Information Gathering

1) Multiple open ports have been found

```
-(vigneswar⊛vigneswar)-[~]
 -$ nmap 10.10.10.7
Starting Nmap 7.94 (https://nmap.org) at 2023-09-24 09:18 IST
Nmap scan report for 10.10.10.7
Host is up (0.71s latency).
Not shown: 988 closed tcp ports (conn-refused)
         STATE SERVICE
PORT
22/tcp
        open ssh
25/tcp
         open smtp
80/tcp
        open http
110/tcp
        open pop3
111/tcp open rpcbind
143/tcp
        open imap
443/tcp open https
993/tcp
        open imaps
995/tcp open pop3s
3306/tcp open mysql
4445/tcp open upnotifyp
10000/tcp open snet-sensor-mgmt
Nmap done: 1 IP address (1 host up) scanned in 63.15 seconds
```

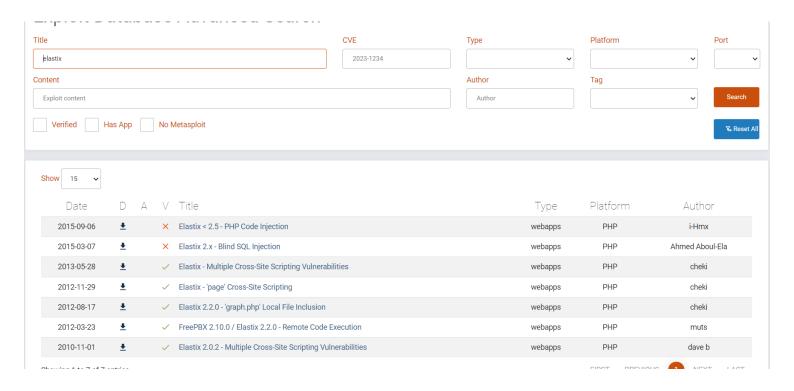
2) further scan has been done

```
-(vigneswar⊛vigneswar)-[~]
sudo nmap 10.10.10.7 -p22,25,80,110,111,143,993,995,3306,4445,10000 -sCV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-24 09:31 IST
Nmap scan report for 10.10.10.7
Host is up (0.55s latency).
PORT
         STATE SERVICE
                          VERSION
         open ssh
                          OpenSSH 4.3 (protocol 2.0)
22/tcp
| ssh-hostkey:
   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
   2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
         open smtp
                          Postfix smtpd
_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES
 8BITMIME, DSN
80/tcp
        open http
                          Apache httpd 2.2.3
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Did not follow redirect to https://10.10.10.7/
110/tcp open pop3
                         Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: PIPELINING USER UIDL AUTH-RESP-CODE STLS IMPLEMENTATION(Cyrus POP3 serve
r v2) EXPIRE(NEVER) APOP RESP-CODES LOGIN-DELAY(0) TOP
                         2 (RPC #100000)
111/tcp
        open rpcbind
rpcinfo:
   program version
                      port/proto service
    100000 2
                        111/tcp
                                  rpcbind
    100000 2
                        111/udp
                                  rpcbind
    100024 1
                        876/udp
                                  status
   100024 1
                        879/tcp
                                  status
143/tcp
                          Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
        open imap
|_imap-capabilities: THREAD=ORDEREDSUBJECT QUOTA STARTTLS SORT=MODSEQ CATENATE Completed LIST
EXT RENAME LITERAL+ OK LIST-SUBSCRIBED IMAP4 URLAUTHA0001 IDLE IMAP4rev1 CONDSTORE BINARY ANN
OTATEMORE SORT THREAD=REFERENCES NAMESPACE MULTIAPPEND MAILBOX-REFERRALS CHILDREN ATOMIC UNSE
LECT ACL X-NETSCAPE ID UIDPLUS NO RIGHTS=kxte
993/tcp
         open ssl/imap
                         Cyrus imapd
| imap-capabilities: CAPABILITY
                          Cyrus pop3d
995/tcp
         open pop3
                          MySQL (unauthorized)
3306/tcp open mysql
4445/tcp open upnotifyp?
10000/tcp open http
                          MiniServ 1.570 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: Hosts: beep.localdomain, 127.0.0.1, example.com
```

