

---

# ASM

**그리고 버그헌팅 자동화**

# Contents

---

## ASM 이란?

- 자산 식별 기술
  - 도메인 확장 기술
  - IP 확장 기술
  - 오픈 소스 도구 활용
- 위협 평가 방법
- 버그헌팅 자동화

# # ASM 이란?

## ASM (Attack Surface Management)

사이버 보안 취약성과 잠재적 공격 벡터를 지속적으로 발견,  
분석, 해결 및 모니터링하는 활동

### 주제 선정 배경

- 클라우드 사용으로 ASM의 중요성이 커지며 많은 솔루션들이 오고 있음  
: Azure EASM, Google Mandiant ASM, IBM Randori 등
- 그리고 회사 업무로 리서치 중 😊

# # ASM 이란?

자산 식별 → 위협 탐지 -> 평가 → 조치



# # ASM 이란?

## 자산 식별

- 알려진 자산
- 알려지지 않은 자산 (**Shadow IT**)

### 식별 자산

IP Address

Domain

GithubRepository

Email

SSL Certificate

...

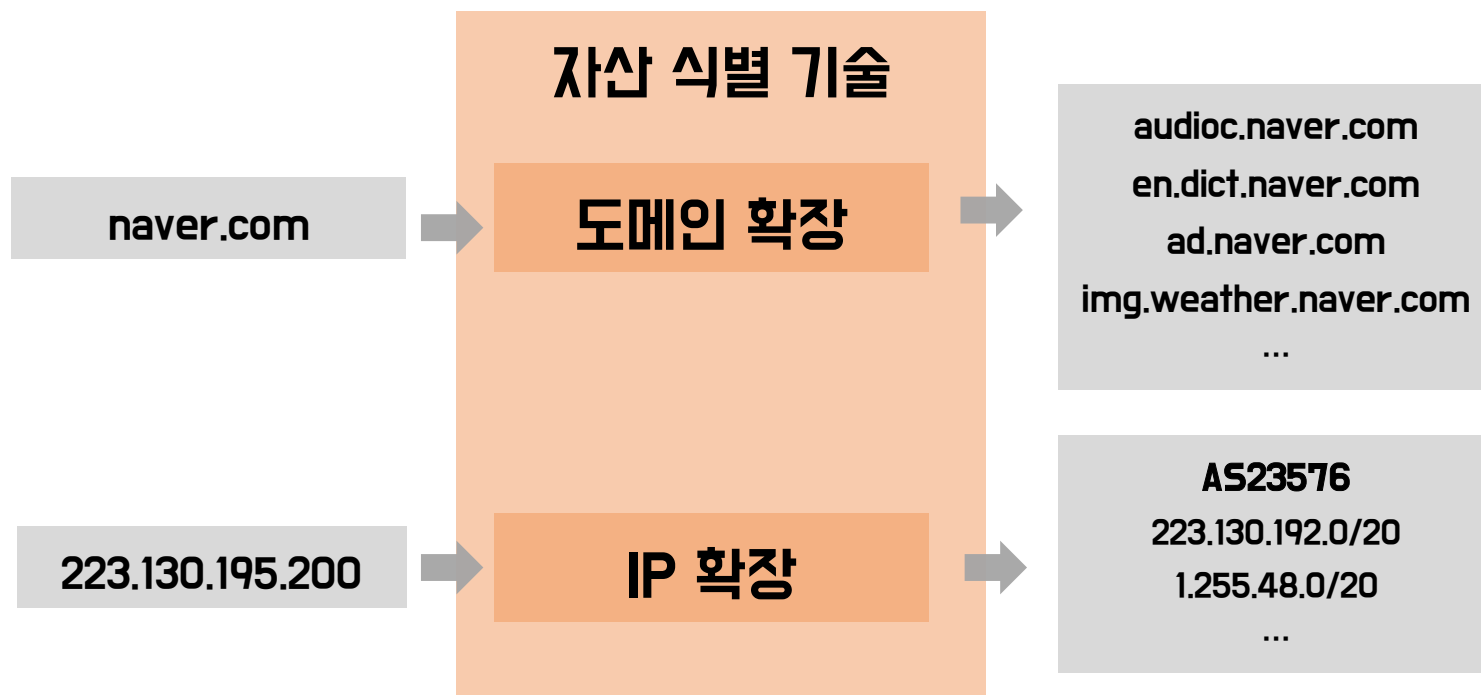
## 위협 평가

- Fingerprint 정보 수집
  - OS, framework 버전 정보 수집
- 취약점 진단
  - port scan
  - CVE 취약점 진단

# # 자산 식별 기술

## Shadow IT 란?

조직에서 승인되지 않은 or 인지하지 못하고 있는 IT 자산



# # 자산 식별 기술

---

## 도메인 확장 기술

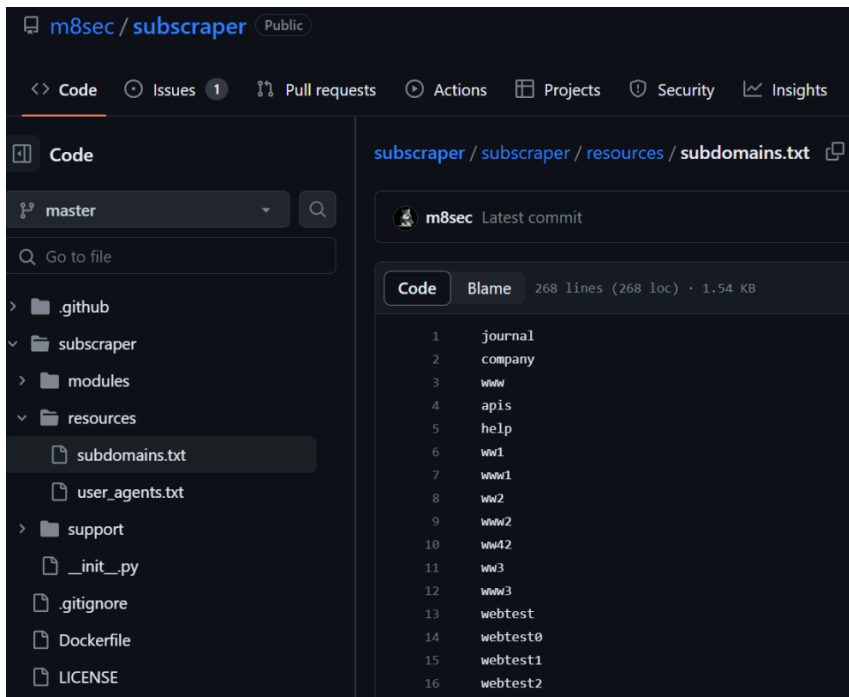
- subdomain brute force
- CT (Certificate Transparency)
- 인증서 대체 도메인(SAN) 추출
- passive DNS
- 웹 크롤링을 통한 도메인 수집
- DNS CNAME 레코드 조회
- Reverse Domain

## IP 확장 기술

- ASN 조회
- DNS Lookup

### Subdomain Brute force

- dictionary 기반으로 DNS 쿼리를 bruteforce 조회
- 대부분의 subdomain 확장 도구에 포함된 기능
- Brute force이다 보니 비효율적 (낮은 탐지율, 오래 걸림, 트래픽 증가)

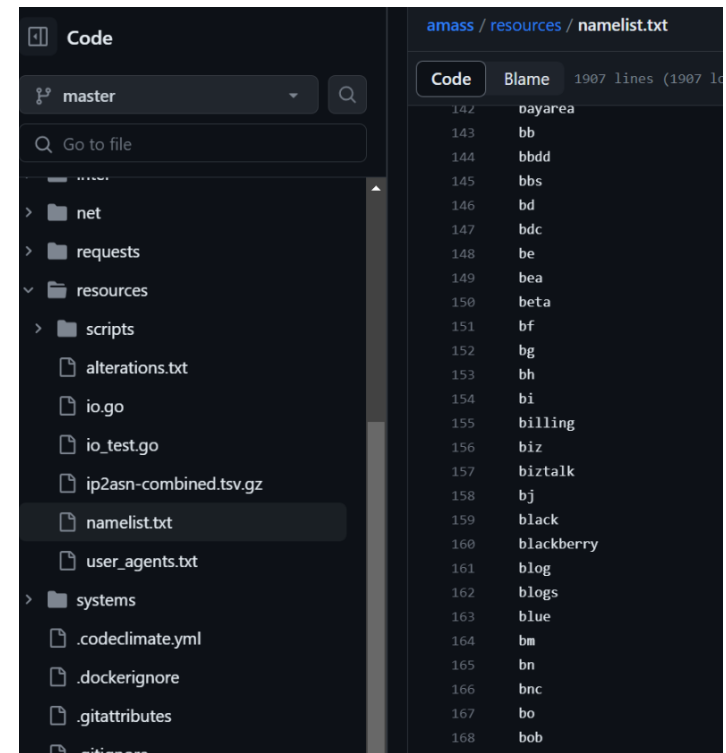


The screenshot shows the GitHub interface for the repository 'm8sec/subscraper'. The left sidebar displays the file tree with the following structure:

- .github
- subscraper
  - modules
  - resources
    - subdomains.txt
    - user\_agents.txt
  - support
    - \_\_init\_\_.py
  - .gitignore
  - Dockerfile
  - LICENSE

The main area shows the content of 'subdomains.txt' with the following lines:

```
1 journal
2 company
3 www
4 apis
5 help
6 www1
7 www1
8 www2
9 www2
10 www42
11 www3
12 www3
13 webtest
14 webtest0
15 webtest1
16 webtest2
```



The screenshot shows the GitHub interface for the repository 'amass/resources'. The left sidebar displays the file tree with the following structure:

- net
- requests
- resources
  - alterations.txt
  - io.go
  - io\_test.go
  - ip2asn-combined.tsv.gz
  - namelist.txt
  - user\_agents.txt
- scripts
- systems
  - .codeclimate.yml
  - .dockerignore
  - .gitattributes
  - .gitignore

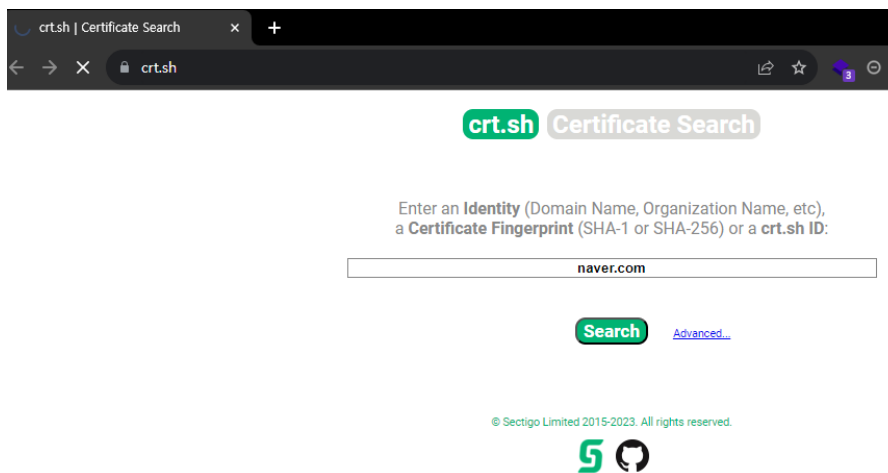
The main area shows the content of 'namelist.txt' with the following lines:

```
142 payarea
143 bb
144 bbdd
145 bbs
146 bd
147 bdc
148 be
149 bea
150 beta
151 bf
152 bg
153 bh
154 bi
155 billing
156 biz
157 biztalk
158 bj
159 black
160 blackberry
161 blog
162 blogs
163 blue
164 bm
165 bn
166 bnc
167 bo
168 bob
```



