IE2062 [2023/JUL]- Web Security

Web Security BB Assignment

Report 06 – Mediahuis Corporate Domains

Lecturer in charge – Ms. Chethana Liyanapathirana

IT21826368 – Nanayakkara Y.D.T.D

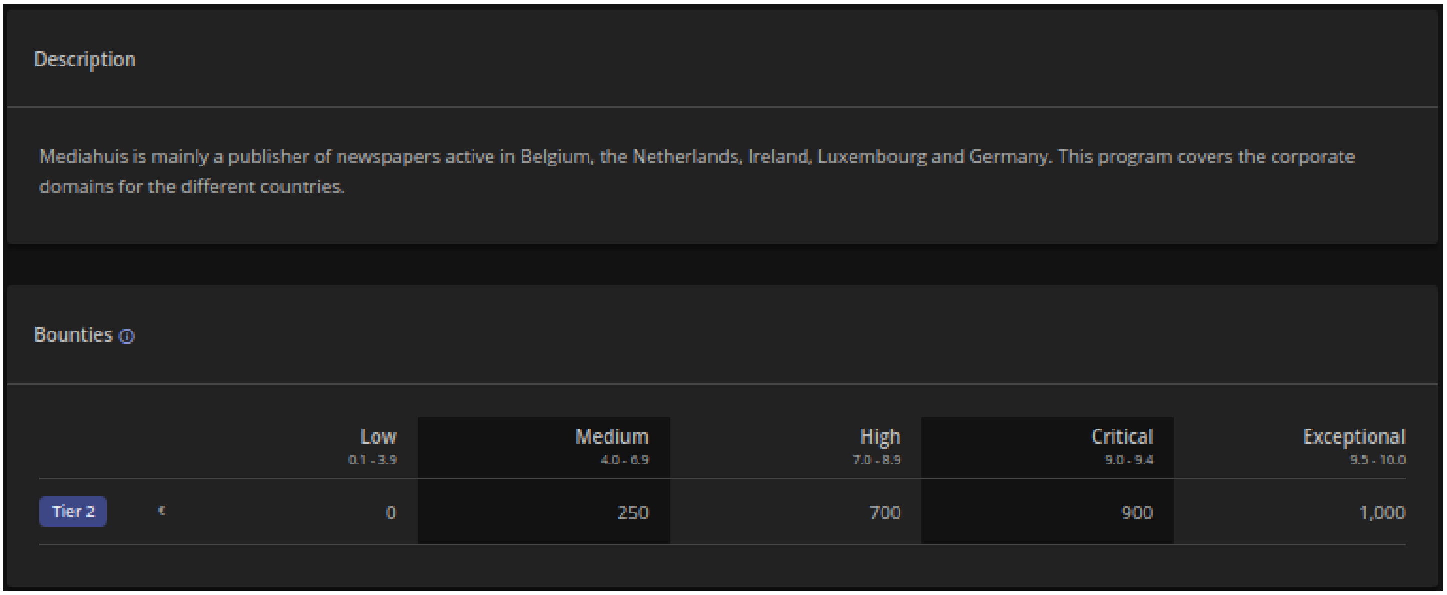
Contents

1. Mediahuis/Mediahuis Corporate Domains/Detail

Registered Open

Mediahuis/Mediahuis Corporate Domains/Detail

1.1. Overview



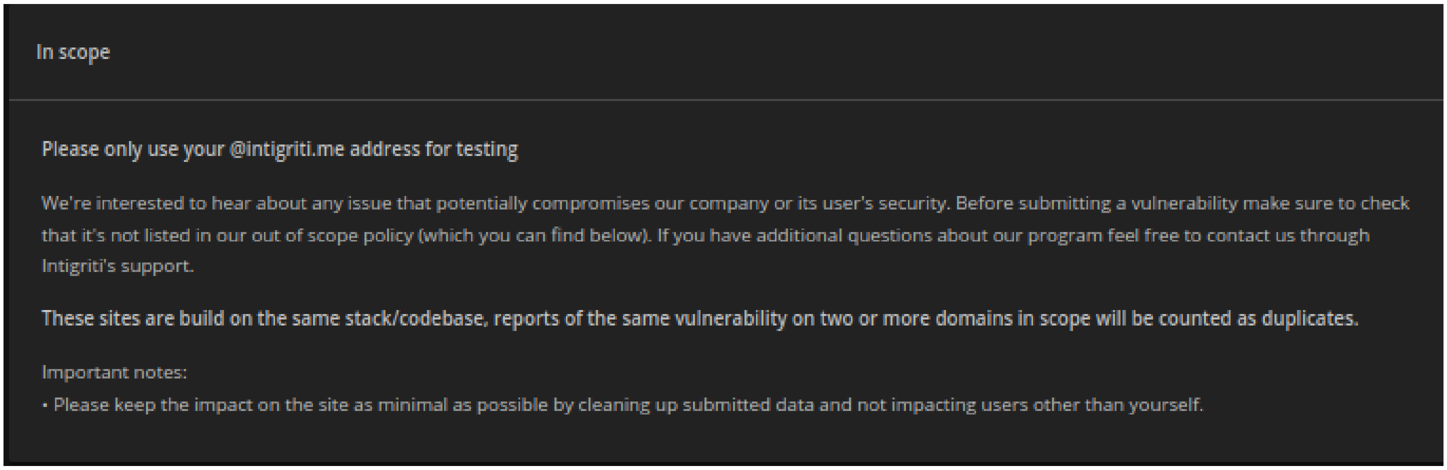
Description

Mediahuis is mainly a publisher of newspapers active in Belgium, the Netherlands, Ireland, Luxembourg and Germany. This program covers the corporate domains for the different countries.

Bounties ⓘ

		Low 0.1 - 3.9	Medium 4.0 - 6.9	High 7.0 - 8.9	Critical 9.0 - 9.4	Exceptional 9.5 - 10.0
Tier 2	€	0	250	700	900	1,000

1.2. Scope



In scope

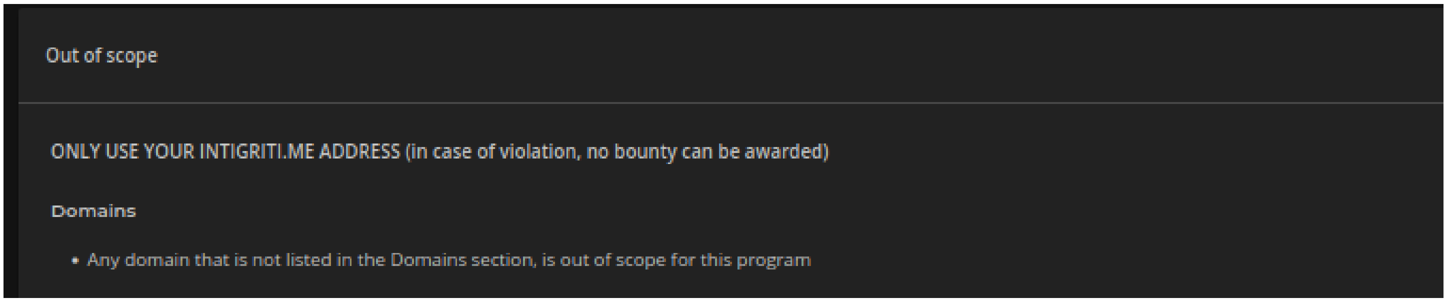
Please only use your @intigriti.me address for testing

We're interested to hear about any issue that potentially compromises our company or its user's security. Before submitting a vulnerability make sure to check that it's not listed in our out of scope policy (which you can find below). If you have additional questions about our program feel free to contact us through Intigriti's support.

