

웹 해킹을 공부해보자

박지윤

목차

1. Wargame.kr의 2문제
2. 웹 해킹 실습

Wargame.kr 의 WTF_Code를 풀어보자



WTF_CODE



450point / bughela

This is another programming language.


Can you read this source code?

FLAG

Auth

Start

Close



이게 진짜 소스코드라고? 아무것도 안보인다고!!

is this source code really???? i can't see anything really!

source_code.ws

WS 확장자란?

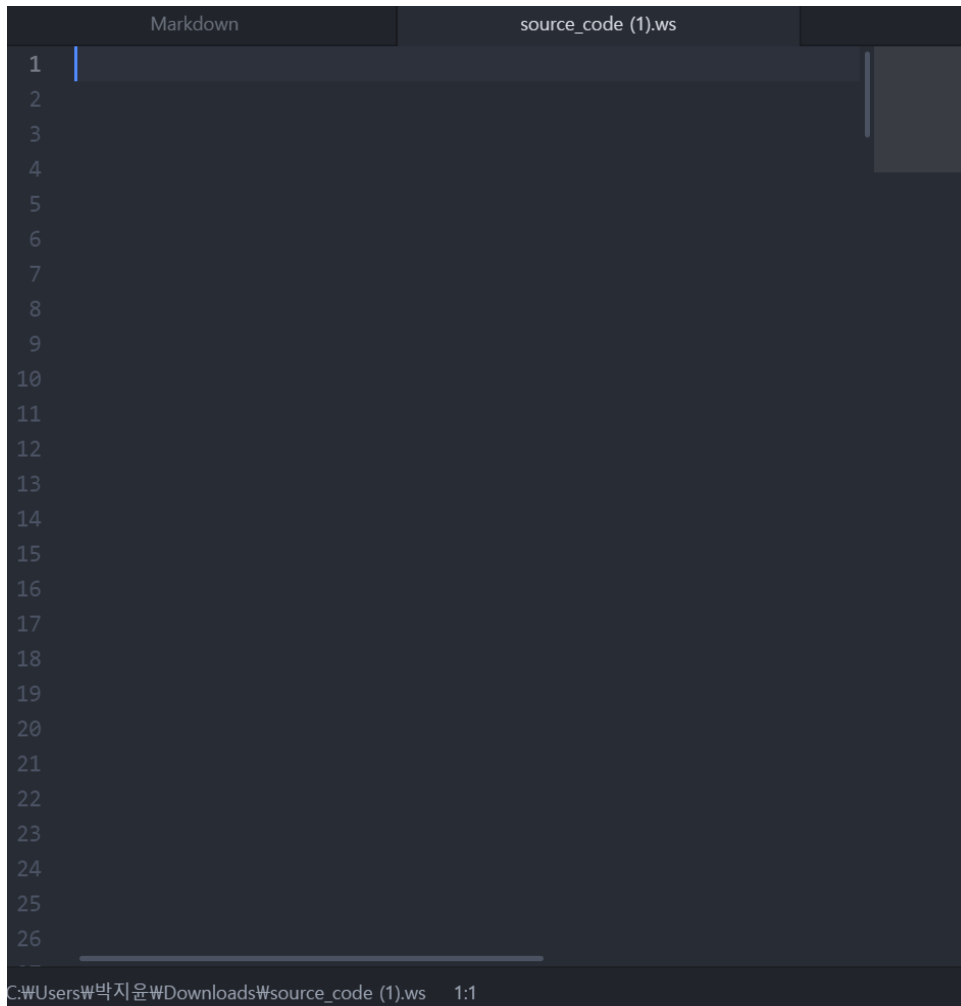
Whitespace : '화면상으로는 아무것도 표시되지 않는 문자.'

라는 뜻으로 많은 부분에 활용되지만 보통 자신이 숨기고 싶은 문구가 있을 때 많이 사용합니다.

좀 자세히 설명하자면 '스택 기반형의 프로그래밍 언어'이고 공백, 탭, 개행문자 이외엔 모든걸 무시해버립니다.



화면상으로는 아무것도 나타나지 않으며, 공백, 탭, 개행문자로만 표현됨



Atom으로 열어보니 내용은
눈에 보이지 않지만 241줄짜리
코드임이 확인 가능!



▼ Output

Wow! Key is



<https://tio.run/#whitespace> 에 코드를 붙여넣기하면 flag 값이 나타남

해결!

