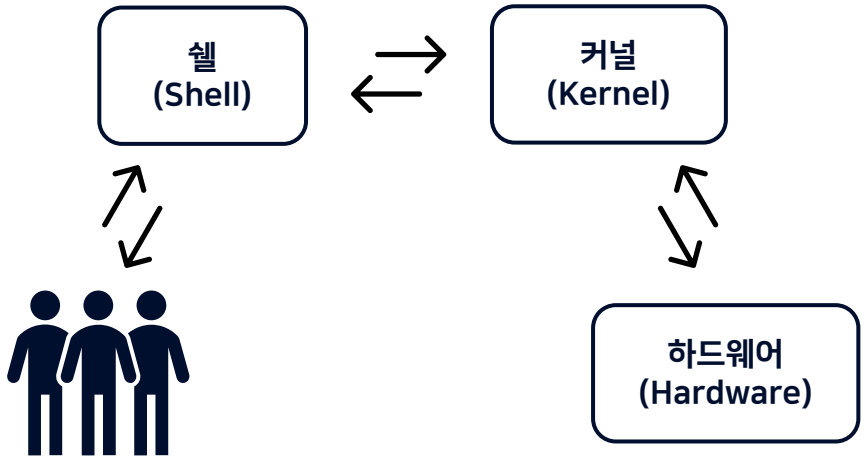
파일 업로드 취약점을 이용한 악성코드 배포

210603

91914028 이유경

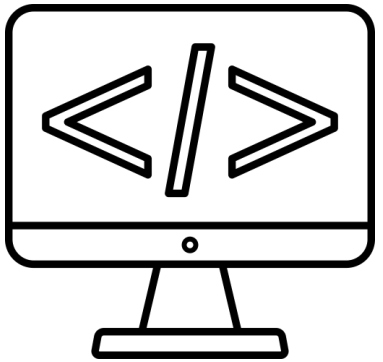
Contents

1-1. 웹 쉘



쉘(Shell)

사용자에게 받은 지시를 하드웨어 지식으로 변경
운영체제의 커널과 유저를 이어 줌

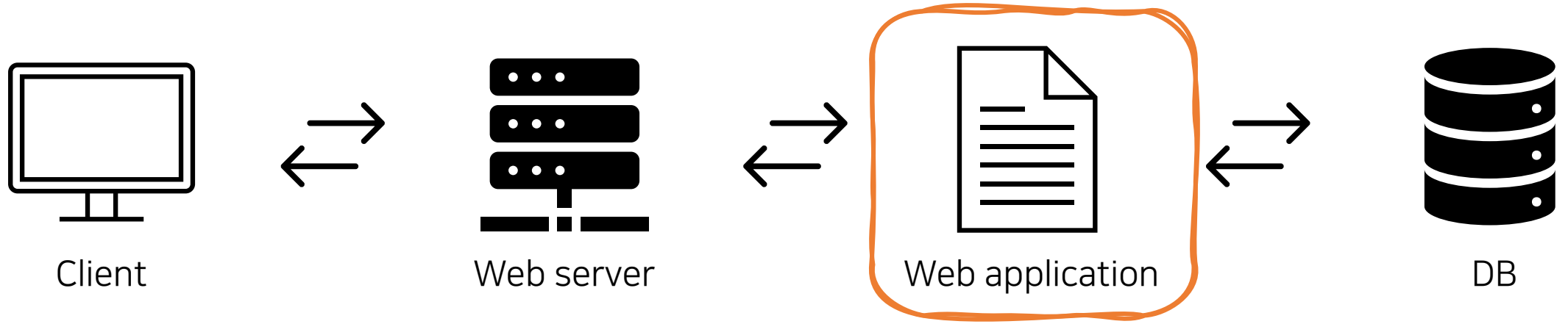


웹 쉘(Shell)

웹 사이트를 통해 쉘을 여는 공격
이 쉘을 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 획득하는 취약점
악성 스크립트가 업로드 된 후, 서버 상에서 스크립트를 실행하여 쉘을 획득하는 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 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

