EC2(칼리눅스 서버)로 DVWA 올리기.

모의해킹환경 구축을 위한 DVWA 설치하기.

앞서 bee-box에 대해서 소개해드렸는데요. 이번에는 DVWA에 대한 소개입니다. DVWA란? Damn Vulnerable Web Application (DVWA) 의 약자로 마찬가지로 모의해킹 테스트를 위한 환경입니다.bee-box와 마찬

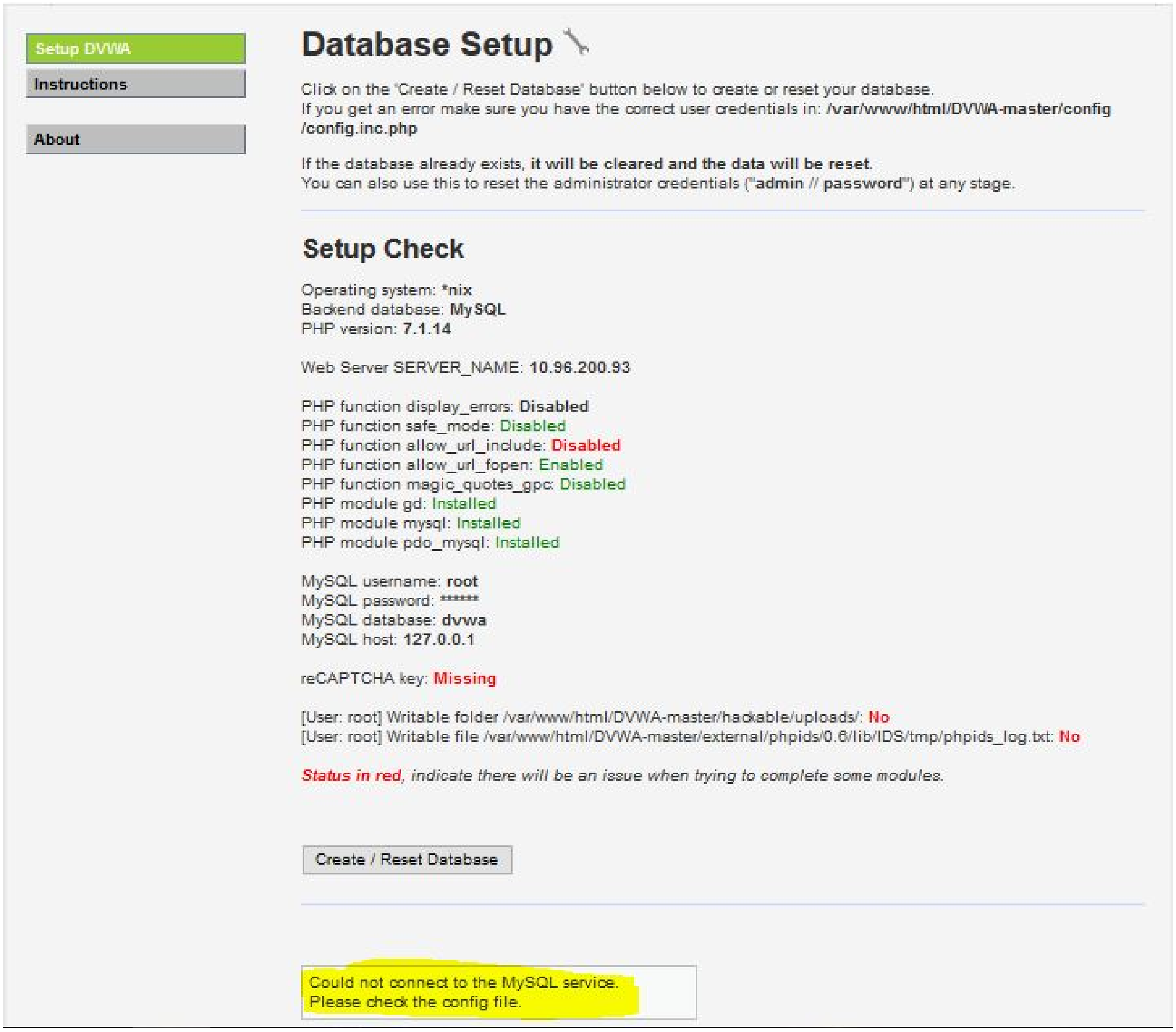
https://blog.dalso.org/article/%EB%AA%A8%EC%9D%98%ED%95%B4%ED%82%B9%ED%99%98%EA%B2%BD-%EA%B5%AC%EC%B6%95%EC%9D%84-%EC%9C%84%ED%95%9C-dvwa-%EC%84%A4%EC%B9%98%ED%95%98%EA%B8%B0

>> 사이트에서 하라는 대로 모두 실행한다.

- 그 후에 다음 코드를 실행한다.

```
service apache2 start   // 아파치 서버를 실행시킨다.
service mysql start   // mysql 서버를 실행시킨다.
```

- 그러면 다음과 같은 문제가 생긴다. 다음의 문제는 내 칼리눅스 서버에 해당 데이터베이스도 없고 계정도 생성되어 있지 않기 때문입니다.



Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **/var/www/html/DVWA-master/config/config.inc.php**

If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

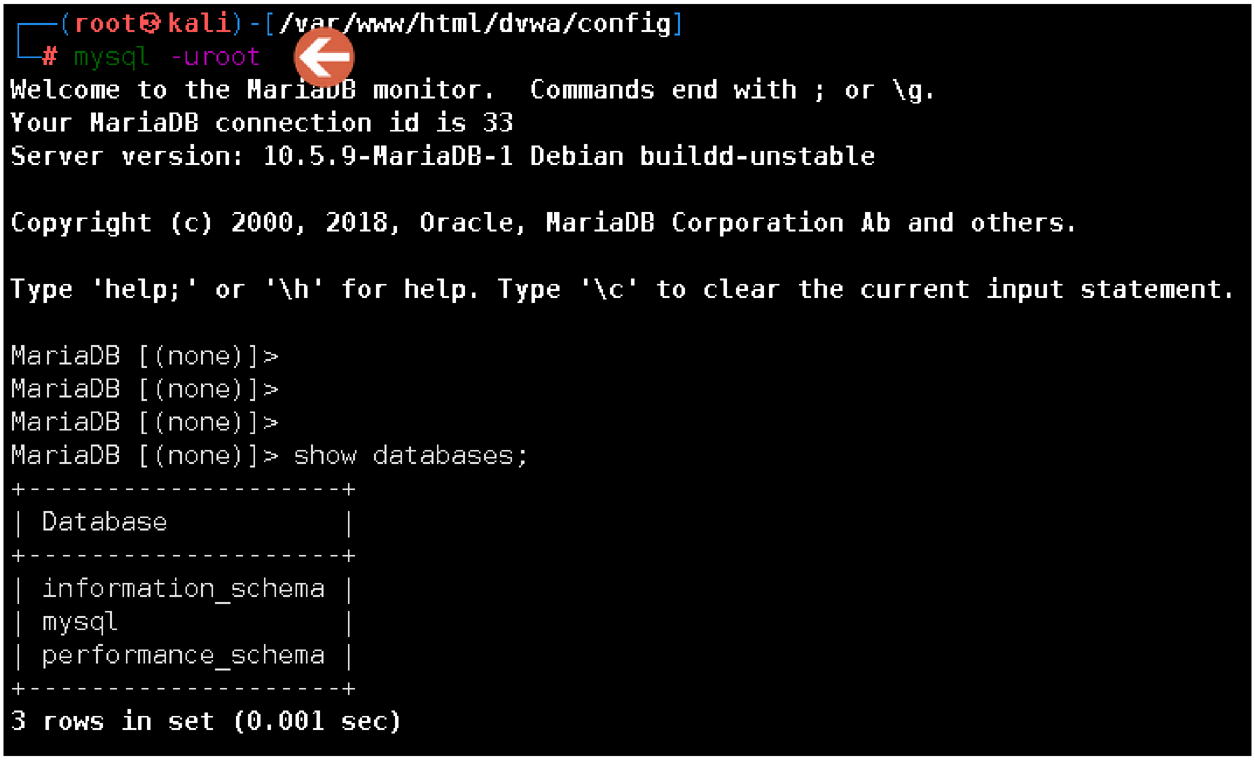
Setup Check

```
Operating system: *nix
Backend database: MySQL
PHP version: 7.1.14

Web Server SERVER_NAME: 10.96.200.93

PHP function display_errors: Disabled
PHP function safe_mode: Disabled
PHP function allow_url_include: Disabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

MySQL username: root
MySQL password: ******
MySQL database: dvwa
MySQL host: 127.0.0.1

reCAPTCHA key: Missing

[User: root] Writable folder /var/www/html/DVWA-master/hackable/uploads/: No
[User: root] Writable file /var/www/html/DVWA-master/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: No
```

Status in red, indicate there will be an issue when trying to complete some modules.

