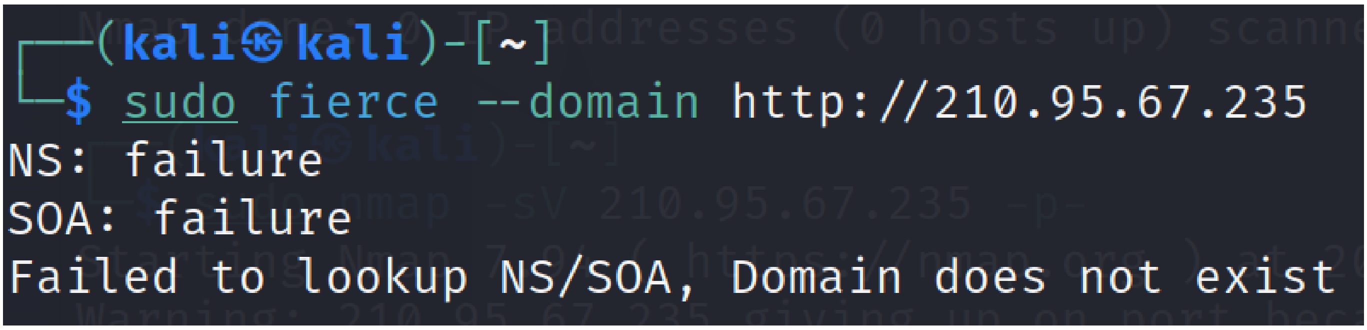
ASP + MSSQL 사이트 환경

- 대상 사이트: http://210.95.67.235:8181/

정보수집단계 - 서브도메인 파악 - fierce

```
sudo fierce --domain http://210.95.67.235:8181/
```

Fierce 수행 결과

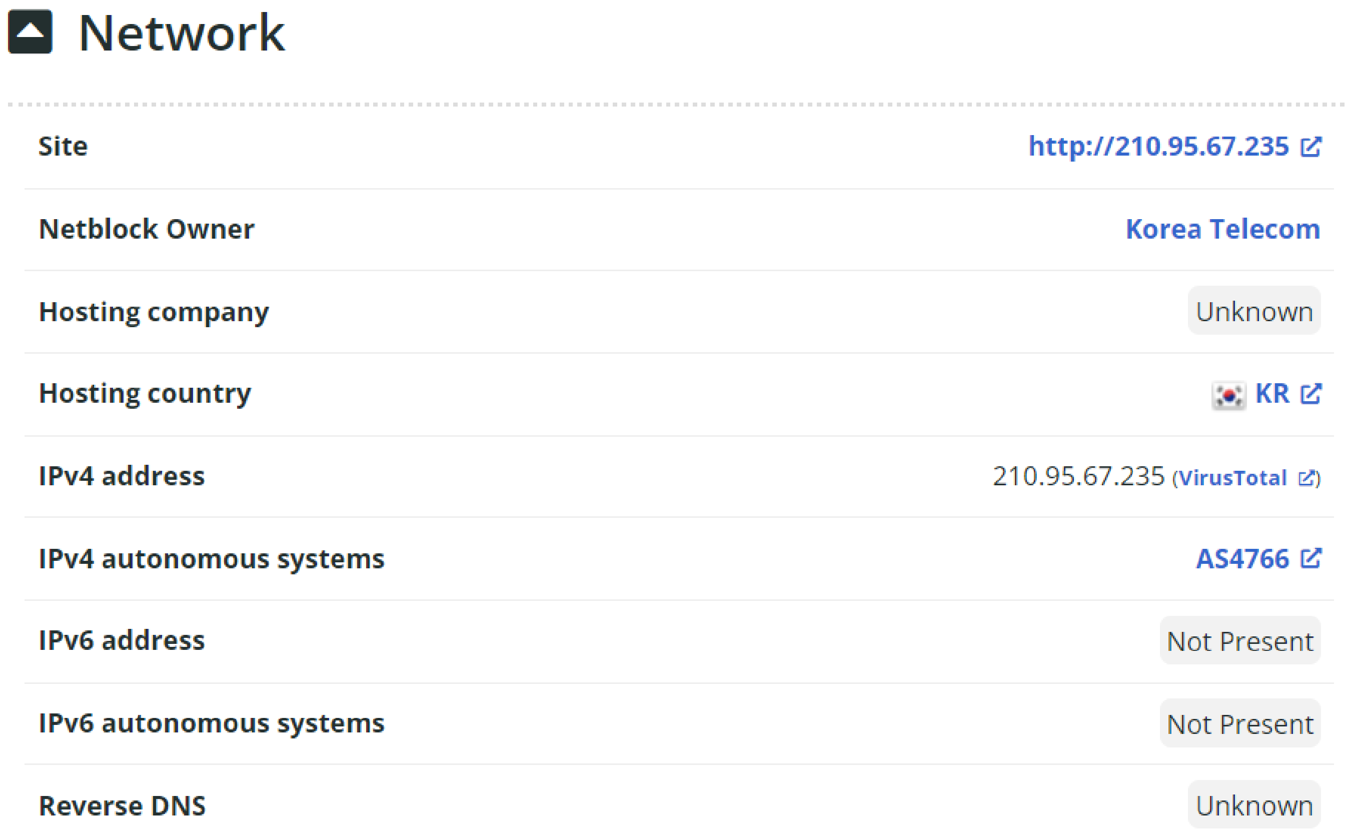


```
┌──(kali㉿kali)-[~]
└─$ sudo fierce --domain http://210.95.67.235
NS: failure
SOA: failure
Failed to lookup NS/SOA, Domain does not exist
```