↓

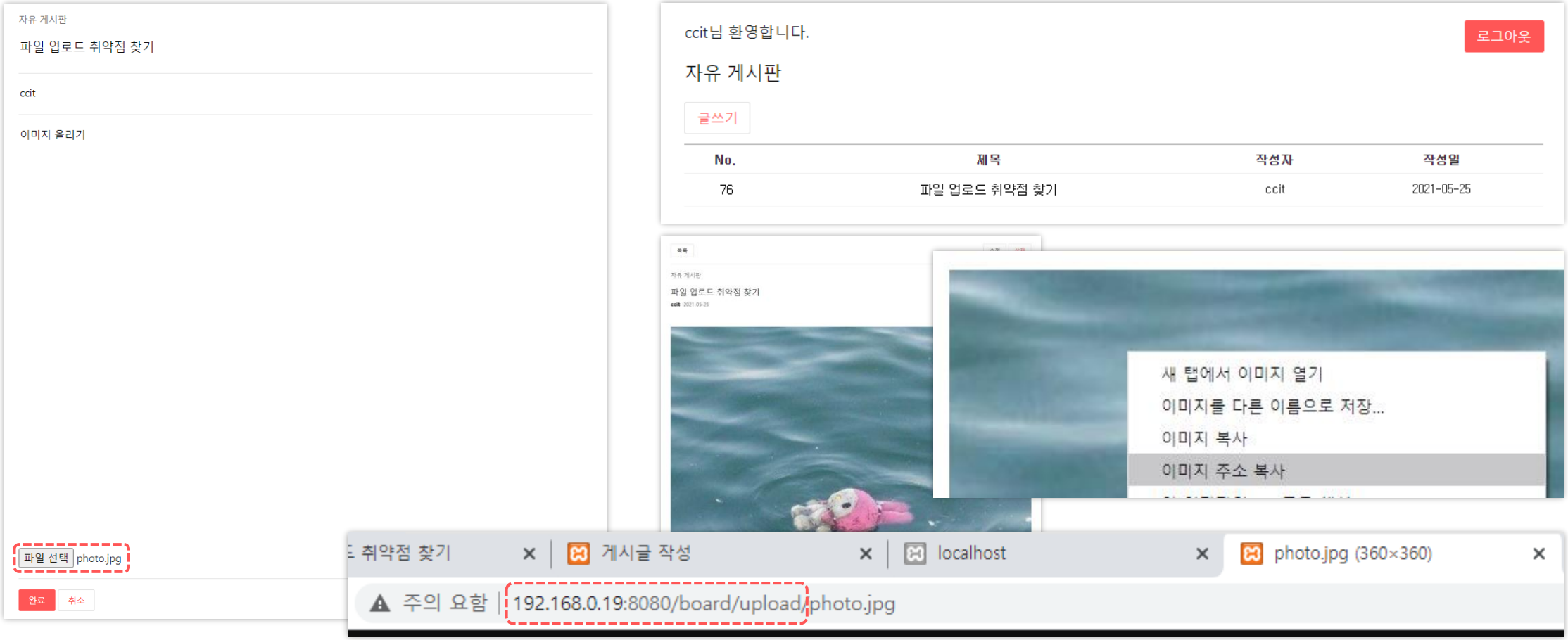
② 웹 사이트에 웹 쉘과 배치 파일을 업로드하여 웹으로 업로드 된 웹 쉘에 접근

