컴퓨터보안 실습

7주차

워게임 / Webhacking.kr
문제 39번 SQL

실습 내용

- SQL 실습 이론 소개
- 실습 사이트 소개
- 39번 문제 확인
- 39번 문제 풀이
- Q & A

SQL 실습 이론 소개

1) 첫번째 조회되는 사용자로 로그인하는 **SQL injection**

ID : ' or 1=1--
PW : abcd

select * from member where id='' or 1=1--' and pwd='abcd'
=> select * from member where id='' or 1=1
=> select * from member
=> 가장 먼저 조회되는 사용자로 로그인됨

-- : 주석처리 **(MS-SQL)**
: 주석처리 **(MySQL)**

SQL 실습 이론 소개

2) 특정 사용자로 로그인하는 방법

select * from member where id='사용자입력값**' and pwd='**사용자입력값**'**

ID : victim'--
PW : ?

select * from member where id='victim'-- and pwd='?'
=> select * from member where id='victim'

SQL 실습 이론 소개

Error Based SQL Injection
=> 에러 메시지를 통해 **DB**의 정보를 파악한다**.**

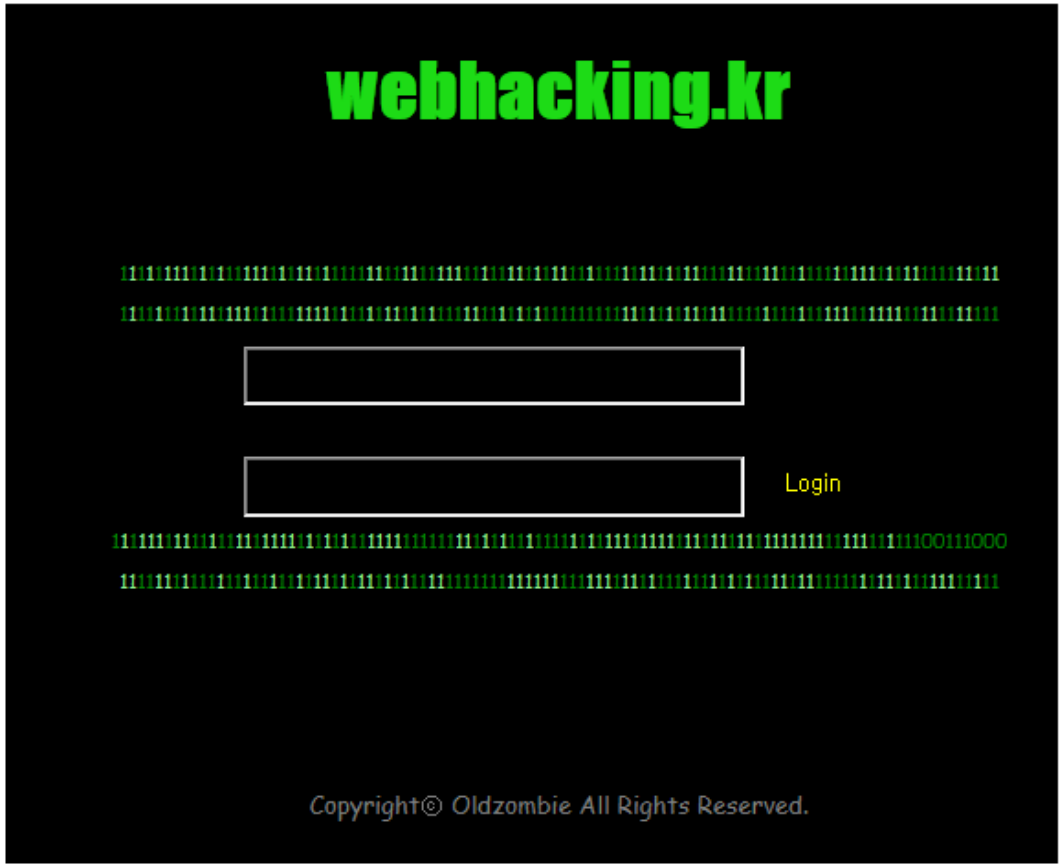
' having 1=1--

로그인 창의 **ID**에 입력 후 제출

member.m_idx 필드명 획득
=> 회원정보가 들어있는 테이블명 **: member**
=> m_idx 필드의 존재여부 확인
' group by memeber.m_idx--
member.m_id 필드명 획득
' group by member.m_idx, member.m_id--
member.m_name 필드명 획득
' group by member.m_idx, member.m_id, member.m_name--

