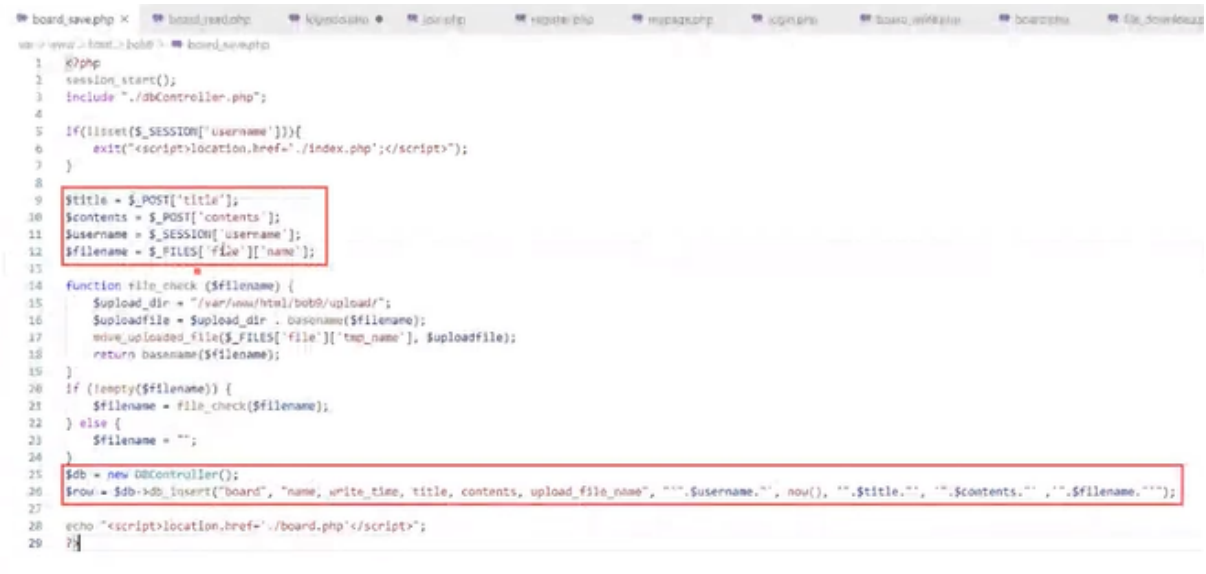
no=(-1)union(select(1),2,3,database(),user(),6,7)#

10. 1:1 문의 게시판 (글 작성 Insert SQL Injection)



- 디비 이름은 게시글 내용에, user는 첨부파일에 보여짐

소스코드



```php
<?php
session_start();
include "./dbController.php";

if(!isset($_SESSION['username'])){
    exit("<script>location.href='./index.php';</script>");
}

$title = $_POST['title'];
$contents = $_POST['contents'];
$username = $_SESSION['username'];
$filename = $_FILES['file']['name'];

function file_check ($filename) {
    $upload_dir = "/var/www/html/bob9/upload/";
    $uploadfile = $upload_dir . basename($filename);
    move_uploaded_file($_FILES['file']['tmp_name'], $uploadfile);
    return basename($filename);
}
if (!empty($filename)) {
    $filename = file_check($filename);
} else {
    $filename = "";
}
$db = new DBController();
$row = $db->db_insert("board", "name, write_time, title, contents, upload_file_name", "'".$username."', now(), '".$title."', '".$contents."' ,'".$filename."'");

echo "<script>location.href='./board.php'</script>";
?>
```