## CT (Certificate Transparency)

- Certificate Transparency란 인터넷상에 발급되는 모든 인증서들을 로깅하고 모니터링하는 것을 말함
- CT 모니터링을 무료로 제공하는 대표적인 사이트로 <https://crt.sh/> 가 있음  
<https://crt.sh/?q=naver.com>



crt.sh | naver.com

crt.sh | naver.com

crt.sh Identity Search

SSL

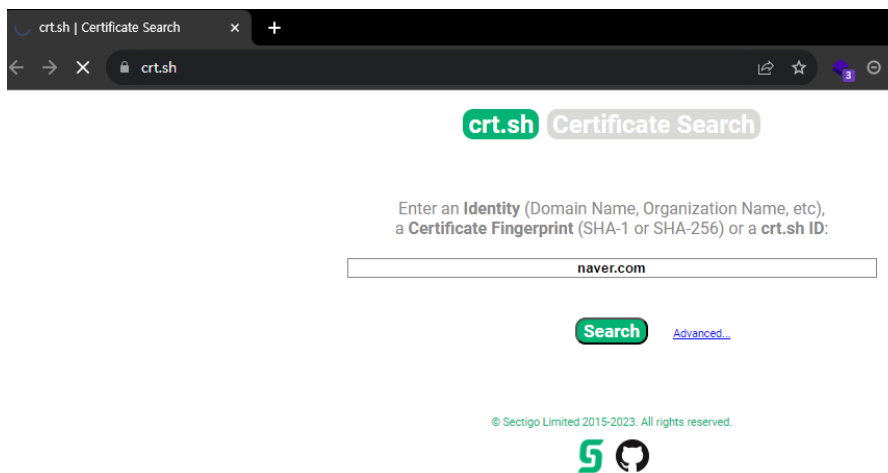
Google Inc

Criteria Type Identity Match: ILIKE Search: 'naver.com'

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	2592061335	2020-03-17	2018-08-01	2020-07-31	m.shop.ya9.naver.com	m.shop.ya9.naver.com	C=US, O=Digicert, Inc, CN=Thawte RSA CA 2018
	2593115677	2020-03-17	2020-03-17	2020-06-15	kstatic.search.naver.com	kstatic.search.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2588494492	2020-03-17	2020-03-17	2020-06-15	kstatic.search.naver.com	kstatic.search.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2582503938	2020-03-15	2018-07-25	2020-07-24	m.nxad.search.naver.com	*m.nxad.search.naver.com m.nxad.search.naver.com	C=US, O=Digicert, Inc, CN=SecureServer CA
	2871165421	2020-03-10	2020-03-10	2020-06-08	dev.adcenter.shopping.naver.com	dev.adcenter.shopping.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2560356516	2020-03-10	2020-03-10	2020-06-08	dev.adcenter.shopping.naver.com	dev.adcenter.shopping.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2559940051	2020-03-10	2020-03-10	2020-04-21	cm-test1.naver.com	cm-test1.naver.com	C=US, O=Digicert, Inc, CN=Thawte RSA CA 2018
	2559939465	2020-03-10	2020-03-10	2020-04-21	cm-test3.naver.com	cm-test3.naver.com	C=US, O=Digicert, Inc, CN=Thawte RSA CA 2018
	2559900158	2020-03-10	2020-03-10	2020-04-21	cm-test2.naver.com	cm-test2.naver.com	C=US, O=Digicert, Inc, CN=Thawte RSA CA 2018
	2532656629	2020-03-01	2020-03-01	2020-05-30	keyboard.naver.com	www.cm-test2.naver.com keyboard.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2518364881	2020-03-01	2020-03-01	2020-05-30	keyboard.naver.com	keyboard.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2534388725	2020-02-29	2020-02-29	2020-05-29	dev.tv.m.dmmmv.naver.com	dev.tv.m.dmmmv.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2517818797	2020-02-29	2020-02-29	2020-05-29	dev.tv.m.dmmmv.naver.com	dev.tv.m.dmmmv.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2534292059	2020-02-29	2020-02-29	2020-05-29	dev.stream.tv.m.dmmmv.naver.com	dev.stream.tv.m.dmmmv.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2518056180	2020-02-29	2020-02-29	2020-05-29	dev.stream.tv.m.dmmmv.naver.com	dev.stream.tv.m.dmmmv.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2517071772	2020-02-27	2020-02-26	2020-05-26	er.search.naver.com	er.search.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2505404587	2020-02-27	2020-02-26	2020-05-26	er.search.naver.com	er.search.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2459750093	2020-02-14	2020-02-13	2020-04-20	ssl.pstatic.net	api-blog.blog.naver.com api-guestbook.blog.naver.com auth.linedict.naver.com blog.naver.com cafe.naver.com comic.naver.com grafolio.naver.com kin.naver.com m.blog.naver.com m.cafe.naver.com m.cookie.naver.com	C=US, O=Digicert, Inc, CN=Thawte RSA CA 2018

## CT (Certificate Transparency)

- Certificate Transparency란 인터넷상에 발급되는 모든 인증서들을 로깅하고 모니터링하는 것을 말함
- CT 모니터링을 무료로 제공하는 대표적인 사이트로 <https://crt.sh/> 가 있음  
<https://crt.sh/?q=naver.com>



crt.sh | naver.com

crt.sh | naver.com

crt.sh Identity Search

Google Inc

Criteria Type Identity Match: ILIKE Search: 'naver.com'

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	2592061335	2020-03-17	2018-08-01	2020-07-31	m.shop.ya9.naver.com	m.shop.ya9.naver.com	C=US, O=Digicert, Inc, CN=Thawte RSA CA 2018
	2593115677	2020-03-17	2020-03-17	2020-06-15	kstatic.search.naver.com	kstatic.search.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2588494492	2020-03-17	2020-03-17	2020-06-15	kstatic.search.naver.com	kstatic.search.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2582503938	2020-03-15	2018-07-25	2020-07-24	m.nxad.search.naver.com	*m.nxad.search.naver.com m.nxad.search.naver.com	C=US, O=Digicert, Inc, CN=SecureTrust RSA CA 2018
	2871165421	2020-03-10	2020-03-10	2020-06-08	dev.adcenter.shopping.naver.com	dev.adcenter.shopping.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2560356516	2020-03-10	2020-03-10	2020-06-08	dev.adcenter.shopping.naver.com	dev.adcenter.shopping.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2559940051	2020-03-10	2020-03-10	2020-04-21	cm-test1.naver.com	cm-test1.naver.com	C=US, O=Digicert, Inc, CN=www.digicert.com, CN=SecureTrust RSA CA 2018
	2559939465	2020-03-10	2020-03-10	2020-04-21	cm-test3.naver.com	cm-test3.naver.com	C=US, O=Digicert, Inc, CN=www.digicert.com, CN=Thawte RSA CA 2018
	2559909158	2020-03-10	2020-03-10	2020-04-21	cm-test2.naver.com	cm-test2.naver.com	C=US, O=Digicert, Inc, CN=Thawte RSA CA 2018
	2532656629	2020-03-01	2020-03-01	2020-05-30	keyboard.naver.com	www.cm-test2.naver.com keyboard.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2518364881	2020-03-01	2020-03-01	2020-05-30	keyboard.naver.com	keyboard.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2534388725	2020-02-29	2020-02-29	2020-05-29	dev.tv.m.dmmmv.naver.com	dev.tv.m.dmmmv.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2517818797	2020-02-29	2020-02-29	2020-05-29	dev.tv.m.dmmmv.naver.com	dev.tv.m.dmmmv.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2534292059	2020-02-29	2020-02-29	2020-05-29	dev.stream.tv.m.dmmmv.naver.com	dev.stream.tv.m.dmmmv.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2518056180	2020-02-29	2020-02-29	2020-05-29	dev.stream.tv.m.dmmmv.naver.com	dev.stream.tv.m.dmmmv.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2517071772	2020-02-27	2020-02-26	2020-05-26	er.search.naver.com	er.search.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2505404587	2020-02-27	2020-02-26	2020-05-26	er.search.naver.com	er.search.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2459750093	2020-02-14	2020-02-13	2020-04-20	ssl.pstatic.net	api-blog.blog.naver.com api-guestbook.blog.naver.com auth.linedict.naver.com blog.naver.com cafe.naver.com comic.naver.com grafolio.naver.com kin.naver.com m.blog.naver.com m.cafe.naver.com m.cookie.naver.com	C=US, O=Digicert, Inc, CN=www.digicert.com, CN=SecureTrust RSA CA 2018

## CT (Certificate Transparency) 등장 배경

### CA의 문제점 ("감시자는 누가 감시하는가?")

HTTPS는 인증서 발급 기관(CA: Certificate Authority)에 대한 신뢰를 기반함

만약 CA가 해킹 또는 실수로 인해 잘못된 인증서를 발급하게 되면?

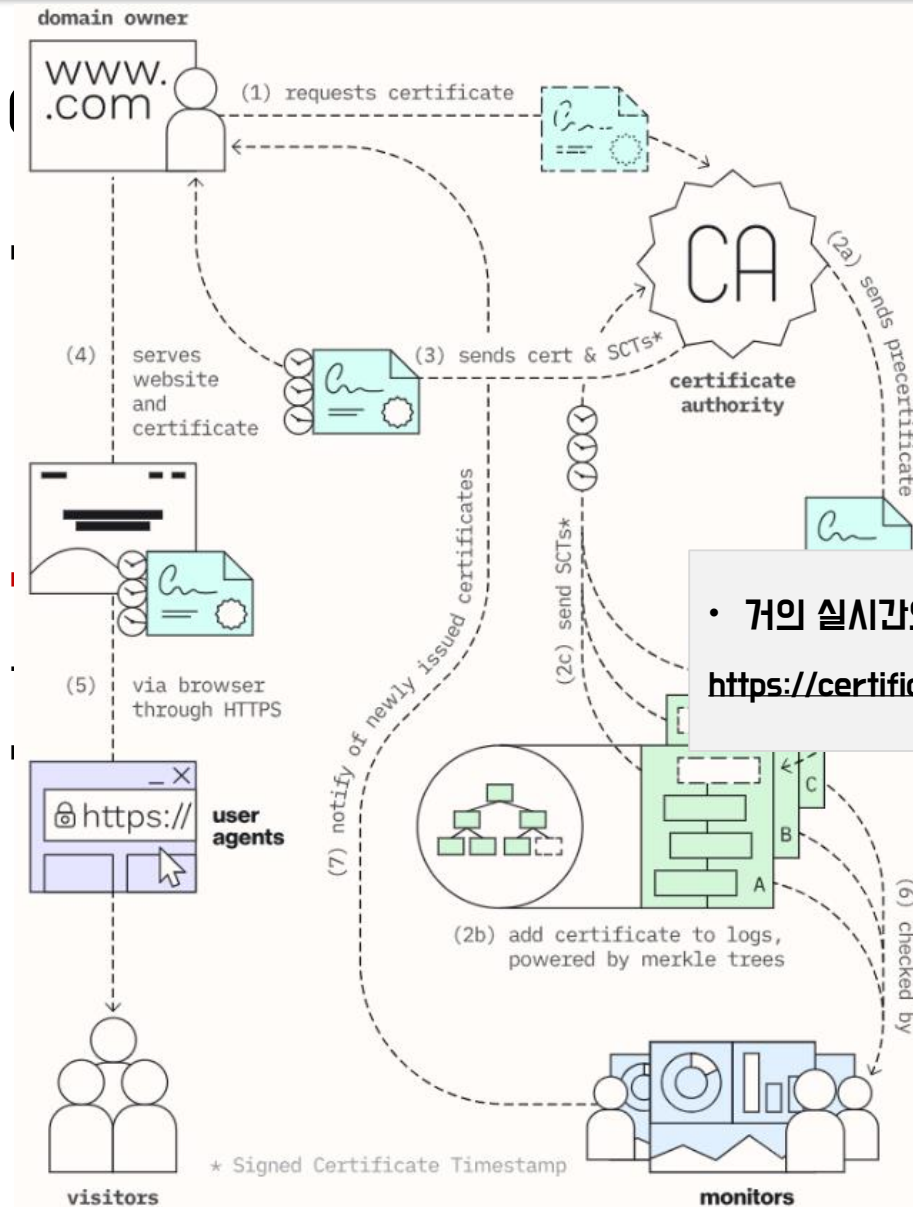
기존 PKI 체계에서는 CA가 발급한 인증서 전체 목록 알기 어려움  
(도메인 소유자도 모름..)

