레드팀 정찰의 핵심

by. arrester

Intro

김주원 (피리기: arrester)
엔키화이트햇 레드팀 내부침투 연구 파트장

Bug Hunter, CTF Player
- Web, Mobile, Internal Pentest, Cyber Weapon

GitHub: https://github.com/arrester
Blog: https://blog.naver.com/lstarrlodyl

Mail: jwkim@enki.co.kr
Mail: arresterloyal@gmail.com

Intro

C사, H사, K사, S사 등 침투테스트 및 레드팀 서비스 경험 다수

컨퍼런스 발표, 해킹대회 문제 출제 및 운영, 공공기관 및 대기업 대상 강의 다수

Intro

CTF Play

Digital Forensic Challenge 2024 8th (illusion)

HITCON CTF 2024 Quals 12th (Odin)

justCTF 2024 teaser 10th (Odin)

Midnight Sun CTF 2024 11th Finalist (Odin)

LINE CTF 2024 5th (Odin)

Insomni'hack teaser 2024 9th (Odin)

BlackHat MEA CTF 2023 Finalist(White_Hat_Kr)

WORMCON 0x01 CTF 8th(Demon)

…

Bug Hunting

BUGCAMP ??? XSS 2건

Wargame ??? XSS 1건

CVE-2024-37656

CVE-2024-37657

CVE-2024-37658

CVE-2024-???? (발급 대기)

…

레드팀 정찰의 핵심

- 레드팀이란?
- 레드팀 활동에서 정찰의 중요성
- 정찰 범위
- 서브도메인 수집 방법론
- 포트 스캔 전략

- 서버 환경 기술 분석
- 엔드포인트 분석
- 오픈소스 소개 및 비교
- SubSurfer
- Q & A

Quiz 1. 취약점을 찾을 때 선행되어야 하는 것은?

Quiz 1. 취약점을 찾을 때 선행되어야 하는 것은?

정보 수집

레드팀이란?

레드팀 활동에서 정찰의 중요성

A

RedTeam ENKI SERVICE

Red Team Service

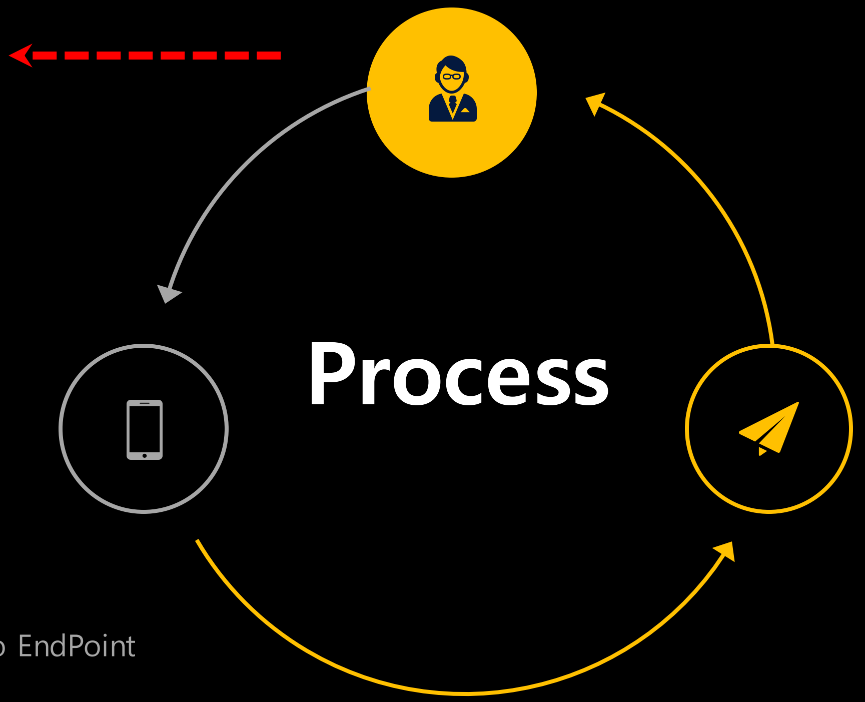
B

APT Group

C

Bug Bounty

레드팀 활동에서 정찰의 중요성: Red Team



Recon

Subdomain Scan

Port Scan

Web Server Scan

...

Process

Attack

SQL Injection, XSS, SSRF, XXE,

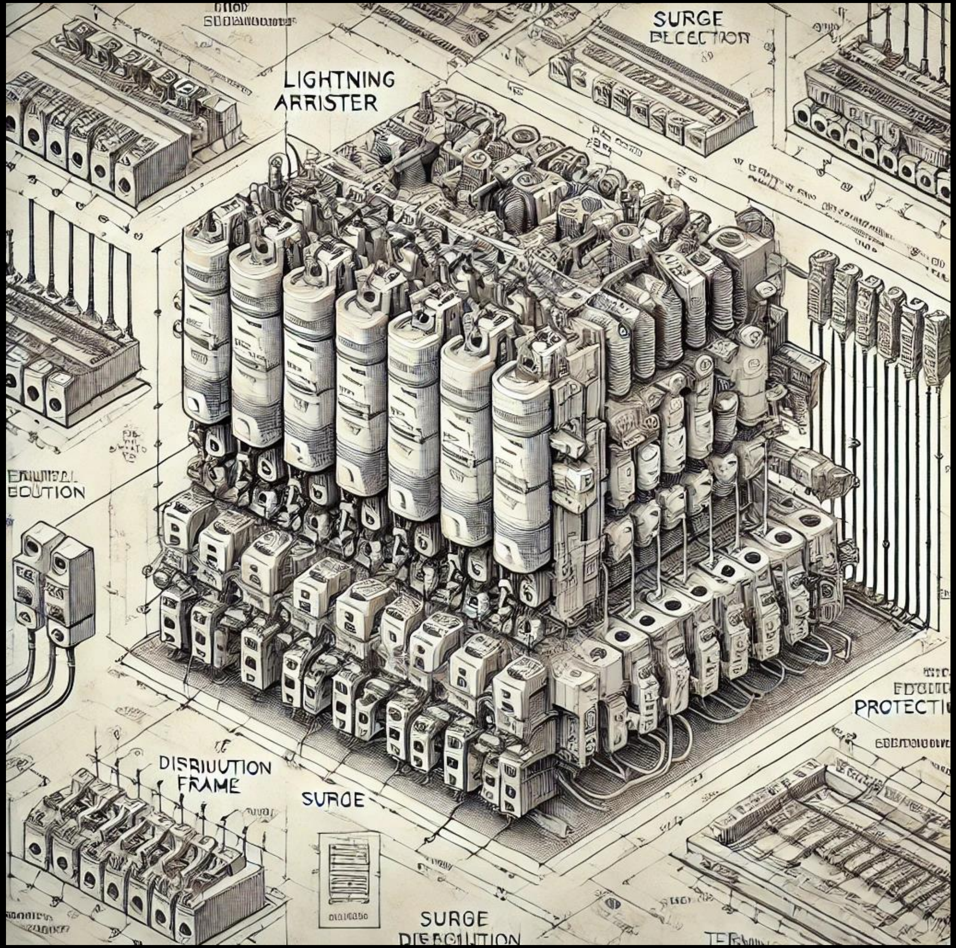
Command Injection ...

EndPoint

Recon Scan Result to EndPoint

Identification

레드팀 활동에서 정찰의 중요성: Red Team

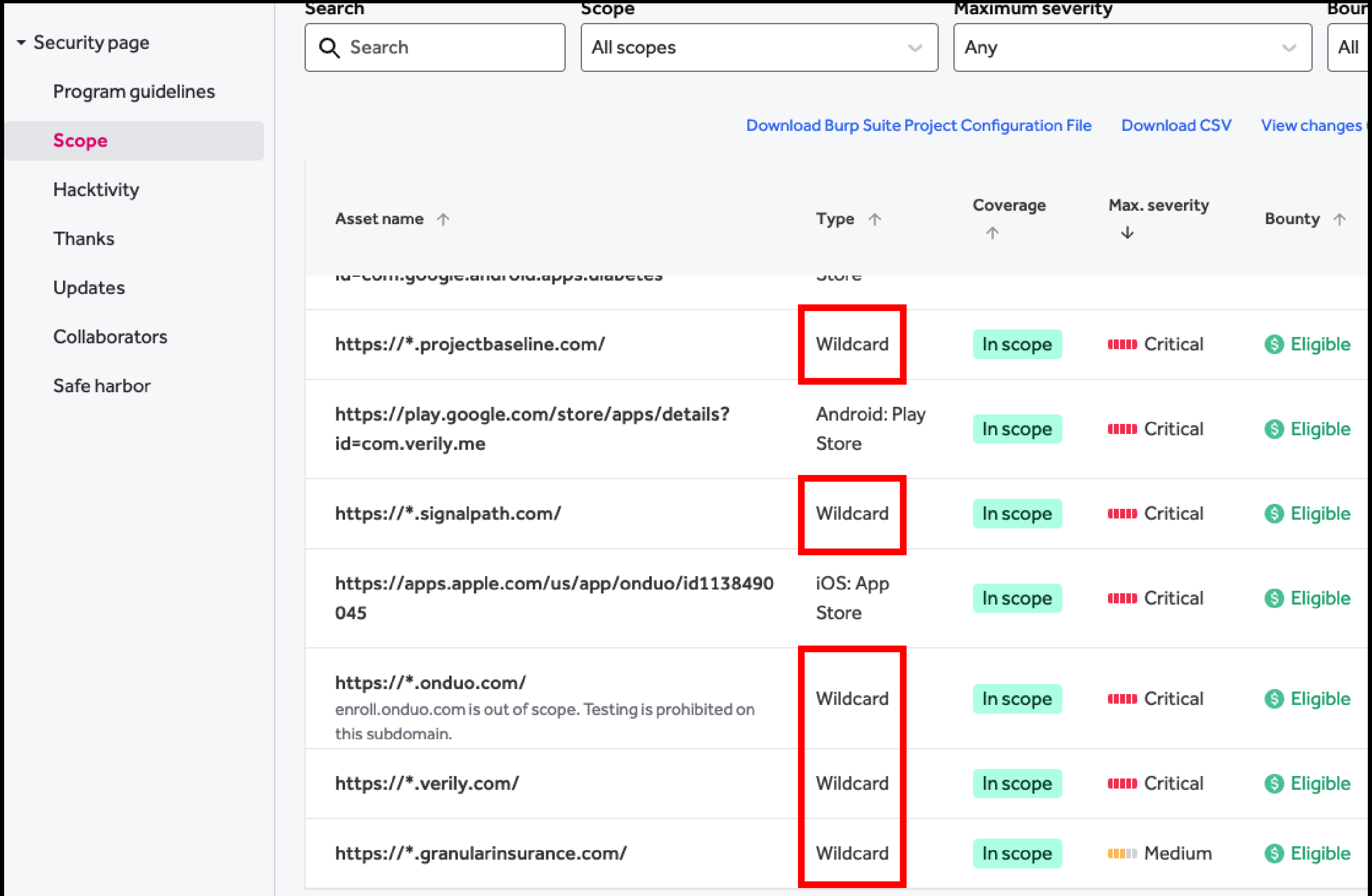


레드팀 활동에서 정찰의 중요성: APT Group

🇰🇵 Lazarus Group

🇷🇺 Cozy Bear(APT29)