These sites are build on the same stack/codebase, reports of the same vulnerability on two or more domains in scope will be counted as duplicates.

Important notes:
• Please keep the impact on the site as minimal as possible by cleaning up submitted data and not impacting users other than yourself.

1.3. Out of Scope

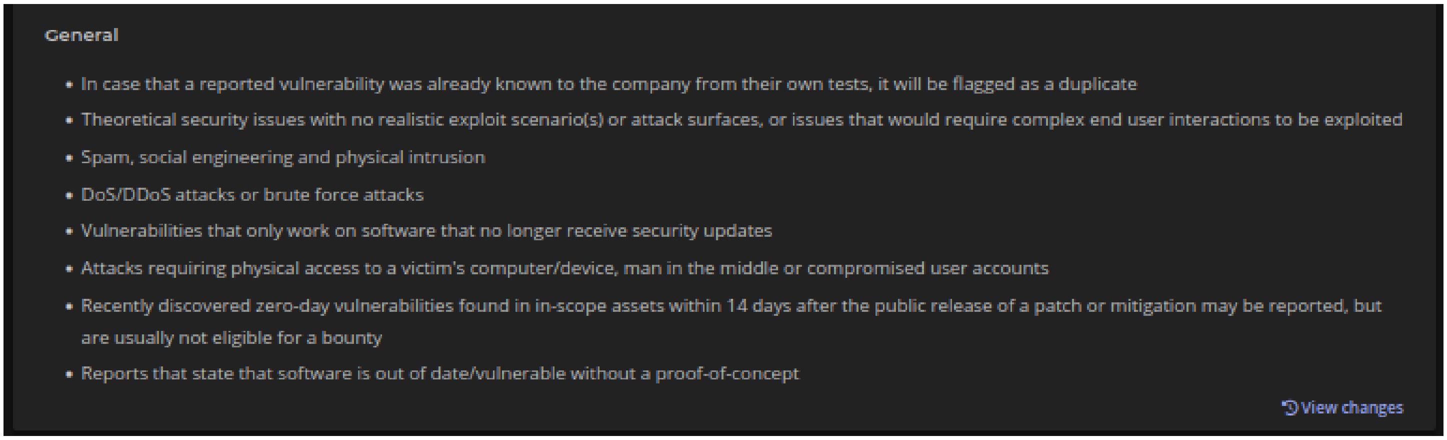


Out of scope

ONLY USE YOUR INTIGRITI.ME ADDRESS (in case of violation, no bounty can be awarded)

Domains

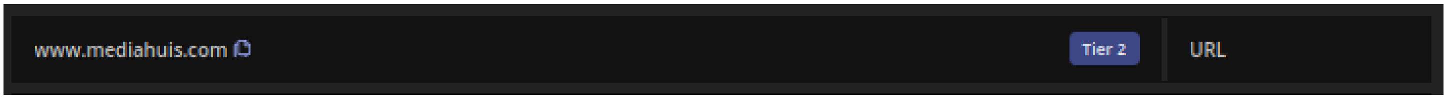
- Any domain that is not listed in the Domains section, is out of scope for this program



General

- In case that a reported vulnerability was already known to the company from their own tests, it will be flagged as a duplicate
- Theoretical security issues with no realistic exploit scenario(s) or attack surfaces, or issues that would require complex end user interactions to be exploited
- Spam, social engineering and physical intrusion
- DoS/DDoS attacks or brute force attacks
- Vulnerabilities that only work on software that no longer receive security updates
- Attacks requiring physical access to a victim's computer/device, man in the middle or compromised user accounts
- Recently discovered zero-day vulnerabilities found in in-scope assets within 14 days after the public release of a patch or mitigation may be reported, but are usually not eligible for a bounty
- Reports that state that software is out of date/vulnerable without a proof-of-concept