## CT (Certificate Transparency) 등장 배경

- 2013년 CA에 의해 여러 Google 도메인 인증서가 무단으로 발급되는 사건을 계기로 Google에서 시작한 프로젝트

<https://security.googleblog.com/2013/12/further-improving-digital-certificate.html>

- CA가 발급하는 인증서를 기록, 감사 및 모니터링하기 위한 것
  - 도메인 소유자 모르게 도메인에 대한 인증서 발급을 방지하는 것이 목표
- 인증서가 발급되면 인증서에 속한 데이터를 가져와 로그에 추가 되며 추가된 로그는 수정 및 삭제 불가 (머클 트리 활용)



## 증장 배경

인증서가 무단으로 발급되는

문제

[g-digital-certificate.html](https://g-digital-certificate.html)

- 거의 실시간으로 또는 몇 시간 지연되어 CT 로그에 기록됨

<https://certificate.transparency.dev/howctworks/>

인증서와 로그에 추가되며 추가된

### CT의 부작용

“도메인 소유자 모르게 도메인에 대한 인증서 발급을 방지하는 것”이 목표였으나..

- 이 로그는 누구나 공개적으로 볼 수 있음
- 공격자의 **Attack Surface 수집**에 큰 도움이 됨
- → 도메인 이름, 하위 도메인 이름, 이메일 주소 등 수집
- 실시간으로 수집해서 초기화전 관리페이지 접근

[https://hdm.io/decks/Modern\\_Internet\\_Scale\\_Reconnaissance.pdf](https://hdm.io/decks/Modern_Internet_Scale_Reconnaissance.pdf)

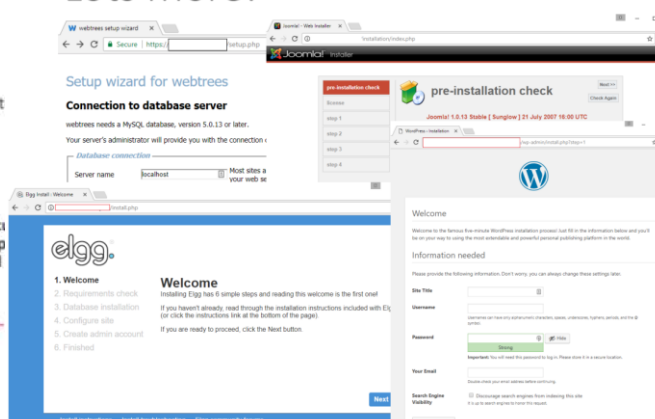
#### Racing to First Setup

Many apps provide admin access to the first person to visit  
We can beat the legitimate user by tailing CT into nmap  
...then backdoor the server and reset the setup =)

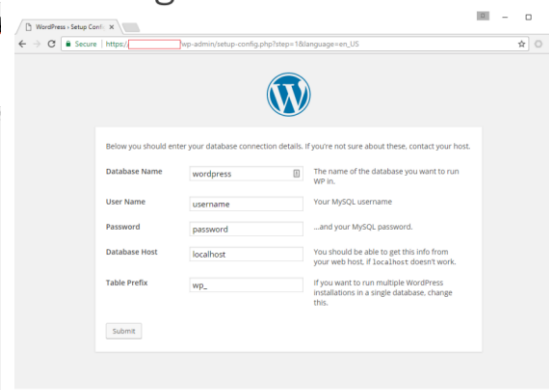
```
$ inetdata-ct-tail -f 2>/dev/null | perl -pe 's/.dns/.n/g' | c  
bloom | grep -v ^\* | nmap -il - --min-rate=1000 -P5443 -p  
retries=1 --script=http-title --min-parallelism=64 -oA ct-tail
```

...  
\_http-title: Did not follow redirect to https://[nooooo]/wp-admin/setup-config.php

#### Lots More!

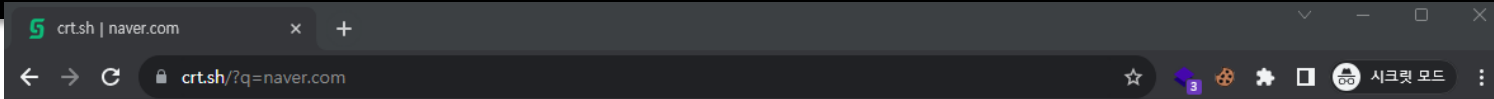


#### Winning a WordPress



# # 도메인 확장 기술

## CT (Certificate Transparency)



CT

내  
영

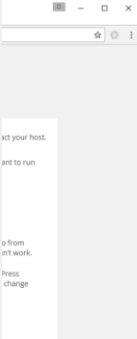
■  
■  
■  
■

F

M:  
W:  
...t

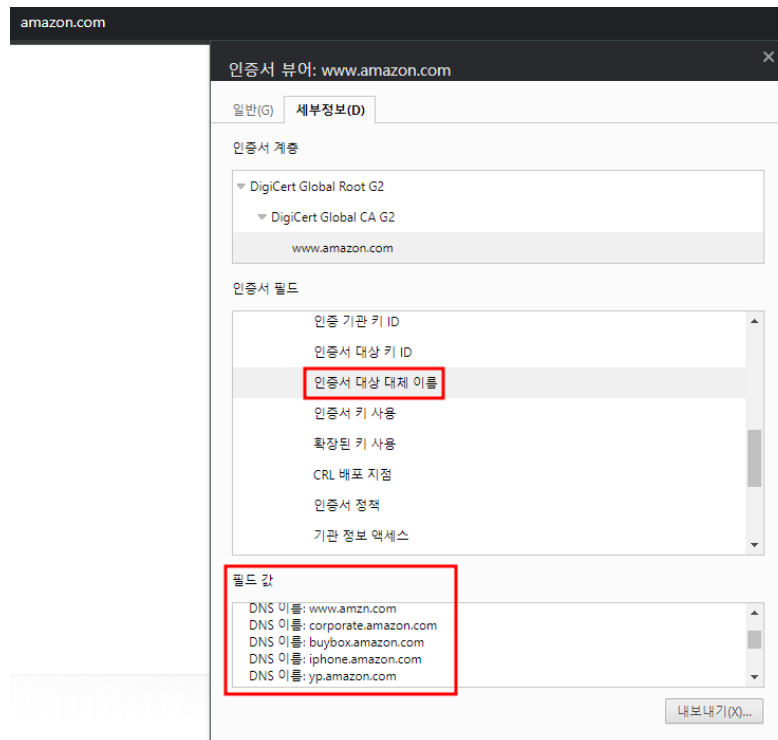
\$ i  
bli  
re!  
...  
I ad

Certificates				Criteria	Type: Identity	Match: ILIKE	Search: 'naver.com'
crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name	
<a href="#">2592061335</a>	2020-03-17	2018-08-01	2020-07-31	m.shop.ya9.naver.com	m.shop.ya9.naver.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Thawte RSA CA 2018	
<a href="#">2593115677</a>	2020-03-17	2020-03-17	2020-06-15	kstatic.search.naver.com	kstatic.search.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	
<a href="#">2588494492</a>	2020-03-17	2020-03-17	2020-06-15	kstatic.search.naver.com	kstatic.search.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	
<a href="#">2582503938</a>	2020-03-15	2018-07-25	2020-07-24	m.nxad.search.naver.com	*m.nxad.search.naver.com m.nxad.search.naver.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018	
<a href="#">2571165421</a>	2020-03-10	2020-03-10	2020-06-08	dev.adcenter.shopping.naver.com	dev.adcenter.shopping.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	
<a href="#">2560356516</a>	2020-03-10	2020-03-10	2020-06-08	dev.adcenter.shopping.naver.com	dev.adcenter.shopping.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	
<a href="#">2559940051</a>	2020-03-10	2020-03-10	2020-04-21	cm-test1.naver.com	cm-test1.naver.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018	
<a href="#">2559939465</a>	2020-03-10	2020-03-10	2020-04-21	cm-test3.naver.com	cm-test3.naver.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Thawte RSA CA 2018	
<a href="#">2559909158</a>	2020-03-10	2020-03-10	2020-04-21	cm-test2.naver.com	cm-test2.naver.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA	
<a href="#">2535265629</a>	2020-03-01	2020-03-01	2020-05-30	keyboard.naver.com	keyboard.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	
<a href="#">2518366881</a>	2020-03-01	2020-03-01	2020-05-30	keyboard.naver.com	keyboard.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	
<a href="#">2534388226</a>	2020-02-29	2020-02-29	2020-05-29	dev.tv.m.drmnmv.naver.com	dev.tv.m.drmnmv.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	
<a href="#">2517813797</a>	2020-02-29	2020-02-29	2020-05-29	dev.tv.m.drmnmv.naver.com	dev.tv.m.drmnmv.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	
<a href="#">2534329059</a>	2020-02-29	2020-02-29	2020-05-29	dev.stream.tv.m.drmnmv.naver.com	dev.stream.tv.m.drmnmv.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	
<a href="#">2518056180</a>	2020-02-29	2020-02-29	2020-05-29	dev.stream.tv.m.drmnmv.naver.com	dev.stream.tv.m.drmnmv.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	
<a href="#">2517071772</a>	2020-02-27	2020-02-26	2020-05-26	er.search.naver.com	er.search.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	
<a href="#">2505404587</a>	2020-02-27	2020-02-26	2020-05-26	er.search.naver.com	er.search.naver.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	
<a href="#">2459750093</a>	2020-02-14	2020-02-13	2020-04-20	ssl.pstatic.net	api-blog.blog.naver.com api-guestbook.blog.naver.com auth.linedict.naver.com blog.naver.com cafe.naver.com comic.naver.com grafolio.naver.com kin.naver.com m.blog.naver.com m.cafe.naver.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018	



## 인증서 대체 도메인(SAN) 추출

- SAN (Subject Alt Names)은 RFC 국제 표준 X.509 확장 기술
- 서비스(도메인)별로 각각 인증서를 발급해야 하는 불편함을 해결  
→ SAN 인증서를 멀티 도메인 인증서라고 부름





## 인증서 대체 도메인(SAN) 추출

- SAN (Subject Alt Names)은 RFC 국제 표준 X.509 확장 기술
- 서비스(도메인)별로 각각 인증서를 발급해야 하는 불편함을 해결  
→ SAN 인증서를 멀티 도메인 인증서라고 부름

```
ttt.py x
1 import ssl
2 import OpenSSL.crypto as crypto
3
4 # 인증서 추출
5 cert_data = ssl.get_server_certificate(('205.251.242.103', 443))
6
7 # 인증서 파싱
8 x509 = crypto.load_certificate(crypto.FILETYPE_PEM, cert_data)
9
10 subject_alt_name = None
11 for i in range(x509.get_extension_count()):
12     ext = x509.get_extension(i)
13     if "subjectAltName" in str(ext.get_short_name()):
14         print(ext)
15         break
```