레드팀 활동에서 정찰의 중요성: Bug Bounty



Search: Search

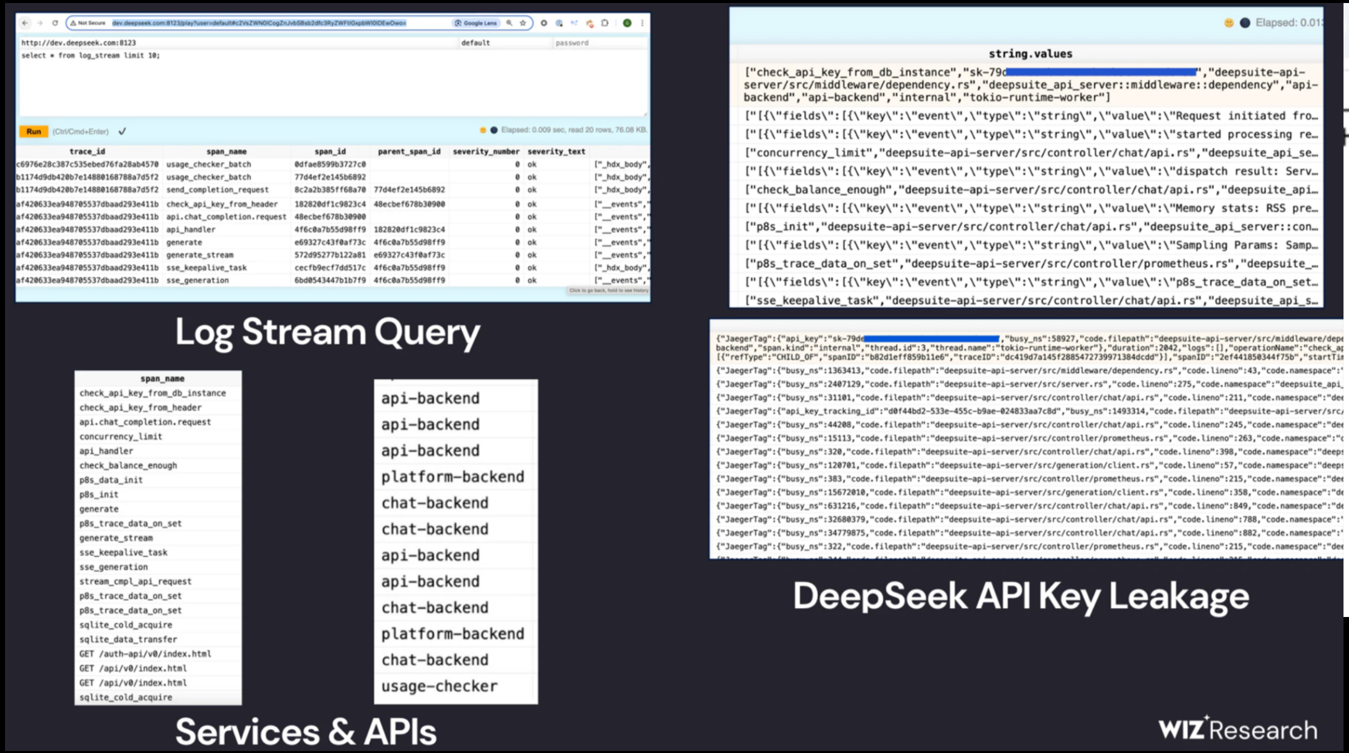
Scope: All scopes

Maximum severity: Any

Boun: All

Asset name	Type	Coverage	Max. severity	Bounty
id=com.google.android.apps.diabetes	Store			
https://*.projectbaseline.com/	Wildcard	In scope	Critical	Eligible
https://play.google.com/store/apps/details?id=com.verily.me	Android: Play Store	In scope	Critical	Eligible
https://*.signalpath.com/	Wildcard	In scope	Critical	Eligible
https://apps.apple.com/us/app/onduo/id1138490045	iOS: App Store	In scope	Critical	Eligible
https://*.onduo.com/ enroll.onduo.com is out of scope. Testing is prohibited on this subdomain.	Wildcard	In scope	Critical	Eligible
https://*.verily.com/	Wildcard	In scope	Critical	Eligible
https://*.granularinsurance.com/	Wildcard	In scope	Medium	Eligible

레드팀 활동에서 정찰의 중요성: 사례



Not Secure
dev.deepseek.com:8123/play?user=default#c2VsZWN0ICogZnJvbSBsb2dfc3RyZWFtIGxpbWl0IDEwOwo=
Google Lens

```
http://dev.deepseek.com:8123        default        password
select * from log_stream limit 10;
```

Elapsed: 0.009 sec, read 20 rows, 76.08 KB.

trace_id	span_name	span_id	parent_span_id	severity_number	severity_text	
c6976e28c387c535ebed76fa28ab4570	usage_checker_batch	0dfae8599b3727c0		0	ok	["_hdx_body",
b1174d9db420b7e14880168788a7d5f2	usage_checker_batch	77d4ef2e145b6892		0	ok	["_hdx_body",
b1174d9db420b7e14880168788a7d5f2	send_completion_request	8c2a2b385ff68a70	77d4ef2e145b6892	0	ok	["_hdx_body",
af420633ea948705537dbaad293e411b	check_api_key_from_header	182820df1c9823c4	48ecbef678b30900	0	ok	["__events","
af420633ea948705537dbaad293e411b	api.chat_completion.request	48ecbef678b30900		0	ok	["__events","
af420633ea948705537dbaad293e411b	api_handler	4f6c0a7b55d98ff9	182820df1c9823c4	0	ok	["__events","
af420633ea948705537dbaad293e411b	generate	e69327c43f0af73c	4f6c0a7b55d98ff9	0	ok	["__events","
af420633ea948705537dbaad293e411b	generate_stream	572d95277b122a81	e69327c43f0af73c	0	ok	["__events","
af420633ea948705537dbaad293e411b	sse_keepalive_task	cecfb9ecf7dd517c	4f6c0a7b55d98ff9	0	ok	["_hdx_body",
af420633ea948705537dbaad293e411b	sse_generation	6bd0543447b1b7f9	4f6c0a7b55d98ff9	0	ok	["__events","

Log Stream Query

span_name
check_api_key_from_db_instance
check_api_key_from_header
api.chat_completion.request
concurrency_limit
api_handler
check_balance_enough
p8s_data_init
p8s_init
generate
p8s_trace_data_on_set
generate_stream
sse_keepalive_task
sse_generation
stream_cmpl_api_request
p8s_trace_data_on_set
p8s_trace_data_on_set
sqlite_cold_acquire
sqlite_data_transfer
GET /auth-api/v0/index.html
GET /api/v0/index.html
GET /api/v0/index.html
sqlite_cold_acquire

```
api-backend
api-backend
api-backend
platform-backend
chat-backend
chat-backend
api-backend
api-backend
chat-backend
platform-backend
chat-backend
usage-checker
```

Services & APIs

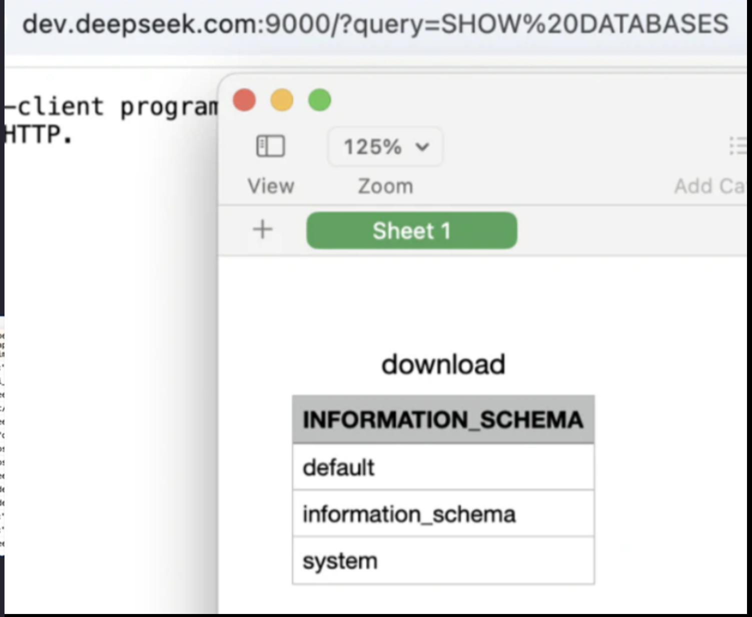
Elapsed: 0.01

```
string.values
["check_api_key_from_db_instance","sk-79d[redacted]","deepsuite-api-server/src/middleware/dependency.rs","deepsuite_api_server::middleware::dependency","api-backend","api-backend","internal","tokio-runtime-worker"]
["[{\"fields\":[{\"key\":\"event\",\"type\":\"string\",\"value\":\"Request initiated fro…
["[{\"fields\":[{\"key\":\"event\",\"type\":\"string\",\"value\":\"started processing re…
["concurrency_limit","deepsuite-api-server/src/controller/chat/api.rs","deepsuite_api_se…
["[{\"fields\":[{\"key\":\"event\",\"type\":\"string\",\"value\":\"dispatch result: Serv…
["check_balance_enough","deepsuite-api-server/src/controller/chat/api.rs","deepsuite_api…
["[{\"fields\":[{\"key\":\"event\",\"type\":\"string\",\"value\":\"Memory stats: RSS pre…
["p8s_init","deepsuite-api-server/src/controller/chat/api.rs","deepsuite_api_server::con…
["[{\"fields\":[{\"key\":\"event\",\"type\":\"string\",\"value\":\"Sampling Params: Samp…
["p8s_trace_data_on_set","deepsuite-api-server/src/controller/prometheus.rs","deepsuite_…
["[{\"fields\":[{\"key\":\"event\",\"type\":\"string\",\"value\":\"p8s_trace_data_on_set…
["sse_keepalive_task","deepsuite-api-server/src/controller/chat/api.rs","deepsuite_api_s…
```

```
{"JaegerTag":{"api_key":"sk-79d[redacted],"busy_ns":58927,"code.filepath":"deepsuite-api-server/src/middleware/depe
backend","span.kind":"internal","thread.id":3,"thread.name":"tokio-runtime-worker"},"duration":2042,"logs":[],"operationName":"check_ap
[{"refType":"CHILD_OF","spanID":"b82d1eff859b11e6","traceID":"dc419d7a145f2885472739971384dcdd"}],"spanID":"2ef441850344f75b","startTim
{"JaegerTag":{"busy_ns":1363413,"code.filepath":"deepsuite-api-server/src/middleware/dependency.rs","code.lineno":43,"code.namespace":"
{"JaegerTag":{"busy_ns":2407129,"code.filepath":"deepsuite-api-server/src/server.rs","code.lineno":275,"code.namespace":"deepsuite_api_
{"JaegerTag":{"busy_ns":31101,"code.filepath":"deepsuite-api-server/src/controller/chat/api.rs","code.lineno":211,"code.namespace":"dee
{"JaegerTag":{"api_key_tracking_id":"d0f44bd2-533e-455c-b9ae-024833aa7c8d","busy_ns":1493314,"code.filepath":"deepsuite-api-server/src/
{"JaegerTag":{"busy_ns":44208,"code.filepath":"deepsuite-api-server/src/controller/chat/api.rs","code.lineno":245,"code.namespace":"dee
{"JaegerTag":{"busy_ns":15113,"code.filepath":"deepsuite-api-server/src/controller/prometheus.rs","code.lineno":263,"code.namespace":"c
{"JaegerTag":{"busy_ns":320,"code.filepath":"deepsuite-api-server/src/controller/chat/api.rs","code.lineno":398,"code.namespace":"deeps
{"JaegerTag":{"busy_ns":120701,"code.filepath":"deepsuite-api-server/src/generation/client.rs","code.lineno":57,"code.namespace":"deeps
{"JaegerTag":{"busy_ns":383,"code.filepath":"deepsuite-api-server/src/controller/prometheus.rs","code.lineno":215,"code.namespace":"dee
{"JaegerTag":{"busy_ns":15672010,"code.filepath":"deepsuite-api-server/src/generation/client.rs","code.lineno":358,"code.namespace":"de
{"JaegerTag":{"busy_ns":631216,"code.filepath":"deepsuite-api-server/src/controller/chat/api.rs","code.lineno":849,"code.namespace":"de
{"JaegerTag":{"busy_ns":32680379,"code.filepath":"deepsuite-api-server/src/controller/chat/api.rs","code.lineno":788,"code.namespace":"
{"JaegerTag":{"busy_ns":34779875,"code.filepath":"deepsuite-api-server/src/controller/chat/api.rs","code.lineno":882,"code.namespace":"
{"JaegerTag":{"busy_ns":322,"code.filepath":"deepsuite-api-server/src/controller/prometheus.rs","code.lineno":215,"code.namespace":"dee
```

