Frolic(放棄),太多加解密，根本CTF

```
└─# nmap -sT --min-rate 5000 -sU -p- 10.10.10.111
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-11 14:20 EDT
Warning: 10.10.10.111 giving up on port because retransmission cap hit (10).
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 33.02% done; ETC: 14:22 (0:01:37 remaining)
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 33.50% done; ETC: 14:22 (0:01:35 remaining)
Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 34.24% done; ETC: 14:22 (0:01:34 remaining)
Warning: 10.10.10.111 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.10.111
Host is up (0.24s latency).
Not shown: 65468 closed tcp ports (conn-refused), 148 closed udp ports (port-unreach),
65386 open|filtered udp ports (no-response), 62 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1880/tcp open  vsat-control
9999/tcp open  abyss
137/udp  open  netbios-ns

Nmap done: 1 IP address (1 host up) scanned in 181.84 seconds

┌──(root㉿kali)-[~]
└─# nmap -sCV -p 22,139,445,1880,9999,137 -A 10.10.10.111
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-11 14:26 EDT
Nmap scan report for 10.10.10.111
Host is up (0.23s latency).

PORT     STATE  SERVICE     VERSION
22/tcp   open   ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 87:7b:91:2a:0f:11:b6:57:1e:cb:9f:77:cf:35:e2:21 (RSA)
|   256 b7:9b:06:dd:c2:5e:28:44:78:41:1e:67:7d:1e:b7:62 (ECDSA)
|_  256 21:cf:16:6d:82:a4:30:c3:c6:9c:d7:38:ba:b5:02:b0 (ED25519)
137/tcp  closed netbios-ns
139/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

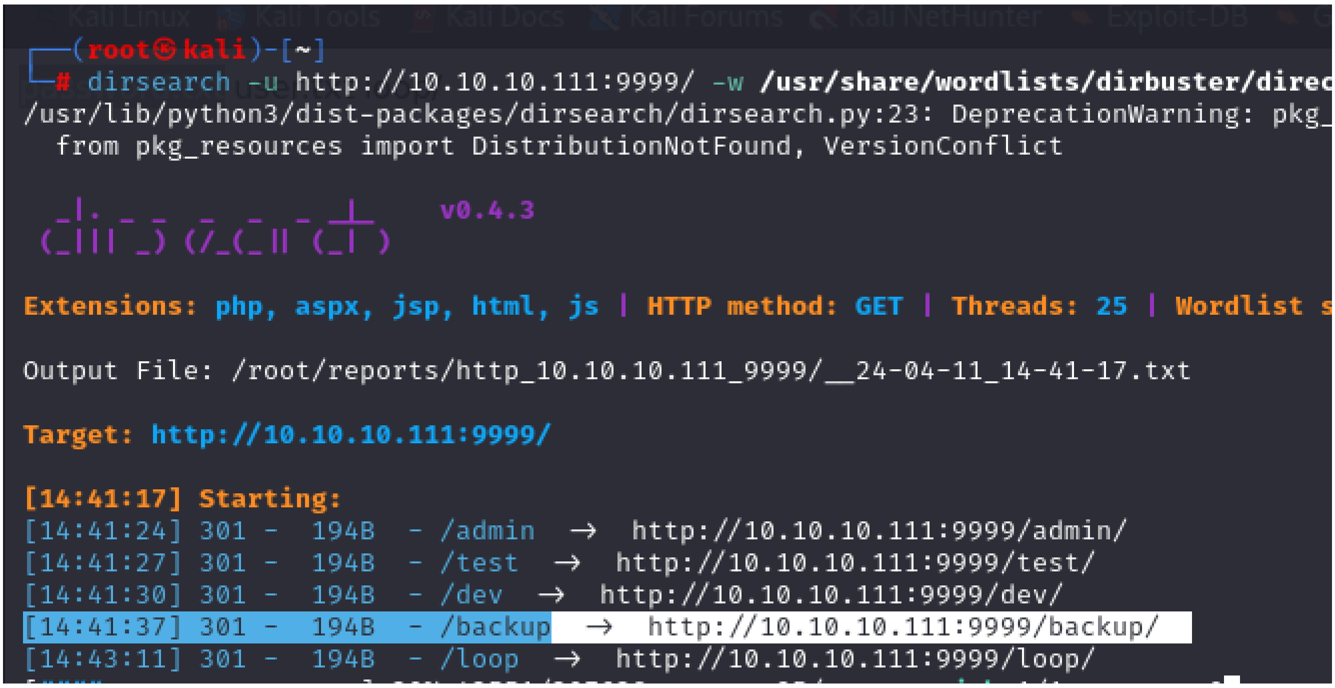
```
445/tcp  open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
1880/tcp open   http        Node.js (Express middleware)
|_http-title: Node-RED
9999/tcp open   http        nginx 1.10.3 (Ubuntu)
|_http-server-header: nginx/1.10.3 (Ubuntu)
|_http-title: Welcome to nginx!
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=4/11%OT=22%CT=137%CU=36399%PV=Y%DS=2%DC=T%G=Y%TM=66
OS:182B7C%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=10E%TI=Z%CI=I%II=I%TS=
OS:8)SEQ(SP=FF%GCD=1%ISR=10E%TI=Z%CI=I%II=I%TS=8)OPS(O1=M53CST11NW7%O2=M53C
OS:ST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1
OS:=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O
OS:=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N
OS:)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=
OS:S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF
OS:=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=
OS:G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: Host: FROLIC; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: FROLIC, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
|_clock-skew: mean: -1h50m00s, deviation: 3h10m30s, median: -1s
| smb2-time:
|   date: 2024-04-11T18:27:00
|_  start_date: N/A
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: frolic
|   NetBIOS computer name: FROLIC\x00
|   Domain name: \x00
|   FQDN: frolic
|_  System time: 2024-04-11T23:57:00+05:30
| smb2-security-mode:
```