DNS:amazon.co.uk, DNS:uedata.amazon.co.uk, DNS:www.amazon.co.uk, DNS:origin-www.amazon.co.uk, DNS:\*.peg.a2z.com, DNS:amazon.com, DNS:amzn.co.uk, DNS:us.amazon.com, DNS:www.amazon.com, DNS:www.amzn.com, DNS:corporate.amazon.com, DNS:buybox.amazon.com, DNS:iphone.amazon.com, DNS:yp.amazon.com, DNS:origin-www.amazon.com, DNS:origin2-www.amazon.com, DNS:buckeye-retail-website.amazon.com, DNS:huddles.amazon.com, DNS:amazon.de, DNS:www.amazon.co.jp, DNS:amazon.jp, DNS:www.amazon.jp, DNS:www.amazon.co.jp, DNS:origin-www.amazon.co.jp, DNS:\*.aa.peg.a2z.com, DNS:\*.ab.peg.a2z.com, DNS:origin-www.amazon.com.au, DNS:www.amazon.com.au, DNS:\*.bz.peg.a2z.com, DNS:amazon.com.au, DNS:origin2-www.amazon.co.jp, DNS:edgeflow.aero, DNS:edgeflow.aero.04f01a85e-frontier.amazon.com.au, DNS:edgeflow.aero.47cf2c8c9-frontier.amazon.com, DNS:edgeflow.aero.abe2c2f23-frontier.amazon.com, DNS:edgeflow.aero.bfbdc3ca1-frontier.amazon.co.uk, DNS:edgeflow-dp.aero.4d5ad1d2b-frontier.amazon.co.jp, DNS:edgeflow-dp.aero.04f01a85e-frontier.amazon.com, DNS:edgeflow-dp.aero.47cf2c8c9-frontier.amazon.com

[Finished in 0.9s]

## Passive DNS

- 직접 DNS 레코드를 요청하지 않고 여러 출처(OSINT)를 활용해 DNS 정보 수집
- 현재 상태에 국한되지 않고 과거의 DNS 매핑 기록까지 포함

- 구글 검색 (site: 옵션 사용)
- github 검색
- Internet Archive/Wayback Machine
- VirusTotal API
- CommonCrawl Index
- Censys
- Shodan
- SecurityTrails
- IntelligenceX
- RiskIQ
- ZoomEye

...

## 그 외 ...

- 웹 크롤링을 통한 도메인 수집
- DNS CNAME 레코드 조회
- Reverse Domain

# # IP 확장 기술

## 도메인 확장 기술

- subdomain brute force
- CT (Certificate Transparency)
- 인증서 대체 도메인(SAN) 추출
- passive DNS
- 웹 크롤링을 통한 도메인 수집
- DNS CNAME 레코드 조회
- Reverse Domain

## IP 확장 기술

- **ASN 조회**
- **DNS Lookup**

## ASN (Autonomous System Number) 조회

- ASN은 인터넷에서 사용되는 네트워크 식별 번호 (라우팅에서 중요한 역할)
- 각 지역에 해당하는 RIR(Regional Internet Registry)에서 ASN을 신청
- ASN을 통해서 "조직 정보, IP 주소 범위, 라우팅 정책, BGP 관련 정보" 등을 확인할 수 있음

## ASN (Autonomous System Number) 조회

- ASN 정보를 제공하는 사이트 이용

: <https://asnlookup.com/>



[Home](#) [Pricing](#) [API](#)

### Search

Quickly lookup updated information about specific Autonomous System Number (ASN), Organization, CIDR, or registered IP addresses (IPv4 and IPv6) among other relevant data. We also offer a free and paid API access!

Search by ASN, IPv4, IPv6, CIDR, Organization name

Lookup!

Facebook

AS15169

31.13.24.0

2620:0:1cfe:face:b00c::3

66.220.144.0/20












2620:0:1c00::/40

## Search


Quickly lookup updated information about specific Autonomous System Number (ASN), Organization, CIDR, or registered IP addresses (IPv4 and IPv6) among other relevant data. We also offer a free and paid API access!

Lookup![Facebook](#)[AS15169](#)[31.13.24.0](#)[2620:0:1cfe:face:b00c::3](#)[66.220.144.0/20](#)[2620:0:1c00::/40](#)

# # IP 확장 기술

Country	ASN	Organization
 South Korea	<a href="#">AS38099</a>	Kakao Corp
 South Korea	<a href="#">AS9958</a>	kakaogames
 South Korea	<a href="#">AS131858</a>	kakaopay insurance
 South Korea	<a href="#">AS131828</a>	KAKAO Enterprise
 South Korea	<a href="#">AS38667</a>	KakaoBank Corp.
 South Korea	<a href="#">AS9764</a>	Kakao Corp
 South Korea	<a href="#">AS10158</a>	Kakao Corp
 South Korea	<a href="#">AS38678</a>	Kakao Corp
 South Korea	<a href="#">AS7625</a>	Kakao Corp
 South Korea	<a href="#">AS23588</a>	KAKAO Enterprise
 South Korea	<a href="#">AS45991</a>	Kakao Corp



Kakao Corp	
AS Handle	AS38099
ASN Name	KAKAO-AS-KR
Organization Name	Kakao Corp
Organization ID	@family-42622
Country	 South Korea
Regional Registry	APNIC
IPv4 CIDRs	<div><ul style="list-style-type: none"><li>1.201.0.0/24</li><li>121.53.176.0/22</li><li>139.150.1.0/24</li><li>210.220.73.0/24</li><li>210.220.95.0/24</li><li>211.231.104.0/22</li><li>211.249.252.0/22</li></ul><ul style="list-style-type: none"><li>27.0.236.0/22</li><li>121.53.180.0/23</li><li>210.103.253.0/24</li><li>210.220.74.0/24</li><li>211.231.97.0/24</li><li>211.231.108.0/24</li><li>219.249.231.0/24</li></ul><ul style="list-style-type: none"><li>103.246.57.0/24</li><li>121.53.200.0/21</li><li>210.103.254.0/24</li><li>210.220.79.0/24</li><li>211.231.98.0/23</li><li>211.231.111.0/24</li><li>220.64.96.0/22</li></ul><ul style="list-style-type: none"><li>121.53.104.0/21</li><li>121.53.244.0/22</li><li>210.220.70.0/24</li><li>210.220.86.0/24</li><li>211.231.100.0/22</li><li>211.249.200.0/21</li><li>220.64.144.0/22</li></ul></div>
IPv6 CIDRs	<ul style="list-style-type: none"><li>2404:4600:6::/48</li></ul>

## DNS Lookup

- 도메인 확장으로 수집한 도메인들의 DNS A레코드 조회  
DNS → IP

# # 오픈 소스 도구 활용

---

## 이미 오픈 소스 툴이 많음 ...

- amass
- subfinder
- assetfinder
- Findomain
- dnsx
- katana
- httpx
- gospider

...

# # 오픈 소스 도구 활용

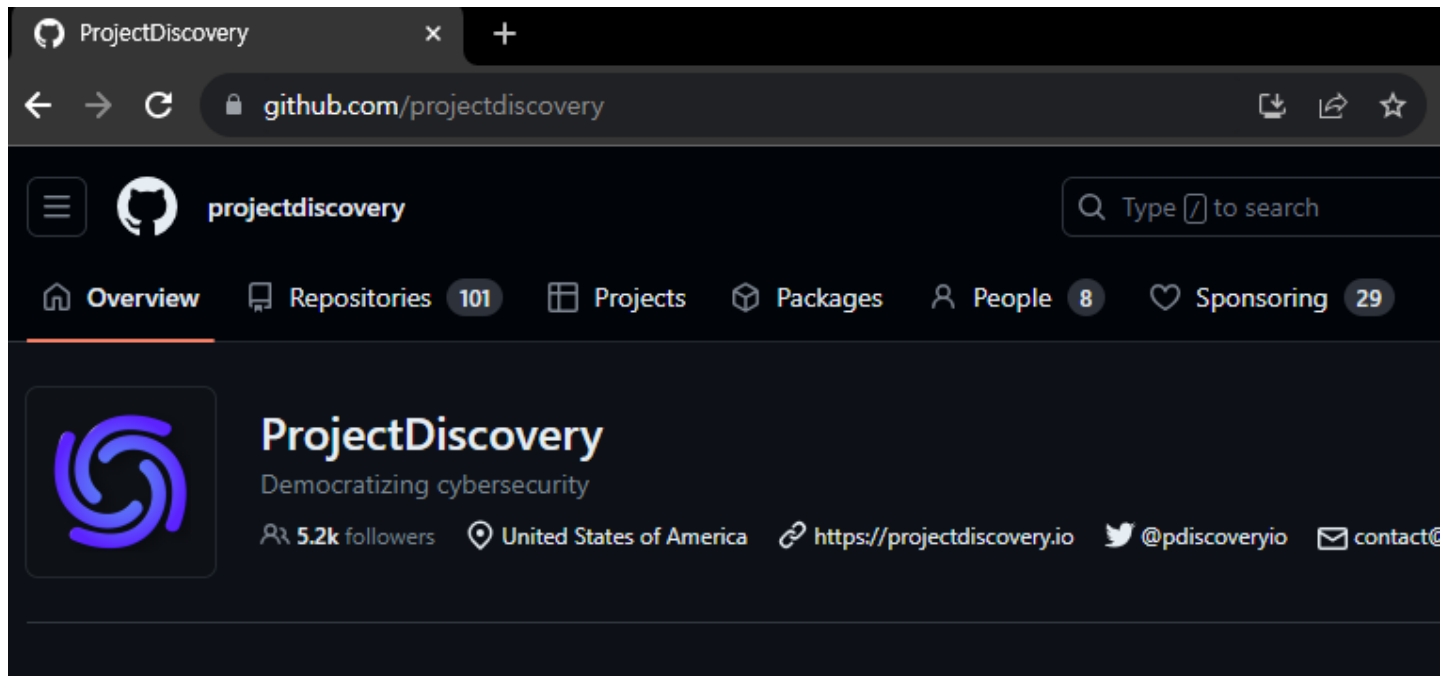
	항목	Amass	* Subfinder	assetfinder	Findomain	* dnsx	* katana	* httpx	gospider
Github ★ (23.8.22기준)	★	9.9k	8.1k	2.5k	2.9k	1.7k	7.3k	5.6k	2.1k
	최근 업데이트	23.7.29	23.8.13	20.4.15	23.6.29	23.4.30	23.8.1	23.7.23	23.1.17
	License	APACHE v2.0	MIT license	MIT License	GPL-3.0	MIT License	MIT License	MIT License	MIT License
도메인 확장	DNS Lookup	CNAME 레코드 조회				•			
		Reverse Domain (IP → Domain)	•			•			
		subdomain brute force	•			•			
	검색 및 API 조회	Passive DNS •DNS history •CT (Certificate Transparency)	•	•	•				
		•web archive •검색 엔진 스크래핑 등 많은 data source가 존재하며 세부 목록은 참고 사항에서 확인	•	•	•				
	브라우저	인증서 대체 도메인(SAN) 추출						•	
		웹 크롤링 (도메인 수집)					•		•
IP 확장	검색 및 API 조회	ASN 조회	•			•		•	
	DNS Lookup	A 레코드 조회 (Domain → IP)				•			