1.4.Selected Domains



www.mediahuis.com

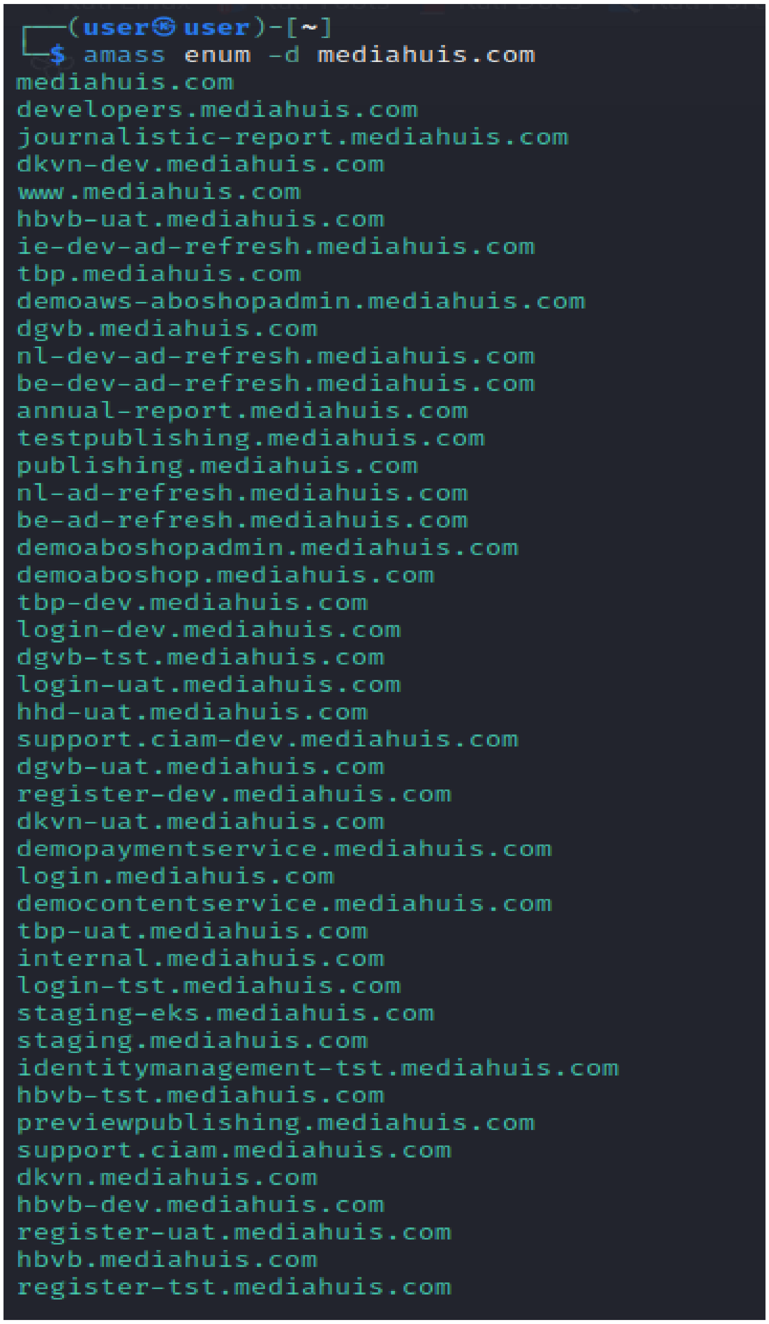
Tier 2

URL

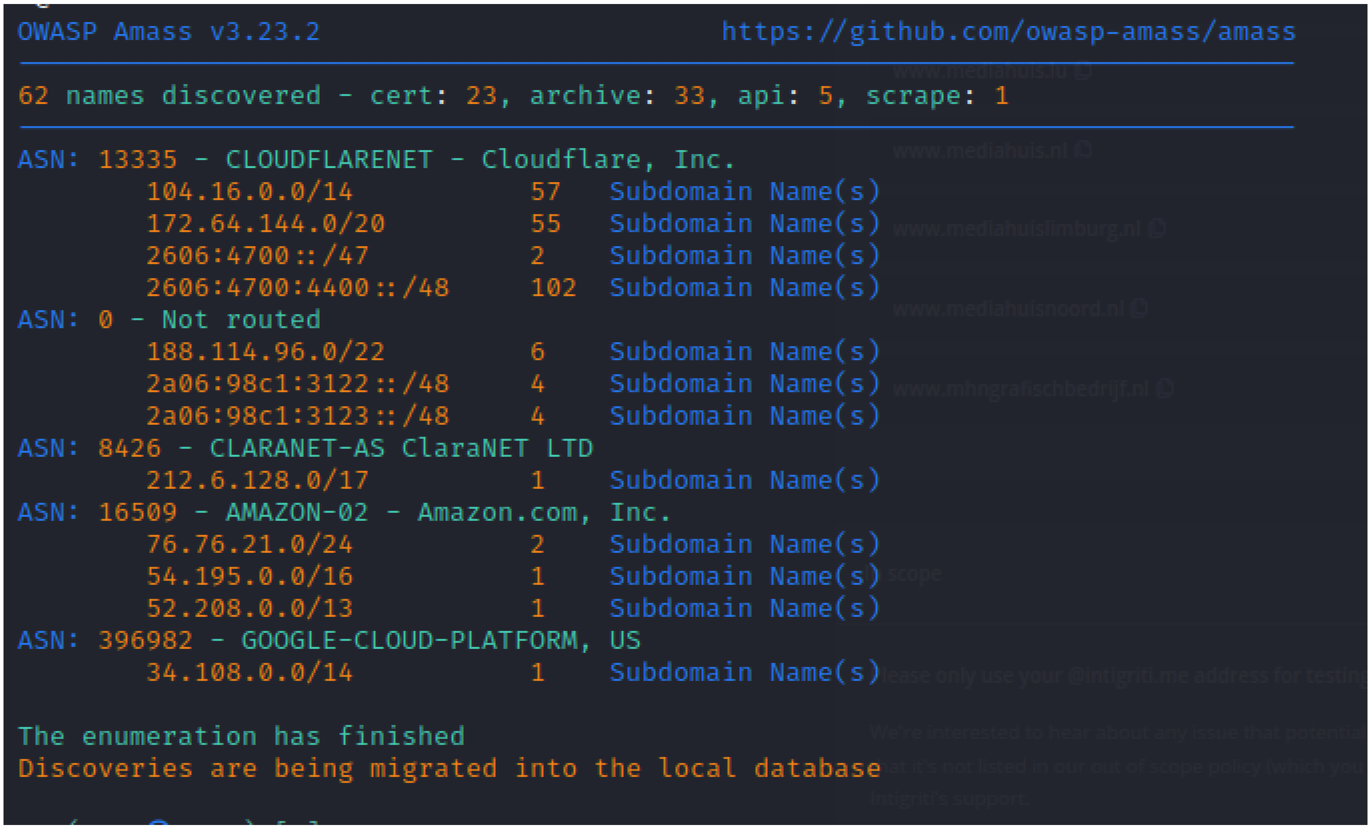
In this URL www.mediahuis.com used for scanning

