NETWORK SECURITY

한양대학교 소프트웨어융합대학 소프트웨어학부
이연준 교수

주요 사항

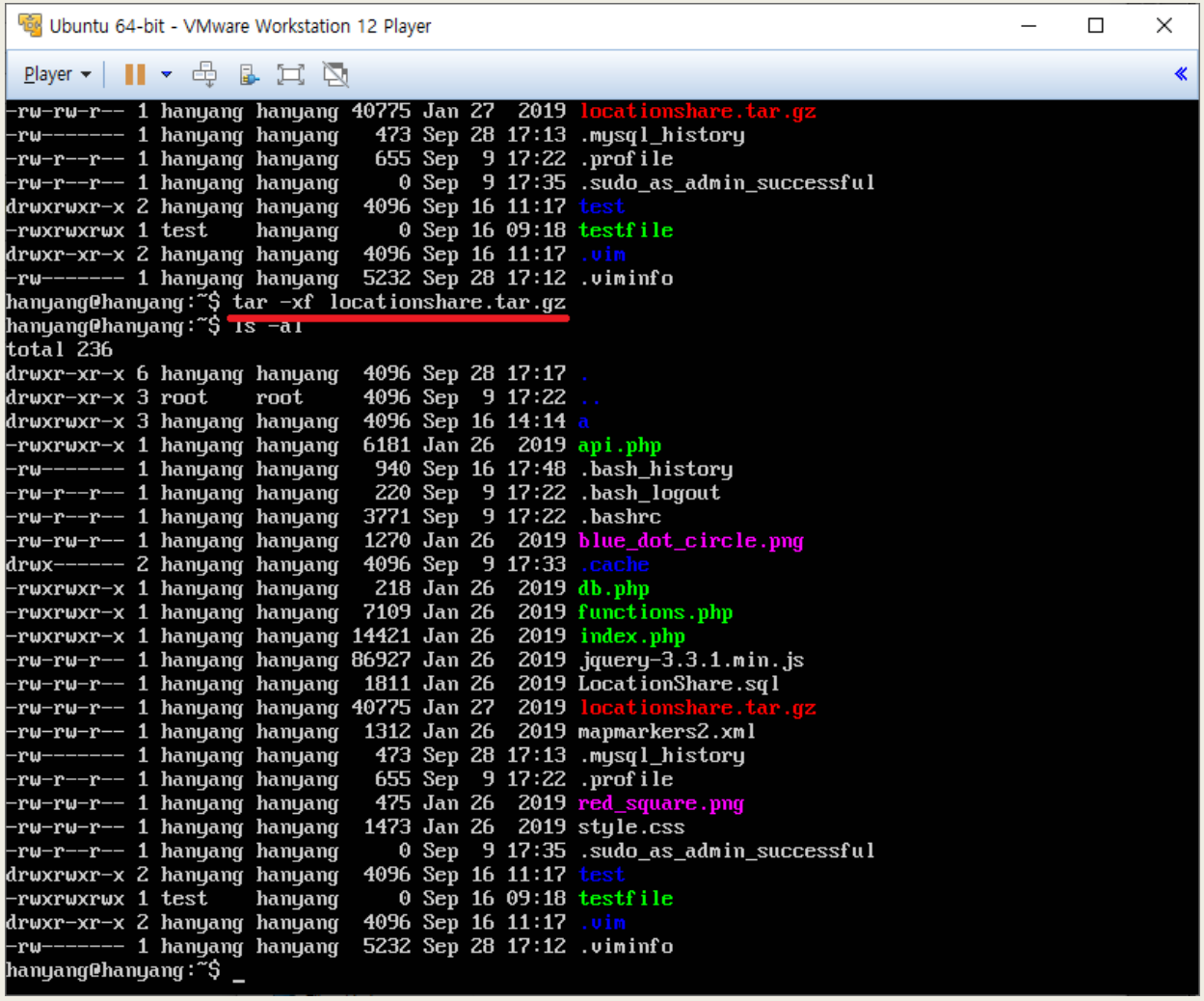
- **SQL Injection**에 대한 이해
- **Lab Preparation**
  - Database 생성 및 SQL Injection 실습 환경 구성 준비
- **Lab Task**
  - SQL Injection 실습
- **Lab Question**
- **Evaluation**

LAB PREPARATION

실습 환경 구성 준비

- 실습에 사용할 **Web App** 다운
- **wget** http://seclab.soic.indiana.edu/B433-S19/files/locationshare.tar.gz
- 압축을 풀어 파일 내용을 확인