정보수집단계 - 서브도메인 파악 - netcraft 검색

- 수행 결과: https://sitereport.netcraft.com/?url=http://210.95.67.235

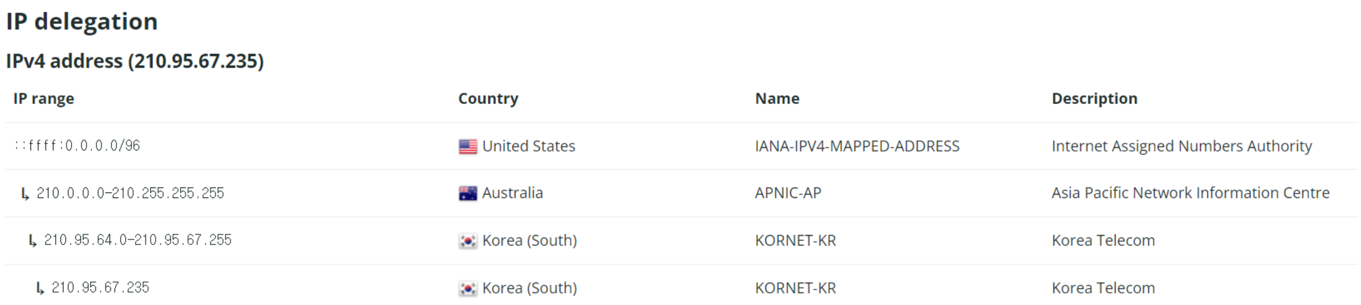
Network 정보



Network

Site	http://210.95.67.235
Netblock Owner	Korea Telecom
Hosting company	Unknown
Hosting country	KR
IPv4 address	210.95.67.235 (VirusTotal)
IPv4 autonomous systems	AS4766
IPv6 address	Not Present
IPv6 autonomous systems	Not Present
Reverse DNS	Unknown

IP 주소 범위



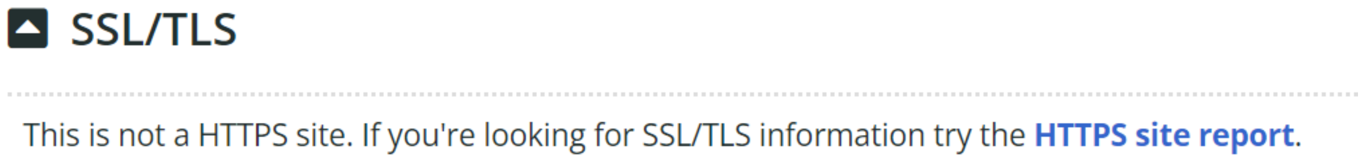
IP delegation

IPv4 address (210.95.67.235)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 210.0.0.0-210.255.255.255	Australia	APNIC-AP	Asia Pacific Network Information Centre
↳ 210.95.64.0-210.95.67.255	Korea (South)	KORNET-KR	Korea Telecom
↳ 210.95.67.235	Korea (South)	KORNET-KR	Korea Telecom

