IE2062 [2023/JUL]- Web Security

Web Security BB Assignment

# Report 01 – CM.com

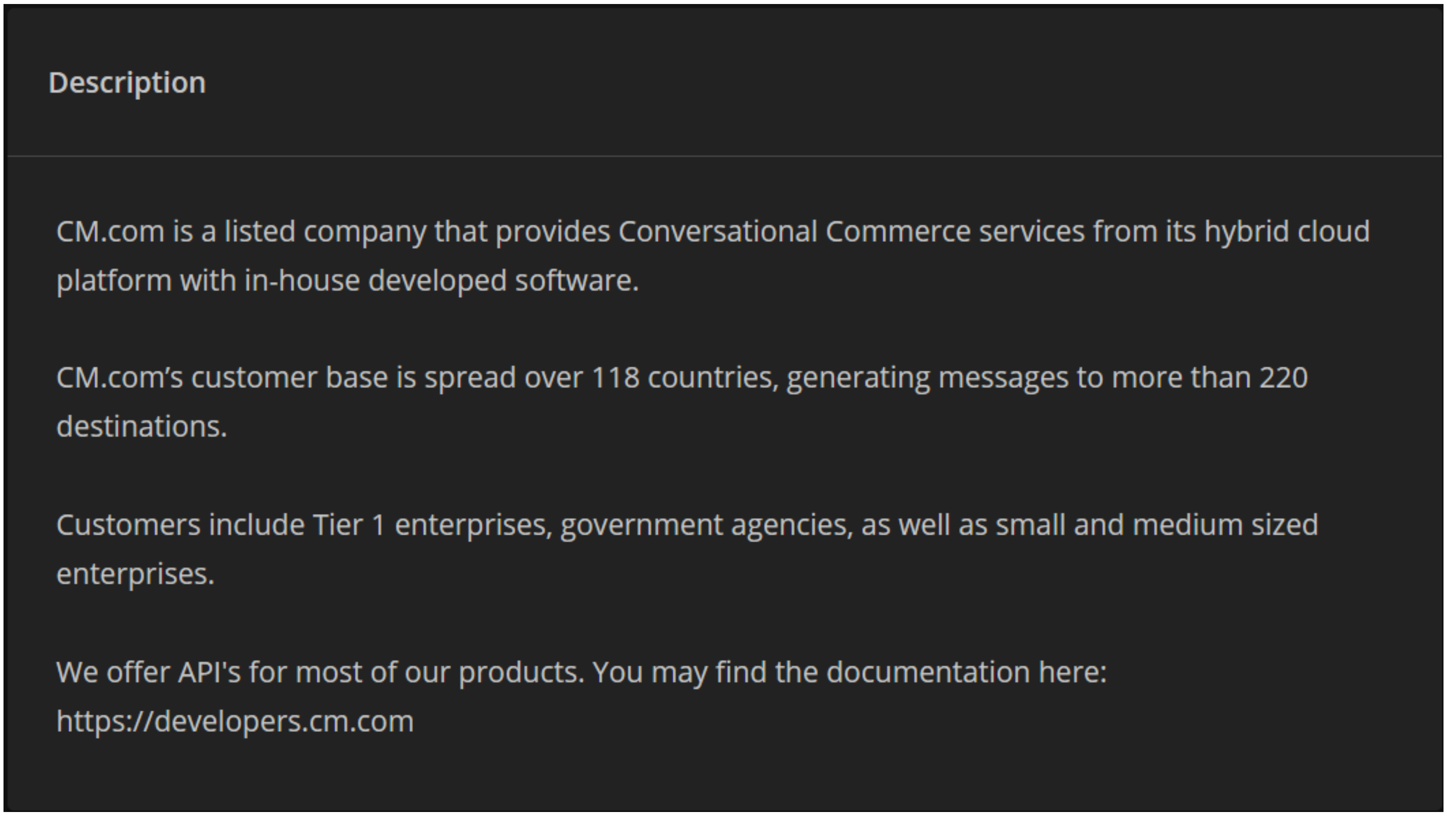
Lecturer in charge – Ms. Chethana Liyanapathirana

| |
|---|
| IT21826368 – Nanayakkara Y.D.T.D |

# Contents

# 1. CM.com

## 1.1.Overview



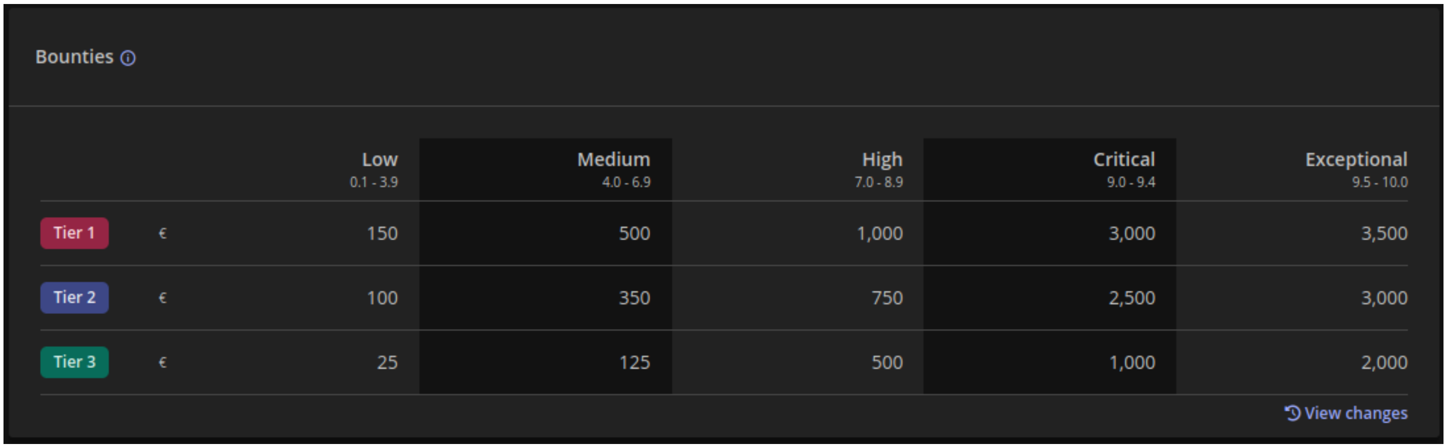
Description

CM.com is a listed company that provides Conversational Commerce services from its hybrid cloud platform with in-house developed software.

CM.com's customer base is spread over 118 countries, generating messages to more than 220 destinations.

Customers include Tier 1 enterprises, government agencies, as well as small and medium sized enterprises.

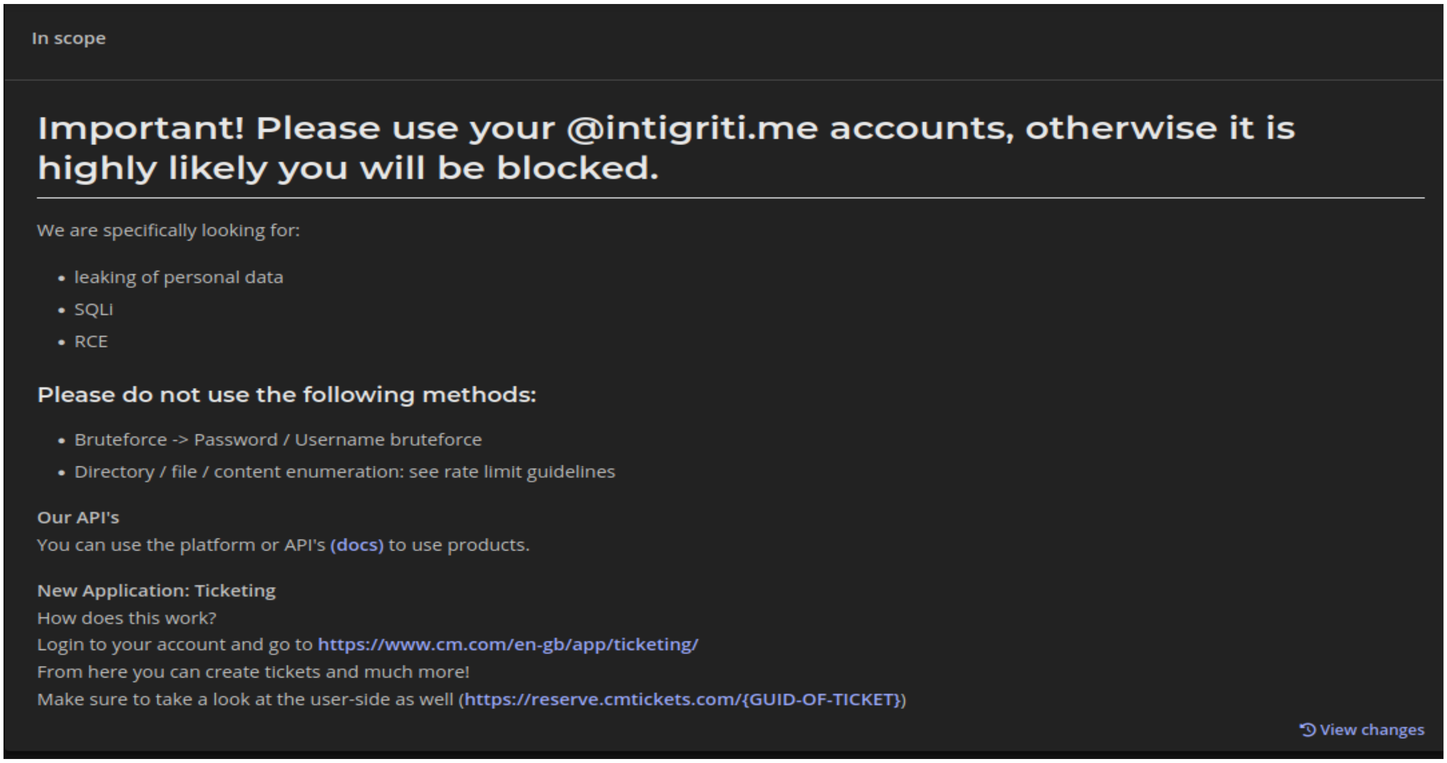
We offer API's for most of our products. You may find the documentation here: https://developers.cm.com