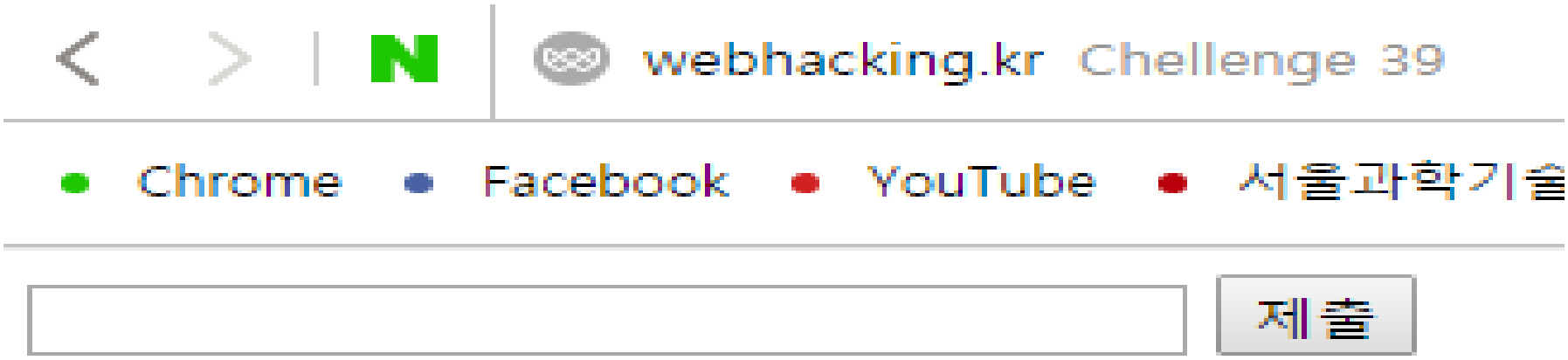
실습 사이트 소개

Webhacking.kr (http://webhacking.kr/)



39번 문제 확인

- 웹해킹 문제 중에 보너스 문제 **(100점)**
- **39**번 문제 사이트 = **http://webhacking.kr/challenge/bonus/bonus-10/**



39번 문제 풀이

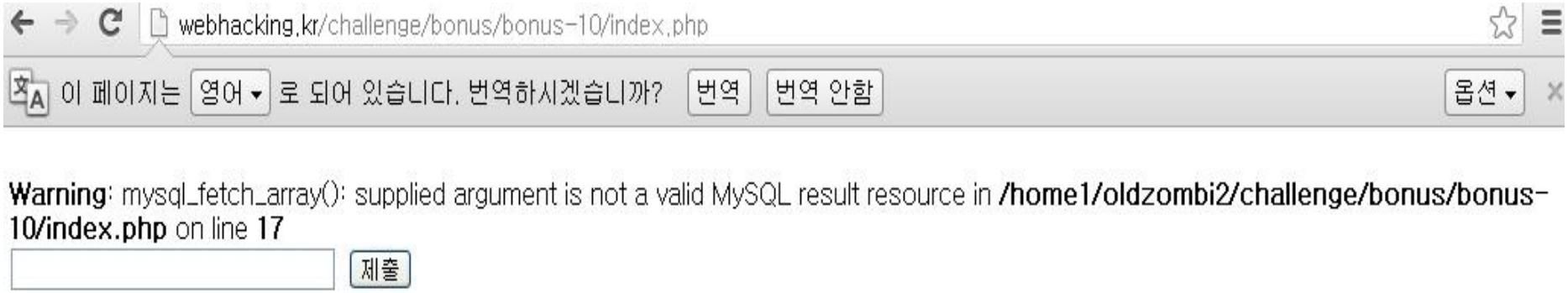
- **소스코드 확인**
- ‘무엇을 해킹하는 문제일까?’고민
- 소스코드 확인(F12)
- 페이지 소스 코드 분석
- 보너스 문제페이지에서 index.phps url 추가

```
1  <html>
2  <head>
3  <title>Chellenge 39</title>
4  </head>
5  <body>
6  <!-- index.phps -->
7
8
9  <form method=post action=index.php>
10 <input type=text name=id maxlength=15 size=30>
11 <input type=submit>
12 </form>
13 </body>
14 </html>
15
16
```

- **소스코드 확인**
- index.phps 을 입력한 소스이다.
- $_POST[id]는 0~15 글자이다.
- \\ 역슬래쉬는 "" 없어지는 것이고, '(싱클쿼터) 는 "(더블쿼터)로 바뀜

  * substr 은 지정된 문자열에서 지정한 부분만 들고 오는 것을 말함

```
<html>
<head>
<title>Chellenge 39</title>
</head>
<body>

<?

$pw="????";

if($_POST[id])
{
$_POST[id]=str_replace("₩₩","",$_POST[id]);
$_POST[id]=str_replace("'","''",$_POST[id]);
$_POST[id]=substr($_POST[id],0,15);
$q=mysql_fetch_array(mysql_query("select 'good' from zmail_member where id='$_POST[id]'"));

if($q[0]=="good") @solve();

}

?>

<form method=post action=index.php>
<input type=text name=id maxlength=15 size=30>
<input type=submit>
</form>
</body>
</html>
```



- 무작위로 글자를 적고 제출하게 되면 위와 같은 오류 발생

- $q=mysql_fetch_array(mysql_query("select 'good' from zmail_member where id='$_POST[id]")); 부분에서 잘보면 id='$_POST[id]에 '(싱글쿼터) 부분이 닫혀있지 않아 오류가 발생하는 부분이 확인가능함

- 위와 같이 입력하거나 15글자에 맞춰 끝에만 ‘ 를 넣어주면 문제 해결 완료

- kor_moon@naver.com 메일 전송
- 화면 캡처하여 **2017날짜_이름(컴퓨터보안).jpg** 형식으로 보내면 완료

Q & A

참고 문헌 :