

Week 28_ Shodan

Refactoring Study

2022.06.09 Kwon Moonjeong

사물인터넷이란?

- 사물인터넷(IoT) : 다른 사물과 데이터를 송수신할 수 있는 센서와 소프트웨어, 기타 기술을 장착하고 유/무선 네트워크로 서로 연결된 사물
→ 가전제품, 모바일 장비, 웨어러블 디바이스, 교통 신호기 등 다양한 임베디드 시스템을 이용한 장비들이 고유 식별자를 가지고 네트워크로 연결된 것
- 외부 환경으로부터의 데이터를 취득하기 위해 센서를 내장해야 함
- 고유의 식별자를 가진 장비들이 네트워크로 연결되었기 때문에 사물인터넷이 적용된 모든 사물이 해킹의 대상이 될 수 있음.
→ 사물인터넷이 발달할 수록 강력한 보안체계가 필요함

Shodan이란?

- 사물인터넷(IoT) 검색엔진으로, 인터넷에 연결된 장치의 위치, 네트워크 정보, 보안 정보 확인 가능
- 쇼단의 크롤러가 인터넷을 사용하는 서버/열려 있는 장비의 포트로 배너를 수집하여 색인을 생성함.
- HTTP 서비스, FTP 서비스, SNMP 서비스 등 다양한 서비스로부터 배너 수집.
 - 배너란? 쇼단이 찾을 수 있는 장치의 서비스를 설명하는 텍스트.
서비스의 유형에 따라 달라짐.
 - ex) HTTP 서비스의 배너. UNIX 서버, 아파치 웹서버를 사용하고 있음.

```
HEAD / HTTP/1.1 200 OK /# service list
HTTP/1.1 408 Request Timeout
Date: Wed, 20 Oct 2018 15:09:28 GMT
Server: Apache/2.4.34 (Unix)
Connection: close /# service ssh restart
Content-Type: text/html; charset=iso-8859-1
```

Shodan이란?

- 쇼단은 IoT의 취약점을 발견하여 보안을 강화할 목적으로 만들어졌으나, 보안 상태가 취약한 기기를 해킹하는 데에 사용한다면 개인 정보 유출 및 사생활 침해 문제를 초래할 수 있음
 - ex) '웹캠' 이라는 키워드 필터로 웹캠을 검색하여 사생활 노출 가능
 - ex) '초기 패스워드' 필터를 통해서 장비의 기본 패스워드를 찾아 무차별 대입 공격 가능
'국가' 키워드로 특정 국가의 장비를 검색 가능, '도시' 키워드로 특정 도시의 장비 검색 가능
- Shodan 검색 방법
 - 불린 연산자('+', '-', '|') 사용 (기본적으로 모든 검색 용어에 "+" 연산자가 포함됨)
 - 쇼단은 다양한 필터를 제공하여 인터넷과 연결된 IoT 장치를 쉽게 찾도록 도와주며, 모든 필터는 'filter:value' 형식을 가지고 있음 (":" 전후에는 띄어쓰기를 하지 않음)

Shodan 필터 종류

필터명	설명	검색 방법	사용 예시
city	도시 검색	city:"도시 이름"	apache city:"Seoul"
country	국가 검색	country:2자리의 국가 코드	apache country:DE,CH,FR
hostname	호스트 이름 검색	hostname:호스트네임	hostname:google.com,facebook.com
org	기관 검색	org:"기관명"	org:"Korea Telecom"
net	서브넷 검색	net:네트워크 CIDR	net:198.133.219.0/24
port	포트 검색	port:포트번호	ssh port:21
product	소프트웨어/서비스 이름	product:소프트웨어나 서비스의 이름	product:Apache
http.title	웹 사이트 이름 검색	http.title:웹 사이트의 이름	http.title:naver
vuln	취약점을 가지고 있는 서비스 검색	vuln:CVE코드	vuln:CVE-2014-0160
http.html	HTML 코드에 특정 단어를 가지고 있는 사이트 검색	http.html:특정 단어	http.html:Apache

검색 예시 1) webcam country:KR

shodan.io/search?query=webcam+country%3AKR+

Shodan Maps Images Monitor Developer More...

SHODAN Explore Downloads Pricing webcam country:KR Account

TOTAL RESULTS

148

TOP CITIES

Daegu	30
Seoul	30
Cheongju-si	16
Incheon	6
Busan	5
More...	

TOP PORTS

8080	36
8081	13
8181	5
1024	3
8083	3
More...	