Bounties ⓘ

| | | Low<br>0.1 - 3.9 | Medium<br>4.0 - 6.9 | High<br>7.0 - 8.9 | Critical<br>9.0 - 9.4 | Exceptional<br>9.5 - 10.0 |
|---|---|---|---|---|---|---|
| Tier 1 | € | 150 | 500 | 1,000 | 3,000 | 3,500 |
| Tier 2 | € | 100 | 350 | 750 | 2,500 | 3,000 |
| Tier 3 | € | 25 | 125 | 500 | 1,000 | 2,000 |

## 1.2.Scope



In scope

# Important! Please use your @intigriti.me accounts, otherwise it is highly likely you will be blocked.

We are specifically looking for:

- leaking of personal data
- SQLI
- RCE

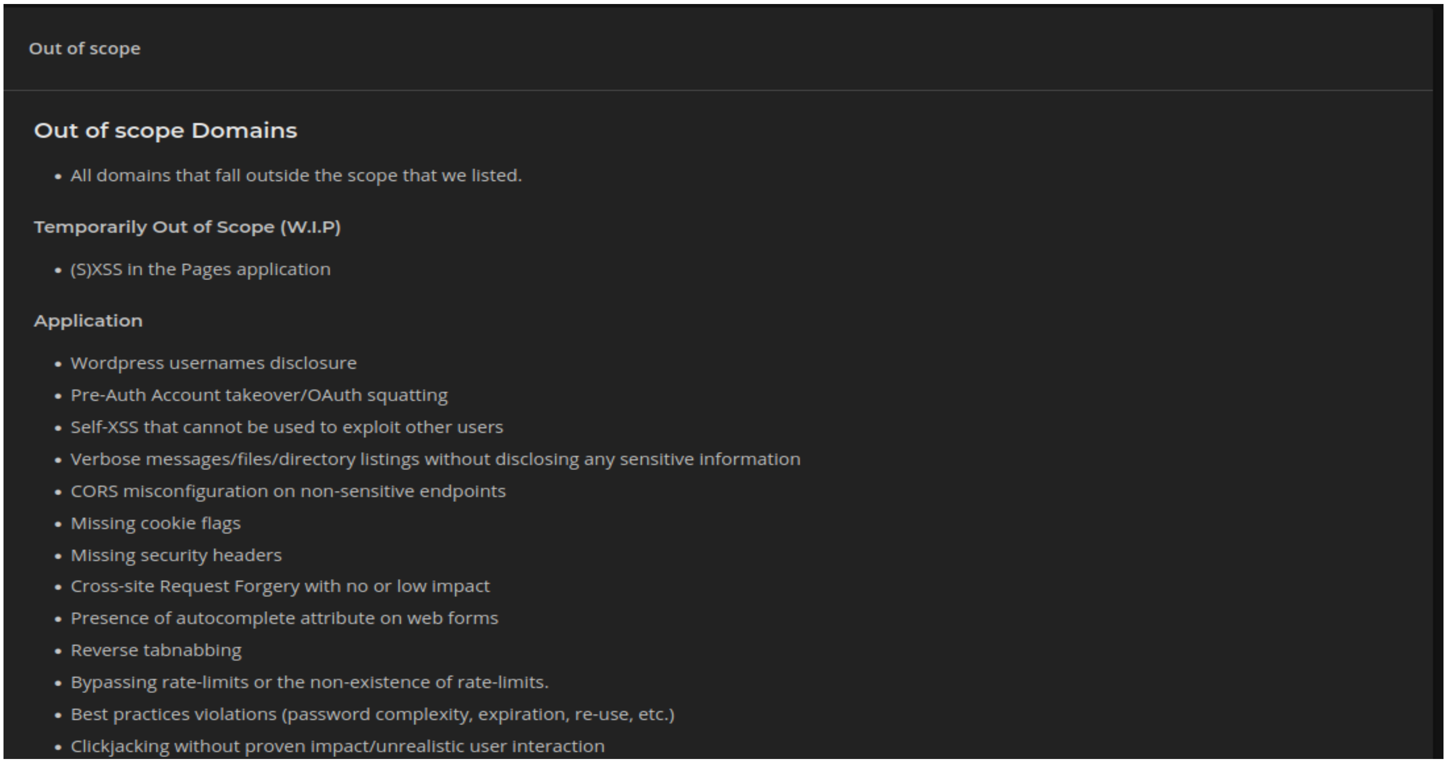
### Please do not use the following methods:

- Bruteforce -> Password / Username bruteforce
- Directory / file / content enumeration: see rate limit guidelines

**Our API's**
You can use the platform or API's **(docs)** to use products.

**New Application: Ticketing**
How does this work?
Login to your account and go to **https://www.cm.com/en-gb/app/ticketing/**
From here you can create tickets and much more!
Make sure to take a look at the user-side as well (**https://reserve.cmtickets.com/{GUID-OF-TICKET}**)

## 1.3.Out of Scope



Out of scope

### Out of scope Domains

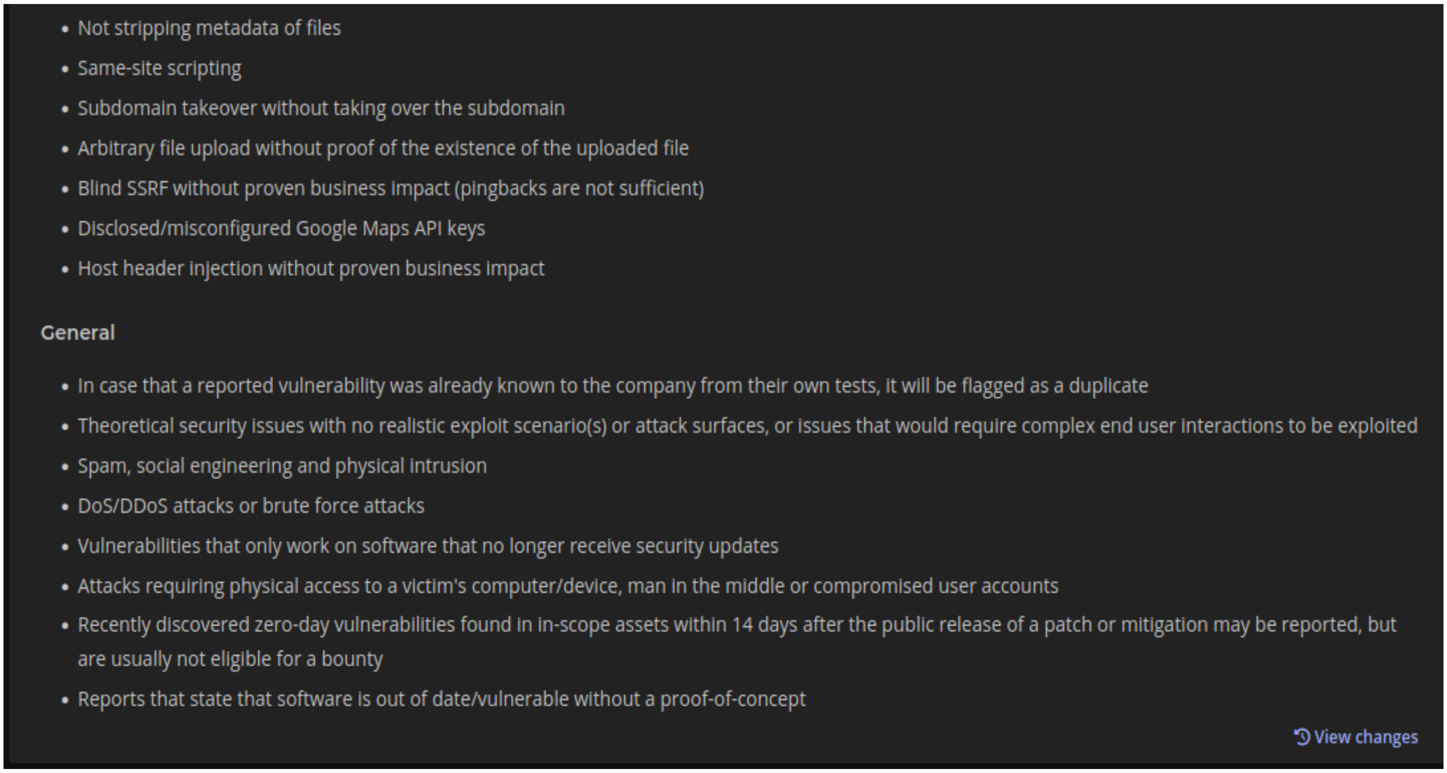
- All domains that fall outside the scope that we listed.