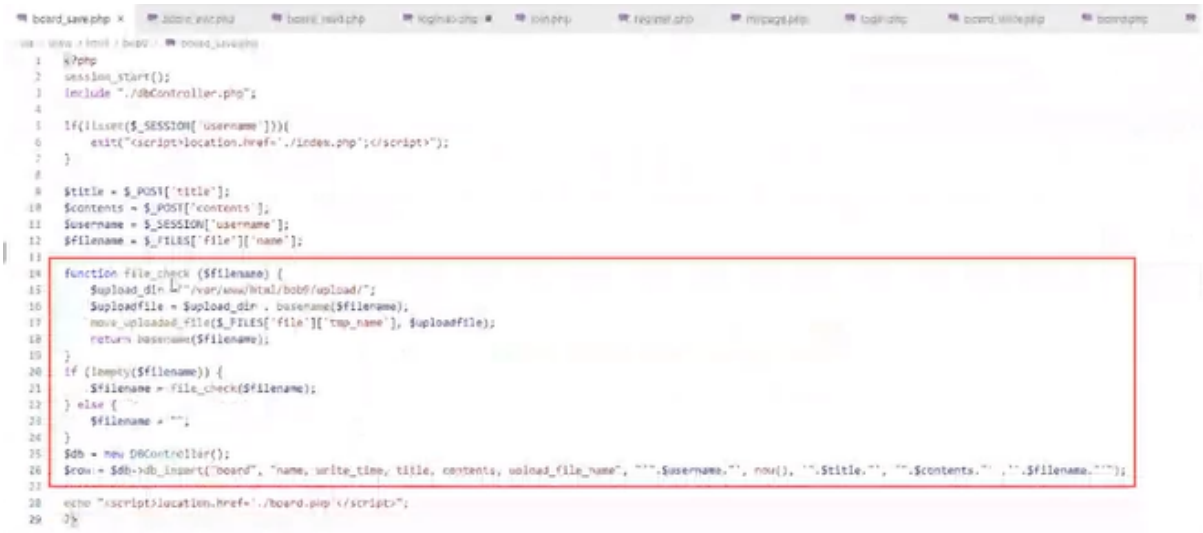
테스트 구문

INSERT SQL Injection',database(),user())#

11. 1:1 문의 게시판 (File upload)

- php 확장자 필터링 안함
    - <?php var_dump(scandir"../")); ?> 등 웹쉘 업로드 가능

소스코드



```php
<?php
session_start();
include "./dbController.php";

if(!isset($_SESSION['username'])){
    exit("<script>location.href='./index.php';</script>");
}

$title = $_POST['title'];
$contents = $_POST['contents'];
$username = $_SESSION['username'];
$filename = $_FILES['file']['name'];

function file_check ($filename) {
    $upload_dir = "/var/www/html/bob0/upload/";
    $uploadfile = $upload_dir . basename($filename);
    move_uploaded_file($_FILES['file']['tmp_name'], $uploadfile);
    return basename($filename);
}
if (!empty($filename)) {
    $filename = file_check($filename);
} else {
    $filename = "";
}
$db = new DBController();
$row = $db->db_insert("board", "name, write_time, title, contents, upload_file_name", "'".$username."', now(), '".$title."', '".$contents."' ,'".$filename."'");

echo "<script>location.href='./board.php'</script>";
?>
```

12. 1:1 문의 게시판 (글 수정 SQL Injection)

- 타인의 글 수정

13. 1:1 문의 게시판 (글 삭제 SQL Injection)

- 타인의 글 삭제

14. 1:1 문의 게시판 (파일 다운로드)

소스코드

transferoo.php | file_download.php × | logindo.php | register.php

var > www > html > bob9 > file_download.php

```php
<?php
session_start();
if(!isset($_SESSION['username'])){
    exit("<script>location.href='./index.php';</script>");
}

$file_name = $_GET['name'];
$file = "./upload/".$file_name;

header('Content-type: application/octet-stream');
header('Content-Disposition: attachment; filename="' . $file_name . '"');
header('Content-Transfer-Encoding: binary');
header('Content-length: ' . filesize($file));
header('Expires: 0');
header("Pragma: public");

$fp = fopen($file, 'rb');
fpassthru($fp);
fclose($fp);

?>
```