```
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE (using port 137/tcp)
HOP RTT       ADDRESS
1   239.62 ms 10.10.14.1
2   236.17 ms 10.10.10.111

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.73 seconds
```

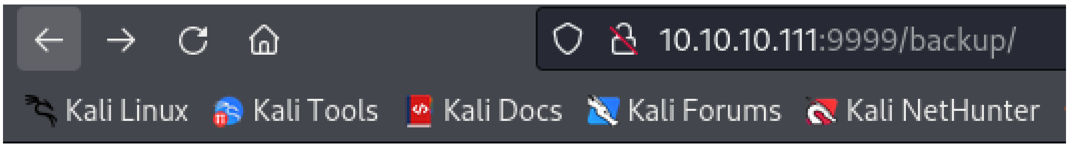
- 2個網站，一個是登入介面
- SMB無資料

目錄爆破發現有趣的，

- /admin登入介面
- /dev有帳密



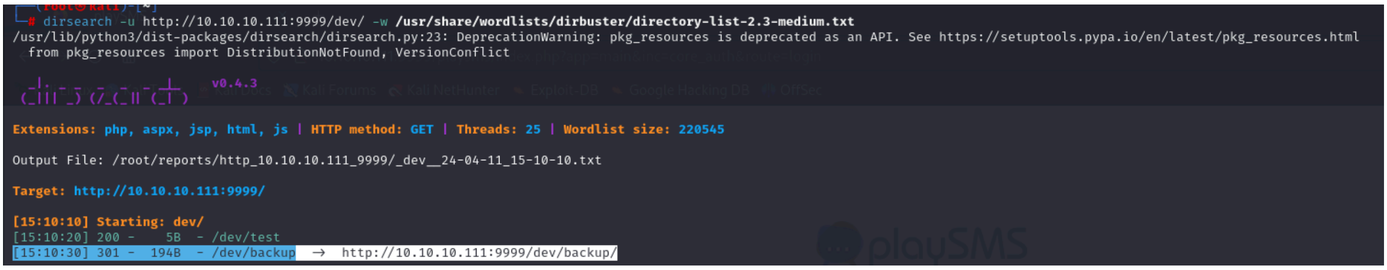
```
┌──(root㉿kali)-[~]
└─# dirsearch -u http://10.10.10.111:9999/ -w /usr/share/wordlists/dirbuster/direc
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist s