IMG Recovery를 풀어보자

img recovery



650point / bughela

Recovery the PNG image file!

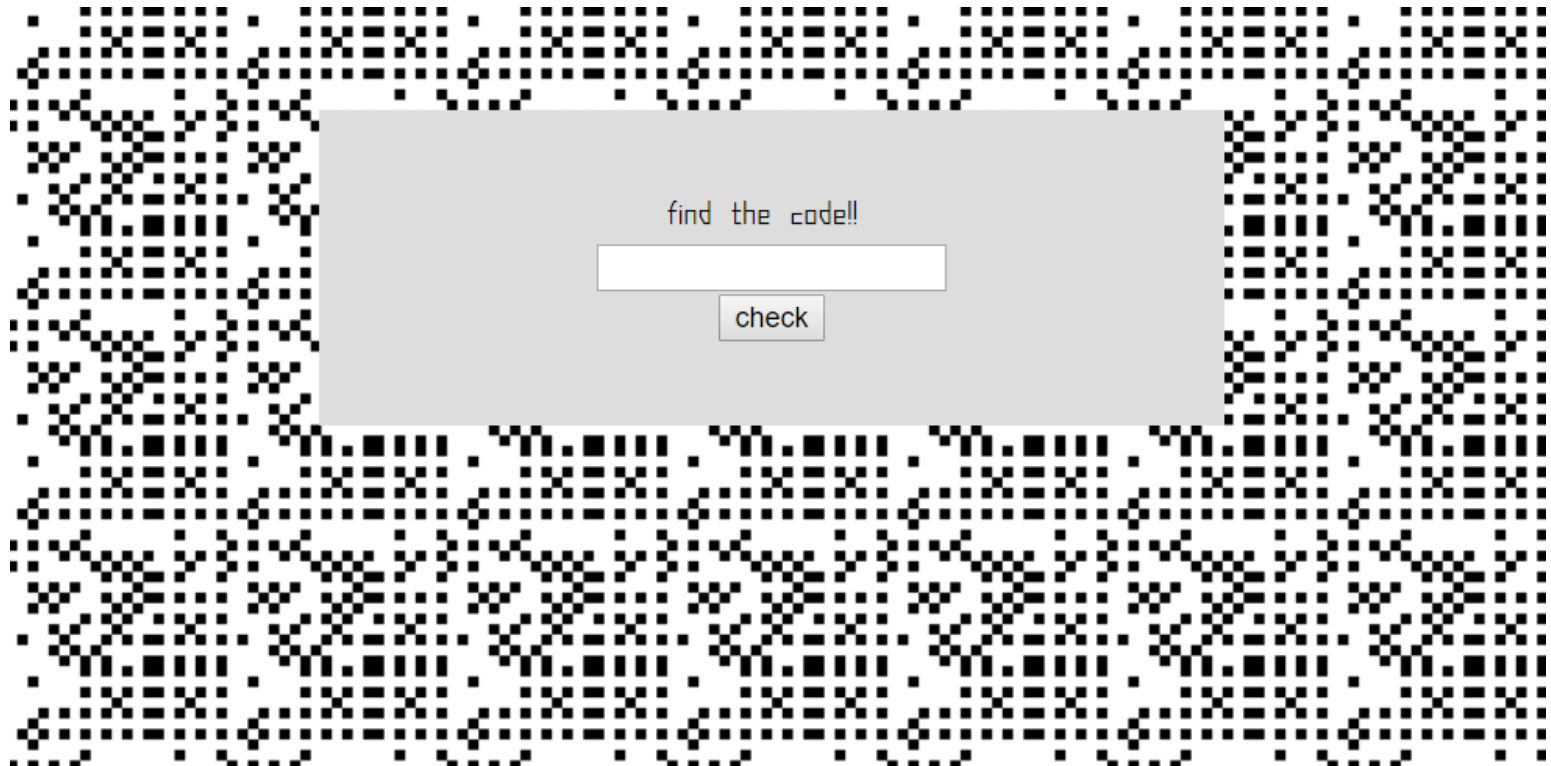
but.. is this really "PNG" file?