TOP ORGANIZATIONS

Korea Telecom	69
SK Broadband Co Ltd	44
LG POWERCOMM	23

View Report Browse Images View on Map

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

221.139.180.138

SK Broadband Co Ltd
Korea, Republic of, Seoul

self-signed

SSL Certificate

Issued By:
Common Name:
IP Webcam

Issued To:
Common Name:
IP Webcam

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 401 Unauthorized
Content-Length: 0
WWW-Authenticate: Digest realm="IP Webcam", nonce="1654631590", qop="auth"

2022-06-07T19:53:16.296439

180.229.196.104

LG POWERCOMM
Korea, Republic of, Suwon

self-signed

SSL Certificate

Issued By:
Common Name:
IP Webcam

Issued To:
Common Name:
IP Webcam

HTTP/1.1 401 Unauthorized
Content-Length: 0
WWW-Authenticate: Digest realm="IP Webcam", nonce="1654619917", qop="auth"

2022-06-07T18:38:38.787607

61.77.57.244

Korea Telecom
Korea, Republic of, Anyang-si

self-signed

SSL Certificate

Issued By:
Common Name:
IP Webcam

Issued To:
Common Name:
IP Webcam

HTTP/1.1 401 Unauthorized
Content-Length: 0
WWW-Authenticate: Digest realm="IP Webcam", nonce="1654611889", qop="auth"

2022-06-07T14:24:41.973896

검색 예시 1) webcam country:KR

shodan.io/host/221.139.180.138

221.139.180.138 Regular View Raw Data History

// TAGS self-signed // LAST SEEN: 2022-06-07

General Information

Country	Korea, Republic of
City	Seoul
Organization	SK Broadband Co Ltd
ISP	SK Broadband Co Ltd
ASN	AS9318

Open Ports

25 80 443 2000 8081 8291

// 25 / TCP -1970006096 | 2022-06-03T02:45:55,155821

0x000x0e0x190xc80xdd0xc80x870x000x000x000x00

// 443 / TCP 0 | 2022-05-18T05:45:01,500782

SSL Certificate

Certificate:

Date:

Version: 3 (0x2)

Serial Number: 4232008918183359359 (0x3abb1db05e9ab37f)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=na, ST=na, L=na, O=na, OU=na, CN=84940744a2dd.sn.mynetname.net

Validity

Not Before: Apr 23 07:47:31 2020 GMT

Not After: Apr 21 07:47:31 2030 GMT

Subject: C=na, ST=na, L=na, O=na, OU=na, CN=84940744a2dd.sn.mynetname.net

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

검색 예시 1) webcam country:KR

← → ↻ ⓘ 221.139.180.138:8081

Union SQL Injectio... 상황관제 접근해보... T Dig(DNS 조회) 메모용 [Net]