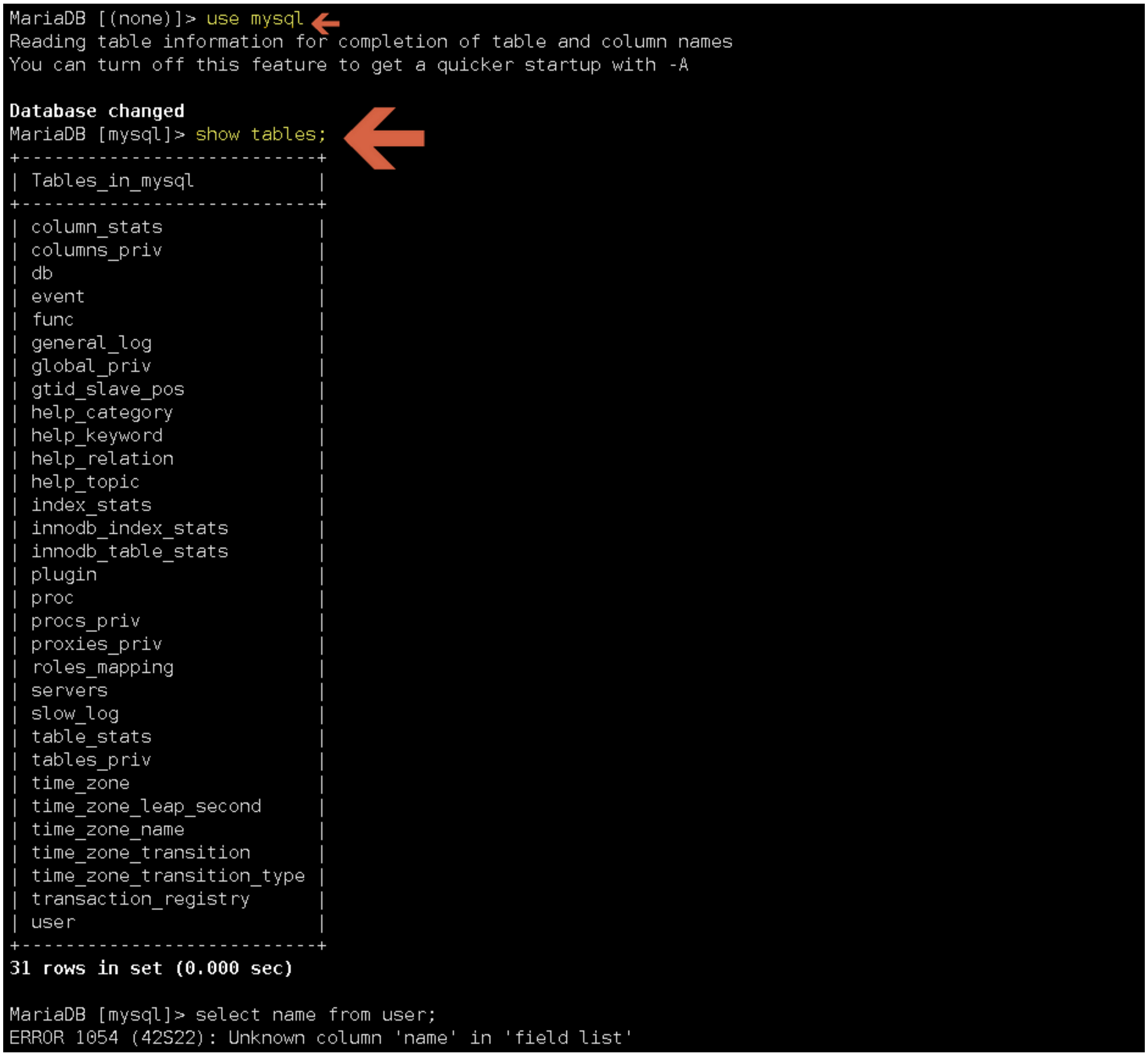
```
Could not connect to the MySQL service.
Please check the config file.
```

- 먼저 mysql에 접속한다.



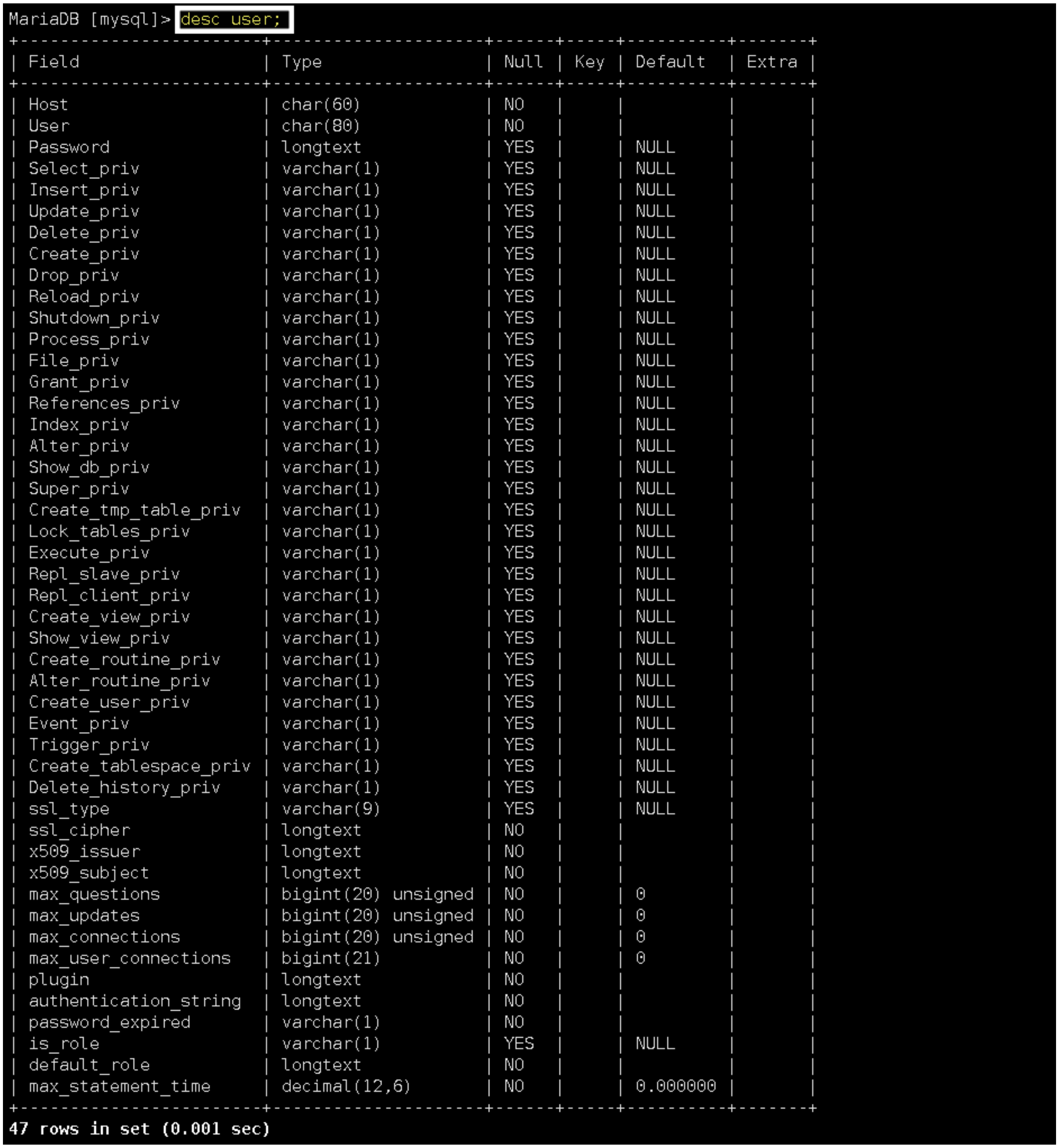
```
┌──(root㉿kali)-[/var/www/html/dvwa/config]
└─# mysql -uroot
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 33
Server version: 10.5.9-MariaDB-1 Debian buildd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
MariaDB [(none)]>
MariaDB [(none)]>
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
3 rows in set (0.001 sec)
```