2. Information Gathering

1.1.Using Amass

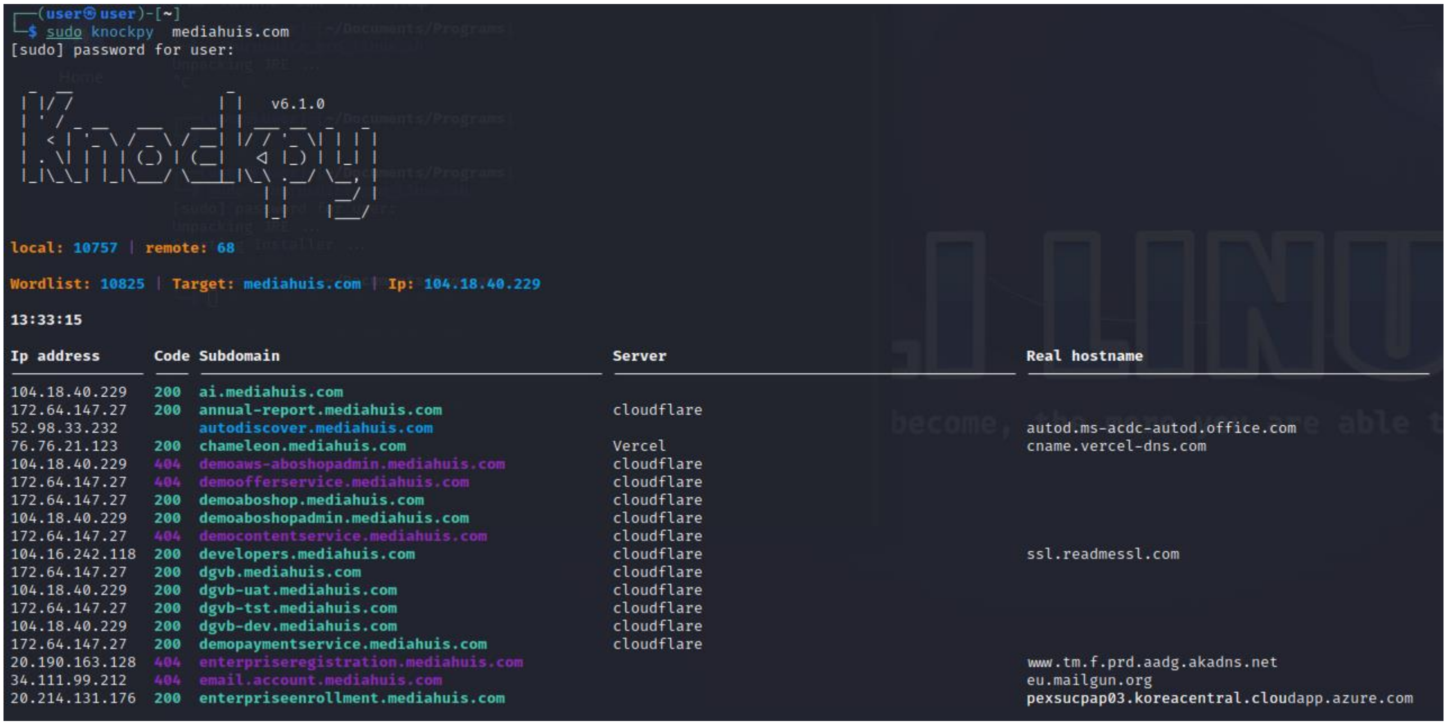


```
┌──(user㉿user)-[~]
└─$ amass enum -d mediahuis.com
mediahuis.com
developers.mediahuis.com
journalistic-report.mediahuis.com
dkvn-dev.mediahuis.com
www.mediahuis.com
hbvb-uat.mediahuis.com
ie-dev-ad-refresh.mediahuis.com
tbp.mediahuis.com
demoaws-aboshopadmin.mediahuis.com
dgvb.mediahuis.com
nl-dev-ad-refresh.mediahuis.com
be-dev-ad-refresh.mediahuis.com
annual-report.mediahuis.com
testpublishing.mediahuis.com
publishing.mediahuis.com
nl-ad-refresh.mediahuis.com
be-ad-refresh.mediahuis.com
demoaboshopadmin.mediahuis.com
demoaboshop.mediahuis.com
tbp-dev.mediahuis.com
login-dev.mediahuis.com
dgvb-tst.mediahuis.com
login-uat.mediahuis.com
hhd-uat.mediahuis.com
support.ciam-dev.mediahuis.com
dgvb-uat.mediahuis.com
register-dev.mediahuis.com
dkvn-uat.mediahuis.com
demopaymentservice.mediahuis.com
login.mediahuis.com
democontentservice.mediahuis.com
tbp-uat.mediahuis.com
internal.mediahuis.com
login-tst.mediahuis.com
staging-eks.mediahuis.com
staging.mediahuis.com
identitymanagement-tst.mediahuis.com
hbvb-tst.mediahuis.com
previewpublishing.mediahuis.com
support.ciam.mediahuis.com
dkvn.mediahuis.com
hbvb-dev.mediahuis.com
register-uat.mediahuis.com
hbvb.mediahuis.com
register-tst.mediahuis.com
```

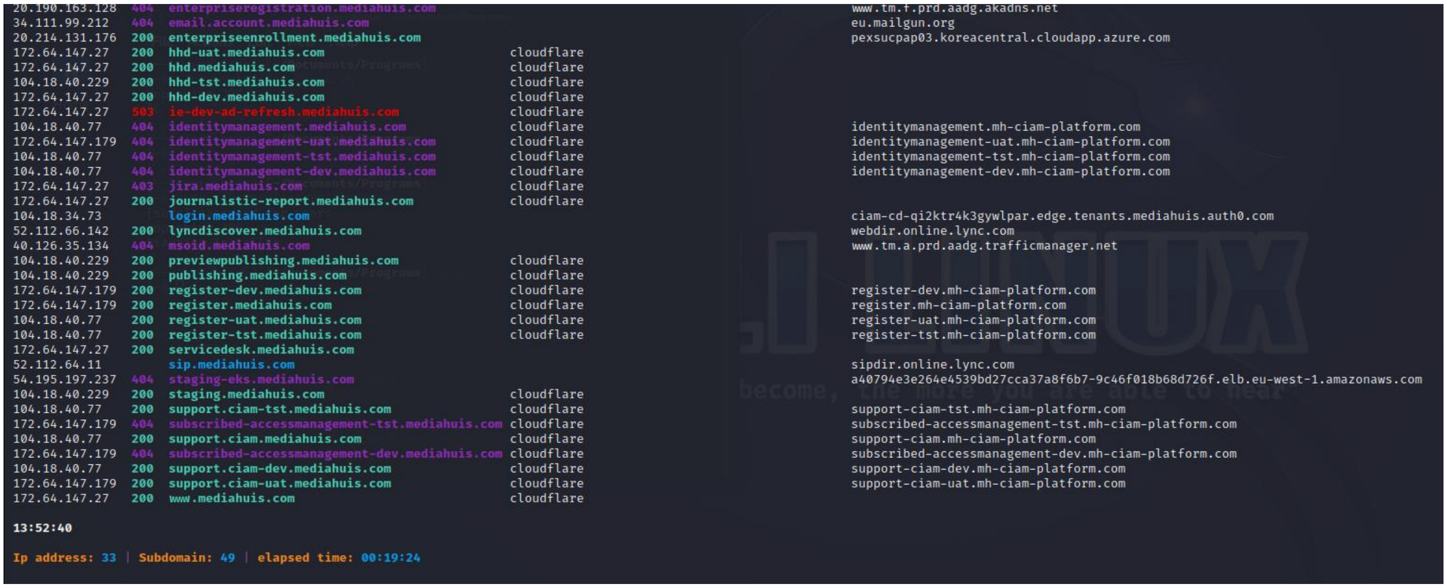


```
OWASP Amass v3.23.2                          https://github.com/owasp-amass/amass
--------------------------------------------------------------------------------
62 names discovered - cert: 23, archive: 33, api: 5, scrape: 1
--------------------------------------------------------------------------------
ASN: 13335 - CLOUDFLARENET - Cloudflare, Inc.
        104.16.0.0/14           57    Subdomain Name(s)
        172.64.144.0/20         55    Subdomain Name(s)
        2606:4700::/47          2     Subdomain Name(s)
        2606:4700:4400::/48     102   Subdomain Name(s)
ASN: 0 - Not routed
        188.114.96.0/22         6     Subdomain Name(s)
        2a06:98c1:3122::/48     4     Subdomain Name(s)
        2a06:98c1:3123::/48     4     Subdomain Name(s)
ASN: 8426 - CLARANET-AS ClaraNET LTD
        212.6.128.0/17          1     Subdomain Name(s)
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
        76.76.21.0/24           2     Subdomain Name(s)
        54.195.0.0/16           1     Subdomain Name(s)
        52.208.0.0/13           1     Subdomain Name(s)
ASN: 396982 - GOOGLE-CLOUD-PLATFORM, US
        34.108.0.0/14           1     Subdomain Name(s)

The enumeration has finished
Discoveries are being migrated into the local database
```