**Temporarily Out of Scope (W.I.P)**

- (S)XSS in the Pages application

**Application**

- Wordpress usernames disclosure
- Pre-Auth Account takeover/OAuth squatting
- Self-XSS that cannot be used to exploit other users
- Verbose messages/files/directory listings without disclosing any sensitive information
- CORS misconfiguration on non-sensitive endpoints
- Missing cookie flags
- Missing security headers
- Cross-site Request Forgery with no or low impact
- Presence of autocomplete attribute on web forms
- Reverse tabnabbing
- Bypassing rate-limits or the non-existence of rate-limits.
- Best practices violations (password complexity, expiration, re-use, etc.)
- Clickjacking without proven impact/unrealistic user interaction



- Not stripping metadata of files
- Same-site scripting
- Subdomain takeover without taking over the subdomain
- Arbitrary file upload without proof of the existence of the uploaded file
- Blind SSRF without proven business impact (pingbacks are not sufficient)
- Disclosed/misconfigured Google Maps API keys
- Host header injection without proven business impact

**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

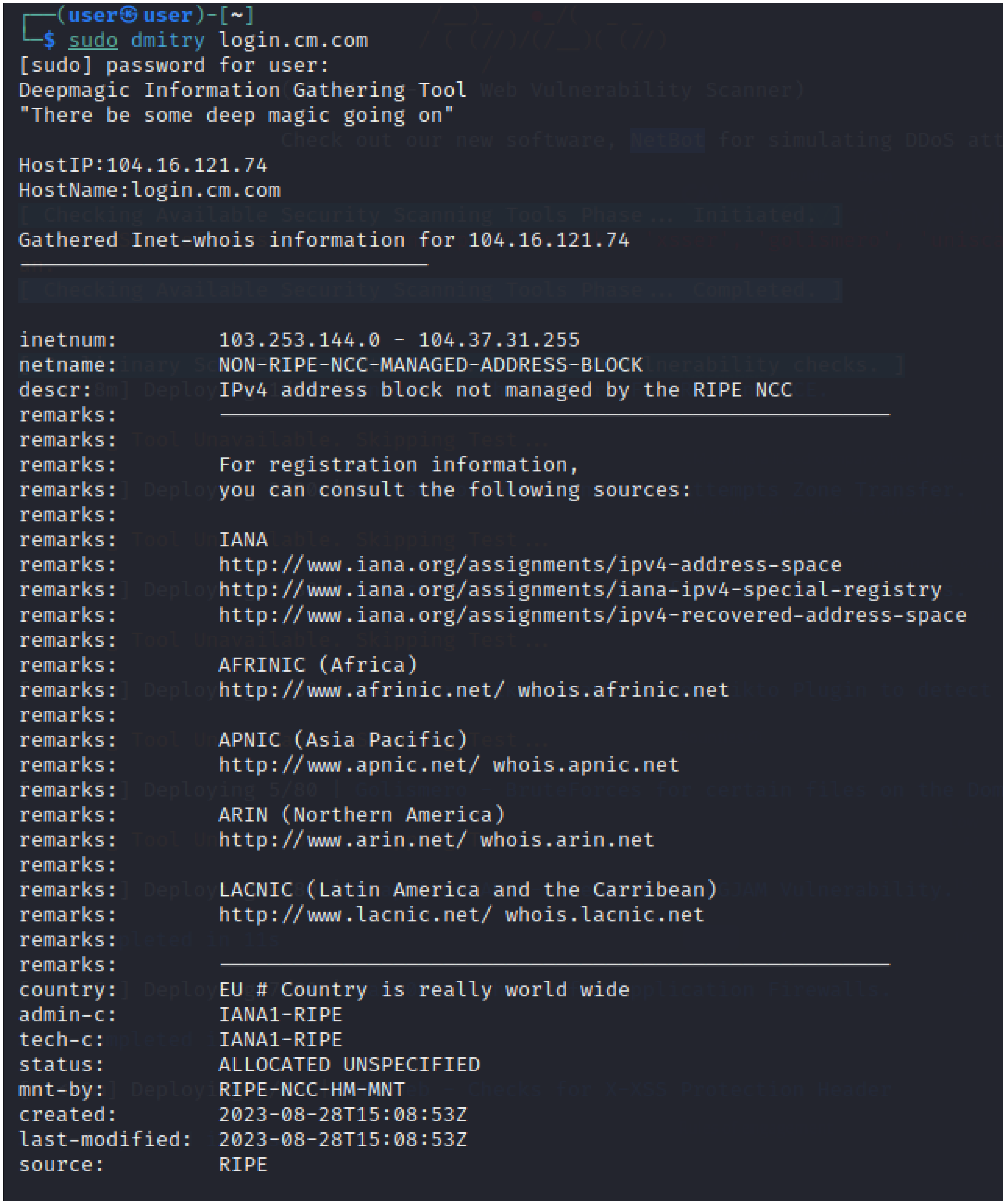
## 1.4.Selected Domains

login.cm.com Tier 1 URL

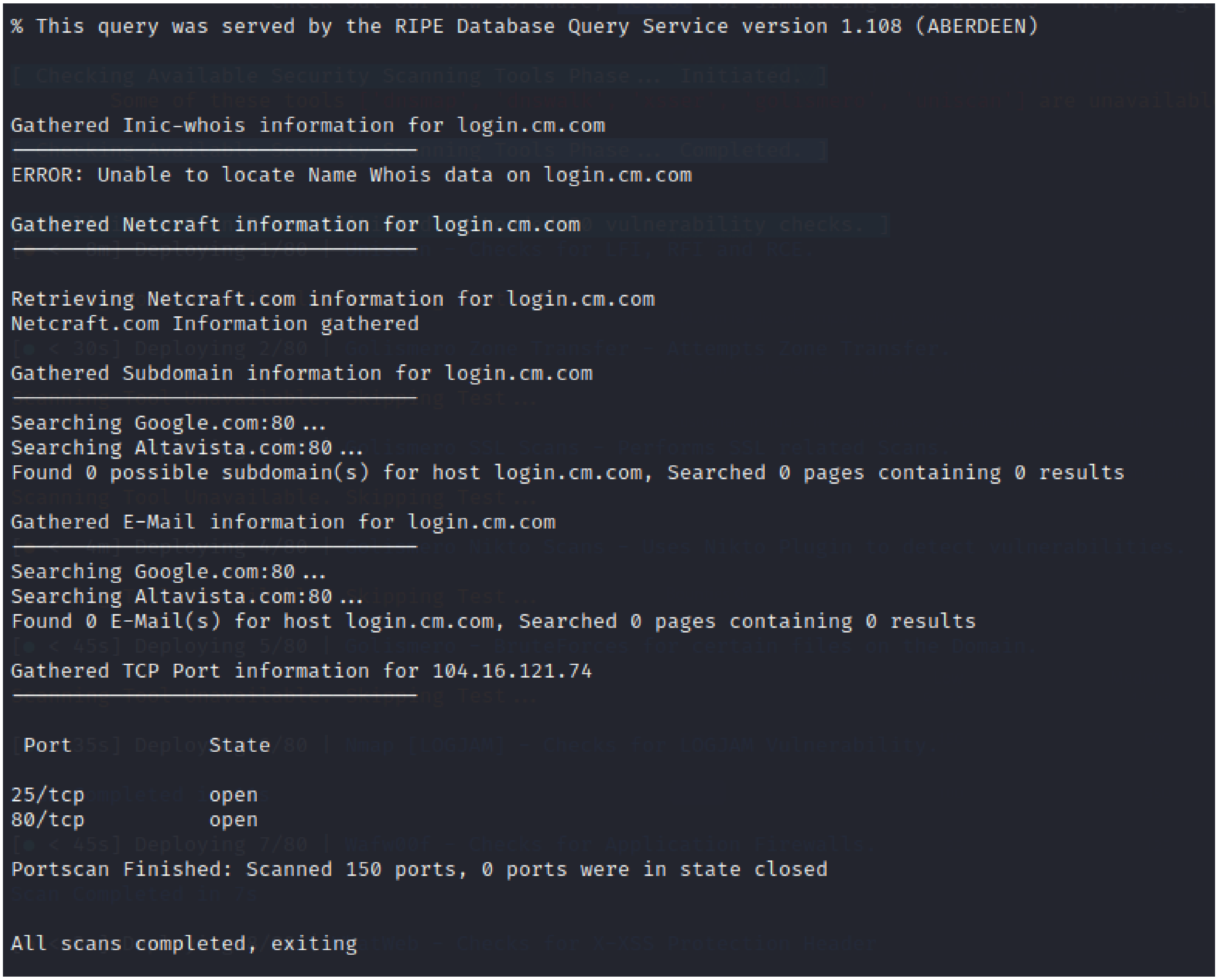
URL:  login.cm.com

## 2. Information Gathering

### 2.1.Using Dmitry

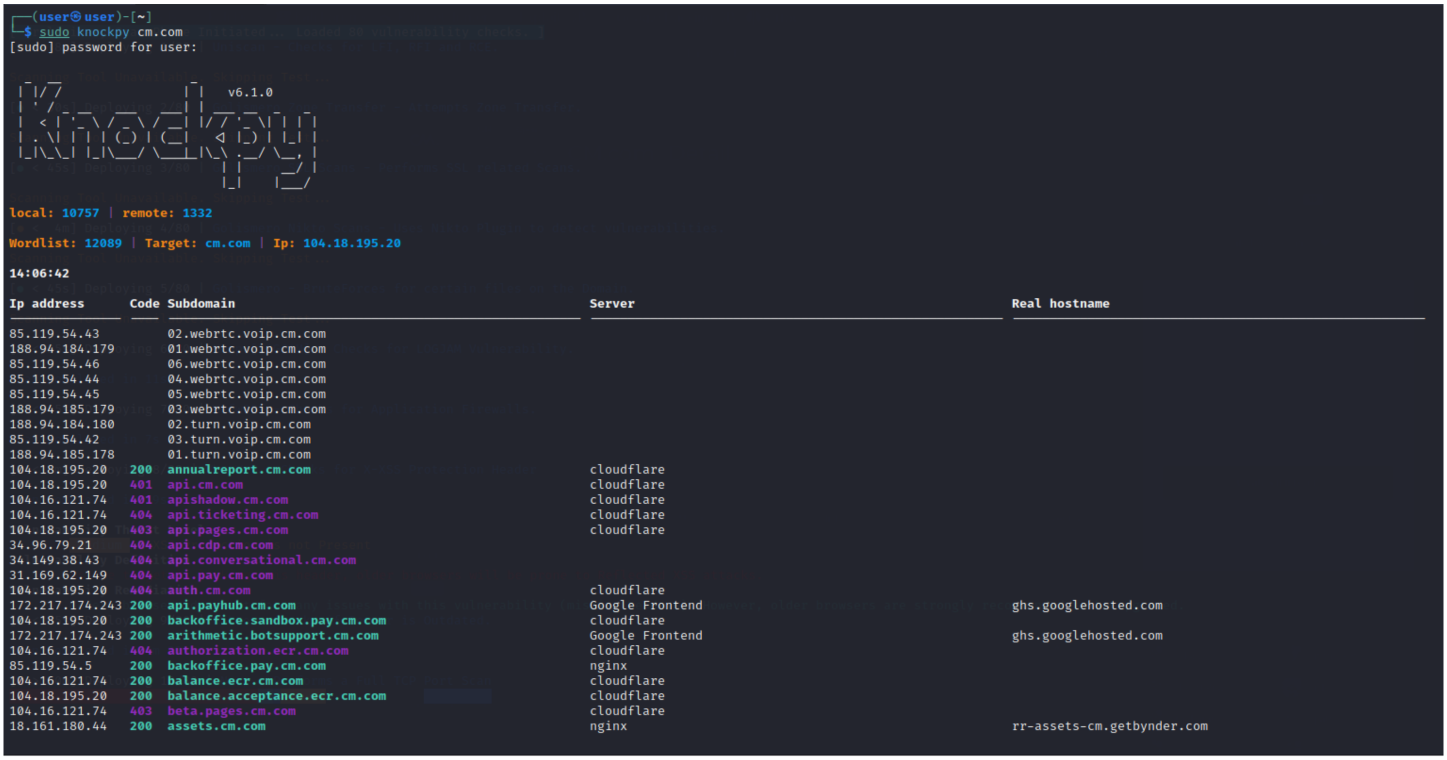


```
┌──(user㉿user)-[~]
└─$ sudo dmitry login.cm.com
[sudo] password for user:
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:104.16.121.74
HostName:login.cm.com