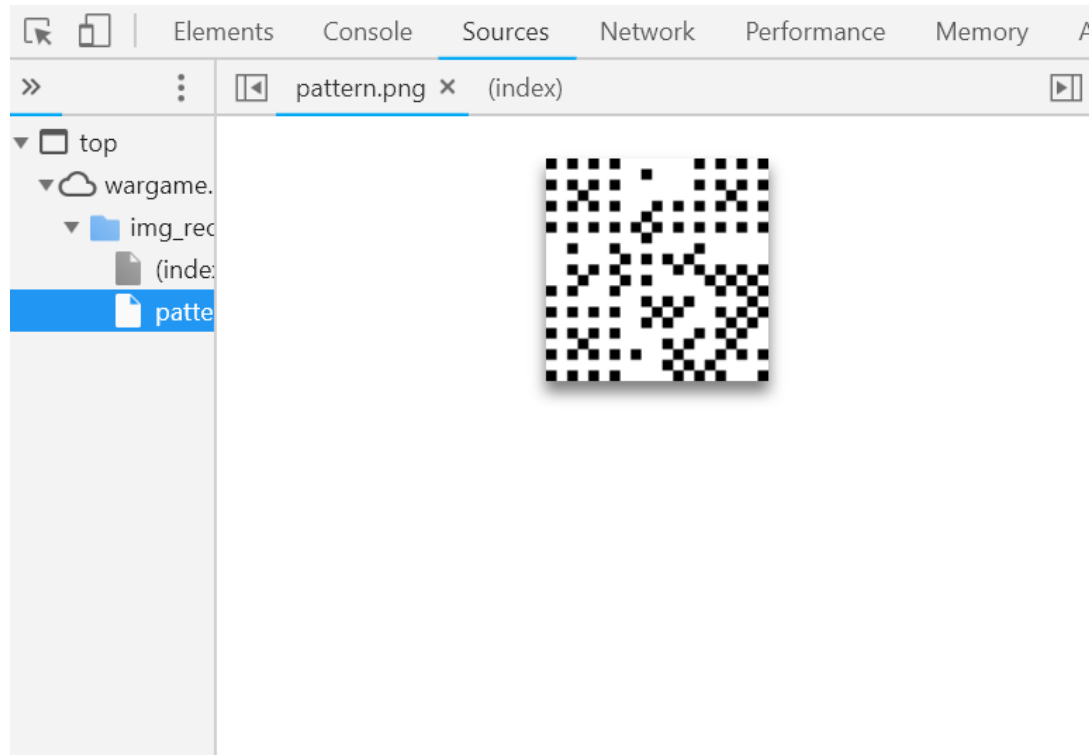
(NO STEGANOGRAPHY. THIS IS FORENSIC CHALLENGE)

Auth

Start

Close

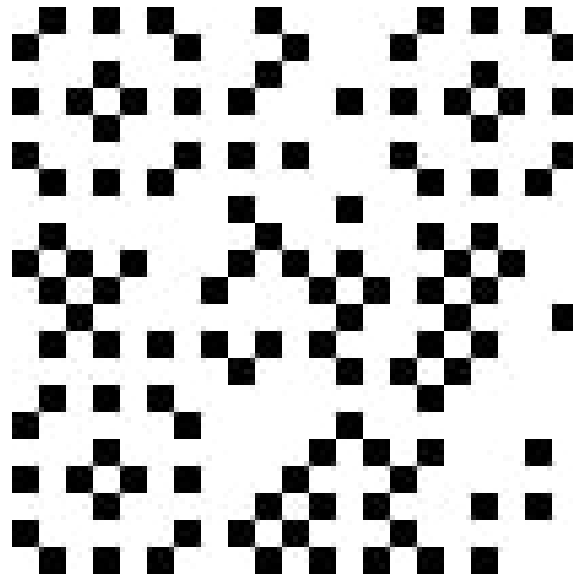




개발자 모드로 들어간 후 파일을 보면 저렇게 생긴 이미지
파일(.png)이 첨부되어 있음을 알 수 있음

문제에서 이게 정말 png파일일까? 라는 부분이 수상해서

<https://png2jpg.com/ko/> 를 이용해서 png파일을 jpg파일로 변환해줌





두 그림을 포토샵으로 합쳐보았더니 QR 코드가 나옴
이를 찍어보면 flag값이 나옴
해결!

웹 해킹을 실습해보자!



목표 : File Upload 공격을 실습해보자!