1.2. Using Knockpy

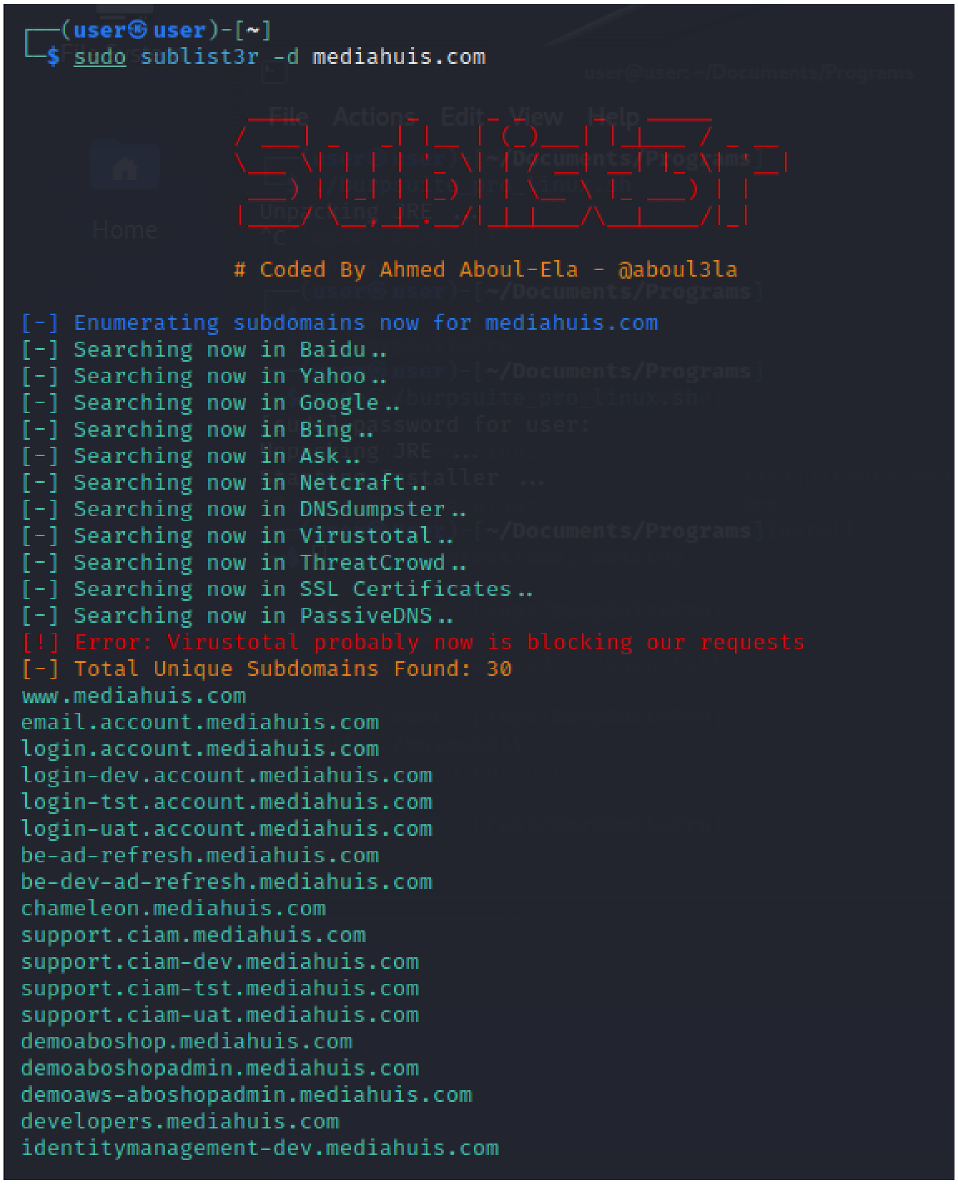


```
┌──(user㉿user)-[~]
└─$ sudo knockpy  mediahuis.com
[sudo] password for user:

  _  __                 _
 | |/ /                | |   v6.1.0
 | ' / _ __   ___   ___| | ___ __  _   _
 |  < | '_ \ / _ \ / __| |/ / '_ \| | | |
 | . \| | | | (_) | (__|   <| |_) | |_| |
 |_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                            | |     __/ |
                            |_|    |___/

local: 10757 | remote: 68

Wordlist: 10825 | Target: mediahuis.com | Ip: 104.18.40.229

13:33:15

Ip address        Code Subdomain                                   Server                                      Real hostname
_______________   ____ ___________________________________________ ___________________________________________ ___________________________________________

104.18.40.229     200  ai.mediahuis.com
172.64.147.27     200  annual-report.mediahuis.com                 cloudflare
52.98.33.232           autodiscover.mediahuis.com                                                              autod.ms-acdc-autod.office.com
76.76.21.123      200  chameleon.mediahuis.com                     Vercel                                      cname.vercel-dns.com
104.18.40.229     404  demoaws-aboshopadmin.mediahuis.com          cloudflare
172.64.147.27     404  demoofferservice.mediahuis.com              cloudflare
172.64.147.27     200  demoaboshop.mediahuis.com                   cloudflare
104.18.40.229     200  demoaboshopadmin.mediahuis.com              cloudflare
172.64.147.27     404  democontentservice.mediahuis.com            cloudflare
104.16.242.118    200  developers.mediahuis.com                    cloudflare                                  ssl.readmessl.com
172.64.147.27     200  dgvb.mediahuis.com                          cloudflare
104.18.40.229     200  dgvb-uat.mediahuis.com                      cloudflare
172.64.147.27     200  dgvb-tst.mediahuis.com                      cloudflare
104.18.40.229     200  dgvb-dev.mediahuis.com                      cloudflare
172.64.147.27     200  demopaymentservice.mediahuis.com            cloudflare
20.190.163.128    404  enterpriseregistration.mediahuis.com                                                    www.tm.f.prd.aadg.akadns.net
34.111.99.212     404  email.account.mediahuis.com                                                             eu.mailgun.org
20.214.131.176    200  enterpriseenrollment.mediahuis.com                                                      pexsucpap03.koreacentral.cloudapp.azure.com
```