SSL/TLS

HTTPS를 사용하고 있지 않으므로 SSL을 적용하지 않음



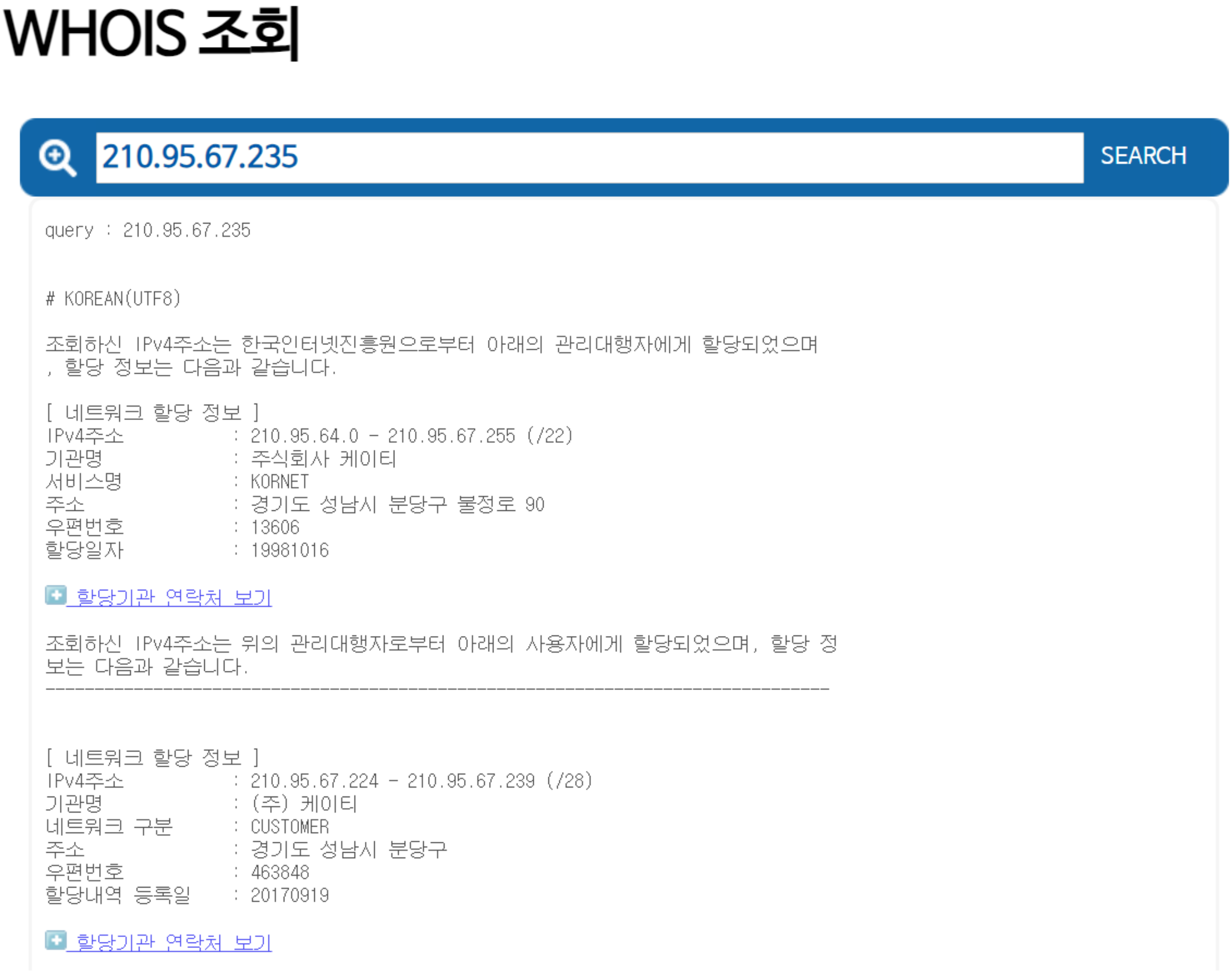
SSL/TLS

This is not a HTTPS site. If you're looking for SSL/TLS information try the **HTTPS site report**.

정보수집단계 - 서브도메인 파악 - whois 검색

KISA 후이즈검색

- 네트워크 할당 정보



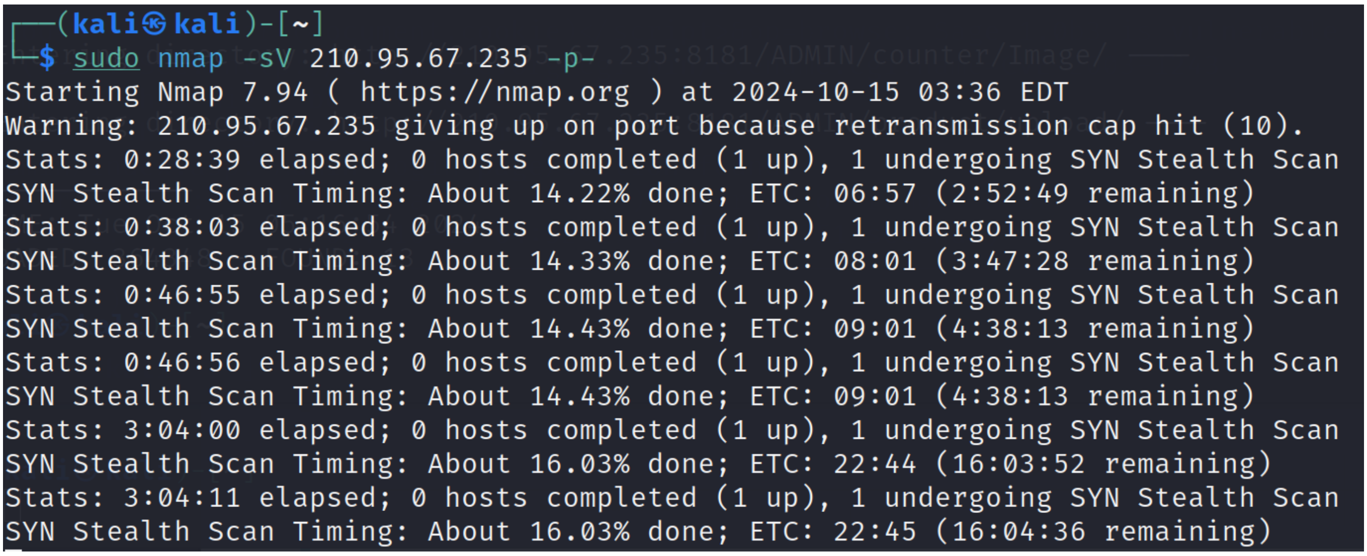
WHOIS 조회

```
query : 210.95.67.235

# KOREAN(UTF8)

조회하신 IPv4주소는 한국인터넷진흥원으로부터 아래의 관리대행자에게 할당되었으며
, 할당 정보는 다음과 같습니다.

[ 네트워크 할당 정보 ]
IPv4주소           : 210.95.64.0 - 210.95.67.255 (/22)
기관명             : 주식회사 케이티
서비스명           : KORNET
주소               : 경기도 성남시 분당구 불정로 90
우편번호           : 13606
할당일자           : 19981016

할당기관 연락처 보기

조회하신 IPv4주소는 위의 관리대행자로부터 아래의 사용자에게 할당되었으며, 할당 정
보는 다음과 같습니다.
--------------------------------------------------------------------------------


[ 네트워크 할당 정보 ]
IPv4주소           : 210.95.67.224 - 210.95.67.239 (/28)
기관명             : (주) 케이티
네트워크 구분      : CUSTOMER
주소               : 경기도 성남시 분당구
우편번호           : 463848
할당내역 등록일    : 20170919

할당기관 연락처 보기
```

정보수집단계 - 포트 점검 - nmap 사용

수집한 IP 주소로 포트 스캔 수행, -sV 옵션으로 버전 정보까지 확인

`sudo nmap -sV http://210.95.67.235 -p-` 아직 진행중입니다..