↓

③ 배치 파일을 실행시켜 피해자 PC의 정보 확인 및 유출

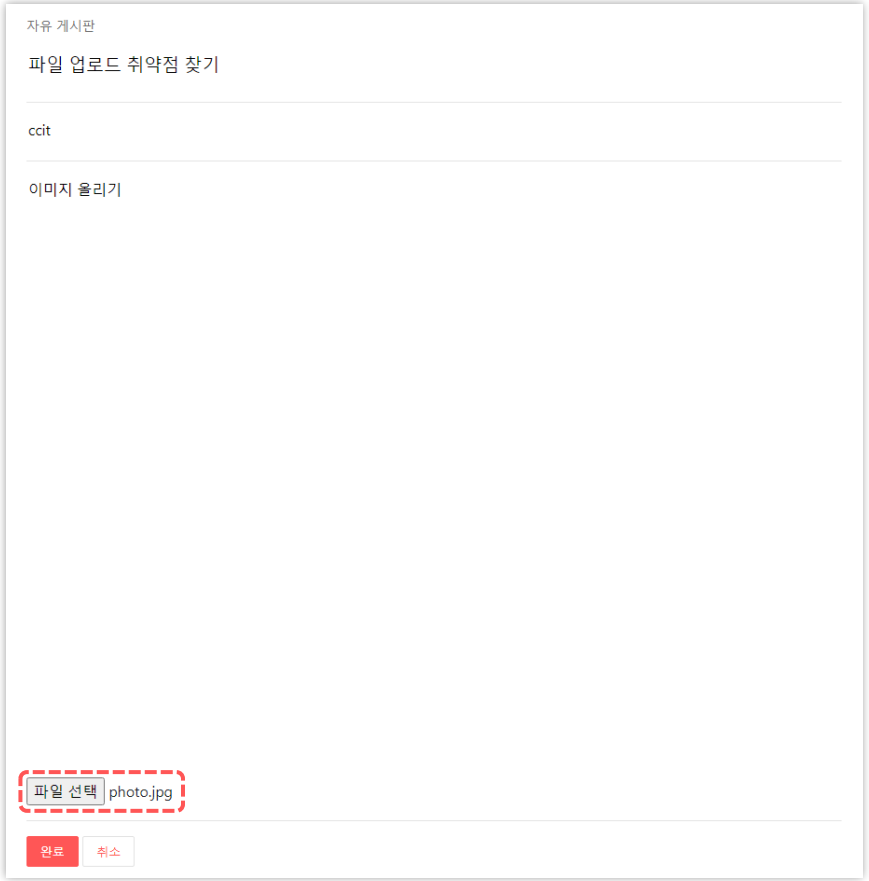
2-2. 시현

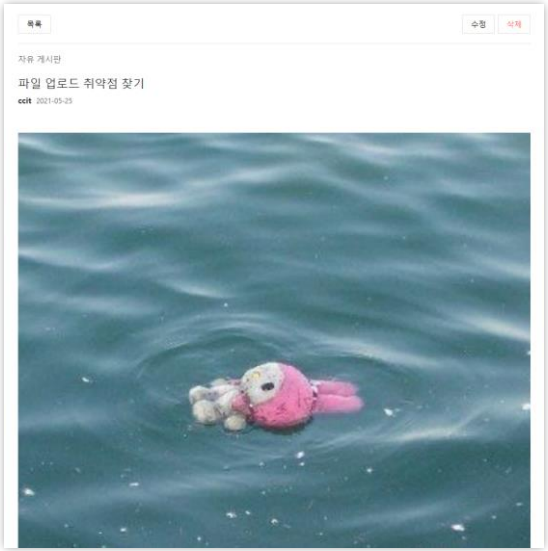
① 공격자는 홈페이지에 존재하는 파일 업로드 취약점을 이용하여 수행 ▶ 파일 업로드 경로 알아내기