- mysql의 테이블에 무엇이 있는지 확인한다.(dvwa 있는지 확인)



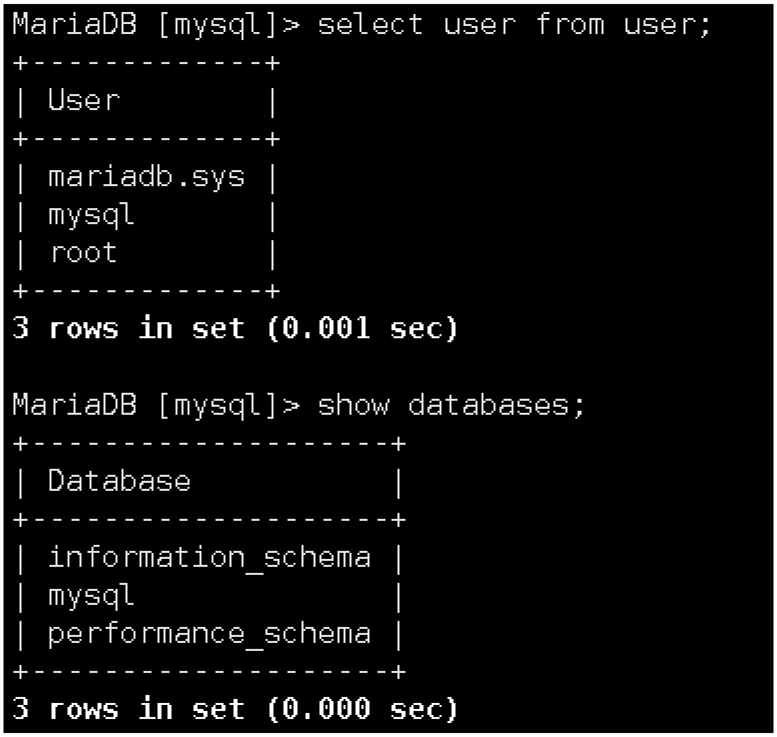
```
MariaDB [(none)]> use mysql
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [mysql]> show tables;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| column_stats              |
| columns_priv              |
| db                        |
| event                     |
| func                      |
| general_log               |
| global_priv               |
| gtid_slave_pos            |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| index_stats               |
| innodb_index_stats        |
| innodb_table_stats        |
| plugin                    |
| proc                      |
| procs_priv                |
| proxies_priv              |
| roles_mapping             |
| servers                   |
| slow_log                  |
| table_stats               |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| transaction_registry      |
| user                      |
+---------------------------+
31 rows in set (0.000 sec)

MariaDB [mysql]> select name from user;
ERROR 1054 (42S22): Unknown column 'name' in 'field list'
```

- user 테이블에 무엇이 있는지 확인한다.(dvwa 있는지 확인)