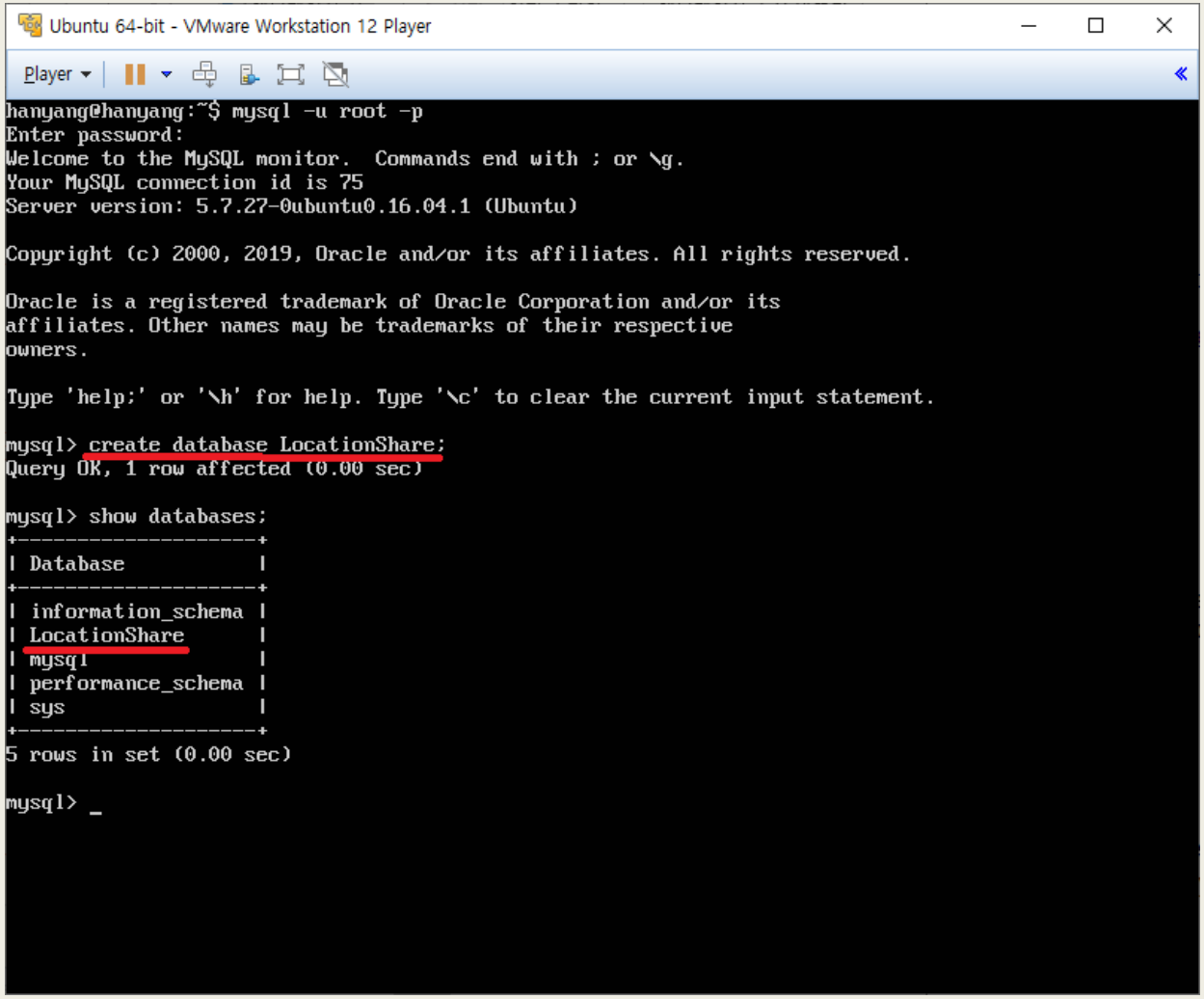
실습 환경 구성 준비


Ubuntu 64-bit - VMware Workstation 12 Player
Player
-rw-rw-r-- 1 hanyang hanyang 40775 Jan 27 2019 locationshare.tar.gz
-rw------- 1 hanyang hanyang 473 Sep 28 17:13 .mysql_history
-rw-r--r-- 1 hanyang hanyang 655 Sep 9 17:22 .profile
-rw-r--r-- 1 hanyang hanyang 0 Sep 9 17:35 .sudo_as_admin_successful
drwxrwxr-x 2 hanyang hanyang 4096 Sep 16 11:17 test
-rwxrwxrwx 1 test hanyang 0 Sep 16 09:18 testfile
drwxr-xr-x 2 hanyang hanyang 4096 Sep 16 11:17 .vim
-rw------- 1 hanyang hanyang 5232 Sep 28 17:12 .viminfo
hanyang@hanyang:~$ tar -xf locationshare.tar.gz
hanyang@hanyang:~$ ls -al
total 236
drwxr-xr-x 6 hanyang hanyang 4096 Sep 28 17:17 .
drwxr-xr-x 3 root root 4096 Sep 9 17:22 ..
drwxrwxr-x 3 hanyang hanyang 4096 Sep 16 14:14 a
-rwxrwxr-x 1 hanyang hanyang 6181 Jan 26 2019 api.php
-rw------- 1 hanyang hanyang 940 Sep 16 17:48 .bash_history
-rw-r--r-- 1 hanyang hanyang 220 Sep 9 17:22 .bash_logout
-rw-r--r-- 1 hanyang hanyang 3771 Sep 9 17:22 .bashrc
-rw-rw-r-- 1 hanyang hanyang 1270 Jan 26 2019 blue_dot_circle.png
drwx------ 2 hanyang hanyang 4096 Sep 9 17:33 .cache
-rwxrwxr-x 1 hanyang hanyang 218 Jan 26 2019 db.php
-rwxrwxr-x 1 hanyang hanyang 7109 Jan 26 2019 functions.php
-rwxrwxr-x 1 hanyang hanyang 14421 Jan 26 2019 index.php
-rw-rw-r-- 1 hanyang hanyang 86927 Jan 26 2019 jquery-3.3.1.min.js
-rw-rw-r-- 1 hanyang hanyang 1811 Jan 26 2019 LocationShare.sql
-rw-rw-r-- 1 hanyang hanyang 40775 Jan 27 2019 locationshare.tar.gz
-rw-rw-r-- 1 hanyang hanyang 1312 Jan 26 2019 mapmarkers2.xml
-rw------- 1 hanyang hanyang 473 Sep 28 17:13 .mysql_history
-rw-r--r-- 1 hanyang hanyang 655 Sep 9 17:22 .profile
-rw-rw-r-- 1 hanyang hanyang 475 Jan 26 2019 red_square.png