Output File: /root/reports/http_10.10.10.111_9999/__24-04-11_14-41-17.txt

Target: http://10.10.10.111:9999/

[14:41:17] Starting:
[14:41:24] 301 -  194B  - /admin  ->  http://10.10.10.111:9999/admin/
[14:41:27] 301 -  194B  - /test  ->  http://10.10.10.111:9999/test/
[14:41:30] 301 -  194B  - /dev  ->  http://10.10.10.111:9999/dev/
[14:41:37] 301 -  194B  - /backup  ->  http://10.10.10.111:9999/backup/
[14:43:11] 301 -  194B  - /loop  ->  http://10.10.10.111:9999/loop/
```



password.txt user.txt loop/

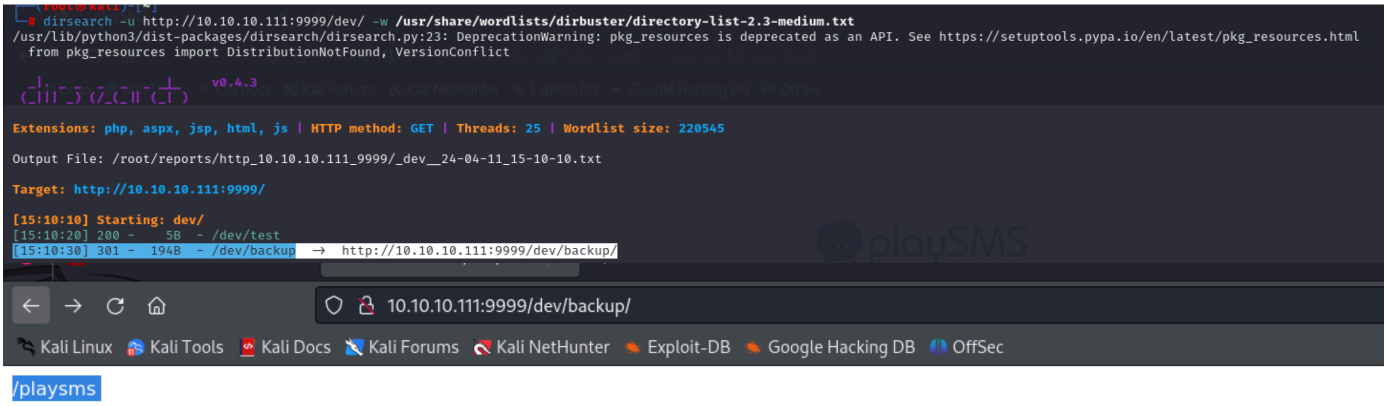
```
先保存帳密，測試都失敗
username : admin
passwd : imnothuman
```

後續繼續爆破



```
└─# dirsearch -u http://10.10.10.111:9999/dev/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

                                  v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 220545

Output File: /root/reports/http_10.10.10.111_9999/_dev__24-04-11_15-10-10.txt

Target: http://10.10.10.111:9999/

[15:10:10] Starting: dev/
[15:10:20] 200 -    5B  - /dev/test
[15:10:30] 301 -  194B  - /dev/backup  ->  http://10.10.10.111:9999/dev/backup/
```

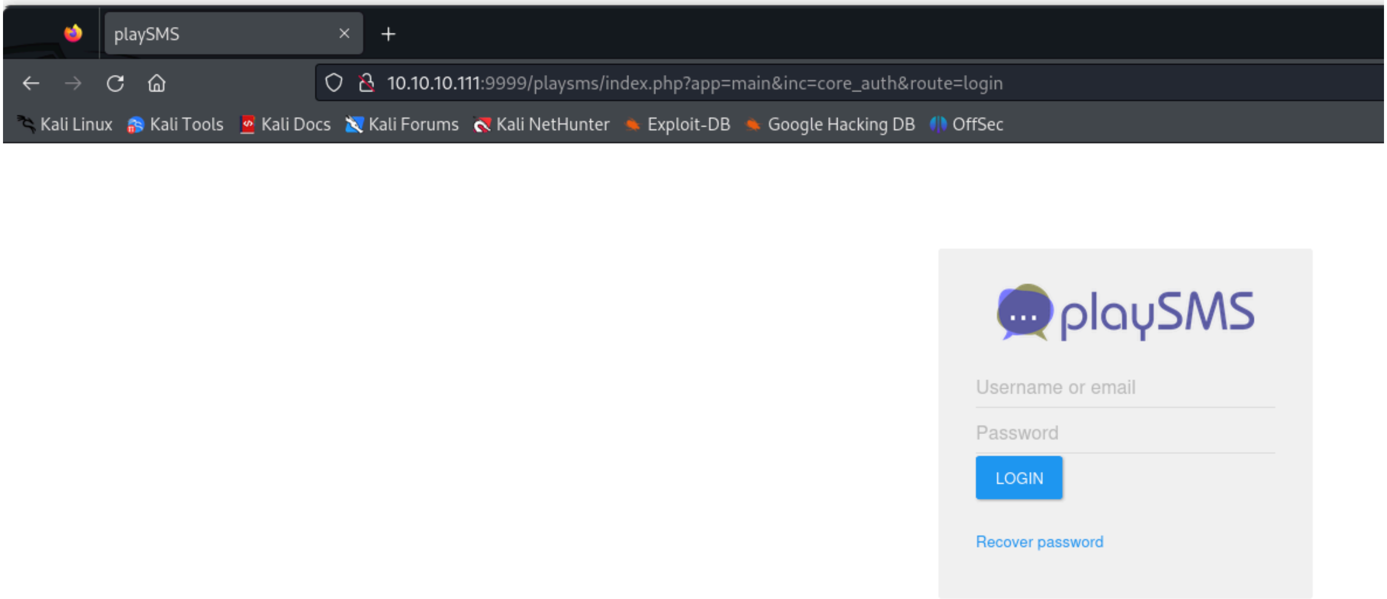
又發現登入介面.....登入失敗