# # 오픈 소스 도구 활용

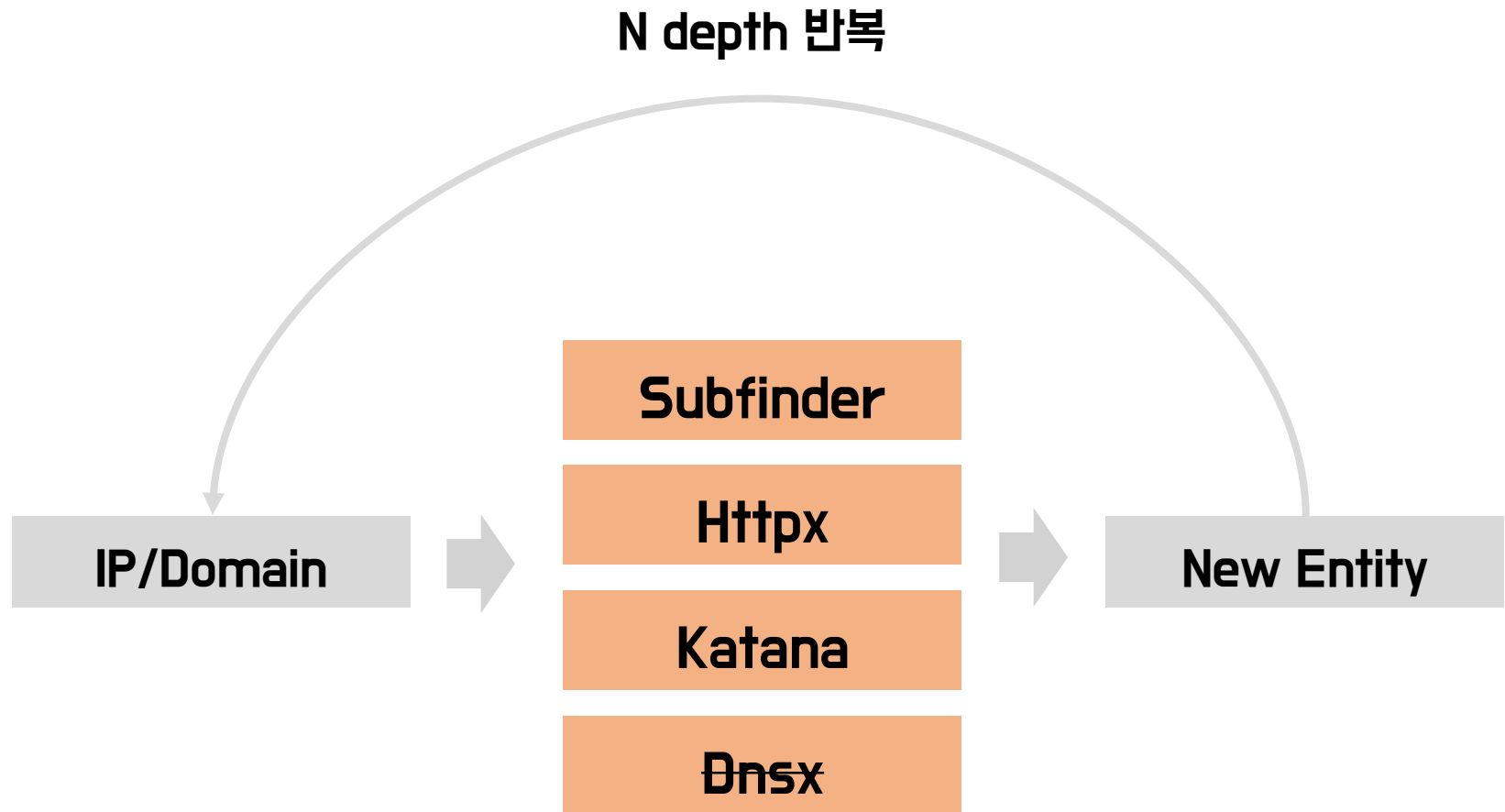
## Project Discovery 도구

- subfinder : passive DNS, 인증서 CT 등
- dnsx : 문 관련 조회
- Katana : 웹 크롤링
- httpx : 인증서 SAN 조회

<https://github.com/projectdiscovery>



# # 오픈 소스 도구 활용



# # 오픈 소스 도구 활용

subfinder -cs -silent -all -d naver.com

```
book.naver.com,[chaos,rapiddns,crtsh,waybackarchive,shodan]
e.cell4.office.naver.com,[rapiddns]
crawl.125-209-235-170.web.naver.com,[anubis,chaos,rapiddns]
cvowlsmtptnoti003.nm.naver.com,[rapiddns,anubis,chaos]
photoimg.naver.com,[chaos]
postmail302.nm.naver.com,[chaos]
test-checkout.naver.com,[chaos,rapiddns,crtsh]
developer.whale.naver.com,[shodan]
golda.cafe.naver.com,[shodan,rapiddns,waybackarchive]
api.gdp.game.naver.com,[chaos]
pb.m.naver.com,[chaos,crtsh]
smtp2.nm2.naver.com,[chaos]
drtest2019-05.naver.com,[crtsh]
creturn04-2.nm.naver.com,[chaos,anubis]
crawl.211-249-46-126.web.naver.com,[anubis,chaos,rapiddns]
gw-zeal.zepeto.io.elb-kr.io.naver.com,[shodan]
gbill.naver.com,[chaos,crtsh]
han932.naver.com,[anubis,chaos]
qamailmx2.naver.com,[anubis,chaos]
newsstand.naver.com,[crtsh,alienvault,waybackarchive,chaos,rapiddns]
trcvmaill1-1.nm.naver.com,[chaos]
www.api.happybean.naver.com,[chaos,crtsh]
d79434.naver.com,[chaos,rapiddns,anubis]
crawl.110-93-150-178.web.naver.com,[anubis,chaos,rapiddns]
bugbounty.naver.com,[shodan,rapiddns]
partnersedu.naver.com,[shodan,chaos,crtsh]
www.cecs.naver.com,[chaos,crtsh]
rudic.naver.com,[shodan,chaos,rapiddns]
hangame.naver.com,[chaos,rapiddns]
crawl.203-104-154-135.web.naver.com,[anubis,chaos,rapiddns]
crawl.211-249-46-197.web.naver.com,[chaos,rapiddns,anubis]
video.search.naver.com,[chaos,rapiddns]
crawl.211-249-46-23.web.naver.com,[anubis,chaos,rapiddns]
m.shop.ya9.naver.com,[crtsh,anubis,shodan,chaos,rapiddns]
ads.naver.com,[chaos]
static.naver.com,[chaos,rapiddns,waybackarchive]
dev.tv.m.drmmv.naver.com,[alienvault,shodan,chaos,rapiddns,crtsh]
archlord2.game.naver.com,[chaos,crtsh]
m.me.naver.com,[chaos,rapiddns]
m.nstore.naver.com,[chaos,rapiddns]
subdomain.dev.io.naver.com,[chaos]
api-biz-catcher.naver.com,[rapiddns]
apis.naver.com,[crtsh,waybackarchive,shodan,chaos,rapiddns]
csmail.help.nmp.naver.com,[shodan,chaos,rapiddns,crtsh]
dev.novel.naver.com,[rapiddns,chaos]
sports.news.naver.com,[chaos,rapiddns,waybackarchive]
```

katana -timeout 5 -silent -u naver.com

```
https://naver.com
https://help.naver.com/alias/search/word/word_17.naver
https://help.naver.com/alias/search/word/word_18.naver
https://help.naver.com/alias/search/word/word_35.naver
https://help.naver.com/alias/search/word/word_16.naver
https://help.naver.com/support/alias/search/word/word_16.naver
https://nid.naver.com/nidlogin.login
https://www.naver.com/
http://www.naver.com/
https://nid.naver.com/login/js/v2/default/default_202105.js?v=20230217
https://nid.naver.com/login/css/global/desktop/w_20220216.css?v=20210812
https://nid.naver.com/user2/api/route?m=routePwInquiry&lang=ko_KR
https://nid.naver.com/login/ext/help_ip3.html
https://help.naver.com/_next/static/css/b148bf50bfff64bb0e540.css
https://help.naver.com/_next/static/chunks/pages/service/%5BserviceAlias%5D/contents/%5BhelpTextAlias%5D-0e6ed34fdeefeb0b76c5.js
https://nid.naver.com/user2/V2Join?m=agree&lang=ko_KR&domain=www.naver.com
https://help.naver.com/alias/membership/p.membership/main.naver
http://www.naver.com/rules/discipliner.html
http://www.naver.com/rules/service.html
https://nid.naver.com/login/js/bvstd.1.3.9.min.js
https://help.naver.com/service/5627/category/5812?lang=ko
https://help.naver.com/service/5627/category/3911?lang=ko
https://help.naver.com/_next/static/rRCVchW_cpUczAMHztuQ/_ssgManifest.js
https://help.naver.com/_next/static/rRCVchW_cpUczAMHztuQ/_buildManifest.js
https://help.naver.com/_next/static/chunks/pages/service/%5BserviceAlias%5D/category/%5BcategoryAlias%5D-00ae75069db9399119b8.js
http://www.naver.com/rules/privacy.html
https://nid.naver.com/login/js/v2/default/common_202201.js?v=20230619
https://help.naver.com/_next/static/chunks/2e1606904ec39773e998044.js
https://help.naver.com/_next/static/chunks/442-fa43d5942a80144af95d.js
https://help.naver.com/service/5627/category/3910?lang=ko
https://help.naver.com/_next/static/chunks/311-5885e26aee65de3db8d3.js
https://help.naver.com/_next/static/chunks/webpack-92cbb7ec579f20ec511d.js
https://help.naver.com/_next/static/chunks/706-48e79fe7fbee5a6deed12.js
https://help.naver.com/service/5627/category/3909?lang=ko
https://www.naver.com
https://help.naver.com/_next/static/chunks/199-2719079eca505fd25eca.js
https://help.naver.com/_next/static/css/22b4878bee35ae91fa07.css
https://help.naver.com/_next/static/css/b93be41b570c057ad15.css
https://help.naver.com/_next/static/css/8d4c635ec0fab6611775.css
https://help.naver.com/_next/static/css/d84d2d917c3d84143713.css
https://help.naver.com/_next/static/chunks/587-5c52c94b9ce2d7f05908.js
https://policy.naver.com/rules/youthpolicy.html
https://help.naver.com/_next/static/chunks/a79515f9-240cebbd9596cd566db.js
https://help.naver.com/_next/static/chunks/polyfills-a40ef1678ba11e696dba45124eadd70.js
https://help.naver.com/service/5627/category/3904?lang=ko
https://help.naver.com/service/5627/category/3905?lang=ko
https://help.naver.com/index.help?lang=ko
https://help.naver.com/service/5627/category/58632?lang=ko
```

httpx -silent -tls-probe -u naver.com

```
https://naver.com
https://naver.net
https://www.naver.net
https://naver.co
https://www.naver.asia
https://naver.kr
https://www.naver.co.kr
https://naver.co.kr
https://www.naver.co
https://www.naver.kr
https://naver.asia
```

# # 위협 평가 방법

## 자산 식별

- 알려진 자산
- 알려지지 않은 자산 (Shadow IT)

### 식별 자산

IP Address

Domain

GithubRepository

Email

SSL Certificate

...

## 위협 평가

- Fingerprint 정보 수집
  - OS, framework 버전 정보 수집
- 취약점 진단
  - port scan
  - CVE 취약점 진단



# # 위협 평가 방법

## 자산 식별

취약점 점검 모듈은  
ASM 솔루션들의 자산이자 경쟁력 😊

GithubRepository

Email

SSL Certificate

...

## 위협 평가

- Fingerprint 정보 수집
  - OS, framework 버전 정보 수집
- 취약점 진단
  - port scan
  - CVE 취약점 진단

# # 위협 평가 방법

## 이것도 Project Discovery 도구 활용

- Nuclei : 기본적인 웹 취약점 스캔 및 CVE 점검까지 다 해줌!

projectdiscovery / nuclei

Search Type to search

Code Issues 176 Pull requests 18 Discussions Actions Projects Security 1 Insights

### Nuclei Templates overview

An overview of the nuclei template project, including statistics on unique tags, author, directory, severity, and type of templates. The table below contains the top ten statistics for each matrix; an expanded version of this is [available here](#), and also available in [JSON](#) format for integration.