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 210.95.67.235 -p-
Starting Nmap 7.94 ( https://nmap.org ) at 2024-10-15 03:36 EDT
Warning: 210.95.67.235 giving up on port because retransmission cap hit (10).
Stats: 0:28:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 14.22% done; ETC: 06:57 (2:52:49 remaining)
Stats: 0:38:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 14.33% done; ETC: 08:01 (3:47:28 remaining)
Stats: 0:46:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 14.43% done; ETC: 09:01 (4:38:13 remaining)
Stats: 0:46:56 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 14.43% done; ETC: 09:01 (4:38:13 remaining)
Stats: 3:04:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 16.03% done; ETC: 22:44 (16:03:52 remaining)
Stats: 3:04:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 16.03% done; ETC: 22:45 (16:04:36 remaining)
```

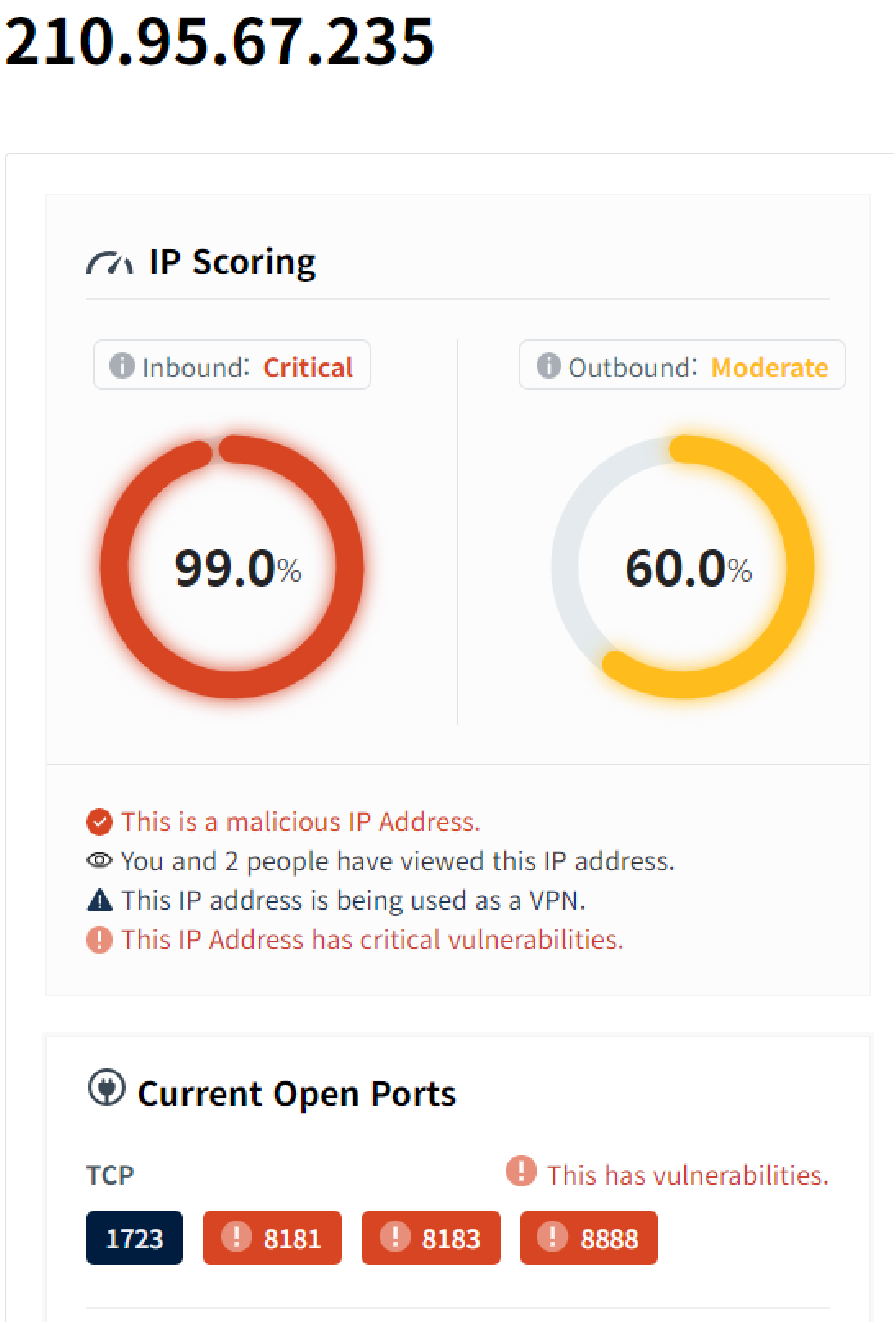
정보수집단계 - OSINT (Criminal IP) 사용

https://www.criminalip.io/ko/asset/report/210.95.67.235

Malicious IP