Media Permissions Security Website Identity Website: 10.10.10.7 Owner: This website does not supply ownership information. Verified by: PortSwigger View Certificate Privacy & History Have I visited this website prior to today? Nο Yes, cookies Clear Cookies and Site Data Is this website storing information on my computer? Have I saved any passwords for this website? View Saved Passwords Nο Technical Details Connection Encrypted (TLS_AES_256_GCM_SHA384, 256 bit keys, TLS 1.3) The page you are viewing was encrypted before being transmitted over the Internet. Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network. Help

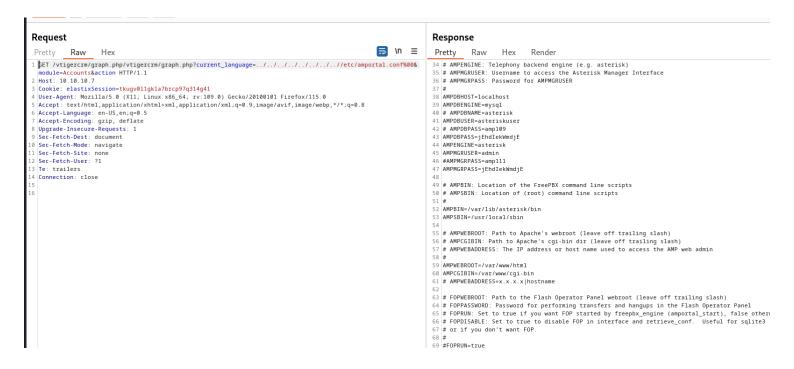
```
–(vigneswar⊛vigneswar)-[~]
 -$ curl https://10.10.10.7 -i -k -vv
    Trying 10.10.10.7:443 ...
* Connected to 10.10.10.7 (10.10.10.7) port 443 (#0)
* ALPN: offers h2,http/1.1
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.0 (IN), TLS handshake, Certificate (11):
* TLSv1.0 (IN), TLS handshake, Server key exchange (12):
* TLSv1.0 (IN), TLS handshake, Server finished (14):
* TLSv1.0 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.0 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.0 (OUT), TLS handshake, Finished (20):
* TLSv1.0 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1 / DHE-RSA-AES256-SHA
* ALPN: server did not agree on a protocol. Uses default.
* Server certificate:
* subject: C=--; ST=SomeState; L=SomeCity; O=SomeOrganization; OU=SomeOrganizationalUnit; CN
=localhost.localdomain; emailAddress=root@localhost.localdomain
* start date: Apr 7 08:22:08 2017 GMT
 expire date: Apr 7 08:22:08 2018 GMT
   issuer: C=--; ST=SomeState; L=SomeCity; O=SomeOrganization; OU=SomeOrganizationalUnit; CN=
localhost.localdomain; emailAddress=root@localhost.localdomain
   SSL certificate verify result: self-signed certificate (18), continuing anyway.
* using HTTP/1.x
> GET / HTTP/1.1
> Host: 10.10.10.7
> User-Agent: curl/7.88.1
 Accept: */*
```

3) Found vulnerabilities on elastix



Exploitation

1) found the password



2) Logged in as root

```
-(vigneswar® vigneswar)-[~]
 _$ ssh 10.10.10.7 -l "root" -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=
The authenticity of host '10.10.10.7 (10.10.10.7)' can't be established.
DSA key fingerprint is SHA256:AGaW4a0uNJ7KPMpSOBD+aVIN75AV3C0y8yKpqFjedTc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.7' (DSA) to the list of known hosts.
root@10.10.10.7's password:
Permission denied, please try again.
root@10.10.10.7's password:
Last login: Tue Jul 16 11:45:47 2019
Welcome to Elastix
To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://10.10.10.7
[root@beep ~]#
```

٠,

3) Got the flag

```
The authenticity of host '10.10.10.7 (10.10.10.7)' can't be established.
DSA key fingerprint is SHA256:AGaW4a0uNJ7KPMpSOBD+aVIN75AV3C0y8yKpqFjedTc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.7' (DSA) to the list of known hosts.
root@10.10.10.7's password:
Permission denied, please try again.
root@10.10.10.7's password:
Last login: Tue Jul 16 11:45:47 2019
Welcome to Elastix
To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://10.10.10.7
[root@beep ~]# cat /root/root.txt
c1940b06376aa83421f9c253f5bb560b
[root@beep ~]# cat /home/fanis/user.txt
6b119d918e808872979e779ab66df17e
[root@beep ~]#
```