-rw-rw-r-- 1 hanyang hanyang 1473 Jan 26 2019 style.css
-rw-r--r-- 1 hanyang hanyang 0 Sep 9 17:35 .sudo_as_admin_successful
drwxrwxr-x 2 hanyang hanyang 4096 Sep 16 11:17 test
-rwxrwxrwx 1 test hanyang 0 Sep 16 09:18 testfile
drwxr-xr-x 2 hanyang hanyang 4096 Sep 16 11:17 .vim
-rw------- 1 hanyang hanyang 5232 Sep 28 17:12 .viminfo
hanyang@hanyang:~$

실습 환경 구성 준비

- **mysql –u root –p**
- 패스워드는 기존에 등록했던 패스워드 입력
- **create database LocationShare;**
- **show databases;**

실습 환경 구성 준비


Ubuntu 64-bit - VMware Workstation 12 Player
Player
hanyang@hanyang:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 75
Server version: 5.7.27-0ubuntu0.16.04.1 (Ubuntu)
Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> create database LocationShare;
Query OK, 1 row affected (0.00 sec)
mysql> show databases;
+--------------------+
| Database |
+--------------------+
| information_schema |
| LocationShare |
| mysql |
| performance_schema |
| sys |
+--------------------+
5 rows in set (0.00 sec)
mysql> _

실습 환경 구성 준비

- **SQL** 파일을 통해 **DB**에 **import**
- **mysql –u root LocationShare –p < /home/**본인계정**/LocationShare.sql**

LAB TASK

Web App Setup

- Import한 SQL을 통해 DB와 Table이 제대로 입력됐는지 확인
- root로 mysql 접속
- show databases;
- use LocationShare;
- show tables;

Web App Setup

- 다운 받았던 **tar** 파일을 압축을 풀 것
- **cd /var/www/html**
- **sudo mkdir locationshare**
- **sudo cp /home/(본인계정directory)/locationshare.tar.gz /var/www/html/locationshare**
- **cd locationshare**
- **sudo tar -xf locationshare.tar.gz**
- 이후 **Web Browser**에서 **http://(본인IP)/locationshare**로 접속하여 작동이 잘 되는지 확인

Web App Setup

- **Web App**과 **DB** 연동을 위해 다음의 파일을 수정할 것
- **/var/www/html/locationshare/db.php**
- 해당 과정을 완료한 후 계정을 생성하여 로그인 할 것.