DeepSeek API Key Leakage

WIZ Research



dev.deepseek.com:9000/?query=SHOW%20DATABASES

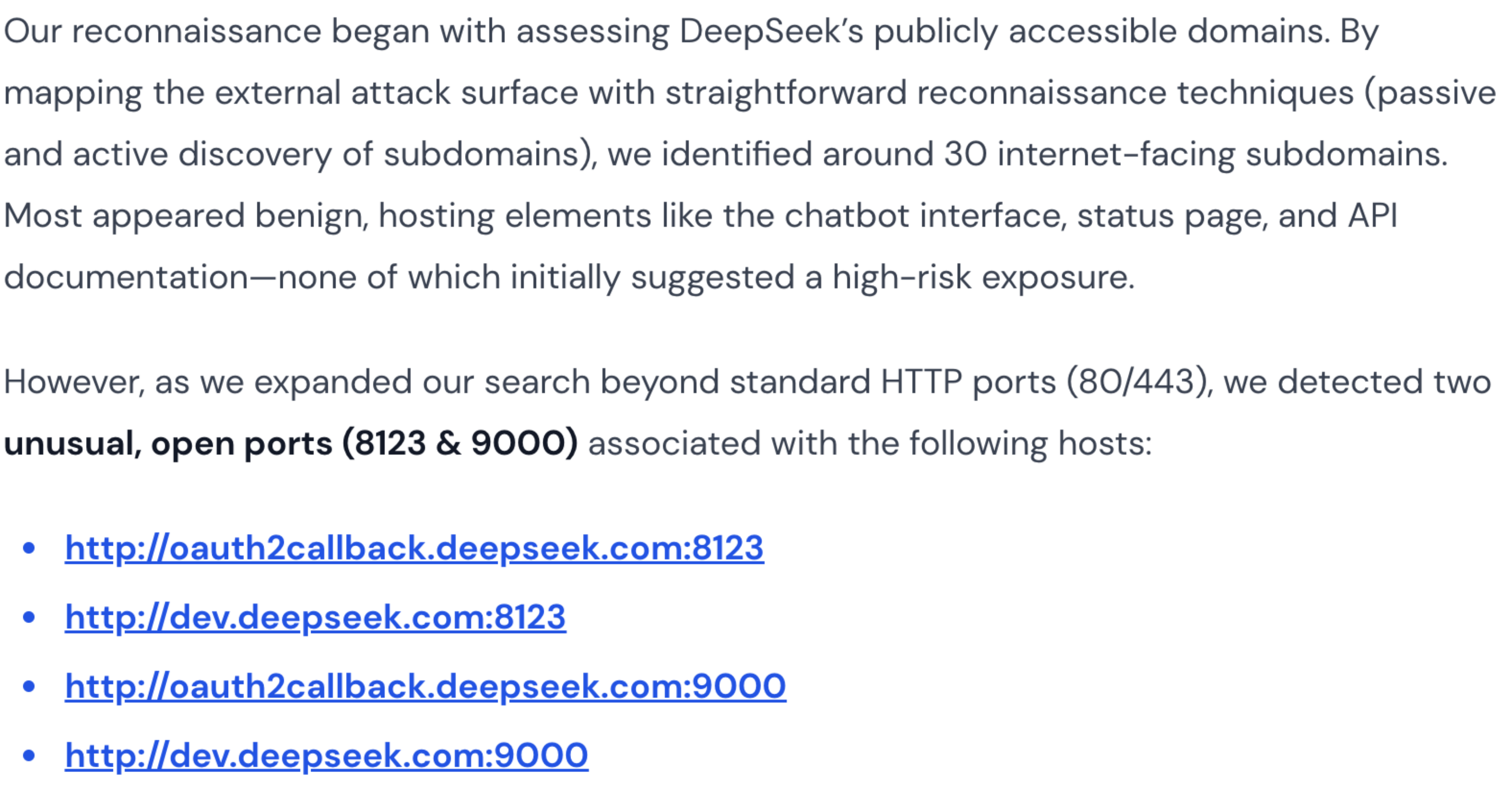
```
-client program
HTTP.
```

download

INFORMATION_SCHEMA
default
information_schema
system

Reference: https://www.wiz.io/blog/wiz-research-uncovers-exposed-deepseek-database-leak

레드팀 활동에서 정찰의 중요성: 사례



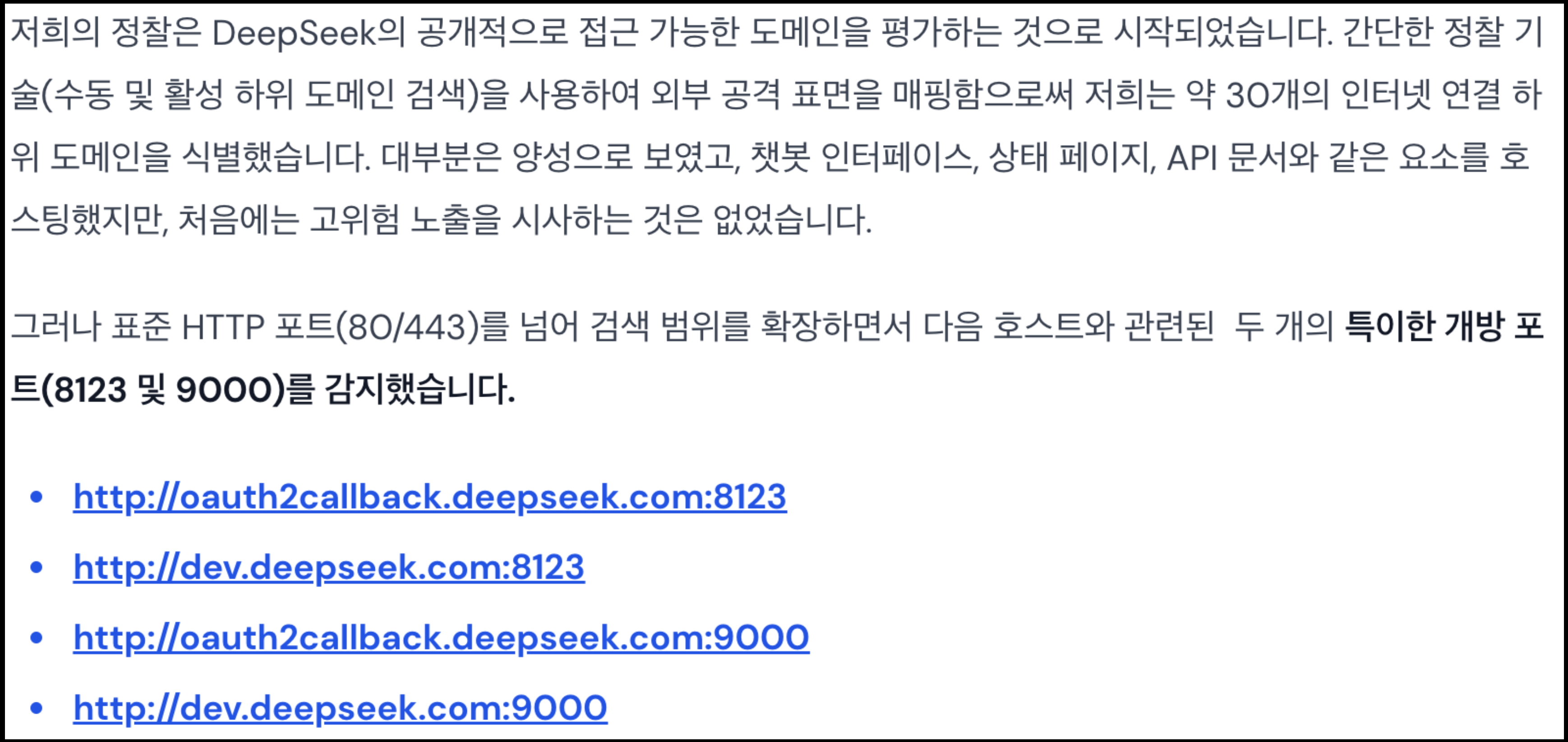
Our reconnaissance began with assessing DeepSeek's publicly accessible domains. By mapping the external attack surface with straightforward reconnaissance techniques (passive and active discovery of subdomains), we identified around 30 internet-facing subdomains. Most appeared benign, hosting elements like the chatbot interface, status page, and API documentation—none of which initially suggested a high-risk exposure.

However, as we expanded our search beyond standard HTTP ports (80/443), we detected two **unusual, open ports (8123 & 9000)** associated with the following hosts:

- http://oauth2callback.deepseek.com:8123
- http://dev.deepseek.com:8123
- http://oauth2callback.deepseek.com:9000
- http://dev.deepseek.com:9000

Reference: https://www.wiz.io/blog/wiz-research-uncovers-exposed-deepseek-database-leak

레드팀 활동에서 정찰의 중요성: 사례



저희의 정찰은 DeepSeek의 공개적으로 접근 가능한 도메인을 평가하는 것으로 시작되었습니다. 간단한 정찰 기술(수동 및 활성 하위 도메인 검색)을 사용하여 외부 공격 표면을 매핑함으로써 저희는 약 30개의 인터넷 연결 하위 도메인을 식별했습니다. 대부분은 양성으로 보였고, 챗봇 인터페이스, 상태 페이지, API 문서와 같은 요소를 호스팅했지만, 처음에는 고위험 노출을 시사하는 것은 없었습니다.