→ 웹 사이트 공격 (서버 공격 X)

먼저 알아야 할 것



Shell – 사용자의 명령을 OS에 전달하는 프로그램

WebShell – 웹 브라우저를 사용해서 OS에 명령을 전달하는 프로그램

File Upload 공격

1. 웹 사이트 자체의 취약점을 이용한 해킹 기법
2. 웹 사이트에서 제공하는 파일 업로드 기능을 악용 (파일, 사진 첨부)
3. 웹 사이트 개발에 사용된 언어와 동일한 언어로 개발된 파일 업로드
4. 업로드 된 파일이 저장되는 경로에 실행 권한이 할당 되어 있어야 함
5. 업로드 된 파일의 경로를 확인할 수 있어야 함
6. 웹 브라우저를 통한 시스템 명령어 실행 권한을 획득함
7. 웹 해킹 피해를 입은 웹 서버의 대부분에서 웹 셸이 발견되었음

공격 절차

1. 개발 언어 확인
2. 파일 업로드 기능 찾기
3. 정상적인 파일 업로드 후 업로드 된 경로 및 실행 권한을 확인
4. 파일 업로드 제한 정책을 확인 후 가능한 확장자를 확인
5. 공격용 파일 업로드
6. 웹 브라우저로 파일을 실행

LOGO

홈 | 장바구니 | 주문내역보기 | 배송정보 | 마이페이지 | 고객센터

NOTICE

1111님이 로그인 중입니다.
포인트 :
최근방문일 :

> 로그인

> 회원가입

> ID/PW 찾기

PRODUCTS CATEGORY

계좌번호

국민은행 / 홍길동
914801-01-330020

고객센터

평일 AM10:00 ~ PM23:00
휴일 AM09:00 ~ PM23:00

공정거래위원회인증
표준약관이용



SEARCH

검색

상세검색

쇼핑몰

QUICK LINK



커뮤니티



고객의소리



자주하는 질문



배송안내

EVENT 01

예력과 함께 하는
스팸 이벤트!



EVENT 02

아직도 C.Jmall에서
즐거운 쇼핑.정.험이
없으셨나요?



히트상품 HIT PRODUCT

신제품 NEW PRODUCT



일반



무료쇼핑몰 솔루션 - 솜위즈(<http://www.shop-wiz.com>)

프로토콜: HyperText Transfer Protocol

유형: Chrome HTML Document

연결: 암호화되지 않음

영역: 인터넷 | 보호 모드: 설정

주소:
(URL) http://10.10.10.10/wizboard.php?
 BID=board04&GID=root

크기: 알 수 없음

만든 날짜: 알 수 없음

수정된 날짜: 알 수 없음

인증서(C)

확인

취소

적용(A)

NOTICE

SEARCH

검색

상세검색

1111님이 로그인 중입니다.
 포인트 :
 최근방문일 :

로그인

회원가입

ID/PW 찾기

PRODUCTS CATEGORY

계좌번호



국민은행 / 홍길동
 914801-01-330020

고객센터



평일 AM10:00 ~ PM23:00
 휴일 AM09:00 ~ PM23:00



공정거래위원회인증
 표준약관이용



VeriSign
 The Value of Trust

BANKWell
 Total Payment Solution - 뱅크웰(주)

제목

a

글쓴이

1111

이메일

a



a

첨부파일

1484247354310.JPEG

답글

수정

삭제

목록

QUICK LINK



커뮤니티



고객의소리



자주하는질문



배송안내

속성



일반



1484247354310.JPG

프로토콜: HyperText Transfer Protocol

유형: 사용할 수 없음

주소:
(URL) <http://10.10.10.10/wizboard/table/root/board04/updir/1484247354310.JPG>