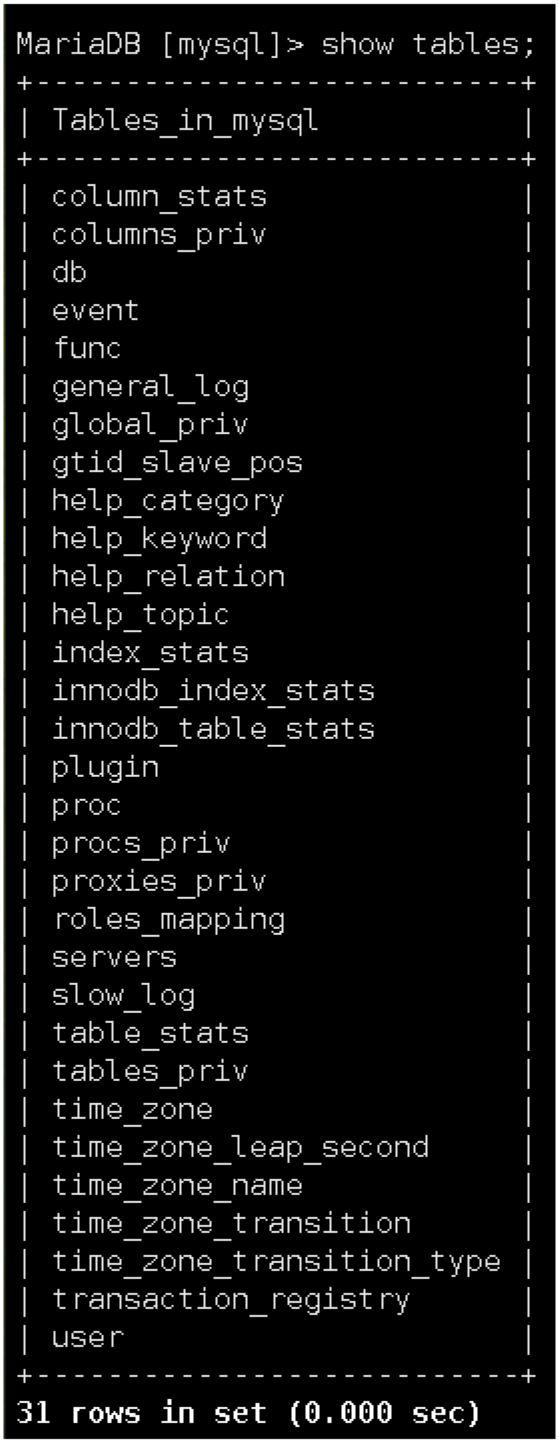
```
MariaDB [mysql]> desc user;
+------------------------+---------------------+------+-----+----------+-------+
| Field                  | Type                | Null | Key | Default  | Extra |
+------------------------+---------------------+------+-----+----------+-------+
| Host                   | char(60)            | NO   |     |          |       |
| User                   | char(80)            | NO   |     |          |       |
| Password               | longtext            | YES  |     | NULL     |       |
| Select_priv            | varchar(1)          | YES  |     | NULL     |       |
| Insert_priv            | varchar(1)          | YES  |     | NULL     |       |
| Update_priv            | varchar(1)          | YES  |     | NULL     |       |
| Delete_priv            | varchar(1)          | YES  |     | NULL     |       |
| Create_priv            | varchar(1)          | YES  |     | NULL     |       |
| Drop_priv              | varchar(1)          | YES  |     | NULL     |       |
| Reload_priv            | varchar(1)          | YES  |     | NULL     |       |
| Shutdown_priv          | varchar(1)          | YES  |     | NULL     |       |
| Process_priv           | varchar(1)          | YES  |     | NULL     |       |
| File_priv              | varchar(1)          | YES  |     | NULL     |       |
| Grant_priv             | varchar(1)          | YES  |     | NULL     |       |
| References_priv        | varchar(1)          | YES  |     | NULL     |       |
| Index_priv             | varchar(1)          | YES  |     | NULL     |       |
| Alter_priv             | varchar(1)          | YES  |     | NULL     |       |
| Show_db_priv           | varchar(1)          | YES  |     | NULL     |       |
| Super_priv             | varchar(1)          | YES  |     | NULL     |       |
| Create_tmp_table_priv  | varchar(1)          | YES  |     | NULL     |       |
| Lock_tables_priv       | varchar(1)          | YES  |     | NULL     |       |
| Execute_priv           | varchar(1)          | YES  |     | NULL     |       |
| Repl_slave_priv        | varchar(1)          | YES  |     | NULL     |       |
| Repl_client_priv       | varchar(1)          | YES  |     | NULL     |       |
| Create_view_priv       | varchar(1)          | YES  |     | NULL     |       |
| Show_view_priv         | varchar(1)          | YES  |     | NULL     |       |
| Create_routine_priv    | varchar(1)          | YES  |     | NULL     |       |
| Alter_routine_priv     | varchar(1)          | YES  |     | NULL     |       |
| Create_user_priv       | varchar(1)          | YES  |     | NULL     |       |
| Event_priv             | varchar(1)          | YES  |     | NULL     |       |
| Trigger_priv           | varchar(1)          | YES  |     | NULL     |       |
| Create_tablespace_priv | varchar(1)          | YES  |     | NULL     |       |
| Delete_history_priv    | varchar(1)          | YES  |     | NULL     |       |
| ssl_type               | varchar(9)          | YES  |     | NULL     |       |
| ssl_cipher             | longtext            | NO   |     |          |       |
| x509_issuer            | longtext            | NO   |     |          |       |
| x509_subject           | longtext            | NO   |     |          |       |
| max_questions          | bigint(20) unsigned | NO   |     | 0        |       |
| max_updates            | bigint(20) unsigned | NO   |     | 0        |       |
| max_connections        | bigint(20) unsigned | NO   |     | 0        |       |
| max_user_connections   | bigint(21)          | NO   |     | 0        |       |
| plugin                 | longtext            | NO   |     |          |       |
| authentication_string  | longtext            | NO   |     |          |       |
| password_expired       | varchar(1)          | NO   |     |          |       |
| is_role                | varchar(1)          | YES  |     | NULL     |       |
| default_role           | longtext            | NO   |     |          |       |
| max_statement_time     | decimal(12,6)       | NO   |     | 0.000000 |       |
+------------------------+---------------------+------+-----+----------+-------+
47 rows in set (0.001 sec)
```

- users 테이블의 user에 dvwa 있는지 확인



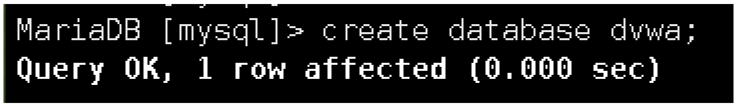
```
MariaDB [mysql]> select user from user;
+-------------+
| User        |
+-------------+
| mariadb.sys |
| mysql       |
| root        |
+-------------+
3 rows in set (0.001 sec)

MariaDB [mysql]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
3 rows in set (0.000 sec)
```