그러나 표준 HTTP 포트(80/443)를 넘어 검색 범위를 확장하면서 다음 호스트와 관련된 두 개의 **특이한 개방 포트(8123 및 9000)를 감지했습니다.**

- http://oauth2callback.deepseek.com:8123
- http://dev.deepseek.com:8123
- http://oauth2callback.deepseek.com:9000
- http://dev.deepseek.com:9000

Reference: https://www.wiz.io/blog/wiz-research-uncovers-exposed-deepseek-database-leak

정찰 범위

도메인

www.mobilehacking.kr

test.mobilehacking.kr

dev.mobilehacking.kr

포트 번호

www.mobilehacking.kr

- 80, 443, 8080

test.mobilehacking.kr

- 443, 8443, 8081

dev.mobilehacking.kr

- 10001, 10002, 10003

엔드포인트

https://www.mobilehacking.kr/test.php

https://test.mobilehacking.kr:8443/register.asp

http://dev.mobilehacking.kr:10001/login.do

정찰 범위

파라미터

test.php

register.asp(id, pw, name)

login.do(id, pw)

이메일

arrester@mobilehacking.kr

arresterloyal@mobilehacking.kr

redteam@mobilehacking.kr

ASN

AS12345

AS67890

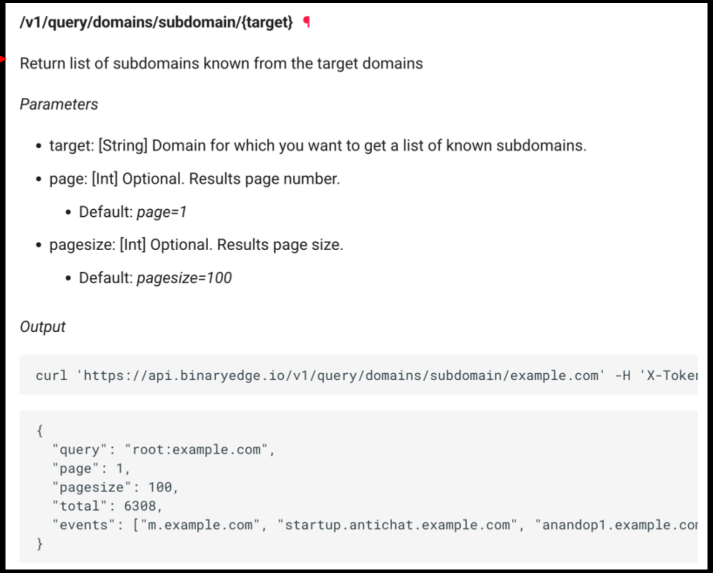
AS124578

서브도메인 수집 방법론

API DNS Certificate

Scrap Archive Whois

BinaryEdge



/v1/query/domains/subdomain/{target}

Return list of subdomains known from the target domains

Parameters

- target: [String] Domain for which you want to get a list of known subdomains.
- page: [Int] Optional. Results page number.
  - Default: *page=1*
- pagesize: [Int] Optional. Results page size.
  - Default: *pagesize=100*

Output

```
curl 'https://api.binaryedge.io/v1/query/domains/subdomain/example.com' -H 'X-Toke
```

```
{
  "query": "root:example.com",
  "page": 1,
  "pagesize": 100,
  "total": 6308,
  "events": ["m.example.com", "startup.antichat.example.com", "anandop1.example.co
}
```

서브도메인 수집 방법론

API

DNS

Certificate

Scrap

Archive

Whois

BinaryEdge

HACKER TARGET

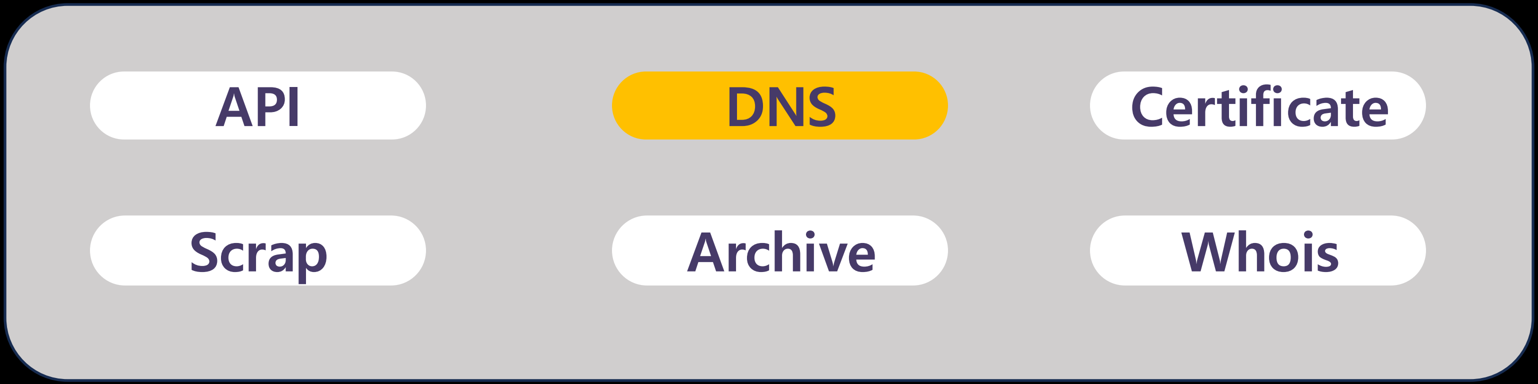
urlscan.io

LeakIX

ZoomEye

VIRUSTOTAL

서브도메인 수집 방법론



API

DNS

Certificate

Scrap

Archive

Whois

Reverse DNS Sweep

Zone walk

Brute Force(All)

Brute Force(wordlist)