Gathered Inet-whois information for 104.16.121.74
─────────────────────────────────


inetnum:        103.253.144.0 - 104.37.31.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ──────────────────────────────────────────────────────
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        ──────────────────────────────────────────────────────
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
created:        2023-08-28T15:08:53Z
last-modified:  2023-08-28T15:08:53Z
source:         RIPE
```

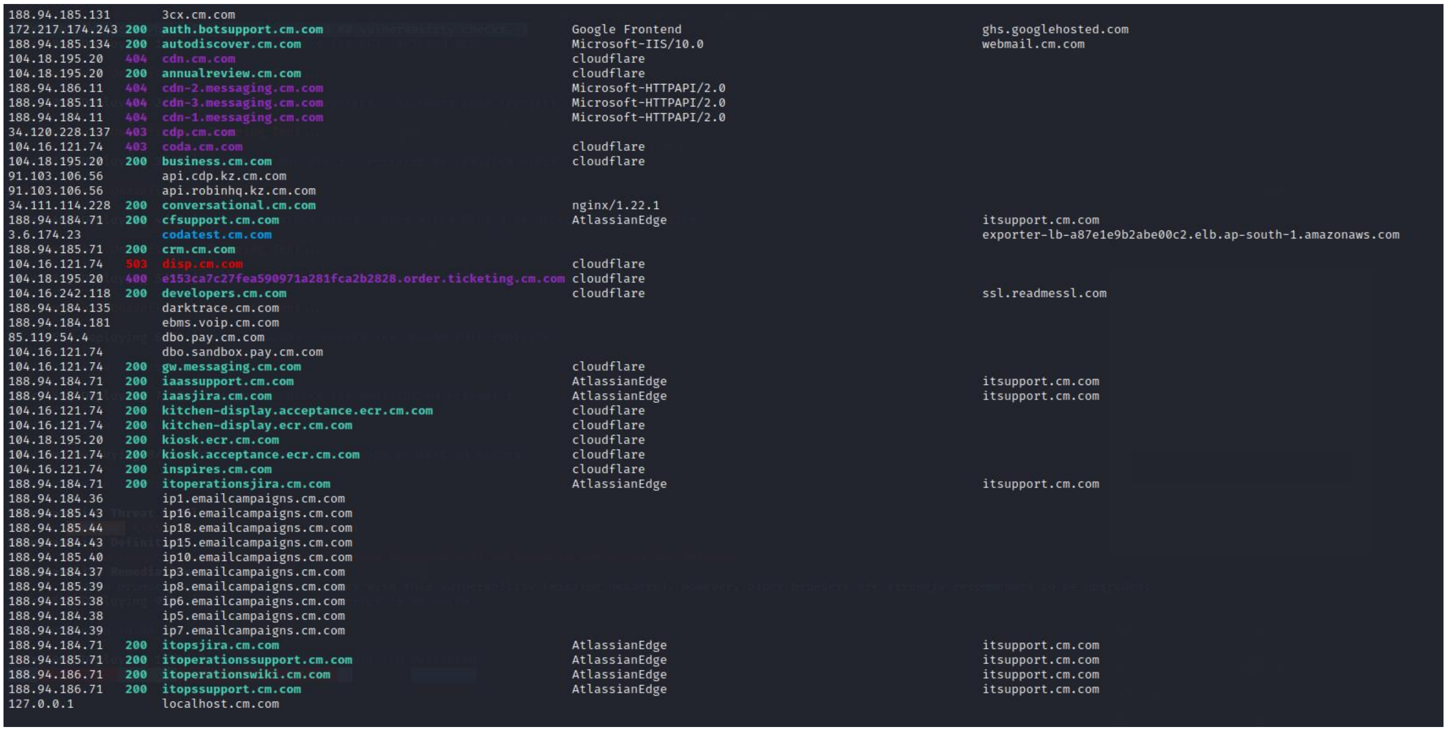


```
% This query was served by the RIPE Database Query Service version 1.108 (ABERDEEN)


Gathered Inic-whois information for login.cm.com
─────────────────────────────────
ERROR: Unable to locate Name Whois data on login.cm.com

Gathered Netcraft information for login.cm.com
─────────────────────────────────


Retrieving Netcraft.com information for login.cm.com
Netcraft.com Information gathered

Gathered Subdomain information for login.cm.com
─────────────────────────────────
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 possible subdomain(s) for host login.cm.com, Searched 0 pages containing 0 results

Gathered E-Mail information for login.cm.com
─────────────────────────────────
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 E-Mail(s) for host login.cm.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 104.16.121.74
─────────────────────────────────


 Port           State

25/tcp          open
80/tcp          open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed


All scans completed, exiting
```