크기: 사용할 수 없음

픽셀 크기: 540 x 303 픽셀

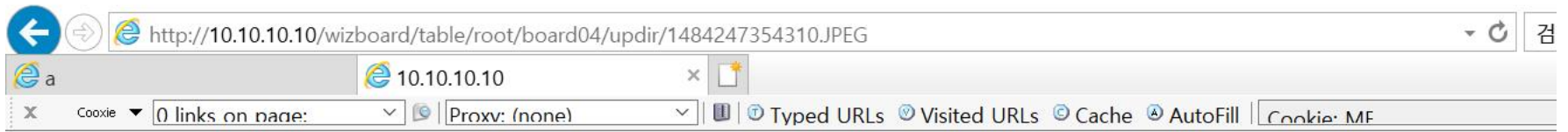
만든 날짜: 2018-07-15

수정한 날짜: 2018-07-15

확인

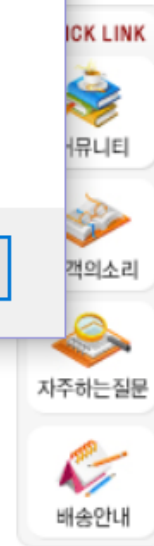
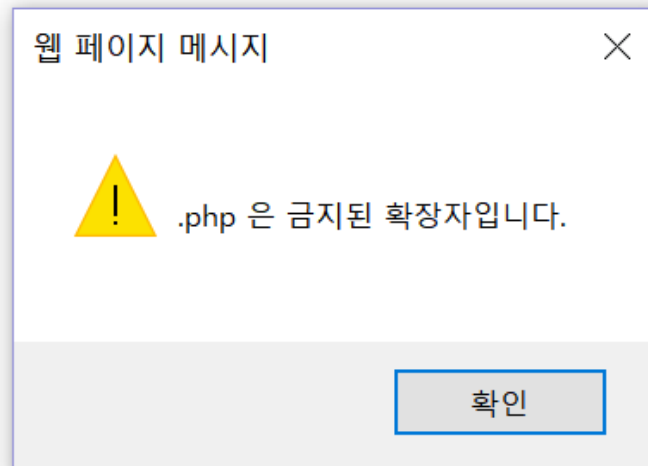
취소

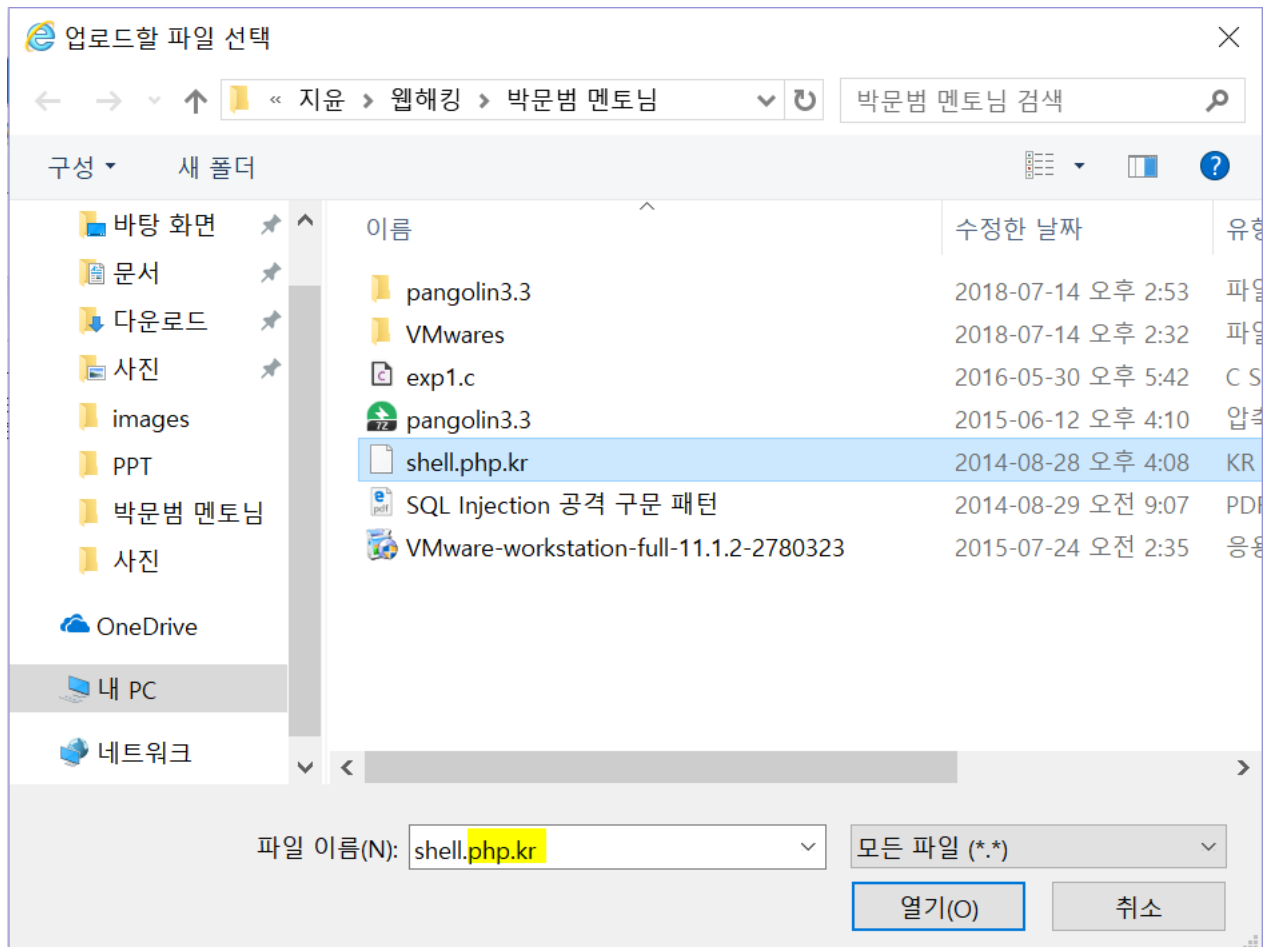
적용(A)