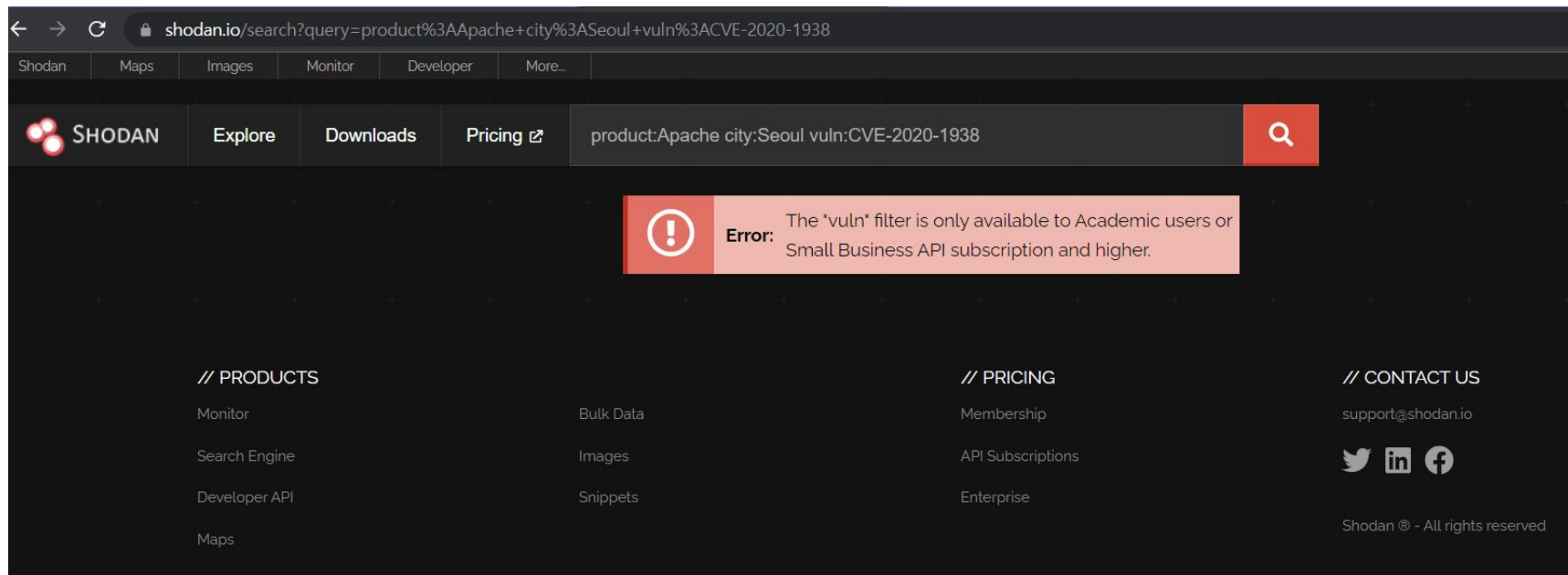
로그인

http://221.139.180.138:8081
이 사이트로의 연결은 비공개가 아닙니다.

사용자이름

비밀번호

검색 예시 2) Apache http.html:"tomcat"



vuln 필터는 유료 회원만 쓸 수 있다고 해서 다른 필터를 사용해보기로 함.
이 필터가 재미있어(?) 보였는데...

검색 예시 2) Apache http.html:"tomcat"

← → ↺

shodan.io/search?query=Apache+http.html%3A"tomcat"

Shodan


Maps

Images

Monitor

Developer


More...

 SHODAN

Explore

Downloads


Pricing ↗

Apache http.html:"tomcat" 

TOTAL RESULTS

173,893

TOP COUNTRIES




China	49,334
United States	33,284
Korea, Republic of	7,437
Germany	6,826
Brazil	6,278
More...	


View Report

View on Map


New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

 HTTP Status [404] â€œ [Not Found] ↗

54.209.239.2


walter-renderer.int.cloud.bb
c.co.uk
ec2-54-209-239-2.compute-
1.amazonaws.com
walter-renderer.int.api.bbc.c
o.uk
walter-renderer.int.api.bbc.c
om
nn2g8cbnfdbpbmc9mfmbkd
88h898262.bbc.co.uk
[Amazon.com, Inc.](#)
 United States, Ashburn


cloud

 SSL Certificate

Issued By:
|- Common Name:
Cloud Development
Servers and Services
|- Organization:
British Broadcasting
Corporation
Issued To:
|- Common Name:
nn2g8cbnfdbpbmc9mfmbkd88h898262.bbc.co.uk
|- Organization:
British Broadcasting
Corporation
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 404
Date: Thu, 09 Jun 2022 08:55:43 GMT
Server: **Apache/2.4.6** (CentOS) OpenSSL/1.0.2k-fips
Content-Type: text/html; charset=UTF-8
Content-Language: en
Content-Length: 1086

 Apache Tomcat/7.0.63 ↗

101.201.176.249
[Aliyun Computing Co., LTD](#)
 China, Beijing

HTTP/1.1 200 OK
Server: **Apache-Coyote/1.1**
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Thu, 09 Jun 2022 08:55:33 GMT

검색 예시 2) Apache http.html:"tomcat"

The screenshot displays the Shodan search results for the IP address 101.201.176.249. The interface includes a map of the location, a search bar, and a sidebar with general information and open ports.

General Information

Country	China
City	Beijing
Organization	Aliyun Computing Co., LTD
ISP	Hangzhou Alibaba Advertising Co.,Ltd.
ASN	AS37963

Open Ports

80

// 80 / TCP

Apache Tomcat/Coyote JSP engine 1.1

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Thu, 09 Jun 2022 08:55:33 GMT

검색 예시 2) Apache http.html:"tomcat"

주의 포함 | 101.201.176.249

[Home](#) [Documentation](#) [Configuration](#) [Examples](#) [Wiki](#) [Mailing Lists](#)

[Find Help](#)

Apache Tomcat/7.0.63



The Apache Software Foundation

<http://www.apache.org/>

If you're seeing this, you've successfully installed Tomcat. Congratulations!