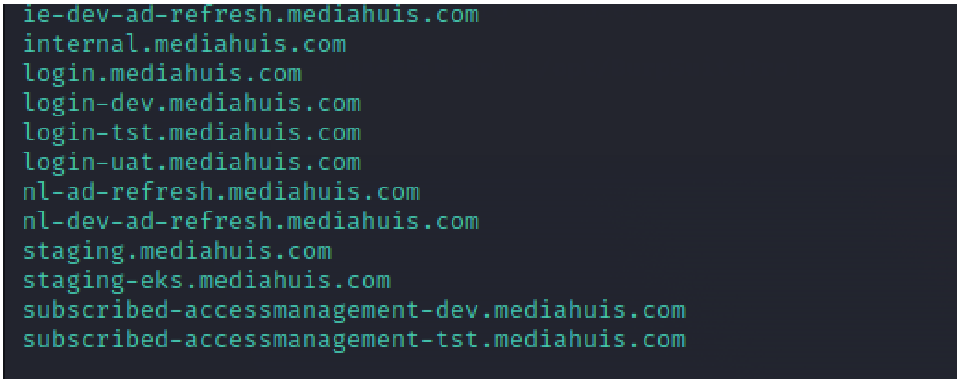


```
20.190.163.128    404  enterpriseregistration.mediahuis.com                                                    www.tm.f.prd.aadg.akadns.net
34.111.99.212     404  email.account.mediahuis.com                                                             eu.mailgun.org
20.214.131.176    200  enterpriseenrollment.mediahuis.com                                                      pexsucpap03.koreacentral.cloudapp.azure.com
172.64.147.27     200  hhd-uat.mediahuis.com                       cloudflare
172.64.147.27     200  hhd.mediahuis.com                           cloudflare
104.18.40.229     200  hhd-tst.mediahuis.com                       cloudflare
172.64.147.27     200  hhd-dev.mediahuis.com                       cloudflare
172.64.147.27     503  ie-dev-ad-refresh.mediahuis.com             cloudflare
104.18.40.77      404  identitymanagement.mediahuis.com            cloudflare                                  identitymanagement.mh-ciam-platform.com
172.64.147.179    404  identitymanagement-uat.mediahuis.com        cloudflare                                  identitymanagement-uat.mh-ciam-platform.com
104.18.40.77      404  identitymanagement-tst.mediahuis.com        cloudflare                                  identitymanagement-tst.mh-ciam-platform.com
104.18.40.77      404  identitymanagement-dev.mediahuis.com        cloudflare                                  identitymanagement-dev.mh-ciam-platform.com
172.64.147.27     403  jira.mediahuis.com                          cloudflare
172.64.147.27     200  journalistic-report.mediahuis.com           cloudflare
104.18.34.73           login.mediahuis.com                                                                     ciam-cd-qi2ktr4k3gywlpar.edge.tenants.mediahuis.auth0.com
52.112.66.142     200  lyncdiscover.mediahuis.com                                                              webdir.online.lync.com
40.126.35.134     404  msoid.mediahuis.com                                                                     www.tm.a.prd.aadg.trafficmanager.net
104.18.40.229     200  previewpublishing.mediahuis.com             cloudflare
104.18.40.229     200  publishing.mediahuis.com                    cloudflare
172.64.147.179    200  register-dev.mediahuis.com                  cloudflare                                  register-dev.mh-ciam-platform.com
172.64.147.179    200  register.mediahuis.com                      cloudflare                                  register.mh-ciam-platform.com
104.18.40.77      200  register-uat.mediahuis.com                  cloudflare                                  register-uat.mh-ciam-platform.com
104.18.40.77      200  register-tst.mediahuis.com                  cloudflare                                  register-tst.mh-ciam-platform.com
172.64.147.27     200  servicedesk.mediahuis.com
52.112.64.11           sip.mediahuis.com                                                                       sipdir.online.lync.com
54.195.197.237    404  staging-eks.mediahuis.com                                                               a40794e3e264e4539bd27cca37a8f6b7-9c46f018b68d726f.elb.eu-west-1.amazonaws.com
104.18.40.229     200  staging.mediahuis.com                       cloudflare
104.18.40.77      200  support.ciam-tst.mediahuis.com              cloudflare                                  support-ciam-tst.mh-ciam-platform.com
172.64.147.179    404  subscribed-accessmanagement-tst.mediahuis.com cloudflare                                subscribed-accessmanagement-tst.mh-ciam-platform.com
104.18.40.77      200  support.ciam.mediahuis.com                  cloudflare                                  support-ciam.mh-ciam-platform.com
172.64.147.179    404  subscribed-accessmanagement-dev.mediahuis.com cloudflare                                subscribed-accessmanagement-dev.mh-ciam-platform.com
104.18.40.77      200  support.ciam-dev.mediahuis.com              cloudflare                                  support-ciam-dev.mh-ciam-platform.com
172.64.147.179    200  support.ciam-uat.mediahuis.com              cloudflare                                  support-ciam-uat.mh-ciam-platform.com
172.64.147.27     200  www.mediahuis.com                           cloudflare

13:52:40

Ip address: 33 | Subdomain: 49 | elapsed time: 00:19:24
```