```
└─# dirsearch -u http://10.10.10.111:9999/dev/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

                                  v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 220545

Output File: /root/reports/http_10.10.10.111_9999/_dev__24-04-11_15-10-10.txt

Target: http://10.10.10.111:9999/

[15:10:10] Starting: dev/
[15:10:20] 200 -    5B  - /dev/test
[15:10:30] 301 -  194B  - /dev/backup  ->  http://10.10.10.111:9999/dev/backup/
```

10.10.10.111:9999/dev/backup/

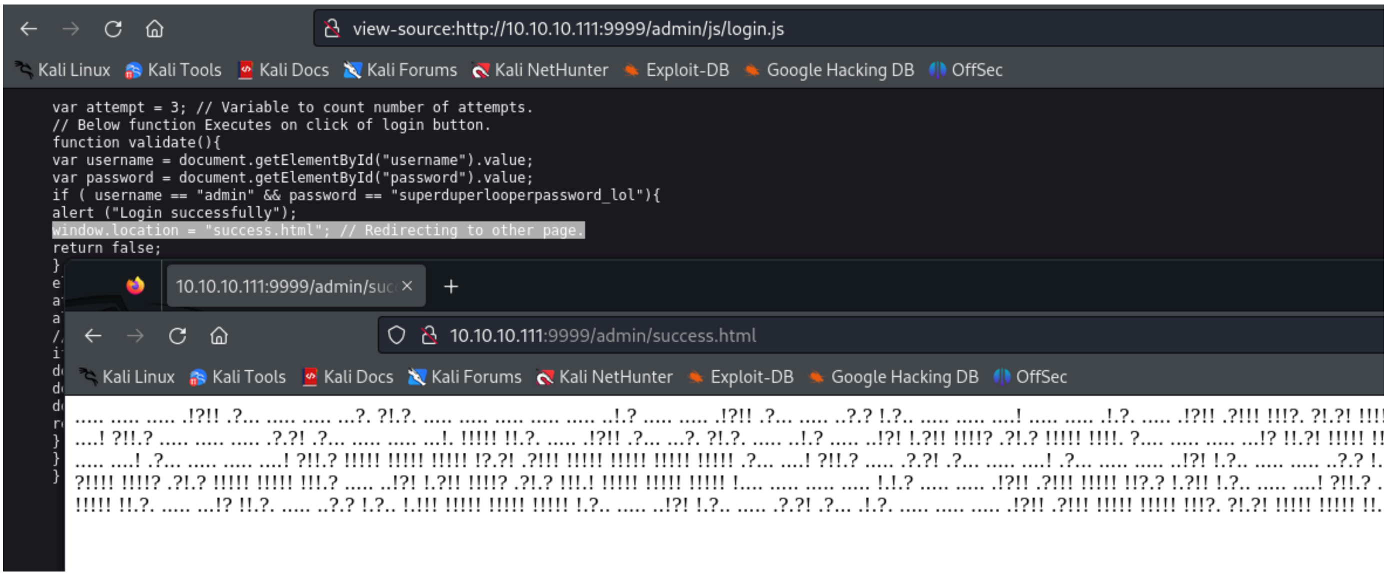
/playsms



playSMS

10.10.10.111:9999/playsms/index.php?app=main&inc=core_auth&route=login

檢查腳本，發現一對OOXX



view-source:http://10.10.10.111:9999/admin/js/login.js