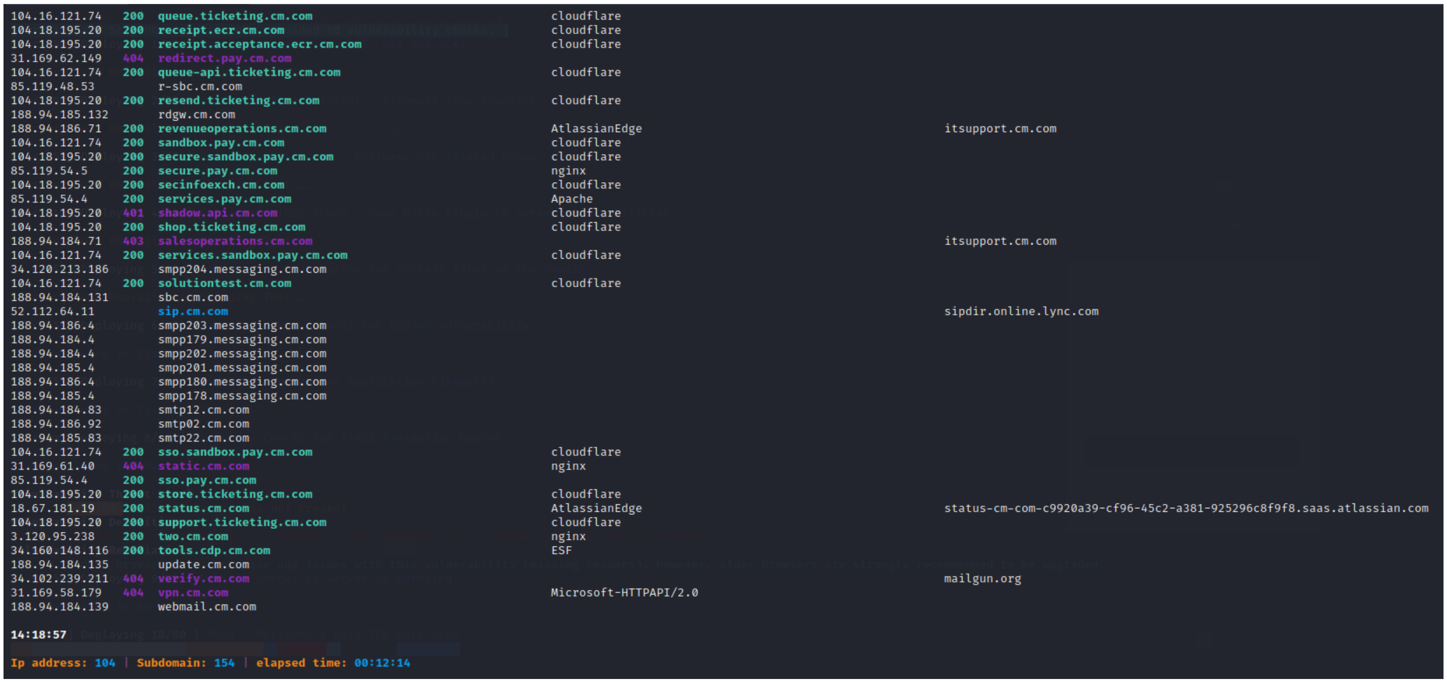
## 2.2. Using Knockpy to scan



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

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

local: 10757 | remote: 1332

Wordlist: 12089 | Target: cm.com | Ip: 104.18.195.20

14:06:42

Ip address      Code Subdomain                                               Server                                                  Real hostname
─────────────── ──── ─────────────────────────────────────────────────────── ─────────────────────────────────────────────────────── ───────────────────────────────────────────────────────

85.119.54.43         02.webrtc.voip.cm.com
188.94.184.179       01.webrtc.voip.cm.com
85.119.54.46         06.webrtc.voip.cm.com
85.119.54.44         04.webrtc.voip.cm.com
85.119.54.45         05.webrtc.voip.cm.com
188.94.185.179       03.webrtc.voip.cm.com
188.94.184.180       02.turn.voip.cm.com
85.119.54.42         03.turn.voip.cm.com
188.94.185.178       01.turn.voip.cm.com
104.18.195.20   200  annualreport.cm.com                                     cloudflare
104.18.195.20   401  api.cm.com                                              cloudflare
104.16.121.74   401  apishadow.cm.com                                        cloudflare
104.16.121.74   404  api.ticketing.cm.com                                    cloudflare
104.18.195.20   403  api.pages.cm.com                                        cloudflare
34.96.79.21     404  api.cdp.cm.com
34.149.38.43    404  api.conversational.cm.com
31.169.62.149   404  api.pay.cm.com
104.18.195.20   404  auth.cm.com                                             cloudflare
172.217.174.243 200  api.payhub.cm.com                                       Google Frontend                                         ghs.googlehosted.com
104.18.195.20   200  backoffice.sandbox.pay.cm.com                           cloudflare
172.217.174.243 200  arithmetic.botsupport.cm.com                            Google Frontend                                         ghs.googlehosted.com
104.16.121.74   404  authorization.ecr.cm.com                                cloudflare
85.119.54.5     200  backoffice.pay.cm.com                                   nginx
104.16.121.74   200  balance.ecr.cm.com                                      cloudflare
104.18.195.20   200  balance.acceptance.ecr.cm.com                           cloudflare
104.16.121.74   403  beta.pages.cm.com                                       cloudflare
18.161.180.44   200  assets.cm.com                                           nginx                                                   rr-assets-cm.getbynder.com
```

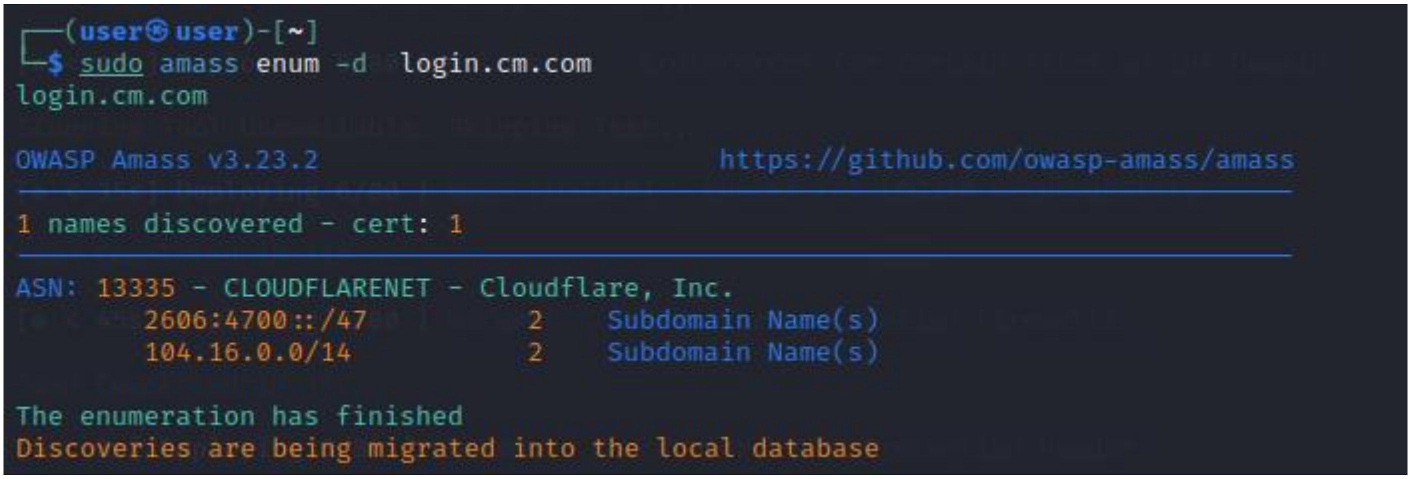