#### Nuclei Templates Top 10 statistics

TAG	COUNT	AUTHOR	COUNT	DIRECTORY	COUNT	SEVERITY	COUNT
cve	2239	dhiyaneshdk	1088	http	6768	info	3275
panel	1018	dwiswant0	798	file	310	medium	1413
wordpress	923	daffainfo	787	workflows	191	high	1412
xss	837	pikpikcu	353	network	119	critical	888
exposure	820	pussycat0x	298	ssl	27	low	234
wp-plugin	807	pdteam	283	dns	17	unknown	31
osint	675	ritikchaddha	275	headless	10		
tech	637	ricardomaia	226	javascript	2		
lfi	614	geeknik	221	TEMPLATES-STATS.json	1		
edb	598	theamanrawat	221	contributors.json	1		

511 directories, 7690 files.

Star 15.2k

Code About

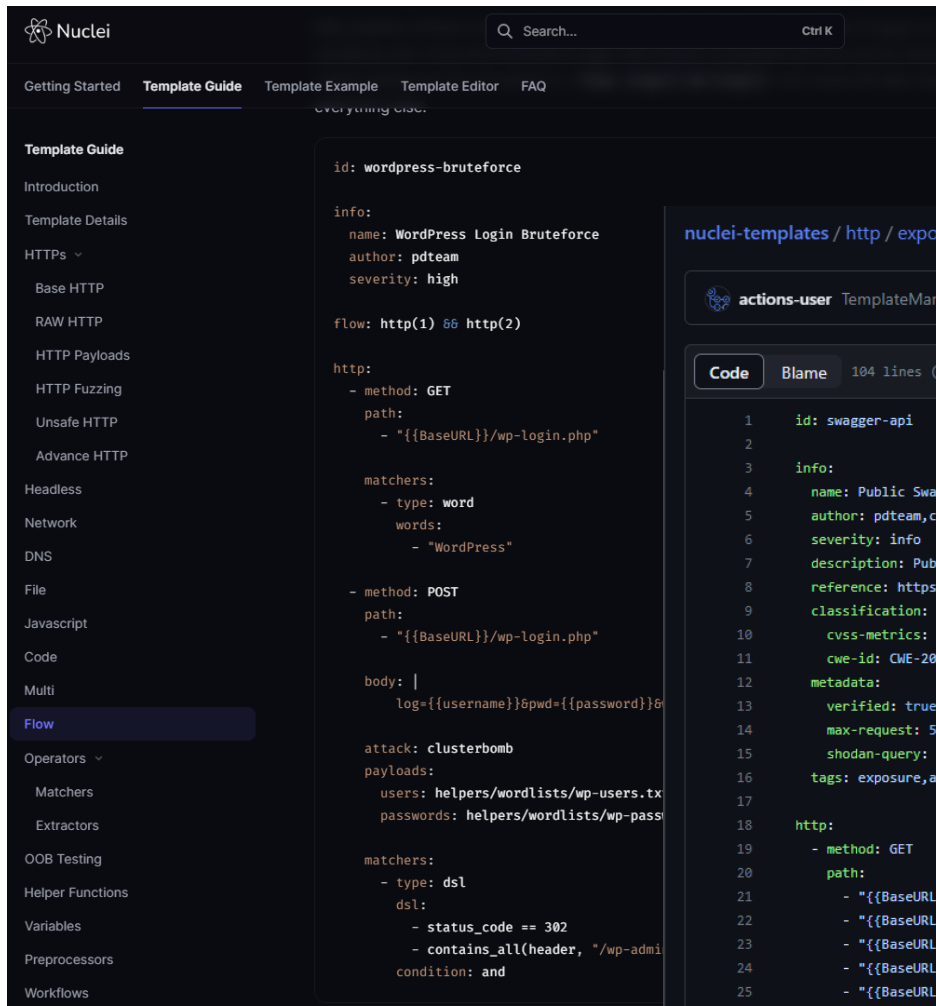
Fast and customizable vulnerability scanner based on simple YAML based

<https://github.com/projectdiscovery/nuclei>

<https://github.com/projectdiscovery/nuclei-templates>

# # 위협 평가 방법

- custom template 제작 가능
  - guide : <https://docs.nuclei.sh/template-guide/introduction>



nuclei-templates / http / exposures / apis / swagg

actions-user TemplateMan Update [Fri Oct 20 11:

Code Blame 104 lines (97 loc) · 3.34 KB

```
1 id: swagger-api
2
3 info:
4   name: Public Swagger API - Detect
5   author: pdteam,c-sh0
6   severity: info
7   description: Public Swagger API was de
8   reference: https://swagger.io/
9   classification:
10    cvss-metrics: CVSS:3.1/AV:N/AC:L/PR:
11    cwe-id: CWE-200
12    metadata:
13     verified: true
14     max-request: 54
15     shodan-query: http.title:"swagger"
16     tags: exposure,api,swagger
17
18 http:
19   - method: GET
20     path:
21       - "{{BaseURL}}/swagger-ui/swagger-
22       - "{{BaseURL}}/swagger/swagger-ui.
23       - "{{BaseURL}}/swagger-ui.js"
24       - "{{BaseURL}}/swagger/ui/swagger-
25       - "{{BaseURL}}/swagger/ui/index"
```

nuclei-templates / http / cves / 2022 / CVE-2022-0817.yaml

actions-user Auto Template Signing [Fri Nov 3 17:10:29 UTC 2023]

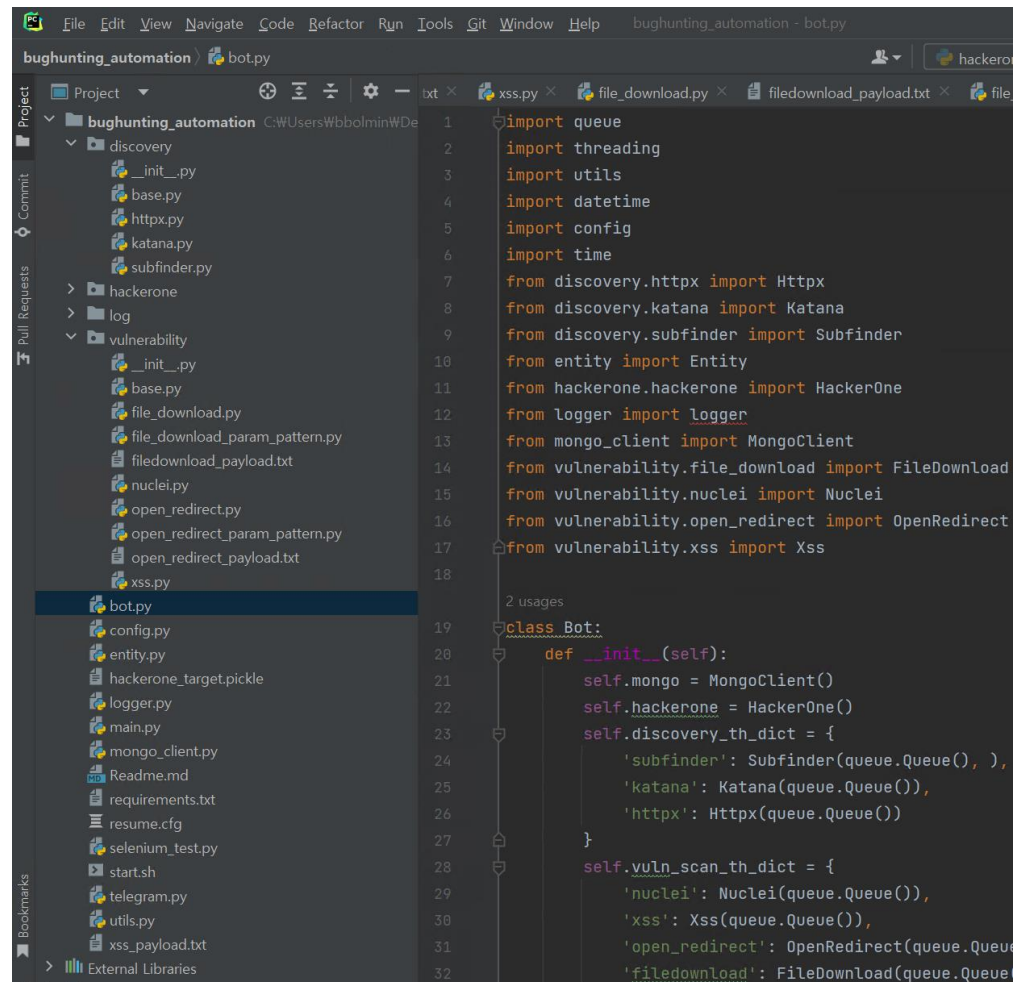
Code Blame 50 lines (46 loc) · 1.98 KB

```
1 id: CVE-2022-0817
2
3 info:
4   name: WordPress BadgeOS <=3.7.0 - SQL Injection
5   author: theamanrawat
6   severity: critical
7   description: |
8     WordPress BadgeOS plugin through 3.7.0 contains a SQL injection vulnerability. It does not
9   remediation: |
10     Update to the latest version of the BadgeOS plugin (>=3.7.1) to mitigate this vulnerability
11   reference:
12     - https://wpscan.com/vulnerability/69263610-f454-4f27-80af-be523d25659e
13     - https://wordpress.org/plugins/badgeos/
14     - https://nvd.nist.gov/vuln/detail/CVE-2022-0817
15   classification:
16     cvss-metrics: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
17     cvss-score: 9.8
18     cve-id: CVE-2022-0817
19     cwe-id: CWE-89
20     epss-score: 0.02409
21     epss-percentile: 0.88751
22     cpe: cpe:2.3:a:badgeos:badgeos:*:*:*:*:wordpress:*:*
23   metadata:
24     verified: true
25     max-request: 1
26     vendor: badgeos
27     product: badgeos
28     framework: wordpress
29     tags: cve2022,wp,unauth,sql,cve,wp-plugin,badgeos,wpscan,wordpress
30   variables:
31     num: "999999999"
```

# # 위협 평가 방법

## 추가로 간단한 웹 취약점 모듈 점검 추가

- Reflected XSS, open redirect, file download
  - <https://github.com/Encryptor-Sec/XSSearch>
  - <https://github.com/aldo-moreno-leon/ORtester>
  - <https://github.com/Indian133t/Gf-Patterns>



The screenshot shows a Python IDE with a project named 'bughunting\_automation'. The left sidebar displays the project structure, including folders for 'discovery', 'hackerone', 'log', and 'vulnerability', and various Python files. The main editor window shows the code for 'bot.py', which imports modules like 'queue', 'threading', 'utils', 'datetime', 'config', 'time', 'Httpx', 'Katana', 'Subfinder', 'Entity', 'HackerOne', 'Logger', 'MongoClient', 'FileDownload', 'Nuclei', 'OpenRedirect', and 'Xss'. The code defines a 'Bot' class with an '\_\_init\_\_' method that initializes various components and a 'vuln\_scan\_th\_dict' dictionary.

```
1 import queue
2 import threading
3 import utils
4 import datetime
5 import config
6 import time
7 from discovery.httpx import Httpx
8 from discovery.katana import Katana
9 from discovery.subfinder import Subfinder
10 from entity import Entity
11 from hackerone.hackerone import HackerOne
12 from logger import Logger
13 from mongo_client import MongoClient
14 from vulnerability.file_download import FileDownload
15 from vulnerability.nuclei import Nuclei
16 from vulnerability.open_redirect import OpenRedirect
17 from vulnerability.xss import Xss
18
19 2 usages
20 class Bot:
21     def __init__(self):
22         self.mongo = MongoClient()
23         self.hackerone = HackerOne()
24         self.discovery_th_dict = {
25             'subfinder': Subfinder(queue.Queue(), ),
26             'katana': Katana(queue.Queue()),
27             'httpx': Httpx(queue.Queue())
28         }
29         self.vuln_scan_th_dict = {
30             'nuclei': Nuclei(queue.Queue()),
31             'xss': Xss(queue.Queue()),
32             'open_redirect': OpenRedirect(queue.Queue()),
33             'filedownload': FileDownload(queue.Queue())
```