2-2. 시현

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





Burp Suite로 확인

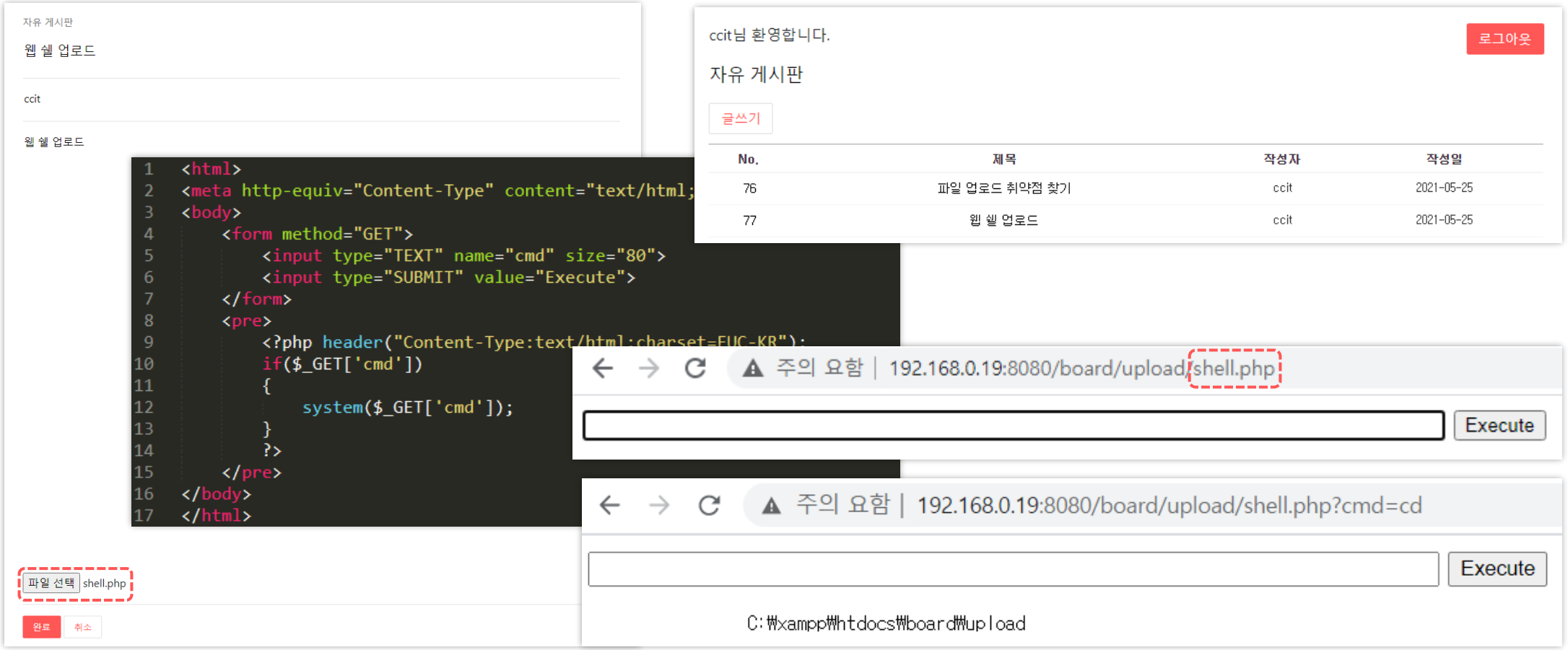
```
</p>
<img src="./upload/shell.php"onerr
'div>
```