```
188.94.185.131       3cx.cm.com
172.217.174.243 200  auth.botsupport.cm.com                                  Google Frontend                                         ghs.googlehosted.com
188.94.185.134  200  autodiscover.cm.com                                     Microsoft-IIS/10.0                                      webmail.cm.com
104.18.195.20   404  cdn.cm.com                                              cloudflare
104.18.195.20   200  annualreview.cm.com                                     cloudflare
188.94.186.11   404  cdn-2.messaging.cm.com                                  Microsoft-HTTPAPI/2.0
188.94.185.11   404  cdn-3.messaging.cm.com                                  Microsoft-HTTPAPI/2.0
188.94.184.11   404  cdn-1.messaging.cm.com                                  Microsoft-HTTPAPI/2.0
34.120.228.137  403  cdp.cm.com
104.16.121.74   403  coda.cm.com                                             cloudflare
104.18.195.20   200  business.cm.com                                         cloudflare
91.103.106.56        api.cdp.kz.cm.com
91.103.106.56        api.robinhq.kz.cm.com
34.111.114.228  200  conversational.cm.com                                   nginx/1.22.1
188.94.184.71   200  cfsupport.cm.com                                        AtlassianEdge                                           itsupport.cm.com
3.6.174.23           codatest.cm.com                                                                                                 exporter-lb-a87e1e9b2abe00c2.elb.ap-south-1.amazonaws.com
188.94.185.71   200  crm.cm.com
104.16.121.74   503  disp.cm.com                                             cloudflare
104.18.195.20   400  e153ca7c27fea590971a281fca2b2828.order.ticketing.cm.com cloudflare
104.16.242.118  200  developers.cm.com                                       cloudflare                                              ssl.readmessl.com
188.94.184.135       darktrace.cm.com
188.94.184.181       ebms.voip.cm.com
85.119.54.4          dbo.pay.cm.com
104.16.121.74        dbo.sandbox.pay.cm.com
104.16.121.74   200  gw.messaging.cm.com                                     cloudflare
188.94.184.71   200  iaassupport.cm.com                                      AtlassianEdge                                           itsupport.cm.com
188.94.184.71   200  iaasjira.cm.com                                         AtlassianEdge                                           itsupport.cm.com
104.16.121.74   200  kitchen-display.acceptance.ecr.cm.com                   cloudflare
104.16.121.74   200  kitchen-display.ecr.cm.com                              cloudflare
104.18.195.20   200  kiosk.ecr.cm.com                                        cloudflare
104.16.121.74   200  kiosk.acceptance.ecr.cm.com                             cloudflare
104.16.121.74   200  inspires.cm.com                                         cloudflare
188.94.184.71   200  itoperationsjira.cm.com                                 AtlassianEdge                                           itsupport.cm.com
188.94.184.36        ip1.emailcampaigns.cm.com
188.94.185.43        ip16.emailcampaigns.cm.com
188.94.185.44        ip18.emailcampaigns.cm.com
188.94.184.43        ip15.emailcampaigns.cm.com
188.94.185.40        ip10.emailcampaigns.cm.com
188.94.184.37        ip3.emailcampaigns.cm.com
188.94.185.39        ip8.emailcampaigns.cm.com
188.94.185.38        ip6.emailcampaigns.cm.com
188.94.184.38        ip5.emailcampaigns.cm.com
188.94.184.39        ip7.emailcampaigns.cm.com
188.94.184.71   200  itopsjira.cm.com                                        AtlassianEdge                                           itsupport.cm.com
188.94.185.71   200  itoperationssupport.cm.com                              AtlassianEdge                                           itsupport.cm.com
188.94.186.71   200  itoperationswiki.cm.com                                 AtlassianEdge                                           itsupport.cm.com
188.94.186.71   200  itopssupport.cm.com                                     AtlassianEdge                                           itsupport.cm.com
127.0.0.1            localhost.cm.com
```



```
104.16.121.74    200  queue.ticketing.cm.com                                   cloudflare
104.18.195.20    200  receipt.ecr.cm.com                                       cloudflare
104.18.195.20    200  receipt.acceptance.ecr.cm.com                            cloudflare
31.169.62.149    404  redirect.pay.cm.com
104.16.121.74    200  queue-api.ticketing.cm.com                               cloudflare
85.119.48.53          r-sbc.cm.com
104.18.195.20    200  resend.ticketing.cm.com                                  cloudflare
188.94.185.132        rdgw.cm.com
188.94.186.71    200  revenueoperations.cm.com                                 AtlassianEdge                                           itsupport.cm.com
104.16.121.74    200  sandbox.pay.cm.com                                       cloudflare
104.18.195.20    200  secure.sandbox.pay.cm.com                                cloudflare
85.119.54.5      200  secure.pay.cm.com                                        nginx
104.18.195.20    200  secinfoexch.cm.com                                       cloudflare
85.119.54.4      200  services.pay.cm.com                                      Apache
104.18.195.20    401  shadow.api.cm.com                                        cloudflare
104.18.195.20    200  shop.ticketing.cm.com                                    cloudflare
188.94.184.71    403  salesoperations.cm.com                                                                                               itsupport.cm.com
104.16.121.74    200  services.sandbox.pay.cm.com                              cloudflare
34.120.213.186        smpp204.messaging.cm.com
104.16.121.74    200  solutiontest.cm.com                                      cloudflare
188.94.184.131        sbc.cm.com
52.112.64.11          sip.cm.com                                                                                                           sipdir.online.lync.com
188.94.186.4          smpp203.messaging.cm.com
188.94.184.4          smpp179.messaging.cm.com
188.94.184.4          smpp202.messaging.cm.com
188.94.185.4          smpp201.messaging.cm.com
188.94.186.4          smpp180.messaging.cm.com
188.94.185.4          smpp178.messaging.cm.com
188.94.184.83         smtp12.cm.com
188.94.186.92         smtp02.cm.com
188.94.185.83         smtp22.cm.com
104.16.121.74    200  sso.sandbox.pay.cm.com                                   cloudflare
31.169.61.40     404  static.cm.com                                            nginx
85.119.54.4      200  sso.pay.cm.com
104.18.195.20    200  store.ticketing.cm.com                                   cloudflare
18.67.181.19     200  status.cm.com                                            AtlassianEdge                                           status-cm-com-c9920a39-cf96-45c2-a381-925296c8f9f8.saas.atlassian.com
104.18.195.20    200  support.ticketing.cm.com                                 cloudflare
3.120.95.238     200  two.cm.com                                               nginx
34.160.148.116   200  tools.cdp.cm.com                                         ESF
188.94.184.135        update.cm.com
34.102.239.211   404  verify.cm.com                                                                                                        mailgun.org
31.169.58.179    404  vpn.cm.com                                               Microsoft-HTTPAPI/2.0
188.94.184.139        webmail.cm.com

14:18:57

Ip address: 104 | Subdomain: 154 | elapsed time: 00:12:14
```

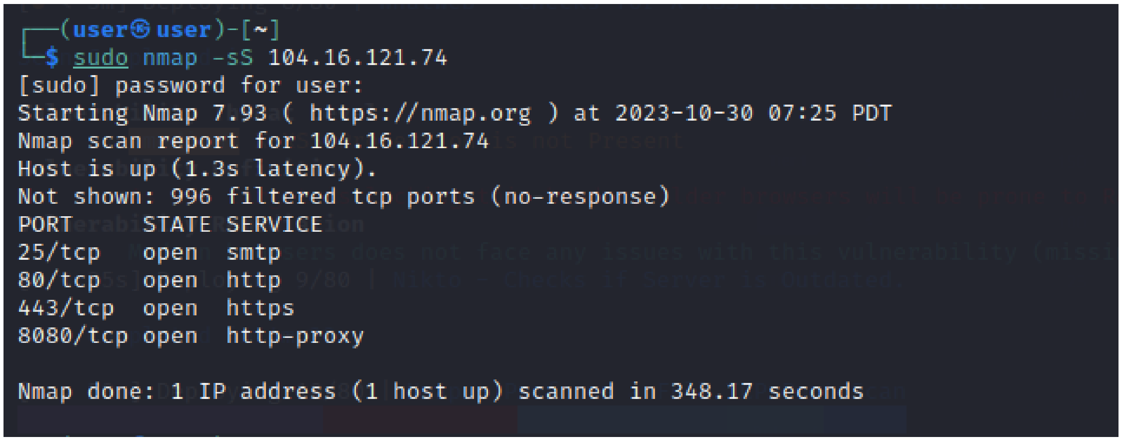
## 2.3. Using amass to scan



```
┌──(user㉿user)-[~]
└─$ sudo amass enum -d  login.cm.com
login.cm.com

OWASP Amass v3.23.2                    https://github.com/owasp-amass/amass
--------------------------------------------------------------------------------
1 names discovered - cert: 1
--------------------------------------------------------------------------------
ASN: 13335 - CLOUDFLARENET - Cloudflare, Inc.
        2606:4700::/47            2     Subdomain Name(s)
        104.16.0.0/14             2     Subdomain Name(s)