```
var attempt = 3; // Variable to count number of attempts.
// Below function Executes on click of login button.
function validate(){
var username = document.getElementById("username").value;
var password = document.getElementById("password").value;
if ( username == "admin" && password == "superduperlooperpassword_lol"){
alert ("Login successfully");
window.location = "success.html"; // Redirecting to other page.
return false;
}
```

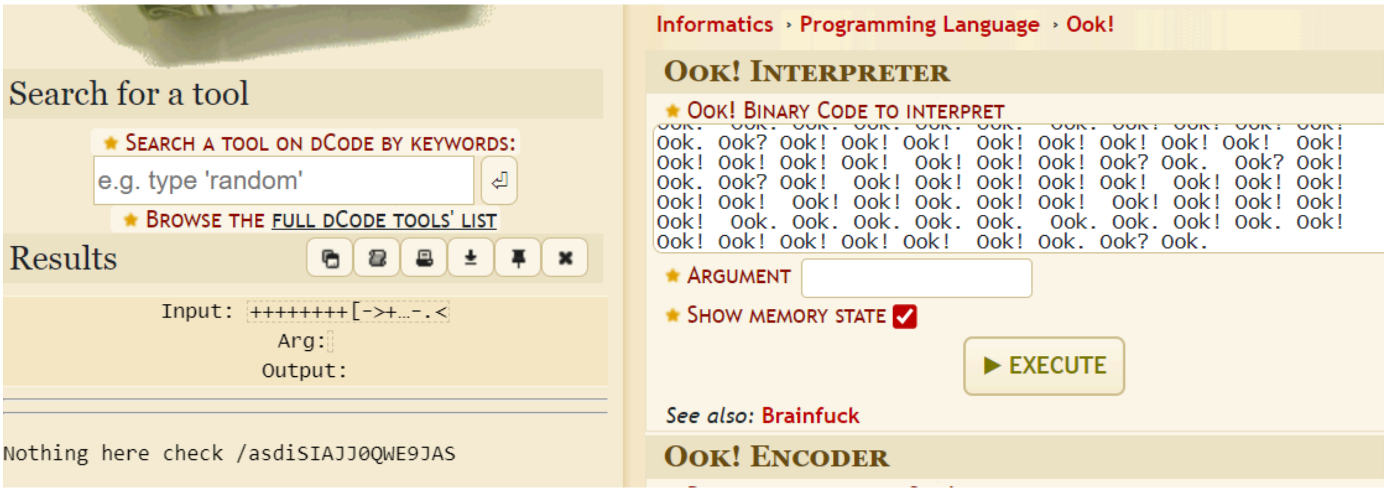
10.10.10.111:9999/admin/success.html

```
..... ..... ..... .!?!! .?... ..... ..... ...?. ?!.?. ..... ..... ..... ..... ..... ..!.? ..... ..... .!?!! .?... ..... ..?.? !.?.. ..... ..... ....! ..... ..... .!.?. ..... .!?!! .?!!! !!!?. ?!.?! !!!!
....! ?!!.? ..... ..... ..... .?.?! .?... ..... ..... ...!. !!!!! !!.?. ..... .!?!! .?... ...?. ?!.?. ..... ..!.? ..... ..!?! !.?!! !!!!? .?!.? !!!!! !!!!. ?.... ..... ..... ...!? !!.?! !!!!! !!
..... ....! .?... ..... ..... ....! ?!!.? !!!!! !!!!! !!!!! !?.?! .?!!! !!!!! !!!!! !!!!! !!!!! .?... ....! ?!!.? ..... .?.?! .?... ..... ....! .?... ..... ..... ..!?! !.?.. ..... ..... ..?.? !.
?!!!! !!!!? .?!.? !!!!! !!!!! !!!.? ..... ..!?! !.?!! !!!!? .?!.? !!!.! !!!!! !!!!! !!!!! !.... ..... ..... ..... !.!.? ..... ..... .!?!! .?!!! !!!!! !!?.? !.?!! !.?.. ..... ....! ?!!.? .
!!!!! !!.?. ..... ...!? !!.?. ..... ..?.? !.?.. !.!!! !!!!! !!!!! !!!!! !.?.. ..... ..!?! !.?.. ..... .?.?! .?... .!.?. ..... ..... ..... .!?!! .?!!! !!!!! !!!!! !!!?. ?!.?! !!!!! !!!!! !!.
```

參考：

- https://esolangs.org/wiki/Ook!
- https://www.dcode.fr/ook-language