# # 위협 평가 방법

## 추가로 간단한 웹 취약점 모듈 점검 추가

- **Reflected XSS**, open redirect, file download

- <https://github.com/Encryptor-Sec/XSSearch>
- <https://github.com/aldo-moreno-leon/ORTester>
- <https://github.com/Indianl33t/Gf-Patterns>

```
xss_payload.txt x
1 <svg%20onload=alert(1)>
2 <img src=x onerror=alert`1`>
3 <script>alert(1)</script>
4 javascript:alert(1)
```

```
87 # Executing a loop for checking valid XSS payload in the given URL
88
89 for payload in open(p, 'r').readlines():
90
91     url = target.replace('{xss}', payload)
92
93     driver.get(url)
94
95 # Checking for a javascript pop-up
96
97     try:
98
99         WebDriverWait(driver, 1).until(EC.alert_is_present())
100
101         alert = driver.switch_to.alert
102
103         alert.accept()
104
105         print ("\033[31m[+] XSS Triggered !\033[0m", payload)
106     except TimeoutException:
107
108         print ("\033[36m[+] XSS not Triggered ! \033[0m", payload)
109
110 driver.close()
```

# # 위협 평가 방법

## 추가로 간단한 웹 취약점 모듈 점검 추가

- Reflected XSS, **open redirect**, file download

- <https://github.com/Encryptor-Sec/XSSearch>
- <https://github.com/aldo-moreno-leon/ORTester>
- <https://github.com/Indian133t/Gf-Patterns>

`requests.request(method, url, **kwargs)`

[source]

Constructs and sends a **Request**.

- Parameters:**
- **method** – method for the new **Request** object: GET, OPTIONS, HEAD, POST, PUT, PATCH, or DELETE.
  - **url** – URL for the new **Request** object.
  - **params** – (optional) Dictionary, list of tuples or bytes to send in the query string for the **Request**.
  - **data** – (optional) Dictionary, list of tuples, bytes, or file-like object to send in the body of the **Request**.
  - **json** – (optional) A JSON serializable Python object to send in the body of the **Request**.
  - **headers** – (optional) Dictionary of HTTP Headers to send with the **Request**.
  - **cookies** – (optional) Dict or CookieJar object to send with the **Request**.
  - **files** – (optional) Dictionary of 'name': file-like-objects (or {'name': file-tuple}) for multipart encoding upload. file-tuple can be a 2-tuple ('filename', fileobj), 3-tuple ('filename', fileobj, 'content\_type') or a 4-tuple ('filename', fileobj, 'content\_type', custom\_headers), where 'content-type' is a string defining the content type of the given file and **custom\_headers** a dict-like object containing additional headers to add for the file.
  - **auth** – (optional) Auth tuple to enable Basic/Digest/Custom HTTP Auth.
  - **timeout** (*float or tuple*) – (optional) How many seconds to wait for the server to send data before giving up, as a float, or a (**connect timeout**, **read timeout**) tuple.
  - **allow\_redirects** (*bool*) – (optional) Boolean. Enable/disable GET/OPTIONS/POST/PUT/PATCH/DELETE/HEAD redirection. Defaults to **True**.

proxies – (optional) Dictionary mapping protocol to the URL of the

```
def open_redirect_test(self, target_value, url, payload):
    try:
        response = requests.get(url, verify=False)
    except requests.exceptions.ConnectionError:
        return ''

    if response.history:
        if str(response.url)[0:19] == "http://www.bing.com" or \
           str(response.url)[0:20] == "https://www.bing.com":
            # result = f'- payload : {payload}\n- {url}\n-> {response.url}'
            result = f'- {url}\n'
            self.save_db(target_value, 'open_redirect', url)
            return result

    return ''
```

Encoding to decode with when accessing r.text.

### headers

Case-insensitive Dictionary of Response Headers. For example, `headers['content-encoding']` will return the value of a 'Content-Encoding' response header.

### history

A list of **Response** objects from the history of the Request. Any redirect responses will end up here. The list is sorted from the oldest to the most recent request.

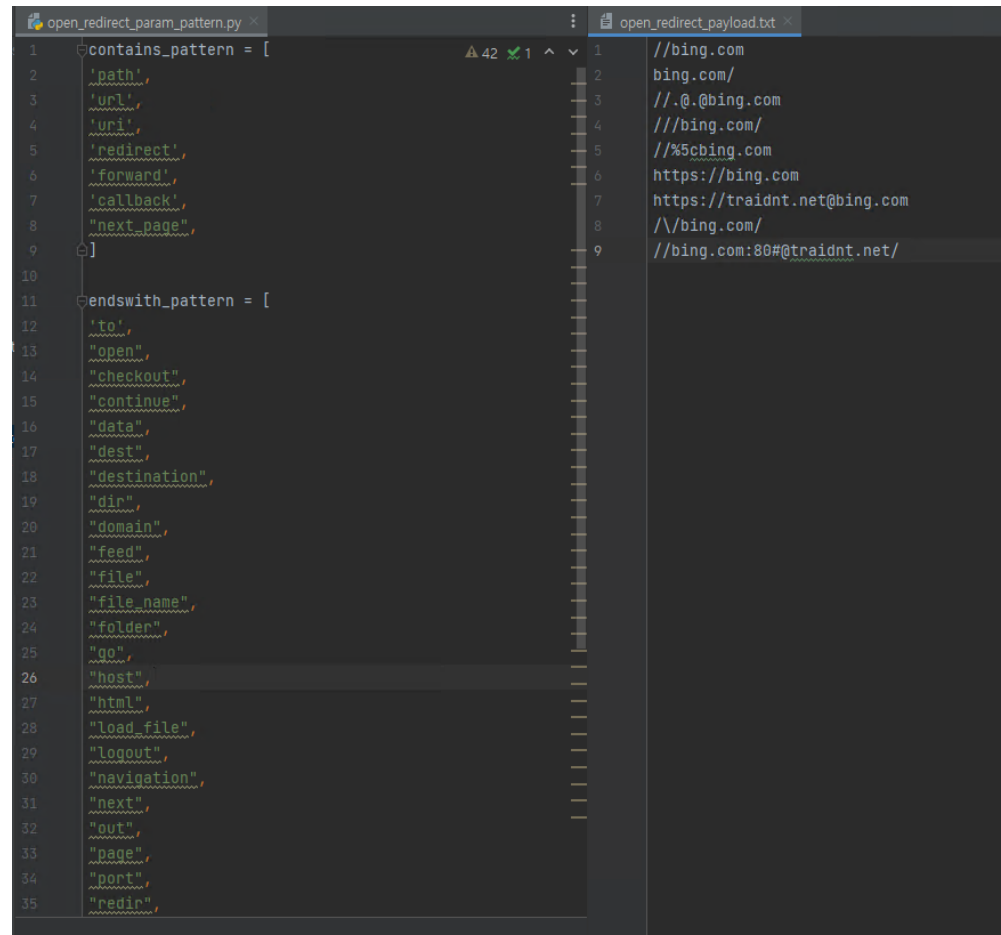
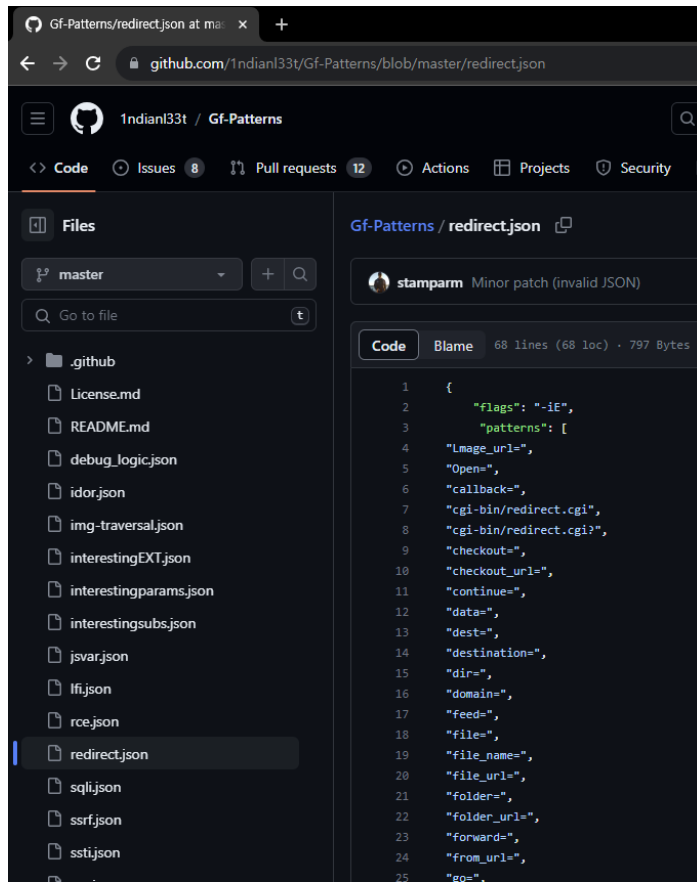
### property is\_permanent\_redirect

True if this Response one of the permanent versions of redirect.