SRV Record

서브도메인 수집 방법론

API

DNS

Certificate

Scrap

Archive

Whois

crt.sh

censys

sslmate

서브도메인 수집 방법론

API	DNS	Certificate
Scrap	Archive	Whois

AbuseIPDB

DNSDumpster.com

Complete DNS

HypeStat

서브도메인 수집 방법론

API

DNS

Certificate

Scrap

Archive

Whois

ARQUIVO.PT

INTERNET ARCHIVE

WayBackMachine

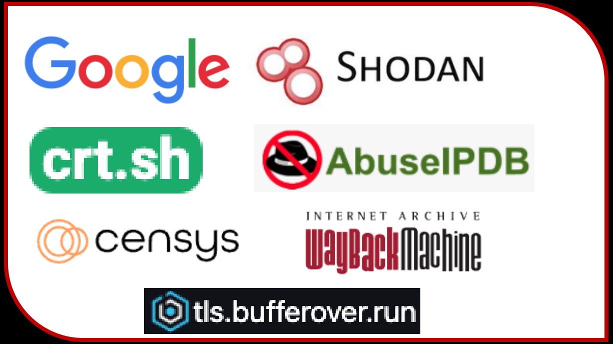
서브도메인 수집 방법론

API	DNS	Certificate
Scrap	Archive	Whois

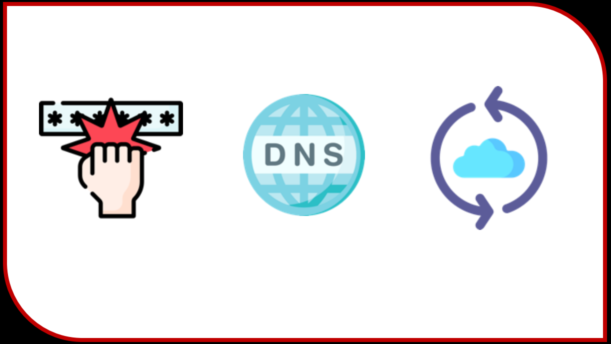
AlienVault

WhoisXMLAPI

서브도메인 수집 방법론



Passive



Active

포트 스캔 전략

대규모 스캔

22, 23, 24, 25 …

80, 81, 82, …

8080, 8443 …

masscan

상세 정보 스캔

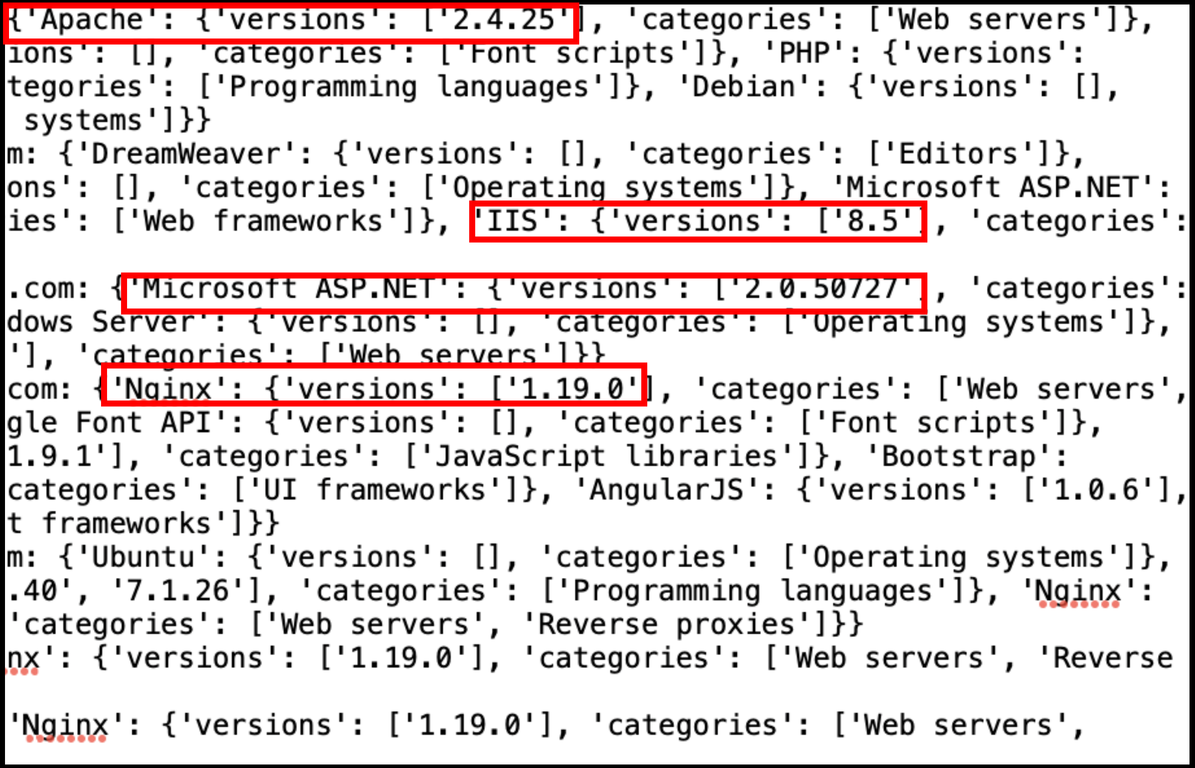
22 SSH OpenSSH 8.1 ver

80 HTTP Apache 2.4 ver

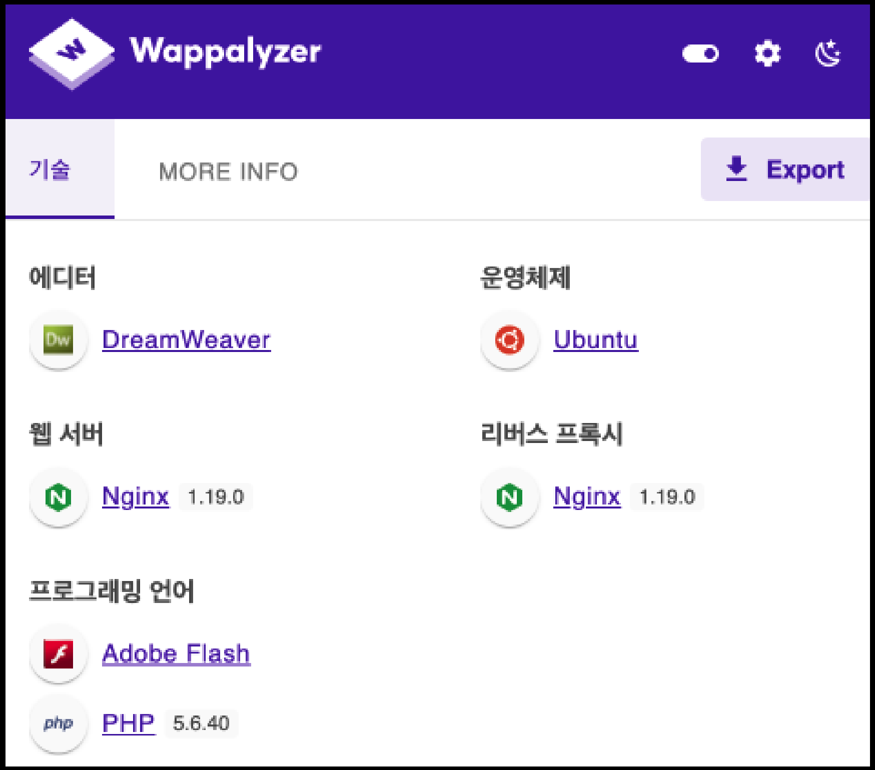
443 HTTPS Apache Tomcat 9.1

nmap

서버 환경 기술 분석



```
{'Apache': {'versions': ['2.4.25'], 'categories': ['Web servers']},
ions': [], 'categories': ['Font scripts']}, 'PHP': {'versions':
tegories': ['Programming languages']}, 'Debian': {'versions': [],
 systems']}}
m: {'DreamWeaver': {'versions': [], 'categories': ['Editors']},
ons': [], 'categories': ['Operating systems']}, 'Microsoft ASP.NET':
ies': ['Web frameworks']}, 'IIS': {'versions': ['8.5'], 'categories':

.com: {'Microsoft ASP.NET': {'versions': ['2.0.50727'], 'categories':
dows Server': {'versions': [], 'categories': ['Operating systems']},
'], 'categories': ['Web servers']}}
com: {'Nginx': {'versions': ['1.19.0'], 'categories': ['Web servers',
gle Font API': {'versions': [], 'categories': ['Font scripts']},
1.9.1'], 'categories': ['JavaScript libraries']}, 'Bootstrap':
categories': ['UI frameworks']}, 'AngularJS': {'versions': ['1.0.6'],
t frameworks']}}
m: {'Ubuntu': {'versions': [], 'categories': ['Operating systems']},
.40', '7.1.26'], 'categories': ['Programming languages']}, 'Nginx':
'categories': ['Web servers', 'Reverse proxies']}}
nx': {'versions': ['1.19.0'], 'categories': ['Web servers', 'Reverse

'Nginx': {'versions': ['1.19.0'], 'categories': ['Web servers',
```



Wappalyzer

기술 | MORE INFO | Export

에디터
- DreamWeaver

운영체제
- Ubuntu

웹 서버
- Nginx 1.19.0

리버스 프록시
- Nginx 1.19.0

프로그래밍 언어
- Adobe Flash
- PHP 5.6.40

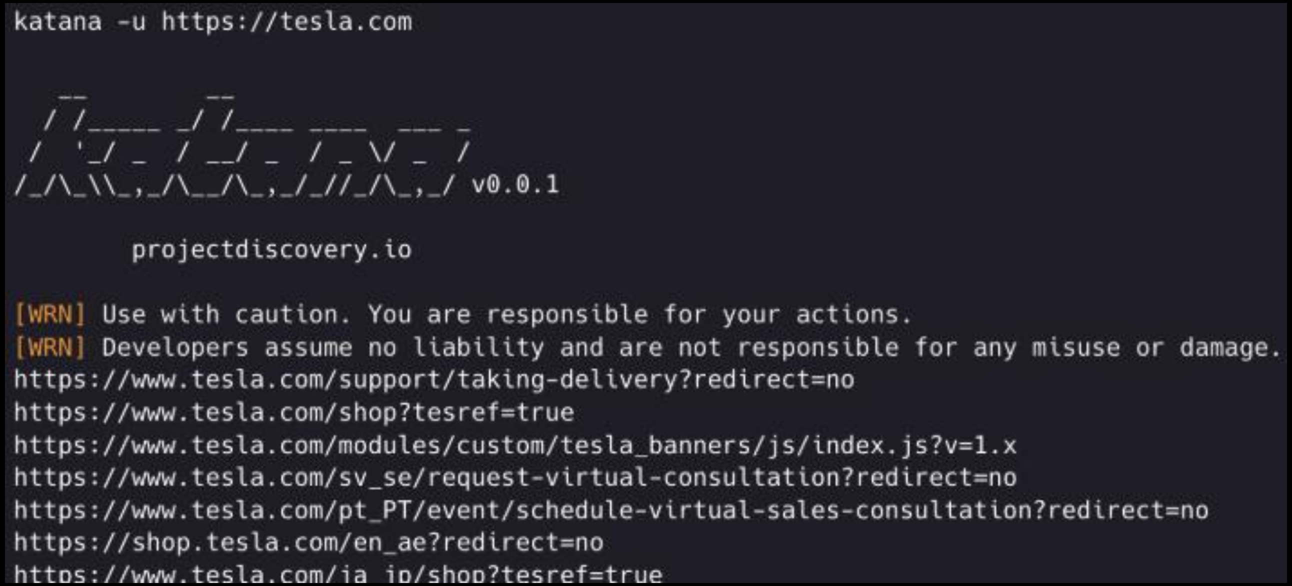
엔드포인트 분석

엔드포인트

https://www.mobilehacking.kr/test.php

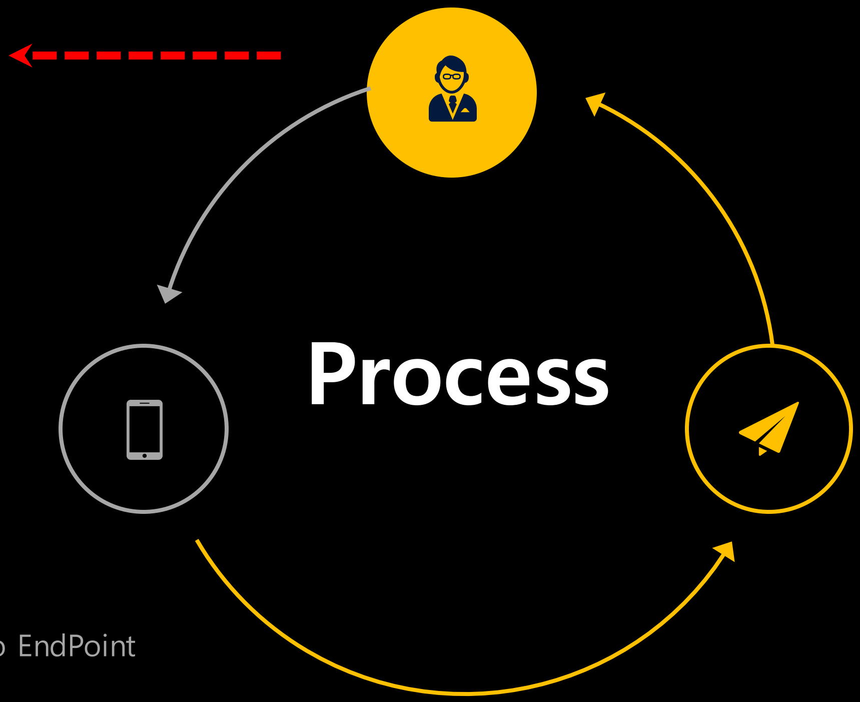
https://test.mobilehacking.kr:8443/register.asp

http://dev.mobilehacking.kr:10001/login.do



```
katana -u https://tesla.com


   __        __
  / /_____ _/ /____ ____  ___ _
 /  '_/ _  / __/ _  / _ \/ _  /
/_/\_\\_,_/\__/\_,_/_//_/\_,_/ v0.0.1

        projectdiscovery.io

[WRN] Use with caution. You are responsible for your actions.
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
https://www.tesla.com/support/taking-delivery?redirect=no
https://www.tesla.com/shop?tesref=true
https://www.tesla.com/modules/custom/tesla_banners/js/index.js?v=1.x
https://www.tesla.com/sv_se/request-virtual-consultation?redirect=no
https://www.tesla.com/pt_PT/event/schedule-virtual-sales-consultation?redirect=no
https://shop.tesla.com/en_ae?redirect=no
https://www.tesla.com/ja_jp/shop?tesref=true
```

레드팀 Process



Process

Recon

Subdomain Scan

Port Scan

Web Server Scan

...

EndPoint

Recon Scan Result to EndPoint

Identification

Attack

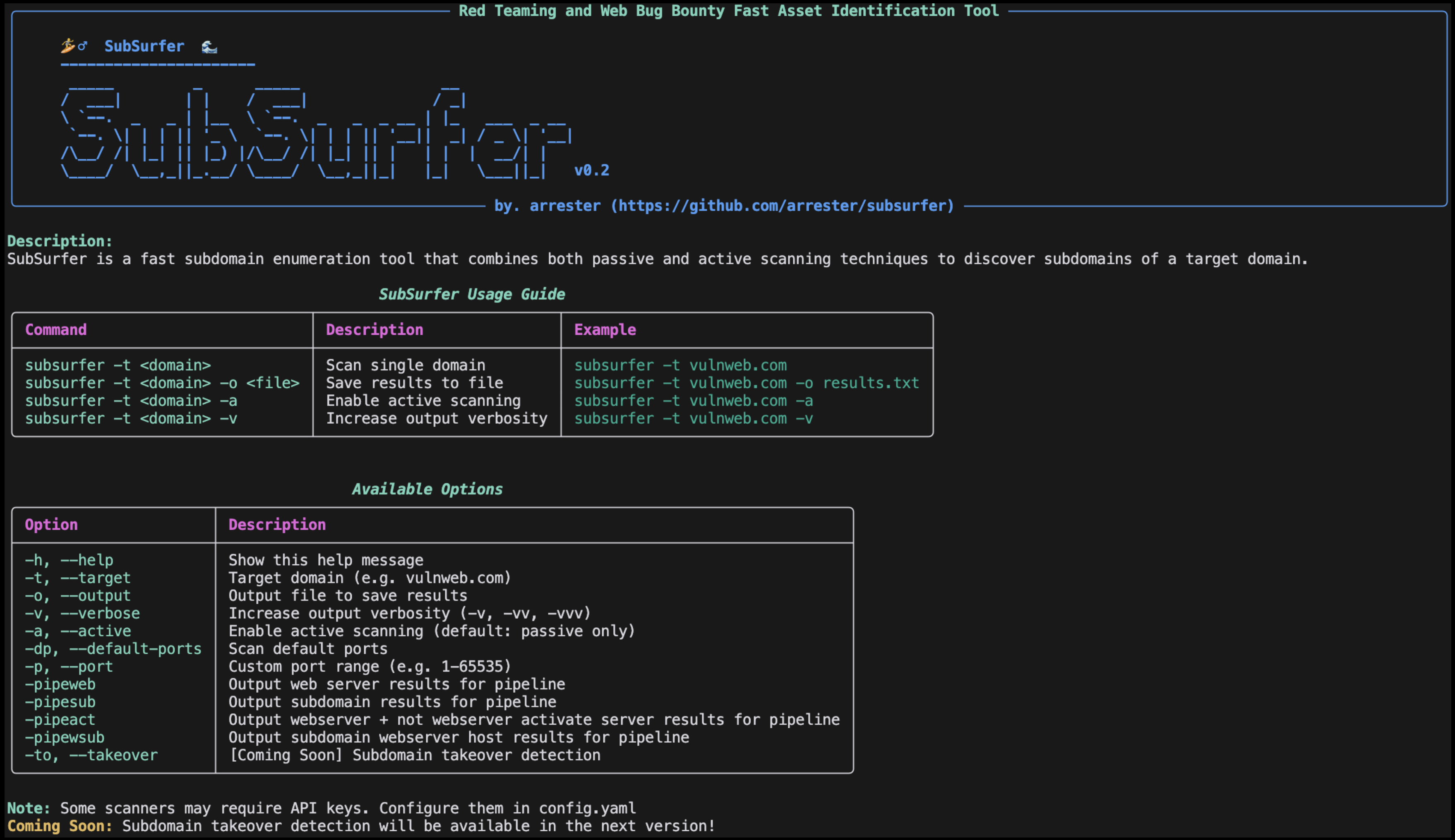
SQL Injection, XSS, SSRF, XXE,

Command Injection ...