- 테이블 중에 dvwa가 있는지 확인



```
MariaDB [mysql]> show tables;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| column_stats              |
| columns_priv              |
| db                        |
| event                     |
| func                      |
| general_log               |
| global_priv               |
| gtid_slave_pos            |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| index_stats               |
| innodb_index_stats        |
| innodb_table_stats        |
| plugin                    |
| proc                      |
| procs_priv                |
| proxies_priv              |
| roles_mapping             |
| servers                   |
| slow_log                  |
| table_stats               |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| transaction_registry      |
| user                      |
+---------------------------+
31 rows in set (0.000 sec)
```

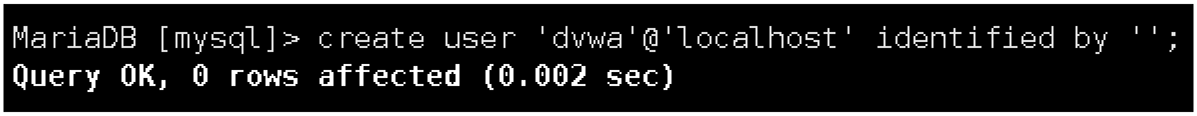
- dvwa 데이터베이스를 만든다.



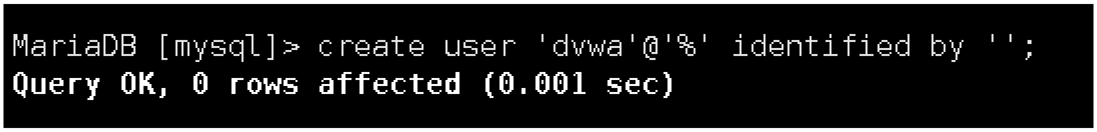
```
MariaDB [mysql]> create database dvwa;
Query OK, 1 row affected (0.000 sec)
```

- user명은 dvwa로 합니다. `@’%’ 는 어떤 클라이언트에서든 접근이 가능하다는 의미이고, @’localhost’ 는 해당 컴퓨터에서만 접근이 가능하다는 의미입니다.`

```
mysql> CREATE USER '{username}'@'localhost' IDENTIFIED BY '{password}';
mysql> CREATE USER '{username}'@'%' IDENTIFIED BY '{password}';
```



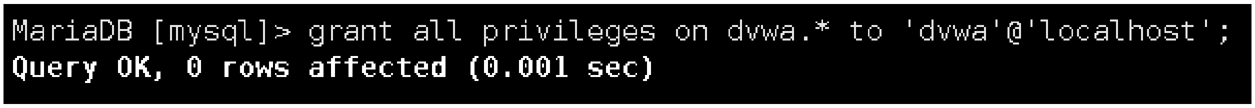
```
MariaDB [mysql]> create user 'dvwa'@'localhost' identified by '';
Query OK, 0 rows affected (0.002 sec)
```



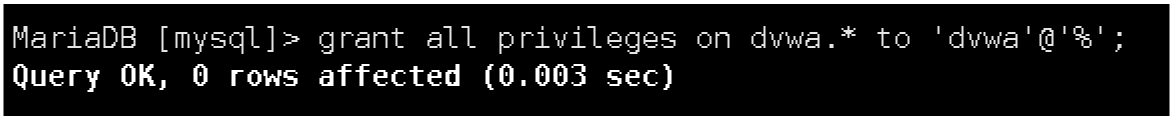
```
MariaDB [mysql]> create user 'dvwa'@'%' identified by '';
Query OK, 0 rows affected (0.001 sec)
```

- 생성한 계정에 권한을 부여한다.

```
mysql> GRANT ALL PRIVILEGES ON {database}.* TO '{username}'@'localhost';
mysql> FLUSH PRIVILEGES;
```

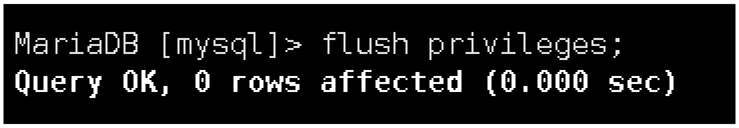


```
MariaDB [mysql]> grant all privileges on dvwa.* to 'dvwa'@'localhost';
Query OK, 0 rows affected (0.001 sec)
```



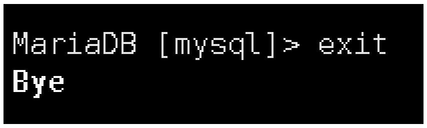
```
MariaDB [mysql]> grant all privileges on dvwa.* to 'dvwa'@'%';
Query OK, 0 rows affected (0.003 sec)
```

- 권한 부여한것을 다시 실행시킨다.



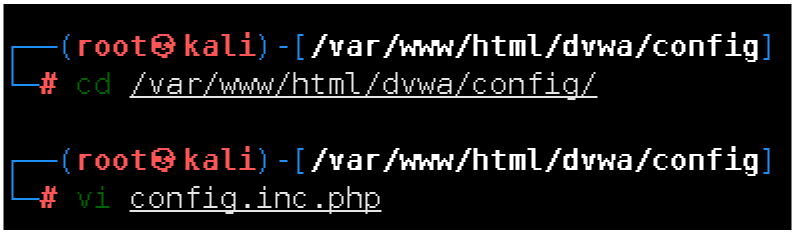
```
MariaDB [mysql]> flush privileges;
Query OK, 0 rows affected (0.000 sec)
```

- 나간다.