```python
#!/usr/bin/python3

import sys

if len(sys.argv) != 3:
    print(f"{sys.argv[0]} [infile] [outfile]")
    sys.exit(0)

try:
    with open(sys.argv[1], 'r') as f:
        with open(sys.argv[2], 'w') as fout:
            fout.write(f.read().replace('.', 'Ook. ').replace('?','Ook? ').replace('!','Ook! '))
except:
    print("Failed")
```



Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type 'random'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

```
Input: ++++++++[->+…-.<
  Arg:
Output:

Nothing here check /asdiSIAJJ0QWE9JAS
```

Informatics › Programming Language › Ook!

OOK! INTERPRETER

★ OOK! BINARY CODE TO INTERPRET

```
Ook. Ook? Ook! Ook! Ook!  Ook! Ook! Ook! Ook! Ook!  Ook!
Ook! Ook! Ook! Ook!  Ook! Ook! Ook! Ook? Ook.  Ook? Ook!
Ook. Ook? Ook!  Ook! Ook! Ook! Ook! Ook!  Ook! Ook! Ook!
Ook! Ook!  Ook! Ook! Ook. Ook! Ook!  Ook! Ook! Ook! Ook!
Ook!  Ook. Ook. Ook. Ook. Ook.  Ook. Ook. Ook! Ook. Ook!
Ook! Ook! Ook! Ook! Ook!  Ook! Ook. Ook? Ook.
```

★ ARGUMENT

★ SHOW MEMORY STATE ☑

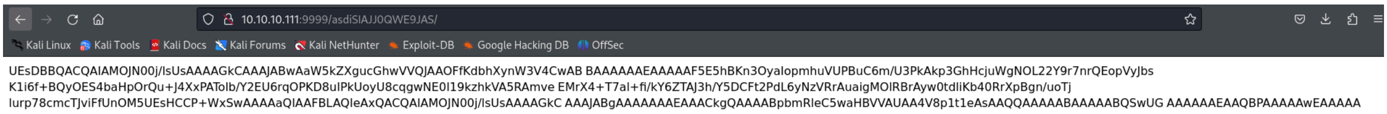
▶ EXECUTE

See also: Brainfuck

OOK! ENCODER

`Nothing here check /asdiSIAJJ0QWE9JAS` <= 一個目錄

又是密碼



10.10.10.111:9999/asdiSIAJJ0QWE9JAS/

UEsDBBQACQAIAMOJN00j/lsUsAAAAGkCAAAJABwAaW5kZXgucGhwVVQJAAOFfKdbhXynW3V4CwAB BAAAAAAEAAAAAF5E5hBKn3OyaIopmhuVUPBuC6m/U3PkAkp3GhHcjuWgNOL22Y9r7nrQEopVyJbs
K1i6f+BQyOES4baHpOrQu+J4XxPATolb/Y2EU6rqOPKD8uIPkUoyU8cqgwNE0I19kzhkVA5RAmve EMrX4+T7al+fi/kY6ZTAJ3h/Y5DCFt2PdL6yNzVRrAuaigMOIRBrAyw0tdliKb40RrXpBgn/uoTj
lurp78cmcTJviFfUnOM5UEsHCCP+WxSwAAAAaQIAAFBLAQIeAxQACQAIAMOJN00j/lsUsAAAAGkC AAAJABgAAAAAAAEAAACkgQAAAABpbmRleC5waHBVVAUAA4V8p1t1eAsAAQQAAAAABAAAAABQSwUG AAAAAAEAAQBPAAAAwEAAAAA