DB 암호화(2)

양유진

한성대학교 HANSUNG UNIVERSITY

유튜브 주소: https://youtu.be/VJzIE0GQ53M

CryptoCraft LAB
https://crypto.modoo.at

Contents

CryptoCraft LAB

실험환경

Vmware Workwtation15 player

Ubuntu 20.04.2.0

VMware 설치 방법

https://it4us.tistory.com/8

Ubuntu 설치 방법

https://m.blog.naver.com/ksseo63/222031982720

기본설정

1) MySQL 설치하기

: https://m.blog.naver.com/jesang1/221993846056

- 'Could not get lock /var/lib/dpkg/lock-frontend' 에러 발생시 해결방법

: https://stricky.tistory.com/181

- MySQL 비밀번호 변경 관련

: https://joonyon.tistory.com/91

- MySQL 권한 설정 관련

: https://url.kr/ythmnu

2) gcc 설치하기

: https://url.kr/8gzq61

3) mysql.h 사용

: https://judynewyork.tistory.com/477

4) [옵션]Vim 설치하기

: https://soobarkbar.tistory.com/219

C언어로 MySQL 사용하기 (1) - 연결초기화&접속 핸들 생성

```c
#include <mysql/mysql.h>
#include <string.h>
#include <stdio.h>
#include <stdlib.h>
#include <time.h>

#define DB_HOST "127.0.0.1"
#define DB_USER "root"
#define DB_PASS
#define DB_NAME "PIPODB"
#define DB_TABLE "TEST"
```

```c
int main()
{
        MYSQL *conn = mysql_init(NULL);
        Set_Connection(conn);
```

접속 핸들 생성

연결초기화

```c
void Set_Connection(MYSQL *conn)
{
        if( conn == NULL )
        {
                fprintf(stderr, "%s\n", mysql_error(conn));
                exit(1);
        }

        if (mysql_real_connect(conn, DB_HOST, DB_USER, DB_PASS, NULL, 0, NULL, 0) == NULL )
        {
                fprintf(stderr, "%s\n", mysql_error(conn));
                exit(1);
        }
}
```

C언어로 MySQL 사용하기 (2) - DB/Table 생성

`char query[255];` query 문장을 담는 역할

sprintf(문장을 담고 싶은 변수, “%s”, string)
출력값을 문자열 변수에 저장해주는 함수

mysql_query(연결 핸들러, query문)
: SQL 문장을 실행하는 함수

```
void Create_DB(MYSQL *conn)
{
        sprintf(query, "CREATE DATABASE if not exists %s", DB_NAME);
        if ( mysql_query(conn, query) )
        {
                printError(conn);
        }
}
void Create_Table(MYSQL *conn)
{
        mysql_query(conn, "USE PIPODB");
        sprintf(query, "CREATE TABLE if not exists %s(ID varchar(%d), PW varchar(%d))", DB_TABLE, 20, 300);
        if ( mysql_query(conn, query) )
        {
                printError(conn);
        }
}
```

C언어로 MySQL 사용하기 (3) - 데이터 삽입

(main 함수)

```
Insert_Data(conn);
```

데이터 삽입 함수

```
void Insert_Data(MYSQL *conn)
{
        mysql_query(conn, "USE PIPODB");
        if (mysql_query(conn, "INSERT INTO TEST VALUES ('Mr. Kim', 'password1')") )
{
                printError(conn);
        }
}
```

```
mysql> SELECT * FROM TEST;
+---------+-----------+
| ID      | PW        |
+---------+-----------+
| Mr. Kim | password1 |
+---------+-----------+
1 row in set (0.00 sec)
```

C언어로 MySQL 사용하기 (4) - AES256(CBC방식) 암호문 삽입

(main 함수)

```
const char *plaintext = "Plaintext!!";
const char *key = "1234";

Insert_EncData(conn, plaintext, key);

mysql_close(conn);
exit(0);
```

```
void Insert_EncData(MYSQL *conn, const char* plaintext, const char* key)
{
        srand((unsigned int)time(NULL));
        int iv = rand()%10000+1;

        mysql_query(conn, "USE PIPODB");

        sprintf(query, "SET @iv = %d", iv);
        mysql_query(conn, query); //initial vector

        sprintf(query, "SET @key_str = SHA2(%s, 256)", key);
        mysql_query(conn, query);

        sprintf(query, "INSERT INTO %s VALUES('%s', HEX(AES_ENCRYPT('%s', @key_str, @iv)))", DB_TABLE, "id03", plaintext);
        if ( mysql_query(conn, query) )
        {
                printError(conn);
        }
```

srand(seed)

: seed값에 따라 rand()값 바꿔주는 함수

rand()

: 난수 생성해주는 함수 (srand()에 의존적)

C언어로 MySQL 사용하기 (4) - AES256(CBC방식) 암호문 삽입

(main 함수)

```c
const char *plaintext = "Plaintext!!";
const char *key = "1234";

Insert_EncData(conn, plaintext, key);

mysql_close(conn);
exit(0);
```

```c
void Insert_EncData(MYSQL *conn, const char* plaintext, const char* key)
{
        srand((unsigned int)time(NULL));
        int iv = rand()%10000+1;

        mysql_query(conn, "USE PIPODB");

        sprintf(query, "SET @iv = %d", iv);
        mysql_query(conn, query); //initial vector

        sprintf(query, "SET @key_str = SHA2(%s, 256)", key);
        mysql_query(conn, query);

        sprintf(query, "INSERT INTO %s VALUES('%s', HEX(AES_ENCRYPT('%s', @key_str, @iv)))", DB_TABLE, "id03", plaintext);
        if ( mysql_query(conn, query) )
        {
                printError(conn);
        }
```

SHA2()를 사용하여 key값 단방향 암호화

C언어로 MySQL 사용하기 (5) - AES256(CBC방식) 복호화&출력

2진수 → 문자

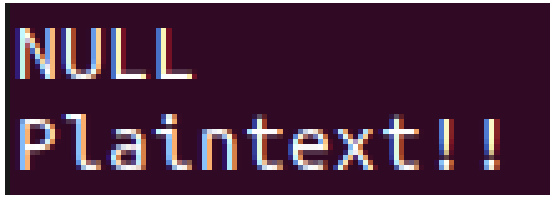
```
sprintf(query, "SELECT CAST(AES_DECRYPT(UNHEX(PW), @key_str, @iv) AS CHAR(127) CHARACTER SET UTF8) FROM %s", DB_TABLE);
mysql_query(conn, query);

//출력
MYSQL_RES *result = mysql_store_result(conn); 결과셋 가져오기
if ( result == NULL ) { printError(conn); }

int num_fields = mysql_num_fields(result); 필드(열)개수
MYSQL_ROW row;
while ( row = mysql_fetch_row(result) ) 행 개수
{
        for( int i = 0; i<num_fields; i++)
                printf("%s ", row[i] ? row[i] : "NULL"); 데이터 없으면 NULL 출력
        printf("\n");
}
mysql_free_result(result);
```

C언어로 MySQL 사용하기 (5) - AES256(CBC방식) 복호화&출력

mysql_config –cflags
: mysql.h 위치 찾는 명령어

gcc -o [실행파일이름] [c파일이름] -I/usr/local/include/mysql -L/usr/local/lib/mysql -lmysqlclient

mysql.h 위치



감사합니다