오픈소스 소개 및 비교

도구 이름	특징	사용된 언어	모듈 사용	포트 스캔	환경 정보
Sublist3r	최근 업데이트 5년전, 비동기 지원X	Python	O	O	X
Amass	최근 업데이트 2년전, ASE 지원	Go	X	X	X
SubFinder	최근 업데이트 1달전, 다른 도구들과 연계하기 위한 pipe 옵션 지원	Go	X	X	X
Subdominator	최근 업데이트 2달전, 50개 이상 Passive 지원	Python	X	X	X

SubSurfer



```
─── Red Teaming and Web Bug Bounty Fast Asset Identification Tool ───

   🏄‍♂️  SubSurfer  🌊
   ──────────────────────
    _____       _     _____              __
   /  ___|     | |   /  ___|            / _|
   \ `--. _   _| |__ \ `--. _   _ _ __ | |_ ___ _ __
    `--. \ | | | '_ \ `--. \ | | | '__||  _/ _ \ '__|
   /\__/ / |_| | |_) /\__/ / |_| | |   | ||  __/ |
   \____/ \__,_|_.__/\____/ \__,_|_|   |_| \___|_|   v0.2

─── by. arrester (https://github.com/arrester/subsurfer) ───

Description:
SubSurfer is a fast subdomain enumeration tool that combines both passive and active scanning techniques to discover subdomains of a target domain.
```

SubSurfer Usage Guide

Command	Description	Example
subsurfer -t <domain>	Scan single domain	subsurfer -t vulnweb.com
subsurfer -t <domain> -o <file>	Save results to file	subsurfer -t vulnweb.com -o results.txt
subsurfer -t <domain> -a	Enable active scanning	subsurfer -t vulnweb.com -a
subsurfer -t <domain> -v	Increase output verbosity	subsurfer -t vulnweb.com -v

Available Options

Option	Description
-h, --help	Show this help message
-t, --target	Target domain (e.g. vulnweb.com)
-o, --output	Output file to save results
-v, --verbose	Increase output verbosity (-v, -vv, -vvv)
-a, --active	Enable active scanning (default: passive only)
-dp, --default-ports	Scan default ports
-p, --port	Custom port range (e.g. 1-65535)
-pipeweb	Output web server results for pipeline
-pipesub	Output subdomain results for pipeline
-pipeact	Output webserver + not webserver activate server results for pipeline
-pipewsub	Output subdomain webserver host results for pipeline
-to, --takeover	[Coming Soon] Subdomain takeover detection

Note: Some scanners may require API keys. Configure them in config.yaml
Coming Soon: Subdomain takeover detection will be available in the next version!

SubSurfer Develop?

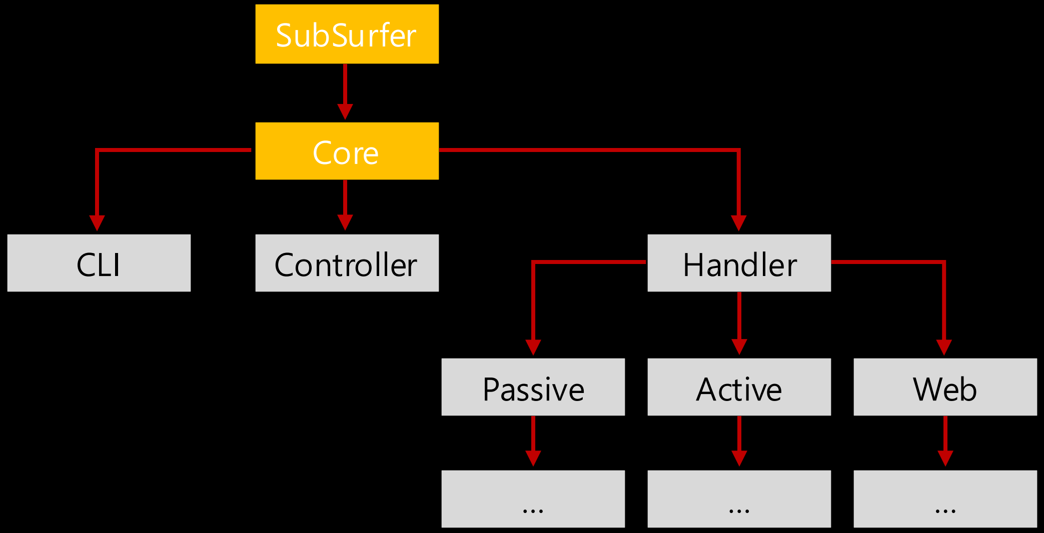
모듈화 및 계층적 구조

비동기 및 병렬 처리

파이프라인 지원

SubSurfer Develop?

모듈화 및 계층적 구조



SubSurfer

Core

CLI

Controller

Handler

Passive

Active

Web

…

…

…

비동기 및 병렬 처리

Async, Semaphore

파이프라인 지원

각 결과마다 pipe 지원

- Web Server Full result
- Subdomain result
- Activedomain result
- Web Server host result

SubSurfer 비교

도구 이름	특징	사용된 언어	모듈 사용	포트 스캔	환경 정보
SubSurfer	최근 업데이트 1주전, 비동기 및 병렬 지원, 다른 도구들과 연계하기 위한 pipe 옵션 지원	Python	O	O	O
Sublist3r	최근 업데이트 5년전, 비동기 지원X	Python	O	O	X
Amass	최근 업데이트 2년전, ASE 지원	Go	X	X	X
SubFinder	최근 업데이트 1달전, 다른 도구들과 연계하기 위한 pipe 옵션 지원	Go	X	X	X
Subdominator	최근 업데이트 2달전, 50개 이상 Passive 지원	Python	X	X	X

SubSurfer 활용 사례

A

RedTeam ENKI SERVICE

Red Team Service

gnuboard

Apache Tomcat®

youngcart

Confluence

Jenkins

spring

ASP.NET, Windows Server, Oracle WebLogic,
Apache Struts, Swagger-UI, …

SubSurfer 실습

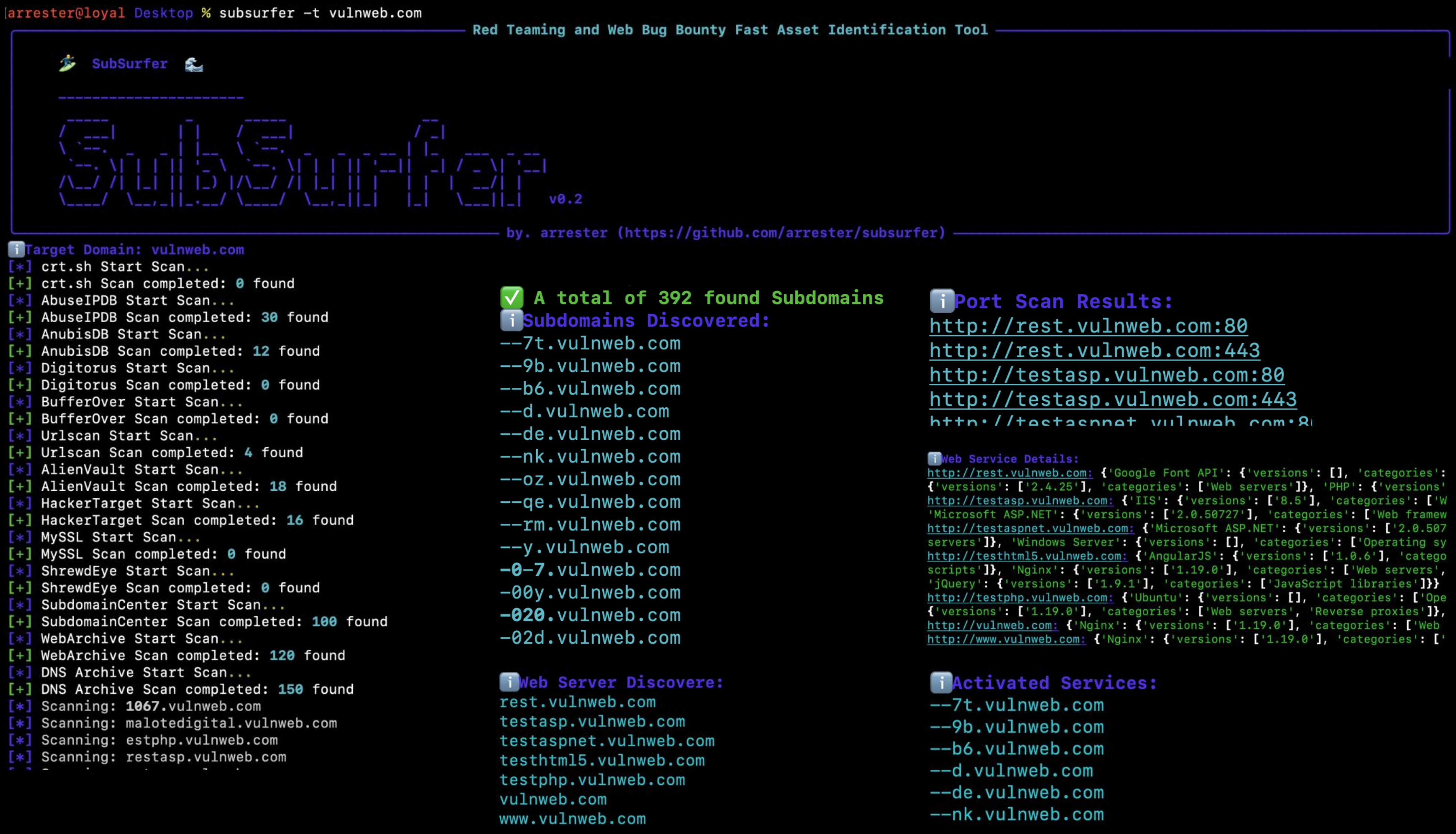
Windows: pip install subsurfer

Linux: pip3 install subsurfer

https://github.com/arrester/SubSurfer

SubSurfer 실습 (기본 옵션)