해당 IP는 Malicious IP 라고 나옴

- malicious IP is any IP address that has been positively associated with malicious activity



210.95.67.235

IP Scoring

Inbound: Critical

99.0%

Outbound: Moderate

60.0%

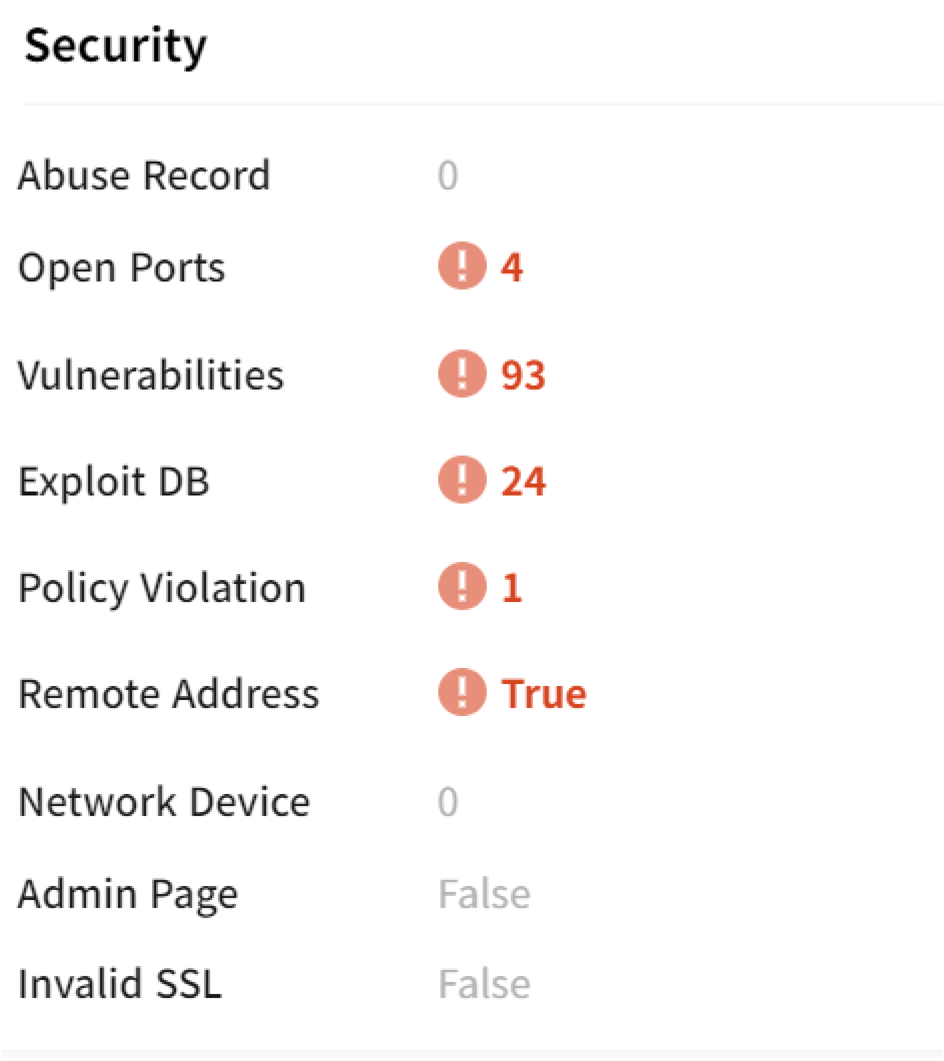
✓ This is a malicious IP Address.
👁 You and 2 people have viewed this IP address.
⚠ This IP address is being used as a VPN.
! This IP Address has critical vulnerabilities.

Current Open Ports

TCP ! This has vulnerabilities.

1723 ! 8181 ! 8183 ! 8888

취약점 요약

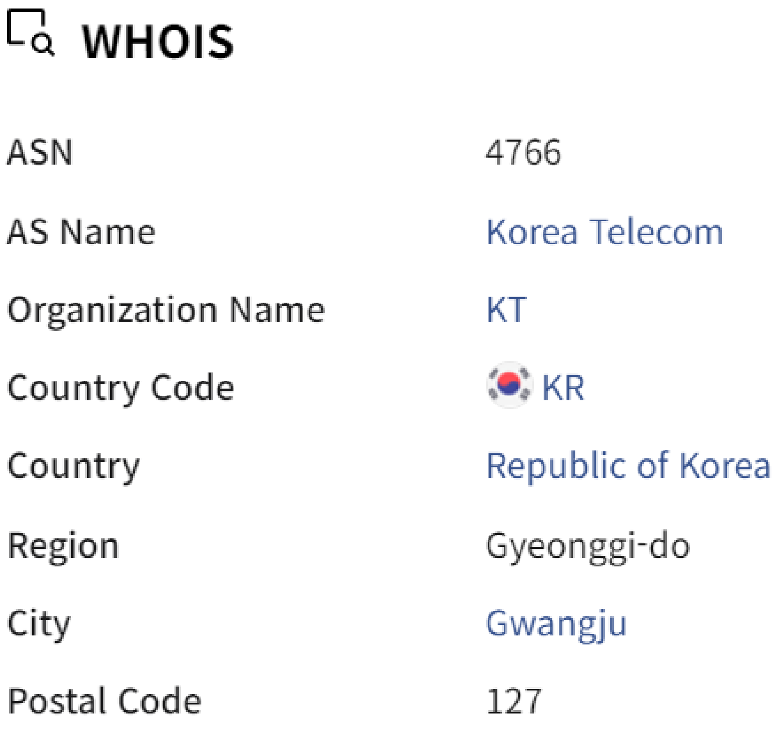


Security

Abuse Record	0
Open Ports	❗ 4
Vulnerabilities	❗ 93
Exploit DB	❗ 24
Policy Violation	❗ 1
Remote Address	❗ True
Network Device	0
Admin Page	False
Invalid SSL	False

- Open Ports: 열려진 포트 4개
- Vulnerabilities: 취약점 93개
- Explot DB: 24개
- 기타 등등

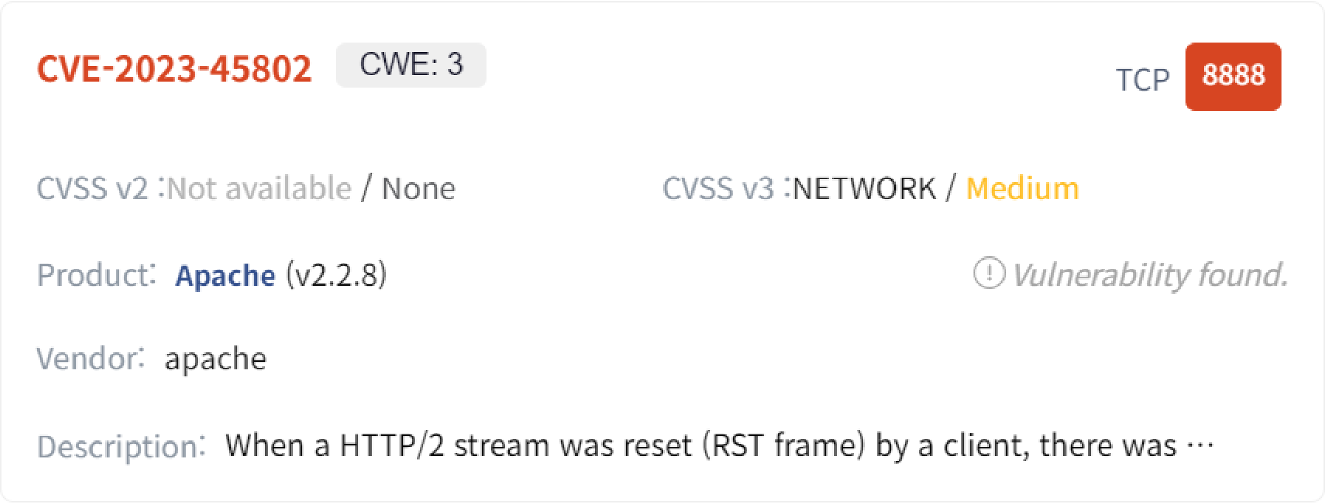
WHOIS 정보



WHOIS

ASN	4766
AS Name	Korea Telecom
Organization Name	KT
Country Code	KR
Country	Republic of Korea
Region	Gyeonggi-do
City	Gwangju
Postal Code	127

취약점1 - CVE-2023-45802