Recommended Reading:

[Security Considerations HOW-TO](#)

[Manager Application HOW-TO](#)

[Clustering/Session Replication HOW-TO](#)

[Server Status](#)

[Manager App](#)

[Host Manager](#)

Developer Quick Start

[Tomcat Setup](#)

[First Web Application](#)

[Realms & AAA](#)

[JDBC DataSources](#)

[Examples](#)

[Servlet Specifications](#)

[Tomcat Versions](#)

Managing Tomcat

For security, access to the [manager.webapp](#) is restricted. Users are defined in:

`$CATALINA_HOME/conf/tomcat-users.xml`

In Tomcat 9.0 access to the manager application is split between different users.

[Read more...](#)

[Release Notes](#)

Documentation

[Tomcat 9.0 Documentation](#)

[Tomcat 9.0 Configuration](#)

[Tomcat Wiki](#)

Find additional important configuration information in:

`$CATALINA_HOME/RUNNING.txt`

Developers may be interested in:

Getting Help

[FAQ](#) and [Mailing Lists](#)

The following mailing lists are available:

[tomcat-announce](#)

Important announcements, releases, security vulnerability notifications. (Low volume).

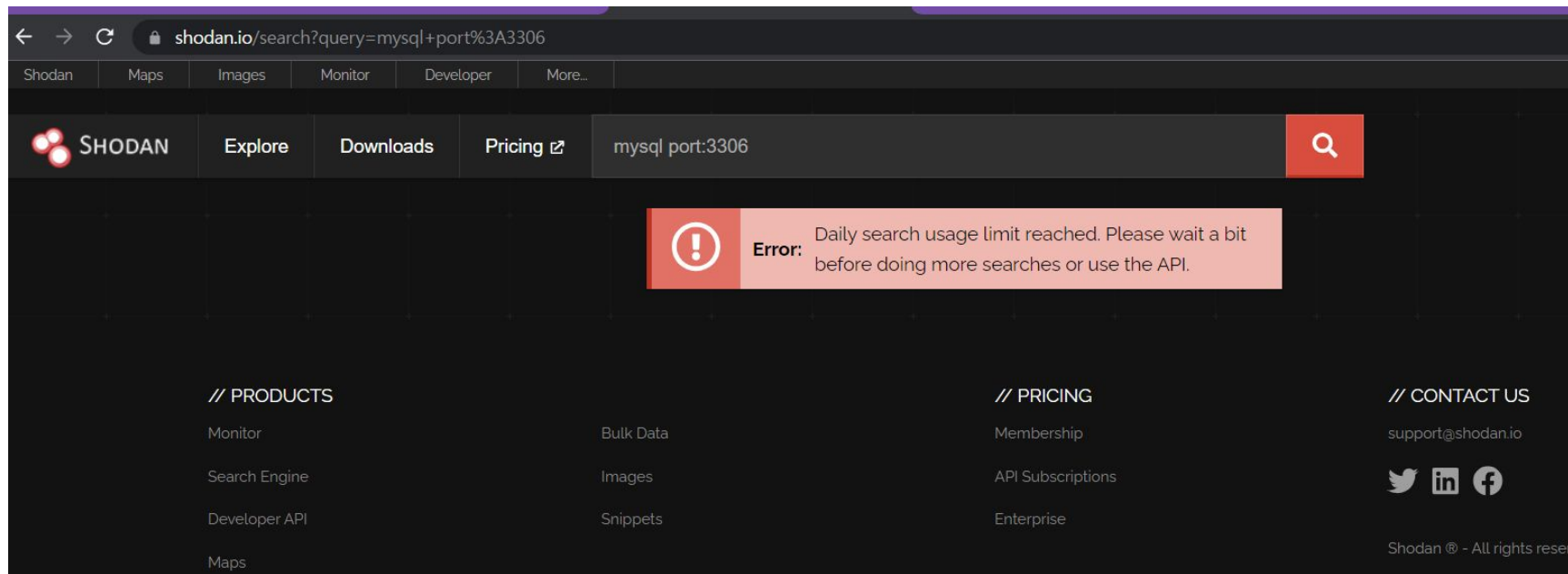
[tomcat-users](#)

User support and discussion

[taglibs-user](#)

User support and discussion for [Apache Taglibs](#)

검색 예시 3) product:mysql port:3306



- 무료 회원은 검색 횟수에도 제한이 있음