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

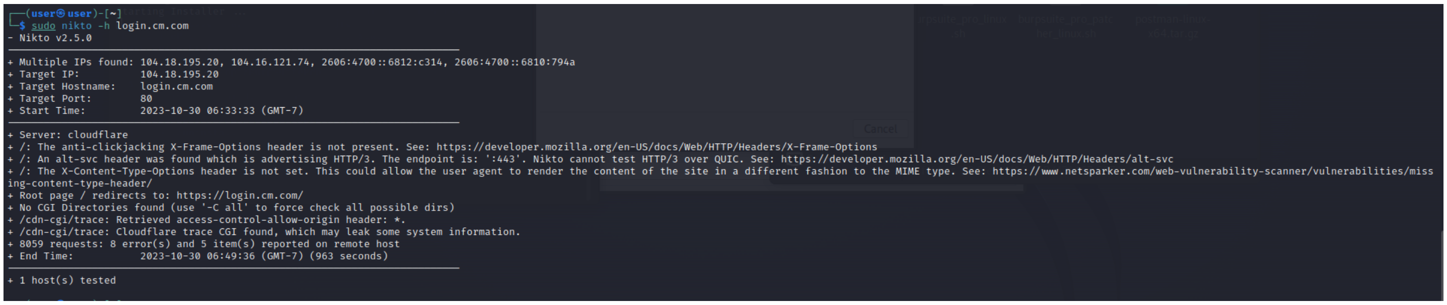
# 3. Scanning Vulnerability

## 3.1. Scan with Nmap



```
┌──(user㉿user)-[~]
└─$ sudo nmap -sS 104.16.121.74
[sudo] password for user:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 07:25 PDT
Nmap scan report for 104.16.121.74
Host is up (1.3s 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 348.17 seconds
```

## 3.2.Scan with Nikto

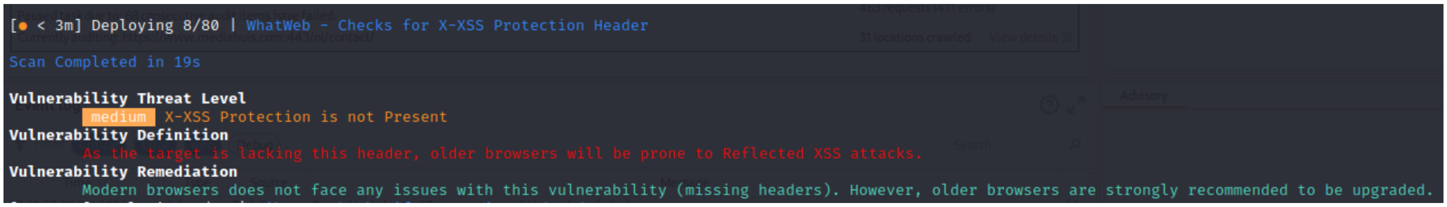


```
┌──(user㉿user)-[~]
└─$ sudo nikto -h login.cm.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 104.18.195.20, 104.16.121.74, 2606:4700::6812:c314, 2606:4700::6810:794a
+ Target IP:          104.18.195.20
+ Target Hostname:    login.cm.com
+ Target Port:        80
+ Start Time:         2023-10-30 06:33:33 (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
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: 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://login.cm.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /cdn-cgi/trace: Retrieved access-control-allow-origin header: *.
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.
+ 8059 requests: 8 error(s) and 5 item(s) reported on remote host
+ End Time:           2023-10-30 06:49:36 (GMT-7) (963 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- Retrieved access control allows origin header.
- Cloudflare trace CGI found which may leak some system information.

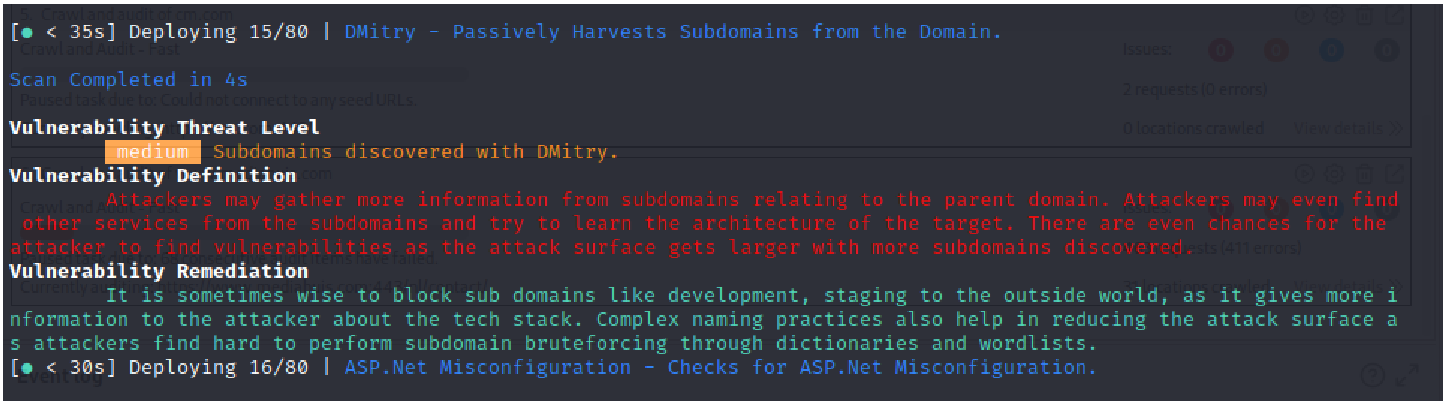
## 3.3.Scan with Rapidscan

- XSS Protection is not present.



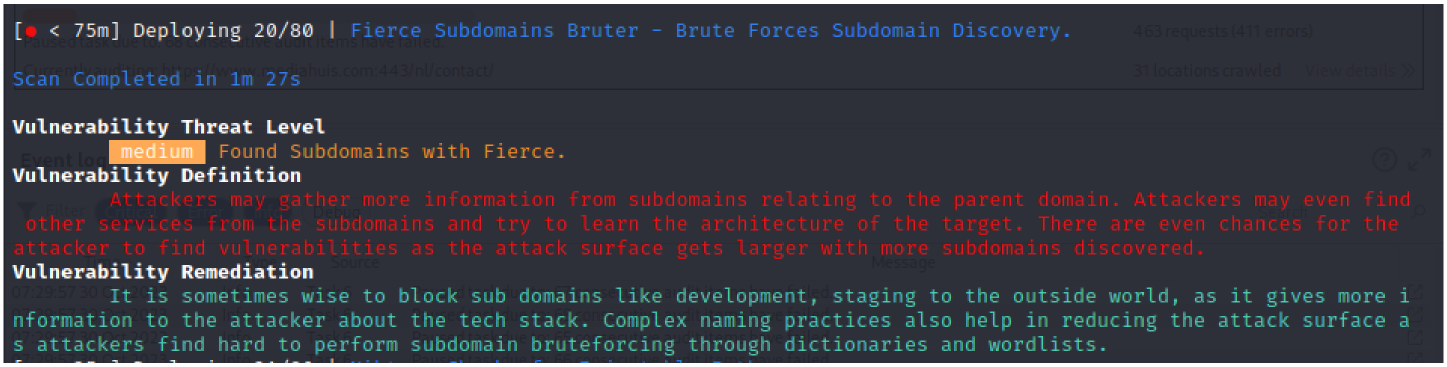
```
[● < 3m] Deploying 8/80 | WhatWeb - Checks for X-XSS Protection Header
Scan Completed in 19s

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.
```

- Subdomains discovered with Dmitry.



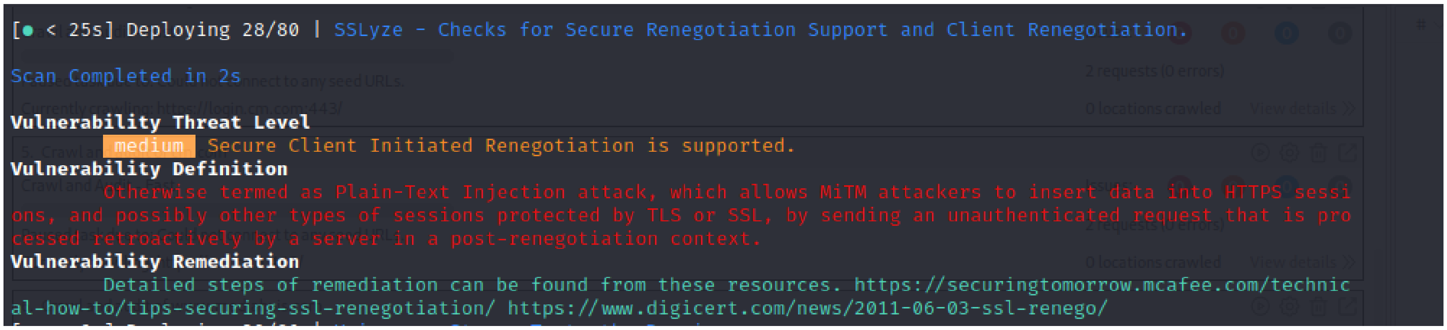
```
[● < 35s] Deploying 15/80 | DMitry - Passively Harvests Subdomains from the Domain.