Command: subsurfer –t vulnweb.com



```
arrester@loyal Desktop % subsurfer -t vulnweb.com
 Red Teaming and Web Bug Bounty Fast Asset Identification Tool

    🏄 SubSurfer 🌊
    ------------------------
                                              v0.2
 by. arrester (https://github.com/arrester/subsurfer)
```

```
ℹ️Target Domain: vulnweb.com
[*] crt.sh Start Scan...
[+] crt.sh Scan completed: 0 found
[*] AbuseIPDB Start Scan...
[+] AbuseIPDB Scan completed: 30 found
[*] AnubisDB Start Scan...
[+] AnubisDB Scan completed: 12 found
[*] Digitorus Start Scan...
[+] Digitorus Scan completed: 0 found
[*] BufferOver Start Scan...
[+] BufferOver Scan completed: 0 found
[*] Urlscan Start Scan...
[+] Urlscan Scan completed: 4 found
[*] AlienVault Start Scan...
[+] AlienVault Scan completed: 18 found
[*] HackerTarget Start Scan...
[+] HackerTarget Scan completed: 16 found
[*] MySSL Start Scan...
[+] MySSL Scan completed: 0 found
[*] ShrewdEye Start Scan...
[+] ShrewdEye Scan completed: 0 found
[*] SubdomainCenter Start Scan...
[+] SubdomainCenter Scan completed: 100 found
[*] WebArchive Start Scan...
[+] WebArchive Scan completed: 120 found
[*] DNS Archive Start Scan...
[+] DNS Archive Scan completed: 150 found
[*] Scanning: 1067.vulnweb.com
[*] Scanning: malotedigital.vulnweb.com
[*] Scanning: estphp.vulnweb.com
[*] Scanning: restasp.vulnweb.com
```

```
✅ A total of 392 found Subdomains
ℹ️Subdomains Discovered:
--7t.vulnweb.com
--9b.vulnweb.com
--b6.vulnweb.com
--d.vulnweb.com
--de.vulnweb.com
--nk.vulnweb.com
--oz.vulnweb.com
--qe.vulnweb.com
--rm.vulnweb.com
--y.vulnweb.com
-0-7.vulnweb.com
-00y.vulnweb.com
-020.vulnweb.com
-02d.vulnweb.com
```

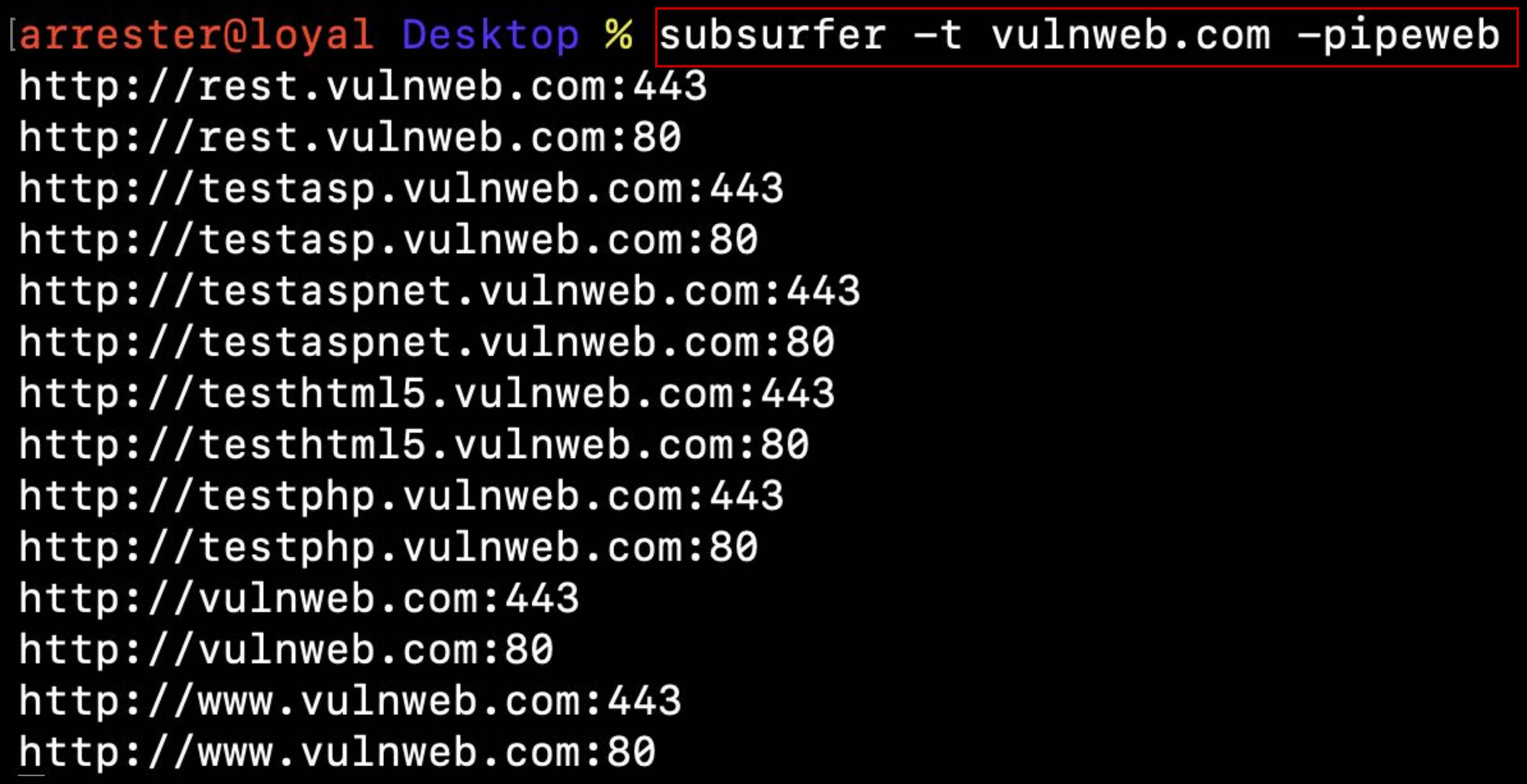
```
ℹ️Web Server Discovere:
rest.vulnweb.com
testasp.vulnweb.com
testaspnet.vulnweb.com
testhtml5.vulnweb.com
testphp.vulnweb.com
vulnweb.com
www.vulnweb.com
```

```
ℹ️Port Scan Results:
http://rest.vulnweb.com:80
http://rest.vulnweb.com:443
http://testasp.vulnweb.com:80
http://testasp.vulnweb.com:443
http://testaspnet.vulnweb.com:8
```

```
ℹ️Web Service Details:
http://rest.vulnweb.com: {'Google Font API': {'versions': [], 'categories':
{'versions': ['2.4.25'], 'categories': ['Web servers']}, 'PHP': {'versions'
http://testasp.vulnweb.com: {'IIS': {'versions': ['8.5'], 'categories': ['W
'Microsoft ASP.NET': {'versions': ['2.0.50727'], 'categories': ['Web framew
http://testaspnet.vulnweb.com: {'Microsoft ASP.NET': {'versions': ['2.0.507
servers']}, 'Windows Server': {'versions': [], 'categories': ['Operating sy
http://testhtml5.vulnweb.com: {'AngularJS': {'versions': ['1.0.6'], 'catego
scripts']}, 'Nginx': {'versions': ['1.19.0'], 'categories': ['Web servers',
'jQuery': {'versions': ['1.9.1'], 'categories': ['JavaScript libraries']}}
http://testphp.vulnweb.com: {'Ubuntu': {'versions': [], 'categories': ['Ope
{'versions': ['1.19.0'], 'categories': ['Web servers', 'Reverse proxies']},
http://vulnweb.com: {'Nginx': {'versions': ['1.19.0'], 'categories': ['Web
http://www.vulnweb.com: {'Nginx': {'versions': ['1.19.0'], 'categories': ['
```

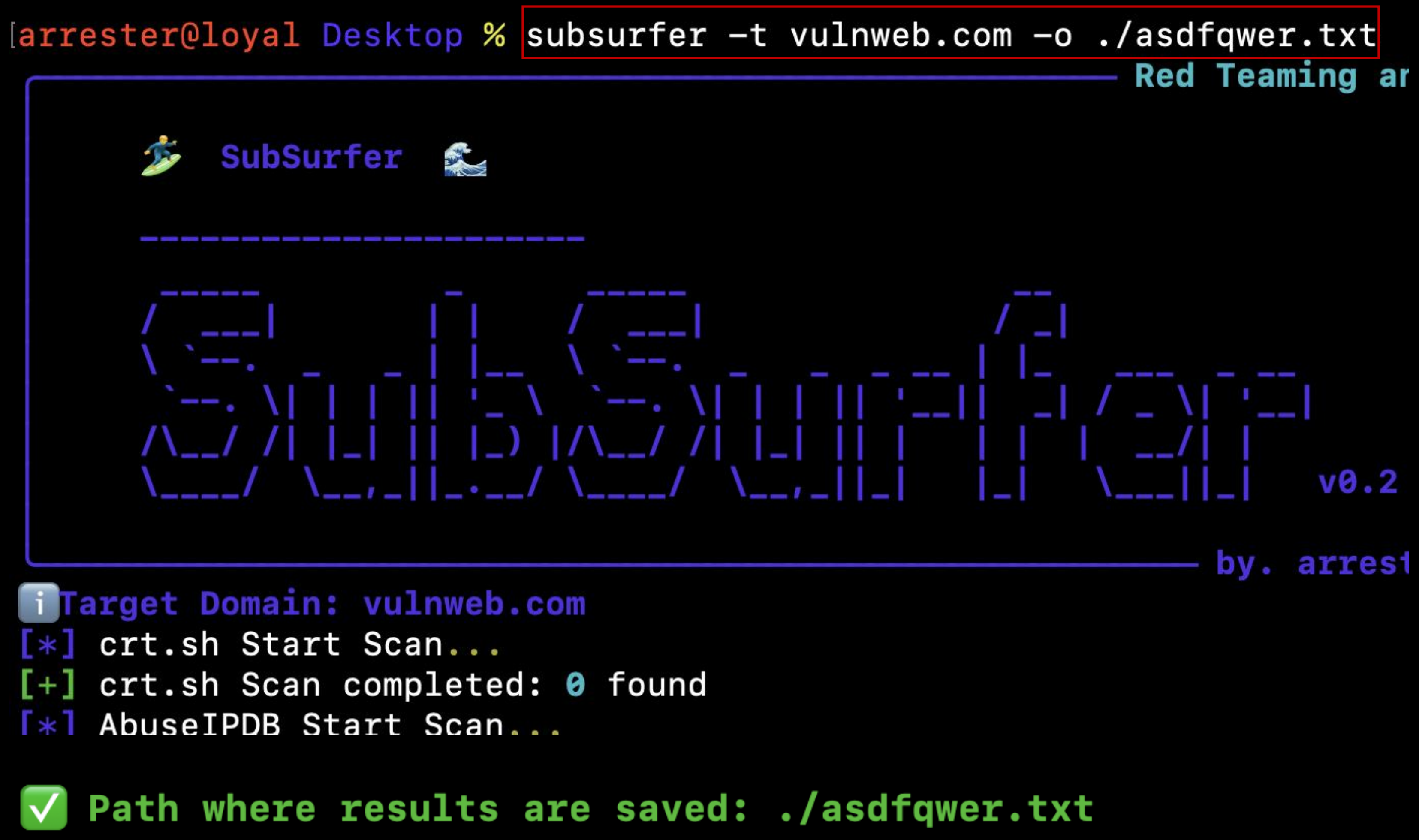
```
ℹ️Activated Services:
--7t.vulnweb.com
--9b.vulnweb.com
--b6.vulnweb.com
--d.vulnweb.com
--de.vulnweb.com
--nk.vulnweb.com
```