제목	a		
글쓴이	1111	비밀번호	●
이메일	a		
옵션	<input type="checkbox"/> HTML사용 <input type="checkbox"/> 비밀게시글		
	<div> a </div>		
첨부파일	C:\Users\박지윤\Desktop\지윤\웹해킹\박문범 멘토님\shell.php 찾아보기...		

제목	a		
글쓴이	1111	비밀번호	●
이메일	a		
옵션	<input type="checkbox"/> HTML사용 <input type="checkbox"/> 비밀게시글		
a	<div>?</div>		
첨부파일	C:\Users\박지윤\Desktop\지윤\웹해킹\박문범 멘토님\shell.php		
<div>찾아보기...</div>			
<div>확인 취소</div>			

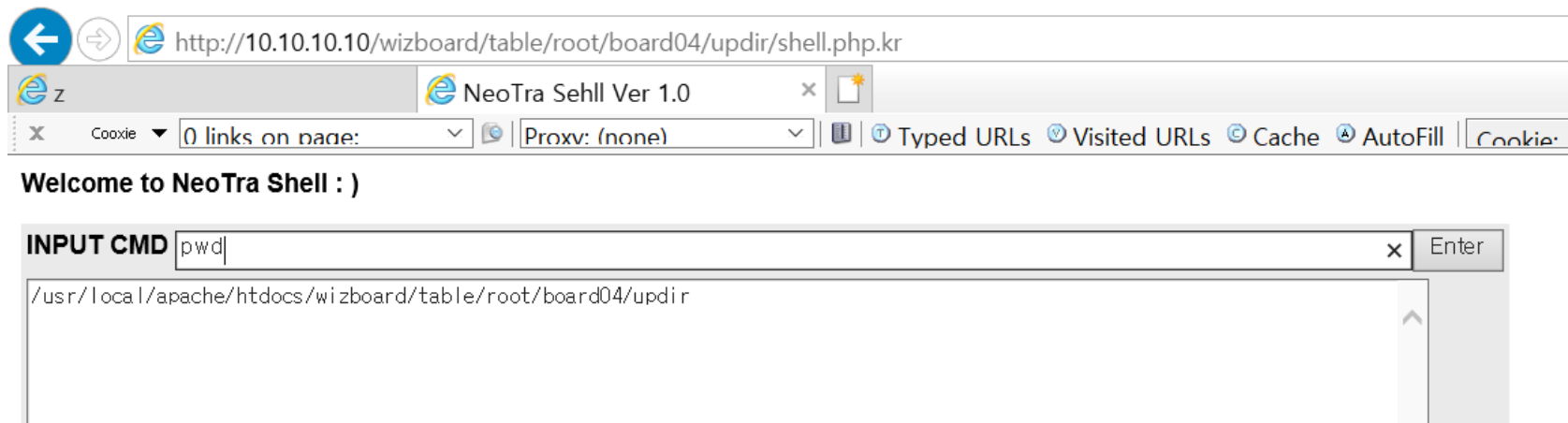




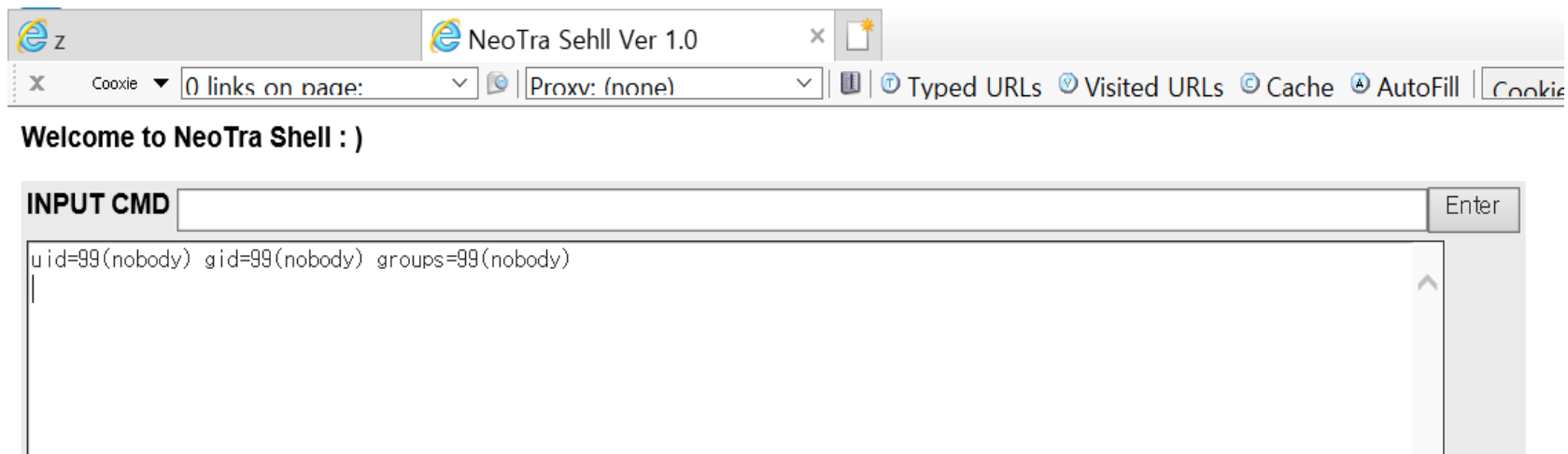
제목	z		
글쓴이	1111	이메일	z
z			
첨부파일	shell.php.kr		

php 확장자를 php.kr로 등록했을 때 php로 실행이 되는 이유?

- .kr이라는 확장자는 존재하지 않기 때문에 php로 인식이 됨



리눅스 명령어 실행됨



Nobody 권한 가짐

Welcome to NeoTra Shell :)

INPUT CMD `ps -ef | grep httpd`

root	2892	1	0	18:23	?	00:00:00	/usr/local/apache/bin/httpd
nobody	2903	2892	0	18:23	?	00:00:00	/usr/local/apache/bin/httpd
nobody	2904	2892	0	18:23	?	00:00:00	/usr/local/apache/bin/httpd
nobody	2905	2892	0	18:23	?	00:00:00	/usr/local/apache/bin/httpd
nobody	2906	2892	0	18:23	?	00:00:00	/usr/local/apache/bin/httpd
nobody	2907	2892	0	18:23	?	00:00:00	/usr/local/apache/bin/httpd