1.3. Using Sublist3r



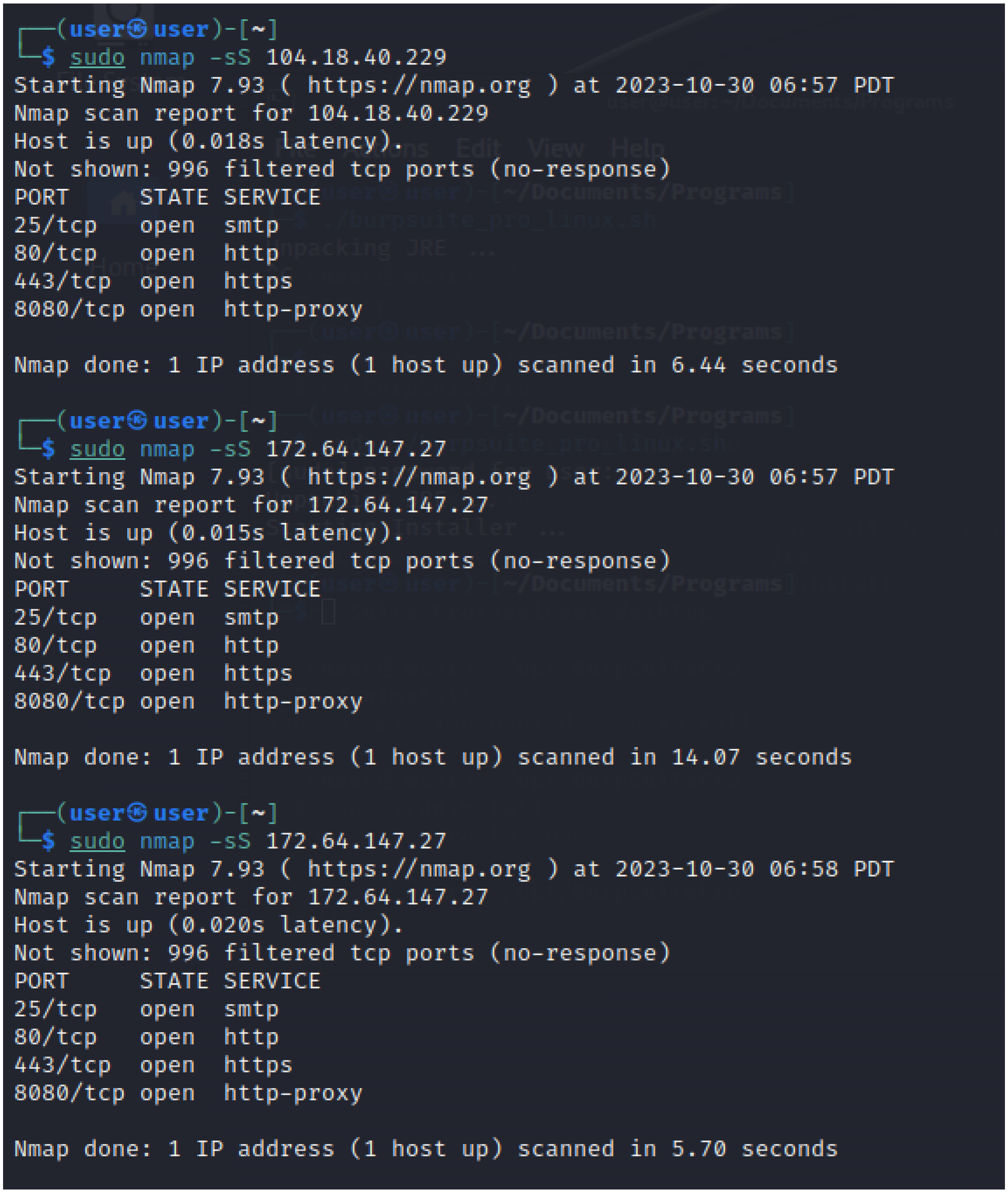
```
┌──(user㉿user)-[~]
└─$ sudo sublist3r -d mediahuis.com

                 ____        _     _ _     _   _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for mediahuis.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 30
www.mediahuis.com
email.account.mediahuis.com
login.account.mediahuis.com
login-dev.account.mediahuis.com
login-tst.account.mediahuis.com
login-uat.account.mediahuis.com
be-ad-refresh.mediahuis.com
be-dev-ad-refresh.mediahuis.com
chameleon.mediahuis.com
support.ciam.mediahuis.com
support.ciam-dev.mediahuis.com
support.ciam-tst.mediahuis.com
support.ciam-uat.mediahuis.com
demoaboshop.mediahuis.com
demoaboshopadmin.mediahuis.com
demoaws-aboshopadmin.mediahuis.com
developers.mediahuis.com
identitymanagement-dev.mediahuis.com
```



```
ie-dev-ad-refresh.mediahuis.com
internal.mediahuis.com
login.mediahuis.com
login-dev.mediahuis.com
login-tst.mediahuis.com
login-uat.mediahuis.com
nl-ad-refresh.mediahuis.com
nl-dev-ad-refresh.mediahuis.com
staging.mediahuis.com
staging-eks.mediahuis.com
subscribed-accessmanagement-dev.mediahuis.com
subscribed-accessmanagement-tst.mediahuis.com
```

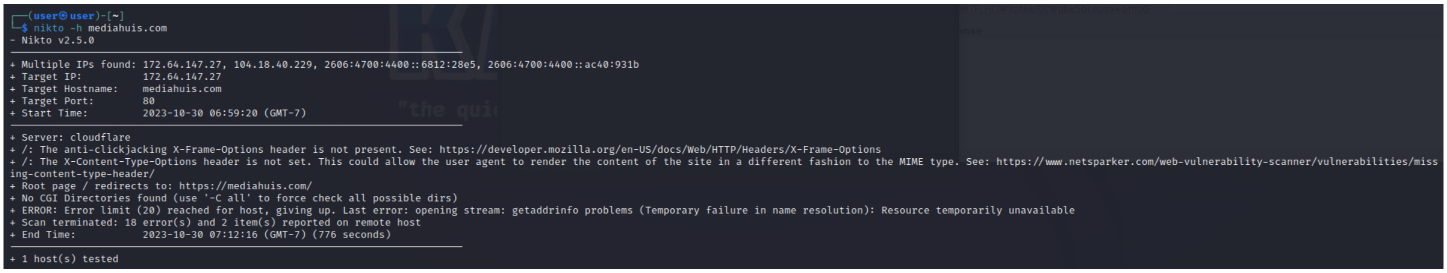
3. Scanning Vulnerability

3.1.Using Nmap



```
┌──(user㉿user)-[~]
└─$ sudo nmap -sS 104.18.40.229
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 06:57 PDT
Nmap scan report for 104.18.40.229
Host is up (0.018s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 6.44 seconds

┌──(user㉿user)-[~]
└─$ sudo nmap -sS 172.64.147.27
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 06:57 PDT
Nmap scan report for 172.64.147.27
Host is up (0.015s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 14.07 seconds

┌──(user㉿user)-[~]
└─$ sudo nmap -sS 172.64.147.27
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 06:58 PDT
Nmap scan report for 172.64.147.27
Host is up (0.020s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 5.70 seconds
```

3.2.Using Nikto



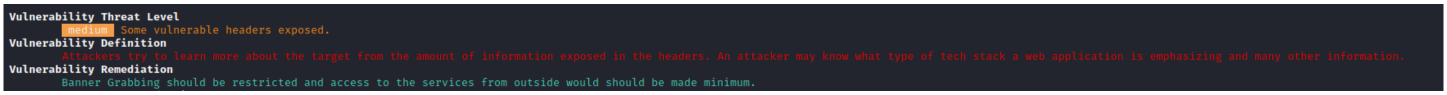
```
┌──(user㉿user)-[~]
└─$ nikto -h mediahuis.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 172.64.147.27, 104.18.40.229, 2606:4700:4400::6812:28e5, 2606:4700:4400::ac40:931b
+ Target IP:          172.64.147.27
+ Target Hostname:    mediahuis.com
+ Target Port:        80
+ Start Time:         2023-10-30 06:59:20 (GMT-7)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: 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/miss
ing-content-type-header/
+ Root page / redirects to: https://mediahuis.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: getaddrinfo problems (Temporary failure in name resolution): Resource temporarily unavailable
+ Scan terminated: 18 error(s) and 2 item(s) reported on remote host
+ End Time:           2023-10-30 07:12:16 (GMT-7) (776 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- X content type options header is not set
- The anti-clickjacking x frame options header is not present

3.3.Using Rapid Scan

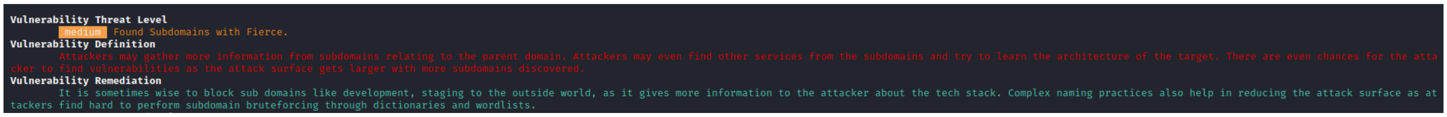
```
                    (The Multi-Tool Web Vulnerability Scanner)