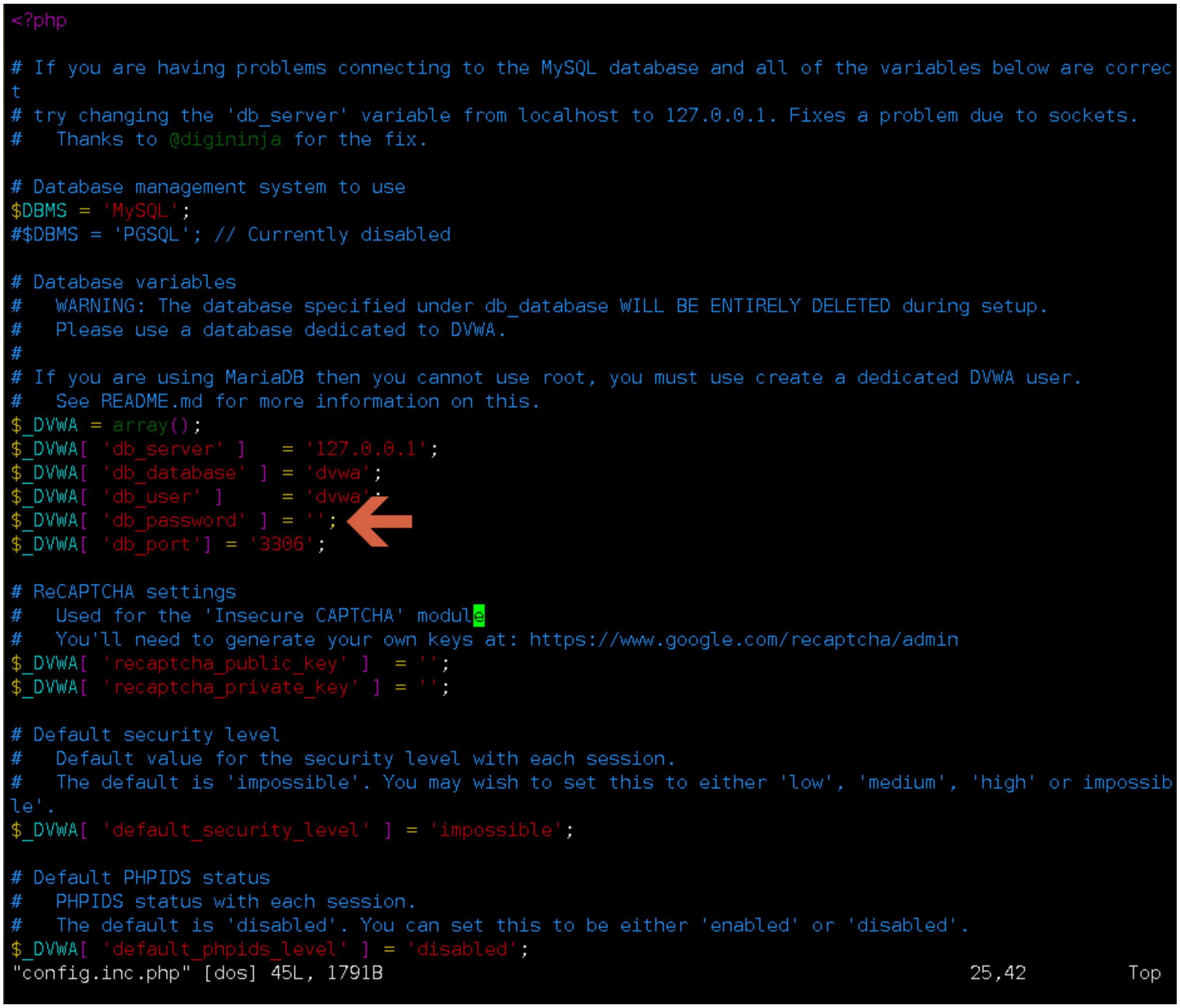


```
MariaDB [mysql]> exit
Bye
```

- dvwa 설정을 다시 입력한다.