nobody	3052	2892	0	18:24	?	00:00:00	/usr/local/apache/bin/httpd
nobody	3053	2892	0	18:24	?	00:00:00	/usr/local/apache/bin/httpd
nobody	3054	2892	0	18:24	?	00:00:00	/usr/local/apache/bin/httpd
nobody	3055	2892	0	18:24	?	00:00:00	/usr/local/apache/bin/httpd
nobody	3056	2892	0	18:24	?	00:00:00	/usr/local/apache/bin/httpd
nobody	3265	2904	0	19:11	?	00:00:00	sh -c ps -ef grep httpd

nobody 권한을 갖고 있음이 확인됨

INPUT CMD `cat/etc/passwd`

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
rpm:x:37:37:/:/var/lib/rpm:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
mailnull:x:47:47:/:/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51:/:/var/spool/mqueue:/sbin/nologin
avahi:x:70:70:Avahi daemon:/:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
pcap:x:77:77:/:/var/arpwatch:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
mysql:x:500:500:/:/home/mysql:/bin/bash
```

Passwd 파일은 읽을 수 있지만 root 권한으로만 읽을 수 있는
shadow 파일은 읽을 수 없음

공부한 내용

□ 업로드 확장자 제한을 우회할 때

- Black List – 업로드 불가능한 확장자 리스트
- White List – 업로드 가능한 확장자 리스트



끝