CVE-2023-45802 CWE: 3

TCP 8888

CVSS v2 :Not available / None

CVSS v3 :NETWORK / Medium

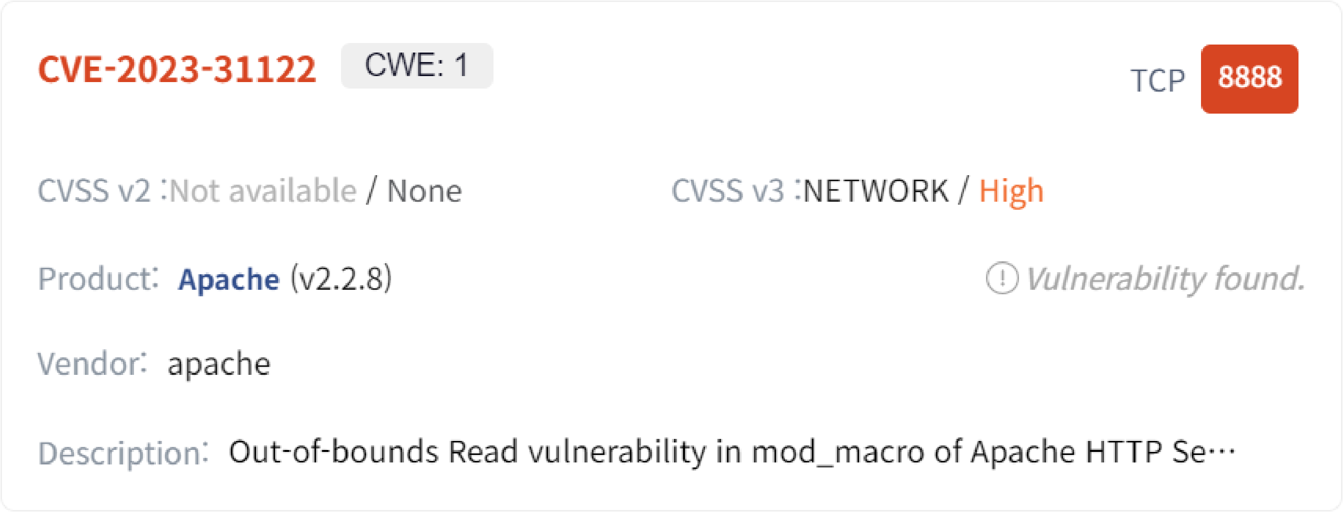
Product: **Apache** (v2.2.8)

Vulnerability found.

Vendor: apache

Description: When a HTTP/2 stream was reset (RST frame) by a client, there was ···

취약점2 - CVE-2023-31122



CVE-2023-31122 CWE: 1 TCP 8888

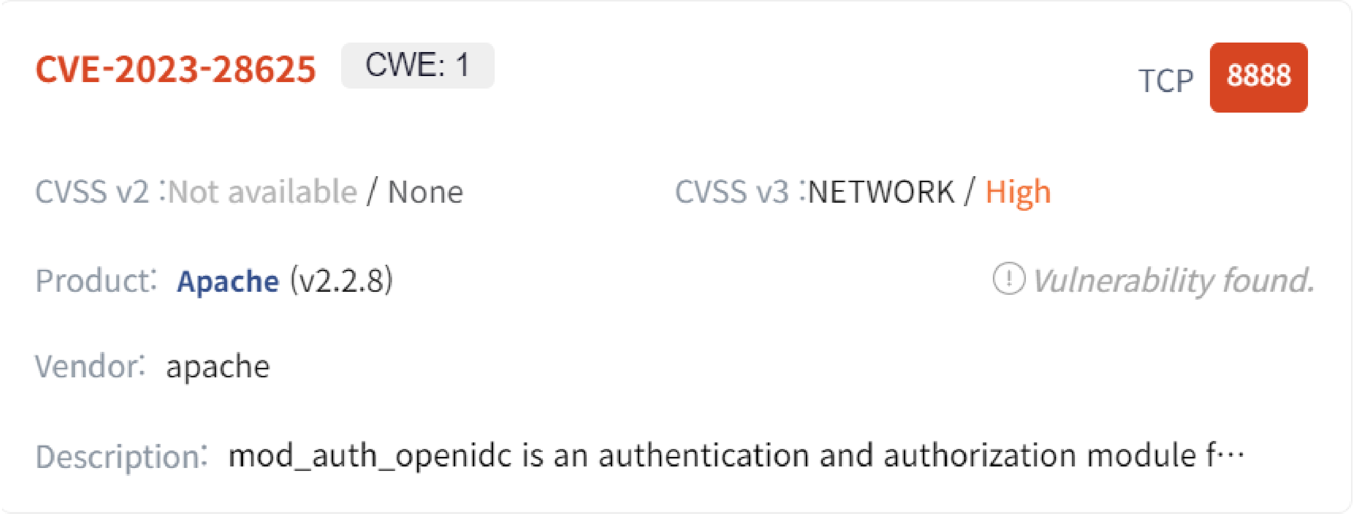
CVSS v2 :Not available / None CVSS v3 :NETWORK / High

Product: Apache (v2.2.8) Vulnerability found.

Vendor: apache

Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Se…

취약점3 - CVE-2023-28625



CVE-2023-28625 CWE: 1 TCP 8888

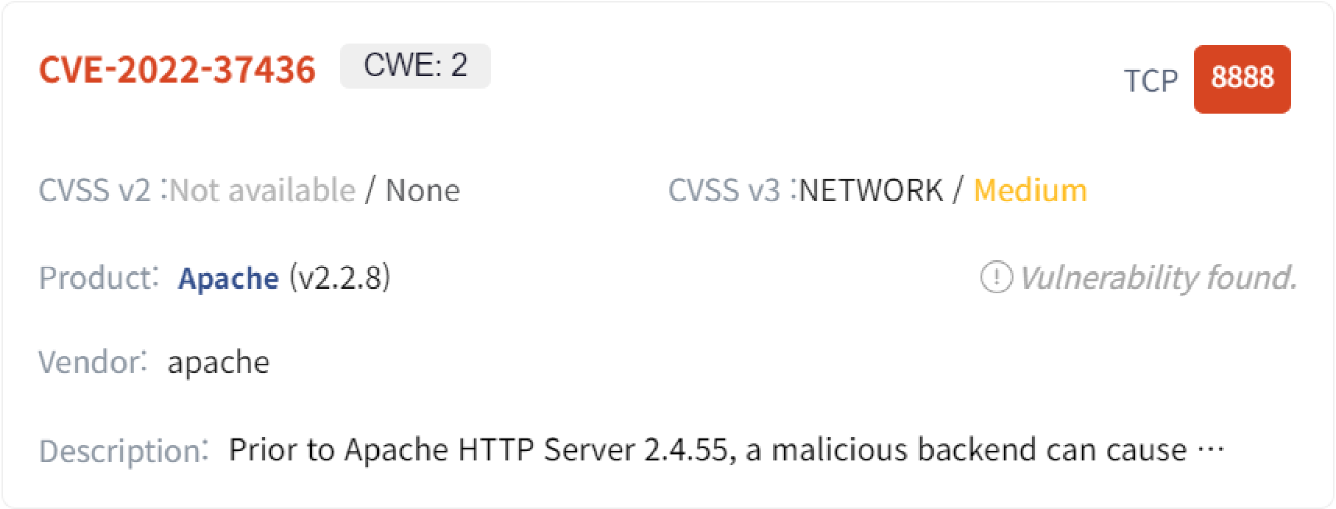
CVSS v2 :Not available / None CVSS v3 :NETWORK / High

Product: Apache (v2.2.8) Vulnerability found.

Vendor: apache

Description: mod_auth_openidc is an authentication and authorization module f…

취약점4 - CVE-2022-37436



CVE-2022-37436 CWE: 2 TCP 8888

CVSS v2 :Not available / None CVSS v3 :NETWORK / Medium

Product: Apache (v2.2.8) Vulnerability found.

Vendor: apache

Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause …

정보수집단계 - 구글 해킹 취약점 체크

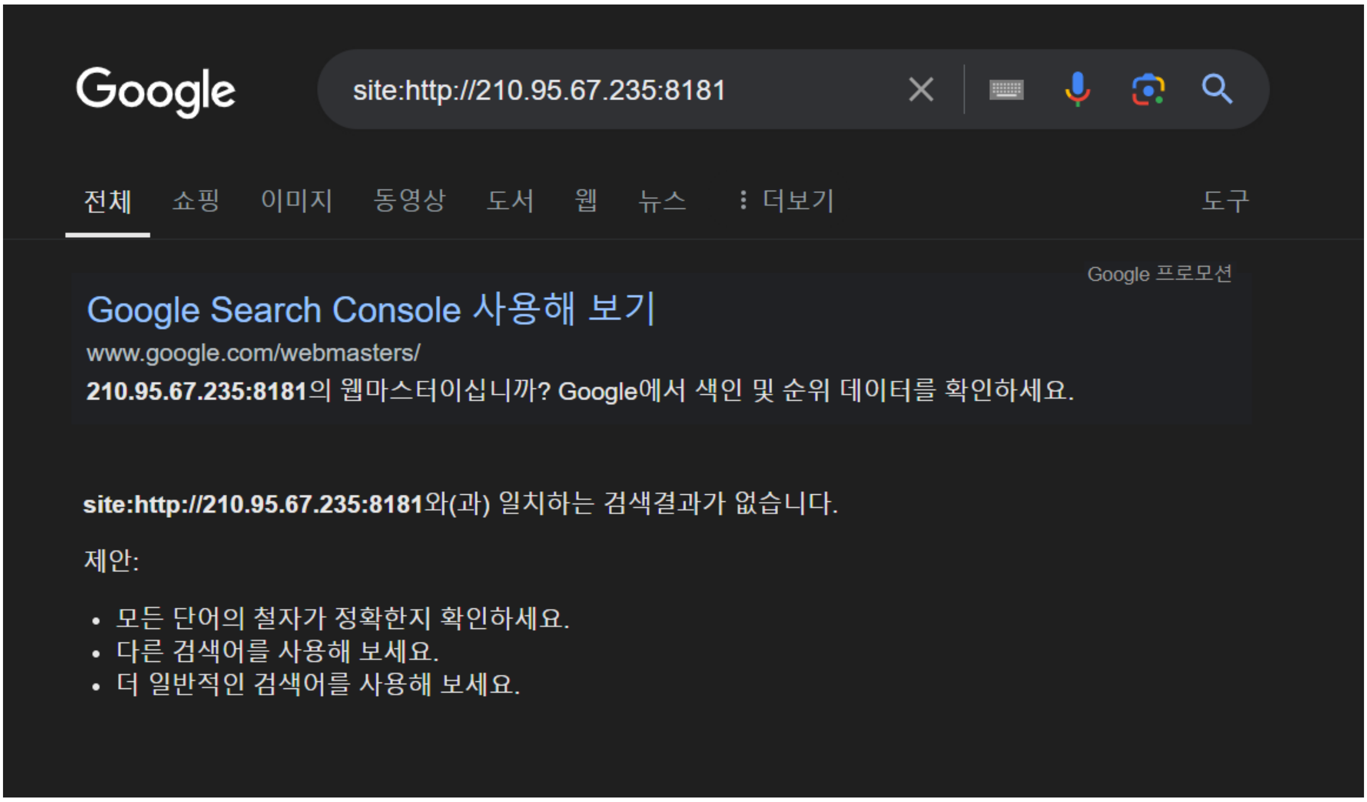
robots.txt 체크

robots.txt 페이지가 존재하지 않음

- https://testphp.vulnweb.com/robots.txt

구글해킹 시도

웹사이트가 구글 검색엔진에 등록되어 있지 않아 구글해킹 취약점은 발견할 수 없었다.



Google Search Console 사용해 보기
www.google.com/webmasters/
210.95.67.235:8181의 웹마스터이십니까? Google에서 색인 및 순위 데이터를 확인하세요.

site:http://210.95.67.235:8181와(과) 일치하는 검색결과가 없습니다.

제안:

- 모든 단어의 철자가 정확한지 확인하세요.
- 다른 검색어를 사용해 보세요.
- 더 일반적인 검색어를 사용해 보세요.

- 사용 검색어
  `site:210.95.67.235:8181 inurl:admin` `site:210.95.67.235:8181 intext:password` `site:210.95.67.235:8181 inurl:admin filetype:xlsx` `site:210.95.67.235:8181 filetype:php` `site:210.95.67.235:8181 filetype:php` `site:210.95.67.235:8181 filetype:php`

취약점 분석 단계 - Nikto

`sudo nikto -h http://210.95.67.235:8181`

```
[sudo] password for kali:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          210.95.67.235
+ Target Hostname:    210.95.67.235
+ Target Port:        8181
+ Start Time:         2024-10-15 04:28:06 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/6.0
+ /: Cookie ASPSESSIONIDQQRRCQBT created without the httponly flag. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Retrieved x-powered-by header: ASP.NET.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /images: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "192.168.0.94". See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0649
+ OPTIONS: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ OPTIONS: Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ /?mod=<script>alert(document.cookie)</script>&op=browse: Sage 1.0b3 is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1243
+ /admin/: This might be interesting.
+ /Admin/: This might be interesting.
+ /admin/index.asp: Admin login page/section found.
+ 8110 requests: 1 error(s) and 11 item(s) reported on remote host
+ End Time:           2024-10-15 04:32:17 (GMT-4) (251 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

취약점 분석 단계 - dirb

`sudo dirb http://210.95.67.235`