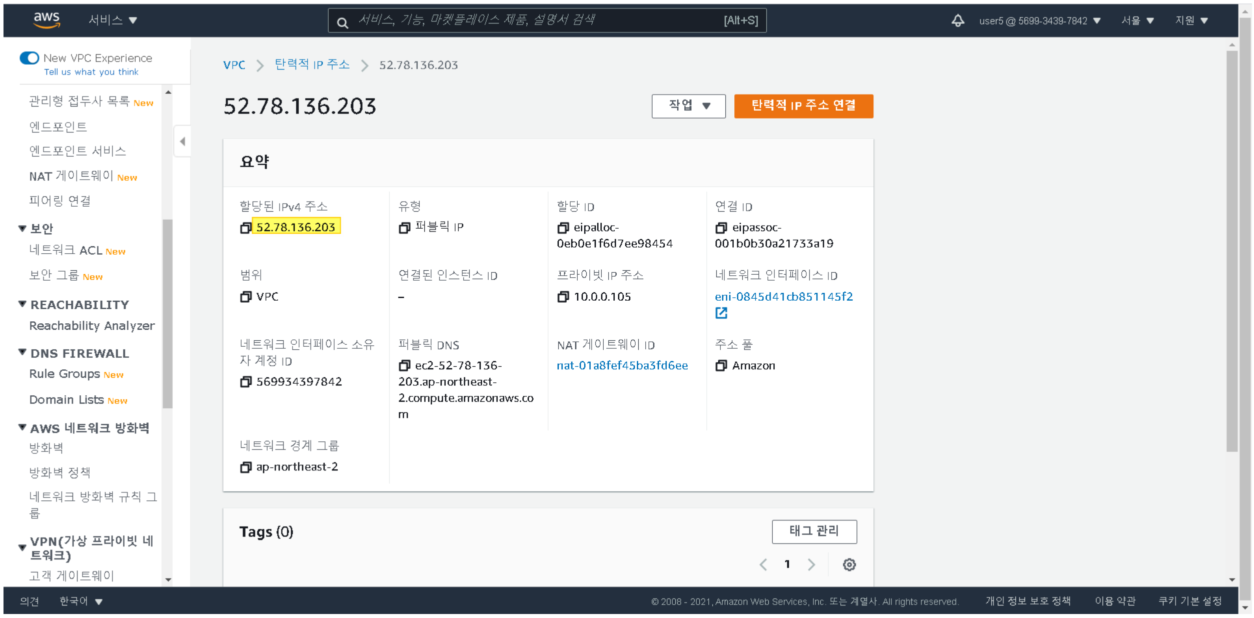


```
┌──(root㉿kali)-[/var/www/html/dvwa/config]
└─# cd /var/www/html/dvwa/config/

┌──(root㉿kali)-[/var/www/html/dvwa/config]
└─# vi config.inc.php
```



```
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correc
t
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'dvwa';
$_DVWA[ 'db_password' ] = '';
$_DVWA[ 'db_port'] = '3306';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ]  = '';
$_DVWA[ 'recaptcha_private_key' ] = '';

# Default security level
#   Default value for the security level with each session.
#   The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossib
le'.
$_DVWA[ 'default_security_level' ] = 'impossible';

# Default PHPIDS status
#   PHPIDS status with each session.
#   The default is 'disabled'. You can set this to be either 'enabled' or 'disabled'.
$_DVWA[ 'default_phpids_level' ] = 'disabled';
"config.inc.php" [dos] 45L, 1791B                                         25,42         Top
```

- 다시 실행하면 실행된다.

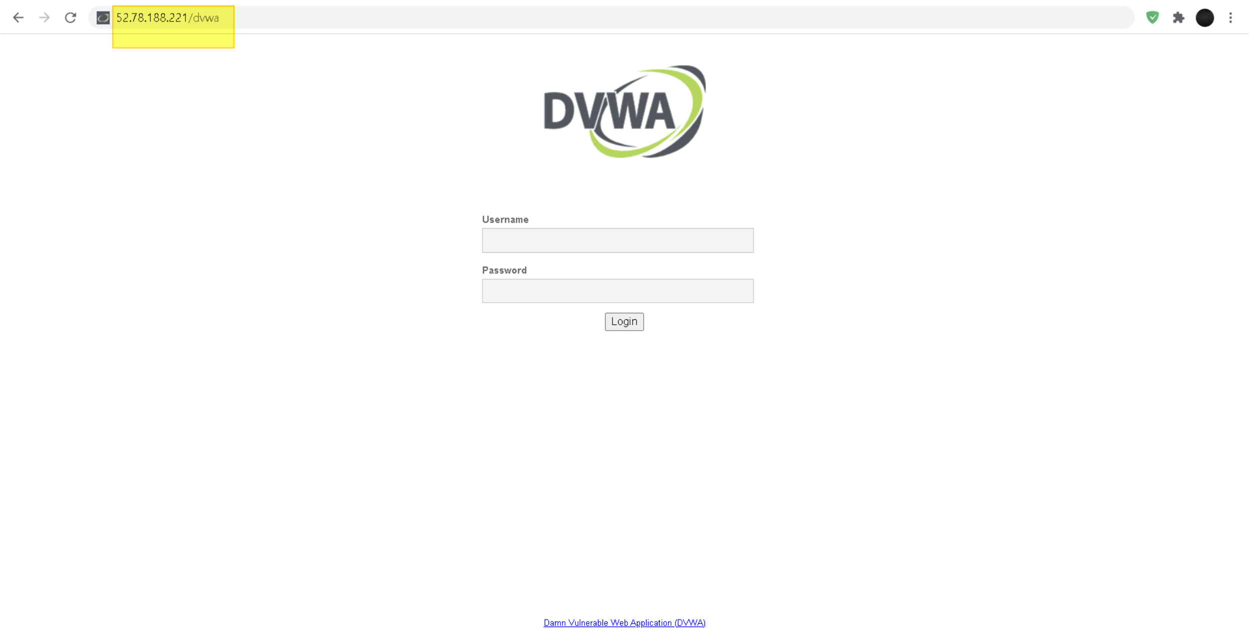


52.78.136.203

요약

할당된 IPv4 주소 52.78.136.203	유형 퍼블릭 IP	할당 ID eipalloc-0eb0e1f6d7ee98454	연결 ID eipassoc-001b0b30a21733a19
범위 VPC	연결된 인스턴스 ID –	프라이빗 IP 주소 10.0.0.105	네트워크 인터페이스 ID eni-0845d41cb851145f2
네트워크 인터페이스 소유자 계정 ID 569934397842	퍼블릭 DNS ec2-52-78-136-203.ap-northeast-2.compute.amazonaws.com	NAT 게이트웨이 ID nat-01a8fef45ba3fd6ee	주소 풀 Amazon
네트워크 경계 그룹 ap-northeast-2			

Tags (0)



52.78.188.221/dvwa

Username

Password

▼ 참고사이트

https://devdhjo.github.io/mysql/2020/01/29/database-mysql-002.html