SubSurfer 실습 (-pipeweb 옵션)



```
arrester@loyal Desktop % subsurfer -t vulnweb.com -pipeweb
http://rest.vulnweb.com:443
http://rest.vulnweb.com:80
http://testasp.vulnweb.com:443
http://testasp.vulnweb.com:80
http://testaspnet.vulnweb.com:443
http://testaspnet.vulnweb.com:80
http://testhtml5.vulnweb.com:443
http://testhtml5.vulnweb.com:80
http://testphp.vulnweb.com:443
http://testphp.vulnweb.com:80
http://vulnweb.com:443
http://vulnweb.com:80
http://www.vulnweb.com:443
http://www.vulnweb.com:80
```

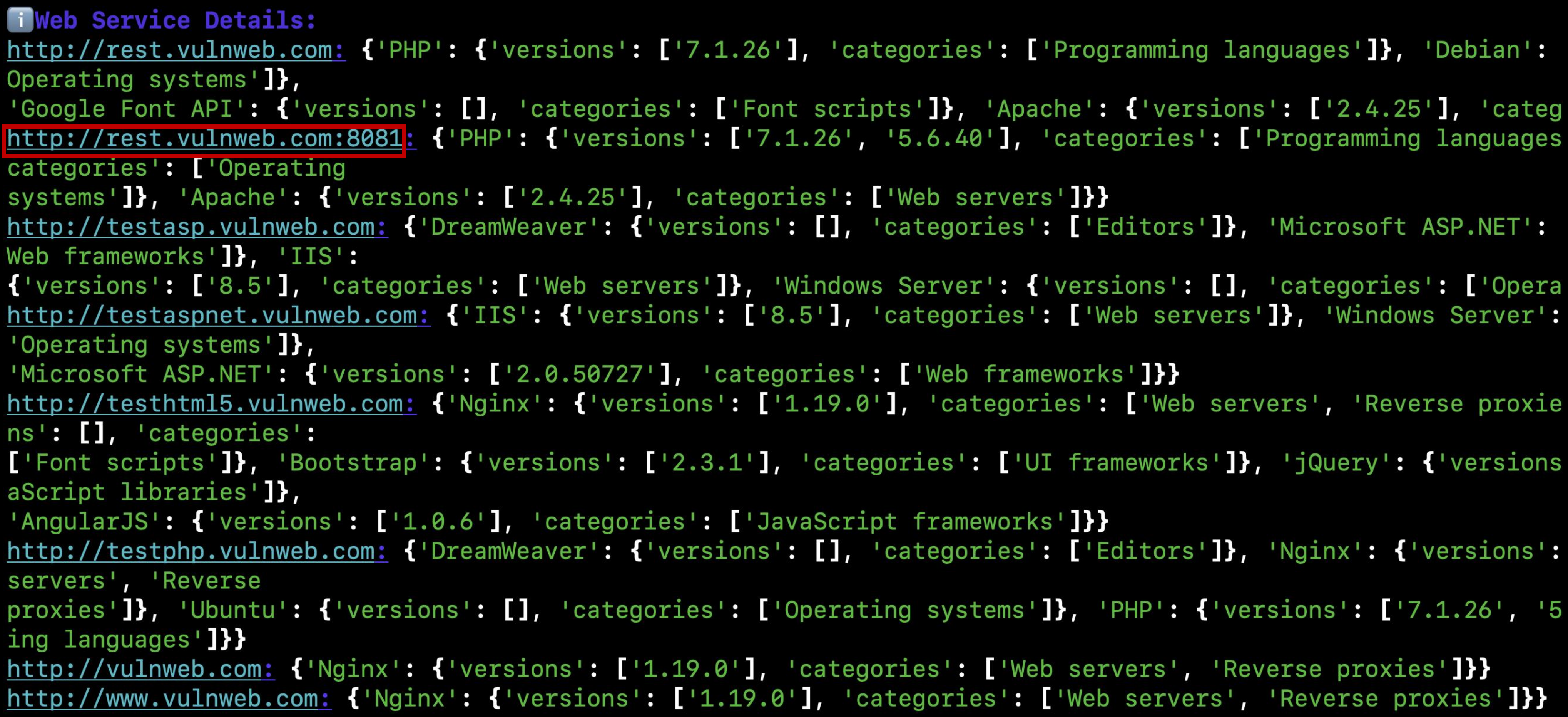
SubSurfer 실습 (-o 옵션)



```
arrester@loyal Desktop % subsurfer -t vulnweb.com -o ./asdfqwer.txt
                                                          Red Teaming ar

    🏄 SubSurfer 🌊

    ----------------------

     _____         _      _____               __
    /  ___|       | |    /  ___|             / _|
    \ `--.  _   _ | |__  \ `--.  _   _  _ __ | |_   ___  _ __
     `--. \| | | || '_ \  `--. \| | | || '__||  _| / _ \| '__|
    /\__/ /| |_| || |_) |/\__/ /| |_| || |   | |  |  __/| |
    \____/  \__,_||_.__/ \____/  \__,_||_|   |_|   \___||_|    v0.2

                                                              by. arrest
ℹ️Target Domain: vulnweb.com
[*] crt.sh Start Scan...
[+] crt.sh Scan completed: 0 found
[*] AbuseIPDB Start Scan...

✅ Path where results are saved: ./asdfqwer.txt
```

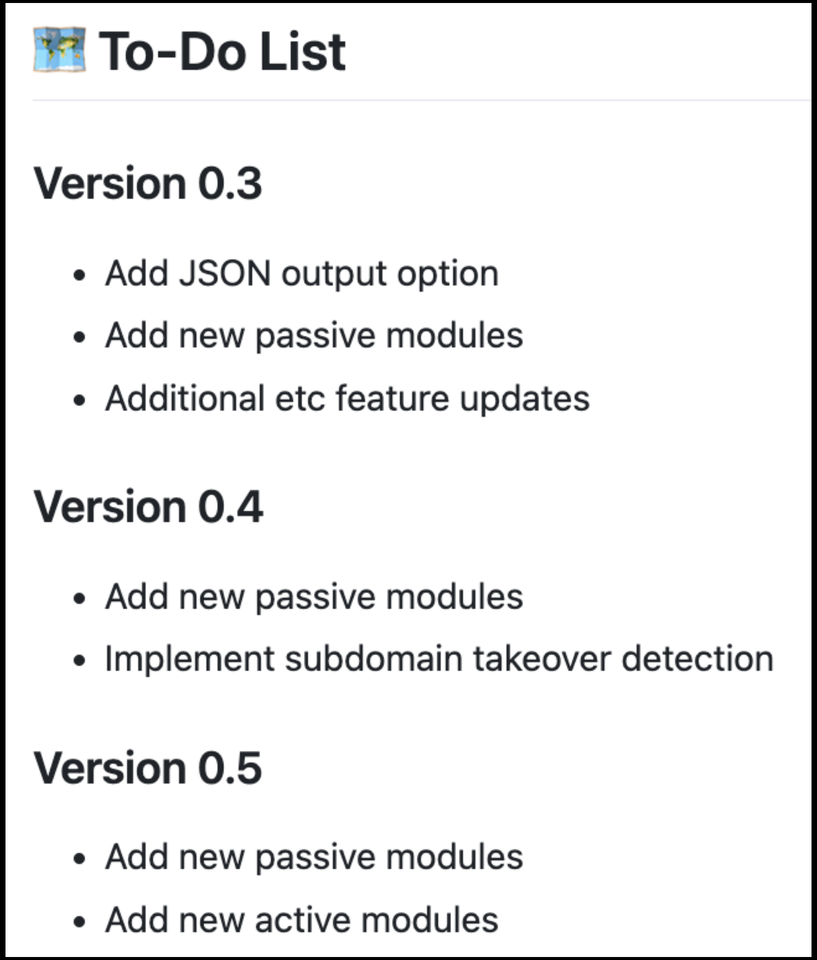
SubSurfer 실습 (포트 스캔)

Command: subsurfer –t vulnweb.com -p 80,8080,8081



```
ℹWeb Service Details:
http://rest.vulnweb.com: {'PHP': {'versions': ['7.1.26'], 'categories': ['Programming languages']}, 'Debian':
Operating systems']},
'Google Font API': {'versions': [], 'categories': ['Font scripts']}, 'Apache': {'versions': ['2.4.25'], 'categ
http://rest.vulnweb.com:8081: {'PHP': {'versions': ['7.1.26', '5.6.40'], 'categories': ['Programming languages
categories': ['Operating
systems']}, 'Apache': {'versions': ['2.4.25'], 'categories': ['Web servers']}}
http://testasp.vulnweb.com: {'DreamWeaver': {'versions': [], 'categories': ['Editors']}, 'Microsoft ASP.NET':
Web frameworks']}, 'IIS':
{'versions': ['8.5'], 'categories': ['Web servers']}, 'Windows Server': {'versions': [], 'categories': ['Opera
http://testaspnet.vulnweb.com: {'IIS': {'versions': ['8.5'], 'categories': ['Web servers']}, 'Windows Server':
'Operating systems']},
'Microsoft ASP.NET': {'versions': ['2.0.50727'], 'categories': ['Web frameworks']}}
http://testhtml5.vulnweb.com: {'Nginx': {'versions': ['1.19.0'], 'categories': ['Web servers', 'Reverse proxie
ns': [], 'categories':
['Font scripts']}, 'Bootstrap': {'versions': ['2.3.1'], 'categories': ['UI frameworks']}, 'jQuery': {'versions
aScript libraries']},
'AngularJS': {'versions': ['1.0.6'], 'categories': ['JavaScript frameworks']}}
http://testphp.vulnweb.com: {'DreamWeaver': {'versions': [], 'categories': ['Editors']}, 'Nginx': {'versions':
servers', 'Reverse
proxies']}, 'Ubuntu': {'versions': [], 'categories': ['Operating systems']}, 'PHP': {'versions': ['7.1.26', '5
ing languages']}}
http://vulnweb.com: {'Nginx': {'versions': ['1.19.0'], 'categories': ['Web servers', 'Reverse proxies']}}
http://www.vulnweb.com: {'Nginx': {'versions': ['1.19.0'], 'categories': ['Web servers', 'Reverse proxies']}}
```

SubSurfer To Do



🗺️ To-Do List

Version 0.3

- Add JSON output option
- Add new passive modules
- Additional etc feature updates

Version 0.4

- Add new passive modules
- Implement subdomain takeover detection

Version 0.5

- Add new passive modules
- Add new active modules

Quiz 2. SubSurfer에서 수집하지 않는 정보는?

(1) 웹 서버 정보

(2) 서브도메인

(3) 포트

(4) 엔드포인트

Quiz 2. SubSurfer에서 수집하지 않는 정보는?

엔드포인트

Q & A