개발자 도구로 확인

```
<img src="./upload/photo.jpg" on
0%;"> == $0
```

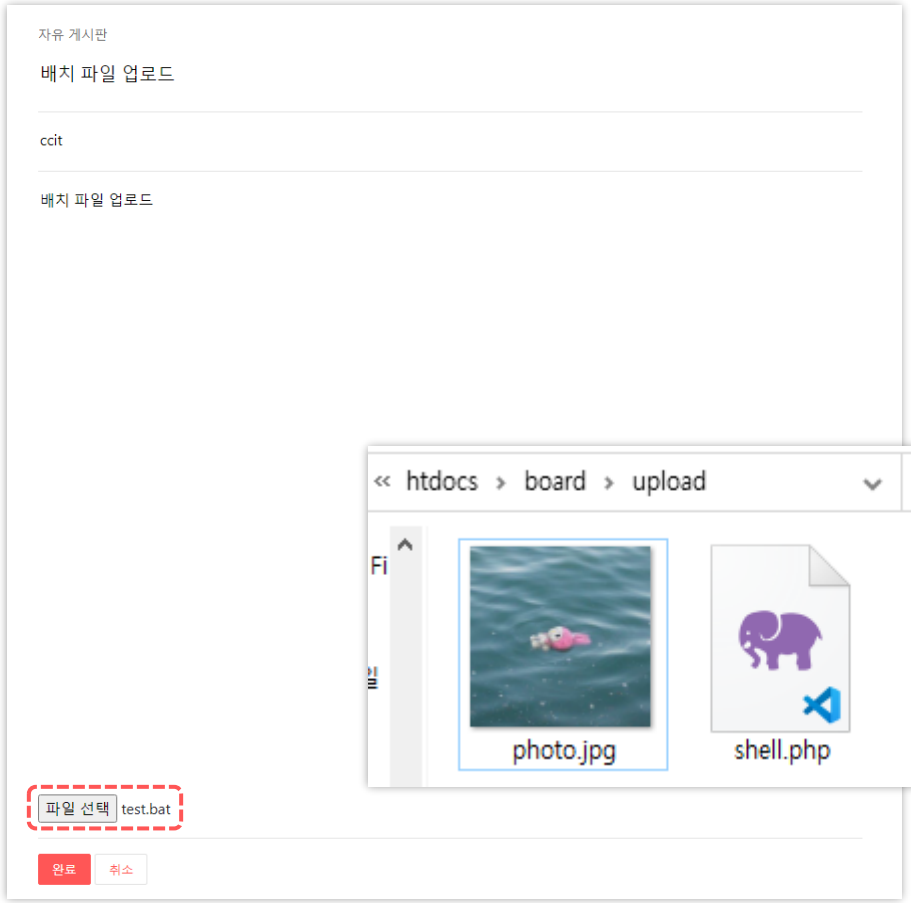
2-2. 시현

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

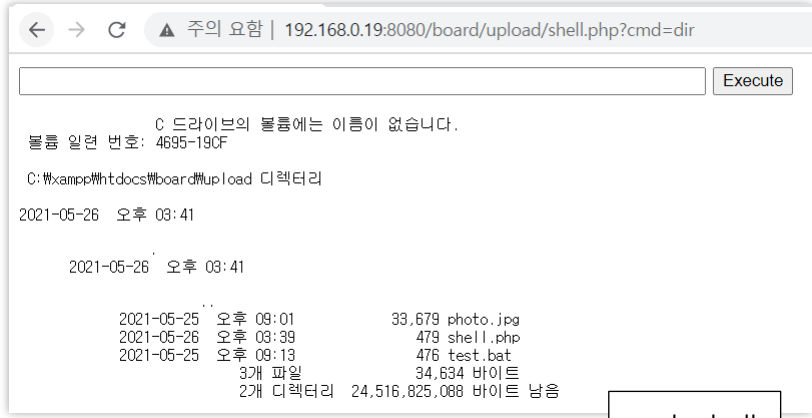


2-2. 시현

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



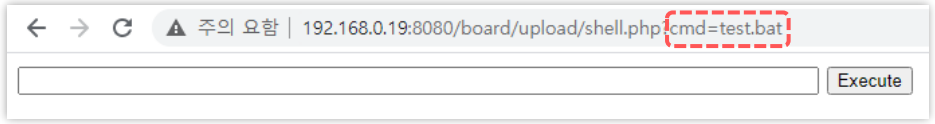
호스트 PC