Create a New Table

- **SQL**문을 통해 새로운 테이블을 만들 것
- 생성할 테이블 요구 조건은 다음과 같음
- 테이블 명 : messages

Attribute Name	Data type & Option
messasgeid	BIGINT, Auto-Increment, Primary Key
senderuserid	NOT NULL
receiveruserid	NOT NULL
timesent	TIMESTAMP, NOT NULL
messagetext	LONGTEXT, NOT NULL
isread	BOOLEAN, NOT NULL

- **senderuserid**와 **receiveruserid** 데이터 타입은 동일할 것
- 테이블 생성 후 테이블의 구조를 캡처할 것

SQL Injection 취약점 찾기

- 해당 **Web App**은 **SQL Injection**에 대한 대비가 되어있지 않으므로 암호를 입력하지 않고 로그인하는 것이 가능함.
- 암호를 입력하지 않고 로그인 하는 방법을 찾아내어 해당 방법을 기술하고 왜 성공했는지에 대한 이유를 이후 제시하는 **Lab Question**에서 기술할 것.
- 다양한 해법이 존재하므로 **Injection** 방법은 취사선택할 것.

SQL Injection 취약점 찾기 (심화)

- 실제로 공격자는 **DB**의 **Schema**를 알고 있는 경우가 거의 없음
- http://seclab.soic.indiana.edu/B433-S19/sqlinj/index.php
- 해당 링크에 접속하여 **SQL Injection**을 수행할 것
- 최종 결과는 본인의 **e-mail** 주소로 메일이 올 수 있도록 할 것
- **Group NO**는 본인의 학번을 기입할 것

SQL Injection 취약점 찾기 (심화)

- **Hint**
  - http://www.unixwiz.net/techtips/sql-injection.html
  - 해당 링크를 참고하여 해결할 것
  - **Injection**을 수행하면서 볼 수 있는 세 가지 결과
  - **"That email address could not be located"**
    - **Query**는 정상 동작하였으나 **email address**를 찾지 못한 것
  - **"The server encountered an error trying to process your request"**
    - **Back-End**에서 처리하지 못해 오류를 발생
    - 주로 **Query** 문법 오류
  - **"Email sent to ..."**
    - **E-mail**이 정상적으로 보내진 것

LAB QUESTION

Lab Question

1. [SQL Injection 취약점 찾기]에서 어떤 문자열을 입력하여 해결했는지 기술하세요. 그리고 왜 가능했는지에 대해 이유를 서술하세요.
2. [SQL Injection 취약점 찾기(심화)]에서 어떤 문자열을 입력하여 해결했는지 기술하세요. 그리고 간략하게 공격을 진행했던 과정을 서술하세요.

※ 현재 사용하는 DBMS는 MySQL이라고 가정하고 다음의 질문들에 답하세요.

3. 1개의 테이블이 가질 수 있는 Primary Key와 Foreign Key는 총 몇 개입니까?

Lab Question

4. 1개의 테이블이 가질 수 있는 **Primary Key**와 **Foreign Key**는 총 몇 개입니까?

5. 다음은 버스 운행과 관련된 테이블입니다.

Driver-ID	Bus-ID	Route-ID	Start-Time	Stop-Time
44	67	6	2019/10/01-14:00:00	2019/10/01-22:00:00
44	62	6	2019/10/02-12:00:00	2019/10/02-16:00:00
54	63	9	2019/10/01-16:00:00	2019/10/01-21:00:00
54	63	8	2019/10/02-09:00:00	2019/10/02-17:00:00

Primary Key로 가장 적합한 필드 또는 필드 조합은 무엇인지, 왜 그런지에 대해서 설명하세요.

Lab Question

6.다음은 어느 산악회의 테이블 구조입니다.

Climber-ID	Name	Skill Level	Age
123	Edmund	Experienced	80
214	Arnold	Beginner	25
313	Bridgett	Experienced	33
212	James	Medium	27

Primary Key가 **Climber-ID**라고 했을 때, 다음 각 행들을 테이블에 추가할 수 있는지에 대한 여부를 설명하세요.

Climber-ID	Name	Skill Level	Age
214	Abbot	Medium	40
	John	Experienced	19
15	Jeff	Medium	42

Evaluation

- **Lab Task** 진행
  - **Web App** 설치 후 **Web Browser**에서 실행 여부 확인
    - 계정 생성 및 로그인까지
  - **DB** 테이블 생성 확인
    - **show tables, desc messages**
  - **SQL Injection** 취약점 찾기 및 심화까지 완료
    - **Injection** 심화 완료 후 **E-mail** 캡처
- **Lab Question**
  - 주어진 문항에 대한 답과 해결 방안에 대해 간략하게 서술
- **Lab Task** 수행 결과를 위와 같이 명시한 대로 캡처하여 **MS Word** 또는 **PDF** 파일로 결과를 제출할 것.

Evaluation

- 과제 제출 기한 : 2019/10/07 23:59
- 과제 제출 시 메일 제목은 ‘본인 이름_학번’으로 제출
  - 예) 이석원_2019101059
- sevenshards00@gmail.com으로 보낼 것.

Q&A