# # 위협 평가 방법

## 추가로 간단한 웹 취약점 모듈 점검 추가

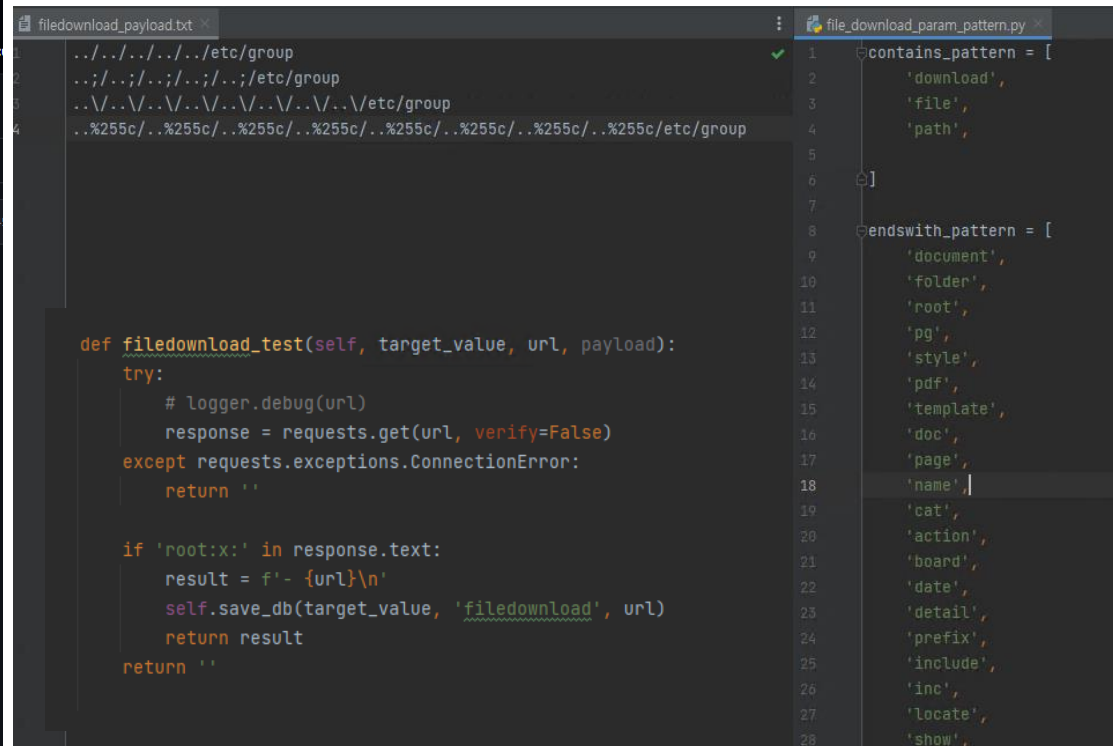
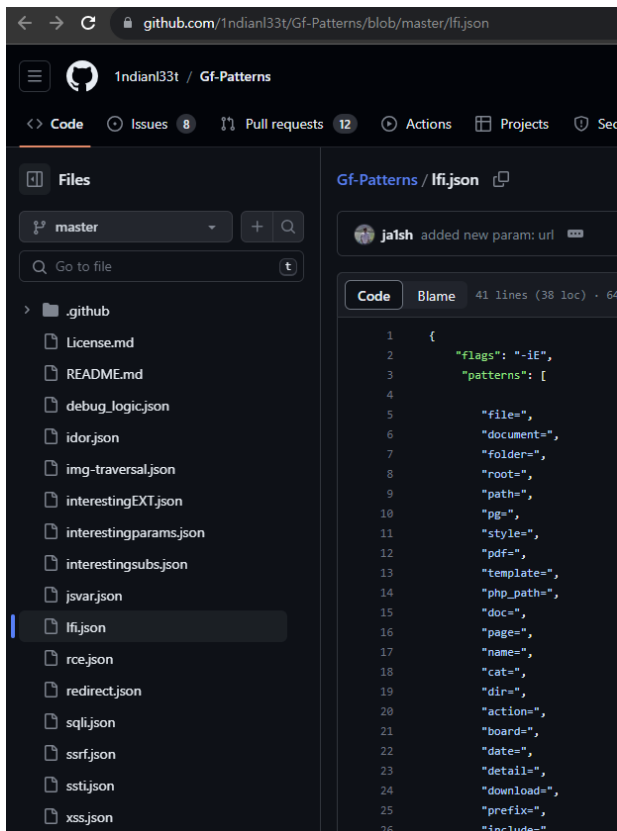
- Reflected XSS, **open redirect**, file download
  - <https://github.com/Encryptor-Sec/XSSearch>
  - <https://github.com/aldo-moreno-leon/ORTester>
  - <https://github.com/Indianl33t/Gf-Patterns>



## # 위협 평가 방법

## 추가로 간단한 웹 취약점 모듈 접점 추가

- **Reflected XSS, open redirect, file download**
  - <https://github.com/Encryptor-Sec/XSSearch>
  - <https://github.com/aldo-moreno-leon/ORTester>
  - <https://github.com/1ndianl33t/Gf-Patterns>





# # 버그헌팅 자동화

---

- ASM을 HackerOne 대상으로 하면 그게 곧 버그헌팅 자동화 😊
- 오픈 소스 도구 (특히 project discovery 툴) 활용해서 버그 헌팅하는 것은 아주 핫한 주제 ... (github repo, blog 포스팅 아주 많음!)

# # 버그헌팅 자동화

## 1. Hackerone 대상 수집

- hackerone 대상 수집 API 제공

<https://github.com/zricethezav/hldomains>

## 2. 자산 확장 및 파라미터 수집

- subfinder, httpx, katana

## 3. 취약점 점검

- Nuclei
- Reflected XSS, open redirect, File download

## 4. 알람 및 Report

- Telegram 사용
- hackerone api로 report 자동화도 가능! (나온게 없어서 굳이 하지는 않음 ☹)

ref) <https://api.hackerone.com>

# # 버그헌팅 자동화

## 딱 1건 정탐 ..

대상 : vimeo.com (동영상 스트리밍 사이트)

URL : [https://vimeo.com/help/zendesk\\_sso?redirect\\_to=%2F%2Fbing.com](https://vimeo.com/help/zendesk_sso?redirect_to=%2F%2Fbing.com)

← B bughunting 봇

10월 19일

[nuclei][embed.tumblr.com]

- name : postMessage - Cross-Site Scripting
- severity : high
- host : <https://embed.tumblr.com>

오전 8:46

10월 22일

[open\_redirect][vimeo.com]

- [https://vimeo.com/help/zendesk\\_sso?redirect\\_to=%2F%2Fbing.com](https://vimeo.com/help/zendesk_sso?redirect_to=%2F%2Fbing.com)

Bing

Spot me if you can!  
It's an all-too-common scene—you are strolling thr

오후 9:10

10월 23일

[nuclei][x.razorpay.com]

- name : Ghost CMS <=4.32 - Cross-Site Scripting
- severity : medium
- host : <https://x.razorpay.com>

Razorpay

RazorpayX

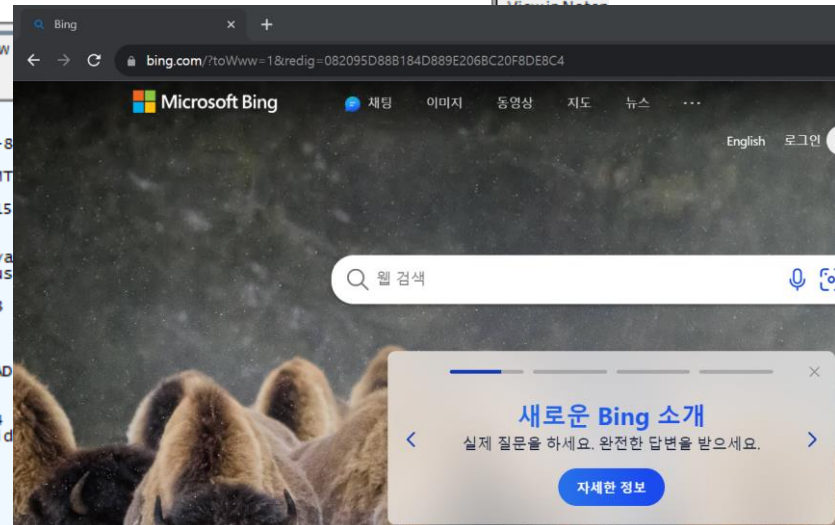
Sign Up for RazorpayX

오후 2:25

```
GET https://vimeo.com/help/zendesk_sso?redirect_to=%2F%2Fbing.com HTTP/1.1
Host: vimeo.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="118", "Google Chrome";v="118", "Not=A?Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: vuid=p1987948204.542673453; player=""; __cf_bm=ZE9NC. agFQ3HoASz_ONoLubt_kbDNJmmR5.3rRZw8A-1699086761-0-AeJ350mGikgvUPa37aQ3jOGjNqVnm9KLRdvd/bg8C4b3UHq9ZnJ51sbkg1e0g8hq0sDyeBKX0G8DeT6yz1Gv7C7g=

Find... (press Ctrl+Enter to highlight all)

Transformer Headers Textview SyntaxView
Raw JSON XML
HTTP/1.1 301 Moved Permanently
Date: Sat, 04 Nov 2023 08:32:51 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
expires: Fri, 03 Nov 2023 20:32:51 GMT
x-vimeo-device: d
strict-transport-security: max-age=315
Location: //bing.com
x-bapp-server: pweb-569c58d466-bd9np
via: 1.1 varnish (Varnish/6.0), 1.1 va
cache-control: no-store, no-cache, mus
x-varnish-cache: 0
x-vserver: web-varnish-prod-varnish-8
x-backend-proxy: webproxy9
Accept-Ranges: bytes
Age: 0
X-Served-By: cache-iad-kjyo7100027-IAO
X-Cache: MISS, MISS
X-Cache-Hits: 0, 0
X-Timer: S1699086771.124355,V50,VE264
Vary: User-Agent,x-http-method-override
CF-Cache-Status: DYNAMIC
Server: cloudflare
CF-RAY: 820b823f6a763269-ICN
Content-Length: 0
```

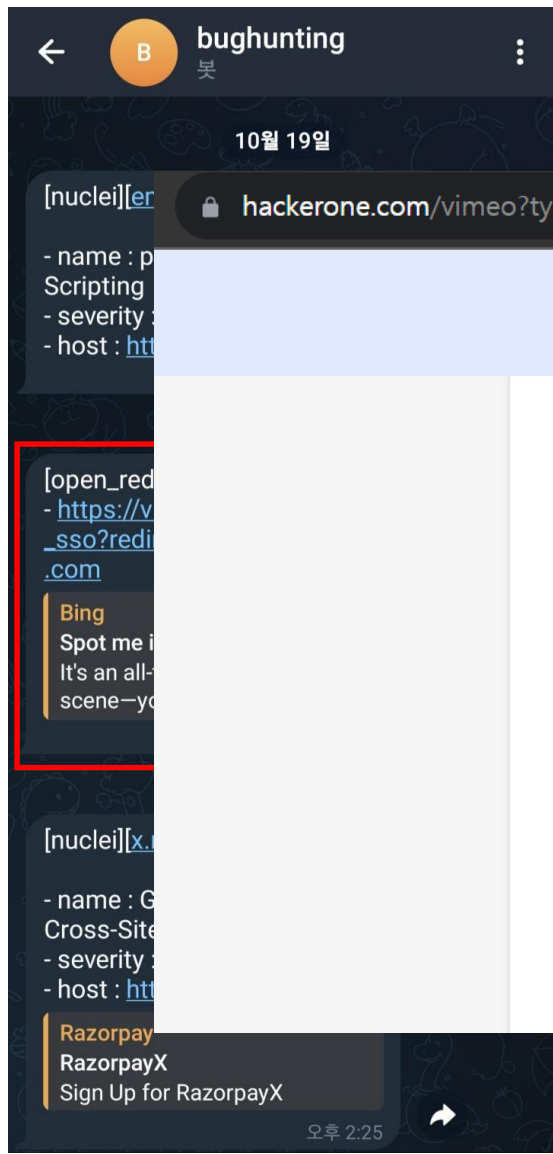


# # 버그헌팅 자동화

## 딱 1건 정탐 ..

대상 : vimeo.com (동영상 스트리밍 사이트)

URL : [https://vimeo.com/help/zendesk\\_sso?redirect\\_to=%2F%2Fbing.com](https://vimeo.com/help/zendesk_sso?redirect_to=%2F%2Fbing.com)



hackerone.com/vimeo?type=team

Learn

### Non-qualifying vulnerabilities (out-of-scope)

- User enumeration
- Open redirect (Unless chained to show an impact)
- Reports from automated tools or scans
- Missing rate limits, unless it can lead to account takeover
- Missing cookie flags on non-sensitive cookies
- Logout CSRF attacks (unless chained to show an impactful exploit)
- Reports of insecure SSL/TLS ciphers (unless you have a working proof of concept)
- Reports of insecure crossdomain.xml configuration (again, unless you have a working proof of concept)
- Reports of window.opener redirects

Server: Cloudflare  
CF-RAY: 820b823f6a763269-ICN  
Content-Length: 0



자세한 정보

# # 결론

- ASM의 주요 기능인 자산 식별 방법 (Shadow IT 탐지) 에 대해서 공유
- 그리고.. hackerone 대상으로 nuclei 돌리는 방법은 이미 **Red Ocean** 관한 시간 낭비하지 마시길... ☹
- 웹 크롤링 또는 취약점 모듈에 있어서 차별화가 있어야 할 듯
  - 로그인 세션을 가지고 크롤링 한다던지...
  - 다양한 취약점 모듈, 점검 방식 고도화 등...

**END**