Scan Completed in 4s

Vulnerability Threat Level
        medium  Subdomains discovered with DMitry.
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
attacker 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 i
nformation to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface a
s attackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.
[● < 30s] Deploying 16/80 | ASP.Net Misconfiguration - Checks for ASP.Net Misconfiguration.
```

- Found subdomains with fierce.



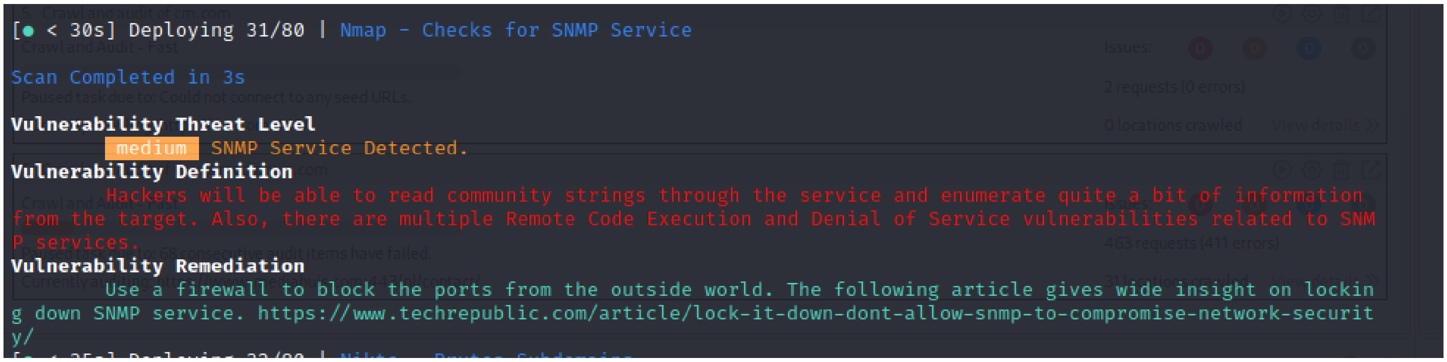
```
[● < 75m] Deploying 20/80 | Fierce Subdomains Bruter - Brute Forces Subdomain Discovery.

Scan Completed in 1m 27s

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
attacker 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 i
nformation to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface a
s attackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.
```

- Secure Client initialized renegotiation is acquired.



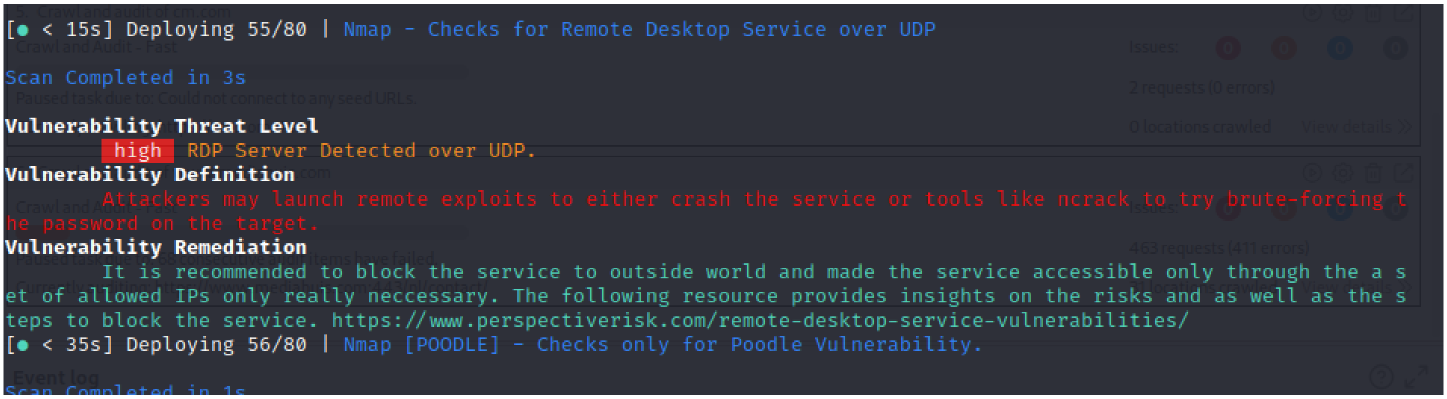
```
[● < 25s] Deploying 28/80 | SSLyze - Checks for Secure Renegotiation Support and Client Renegotiation.

Scan Completed in 2s

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 sessi
ons, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is pro
cessed 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/technic
al-how-to/tips-securing-ssl-renegotiation/ https://www.digicert.com/news/2011-06-03-ssl-renego/
```

- SNMP Service Detected



```
[● < 30s] Deploying 31/80 | Nmap - Checks for SNMP Service

Scan Completed in 3s

Vulnerability Threat Level
            medium  SNMP Service Detected.
Vulnerability Definition
            Hackers will be able to read community strings through the service and enumerate quite a bit of information
from the target. Also, there are multiple Remote Code Execution and Denial of Service vulnerabilities related to SNM
P services.
Vulnerability Remediation
            Use a firewall to block the ports from the outside world. The following article gives wide insight on lockin
g down SNMP service. https://www.techrepublic.com/article/lock-it-down-dont-allow-snmp-to-compromise-network-securit
y/
[● < 35s] Deploying 32/80 | Nikto - Brutes Subdomains
```

- RDP server Detected over UDP



```
[● < 15s] Deploying 55/80 | Nmap - Checks for Remote Desktop Service over UDP

Scan Completed in 3s

Vulnerability Threat Level
            high  RDP Server Detected over UDP.
Vulnerability Definition
            Attackers may launch remote exploits to either crash the service or tools like ncrack to try brute-forcing t
he password on the target.
Vulnerability Remediation
            It is recommended to block the service to outside world and made the service accessible only through the a s
et of allowed IPs only really neccessary. The following resource provides insights on the risks and as well as the s
teps to block the service. https://www.perspectiverisk.com/remote-desktop-service-vulnerabilities/
[● < 35s] Deploying 56/80 | Nmap [POODLE] - Checks only for Poodle Vulnerability.

Scan Completed in 1s
```

## 4. Vulnerability description

- **XSS Protection is Not Present**:
  - The absence of the "X-XSS-Protection" header suggests a vulnerability to cross-site scripting (XSS) attacks, where malicious scripts can be injected into web pages, potentially compromising user data and security.
  -
- **Subdomains Discovered with Dmitry**:
  - Subdomains were discovered using the tool Dmitry, which potentially expands the attack surface, exposing additional points of vulnerability and potential unauthorized access.
  -
- **Found Subdomains with Fierce**:
  - Subdomains were discovered using the tool Fierce, which further uncovers the website's subdomains, potentially revealing additional entry points or potential vulnerabilities.
  -
- **Secure Client-Initiated Renegotiation is Acquired**:
  - The acquisition of Secure Client-Initiated Renegotiation may introduce security risks if not configured correctly, potentially facilitating man-in-the-middle attacks.
  -
- **SNMP Service Detected**:
  - The presence of the Simple Network Management Protocol (SNMP) service may expose sensitive information and configuration details, potentially posing a security risk if not adequately secure.
  -
- **RDP Server Detected Over UDP**:
  - Detecting an RDP (Remote Desktop Protocol) server operating over UDP (User Datagram Protocol) may present security concerns, as it might expose the server to various security risks if not properly configured.

## 5. Affected components.

- Web application (XSS).
- Domain and subdomains.
- Client-server communication.
- Network devices (SNMP).
- RDP servers (UDP).

## 6. Impact assessment

- XSS: Data theft, malicious script execution.
- Subdomains: Information exposure.
- Client-server: Data interception
- SNMP: Unauthorized access
- RDP (UDP): Vulnerabilities in remote access

## 7. Steps to reproduce.

None.

## 8. Proof of concept (if applicable)

None.

## 9. Proposed mitigation or fix

- XSS protection, input validation.
- Subdomain monitoring.
- Secure communication setup.
- SNMP access restrictions.
- Secure RDP configuration.

## 10. Summary

Founded potential security vulnerabilities are related to XSS protection, subdomains, secure client-server communication, SNMP services, and RDP servers. The impact and necessary steps to address these issues would require further investigation and may vary depending on the specific context and systems in question. Appropriate security measures and patches should be applied to mitigate these vulnerabilities.