                    Check out our new software, NetBot for simulating DDoS a
ttacks - https://github.com/skavngr/netbot
```

- Some vulnerable headers exposed.



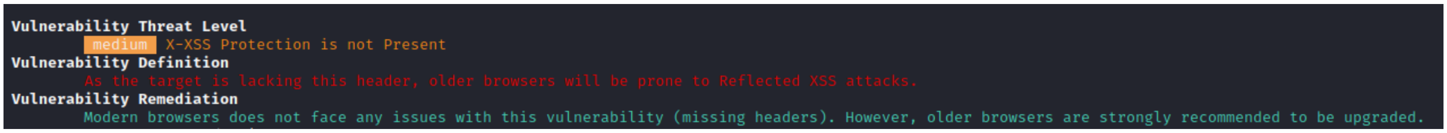
```
Vulnerability Threat Level
        medium  Some vulnerable headers exposed.
Vulnerability Definition
        Attackers try to learn more about the target from the amount of information exposed in the headers. An attacker may know what type of tech stack a web application is emphasizing and many other information.
Vulnerability Remediation
        Banner Grabbing should be restricted and access to the services from outside would should be made minimum.
```

- Found Subdomains with Fierce.



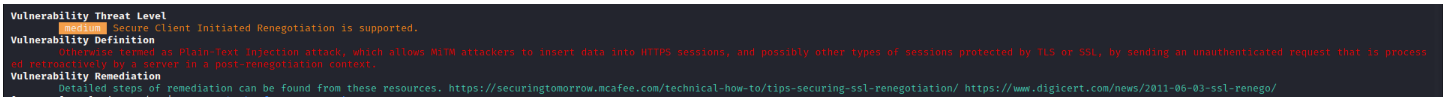
```
Vulnerability Threat Level
        medium  Found Subdomains with Fierce.
Vulnerability Definition
        Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of the target. There are even chances for the atta
cker to find vulnerabilities as the attack surface gets larger with more subdomains discovered.
Vulnerability Remediation
        It is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface as at
tackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.
```

- X-XSS Protection is not Present.

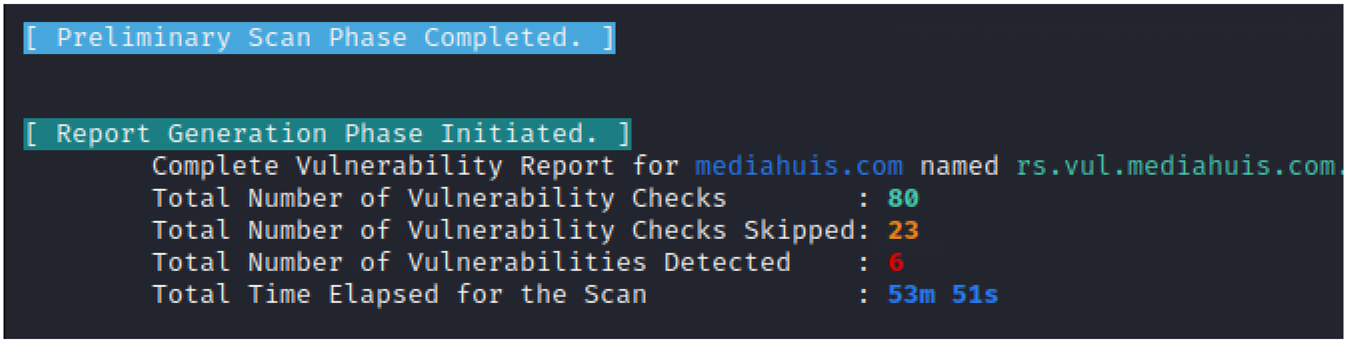


```
Vulnerability Threat Level
        medium  X-XSS Protection is not Present
Vulnerability Definition
        As the target is lacking this header, older browsers will be prone to Reflected XSS attacks.
Vulnerability Remediation
        Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded.
```

- Secure Client Initiated Renegotiation is supported.



```
Vulnerability Threat Level
        medium  Secure Client Initiated Renegotiation is supported.
Vulnerability Definition
        Otherwise termed as Plain-Text Injection attack, which allows MiTM attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is process
ed retroactively by a server in a post-renegotiation context.
Vulnerability Remediation
        Detailed steps of remediation can be found from these resources. https://securingtomorrow.mcafee.com/technical-how-to/tips-securing-ssl-renegotiation/ https://www.digicert.com/news/2011-06-03-ssl-renego/
```



```
[ Preliminary Scan Phase Completed. ]


[ Report Generation Phase Initiated. ]
        Complete Vulnerability Report for mediahuis.com named rs.vul.mediahuis.com.
        Total Number of Vulnerability Checks        : 80
        Total Number of Vulnerability Checks Skipped: 23
        Total Number of Vulnerabilities Detected    : 6
        Total Time Elapsed for the Scan             : 53m 51s
```

4. Vulnerability description

- Some Vulnerable Headers Exposed: Certain headers are exposed, which could potentially be exploited or provide information for further attacks.
- Found Subdomains with Fierce: Subdomains have been discovered using the Fierce tool, potentially expanding the attack surface, and exposing sensitive information.
- Secure Client Initiated Renegotiation Supported: The presence of secure client-initiated renegotiation in a communication protocol, which can have security implications.
- X-XSS Protection is not Present: The absence of an XSS protection header in a web application, potentially making it susceptible to cross-site scripting attacks.

5. Affected components.

- Systems exposing vulnerable headers.
- Domain and its subdomains discovered using Fierce.
- Systems supporting secure client-initiated renegotiation.
- Web application or website without an XSS protection header.

6. Impact assessment

- Some Vulnerable Headers Exposed: Risk of header-based attacks or information exposure.
- Found Subdomains: Expanded attack surface, potential for subdomain-related vulnerabilities.
- Secure Client Initiated Renegotiation: Security implications may lead to unauthorized access or data interception.
- X-XSS Protection is not Present: Risk of cross-site scripting attacks, leading to data theft or unauthorized.

7. Steps to reproduce.

None

8. Proof of concept (if applicable)

None

9. Proposed mitigation or fix

- Vulnerable Headers: Review and secure headers, implement security best practices.
- Subdomains: Carefully manage and secure discovered subdomains to prevent information exposure.
- Secure Client Initiated Renegotiation: Ensure secure communication configurations.
- X-XSS Protection: Add XSS protection headers and implement input validation and output encoding.

10. Summary

Various vulnerabilities have been identified, including the risk of exposed vulnerable headers, expanded attack surface with discovered subdomains, secure client-initiated renegotiation, and the absence of XSS protection. Implementing mitigation measures and conducting security assessments are necessary to protect the affected components and ensure system security.