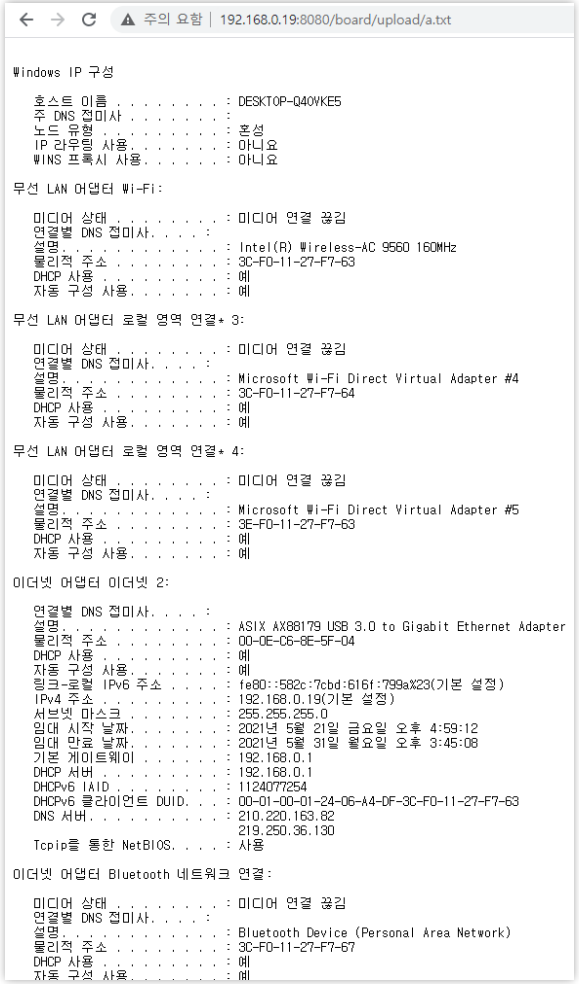
web shell

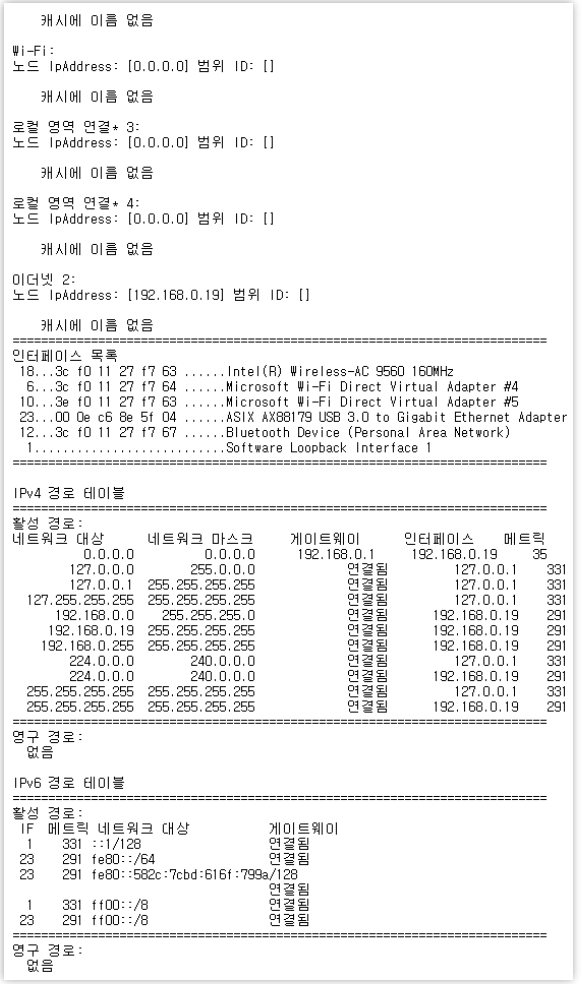
2-2. 시현

③ 배치 파일을 실행시켜 피해자 PC의 정보 확인 및 유출




```bat
@echo off

:ip
ipconfig /all > a.txt

:Network Session
net session >> a.txt

:ARP
arp -a >> a.txt

:Shared Folder/File
net share >> a.txt

:NetBIOS
nbtstat -c >> a.txt

:Routing
netstat -r >> a.txt
```





THANK YOU