

資訊安全

2023/07/02

\$CAICT

自我介紹

- 高一 to 高二
- 中電會資訊組 - 第二屆
- 中興聯合寒訓 - 教學組
- AS199331 - 持有人



@ chao28661



今日課程規劃

- 序 + 基礎網路概論
- 常見攻擊手法
- 常見Tools / Packet
- Linux基礎指令
- 駭客思維 / 相關網站
- CTF time

序 + 基礎網路概論

20 mins



相關法條

- ★ 第358條，無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰款。
- ★ 第359條，無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰款。
- ★ 第360條，無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰款。
- ★ 第361條，對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
- ★ 第362條，製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰款。
- ★ 第363條，第三百五十八條至第三百六十條之罪，須告訴乃論。

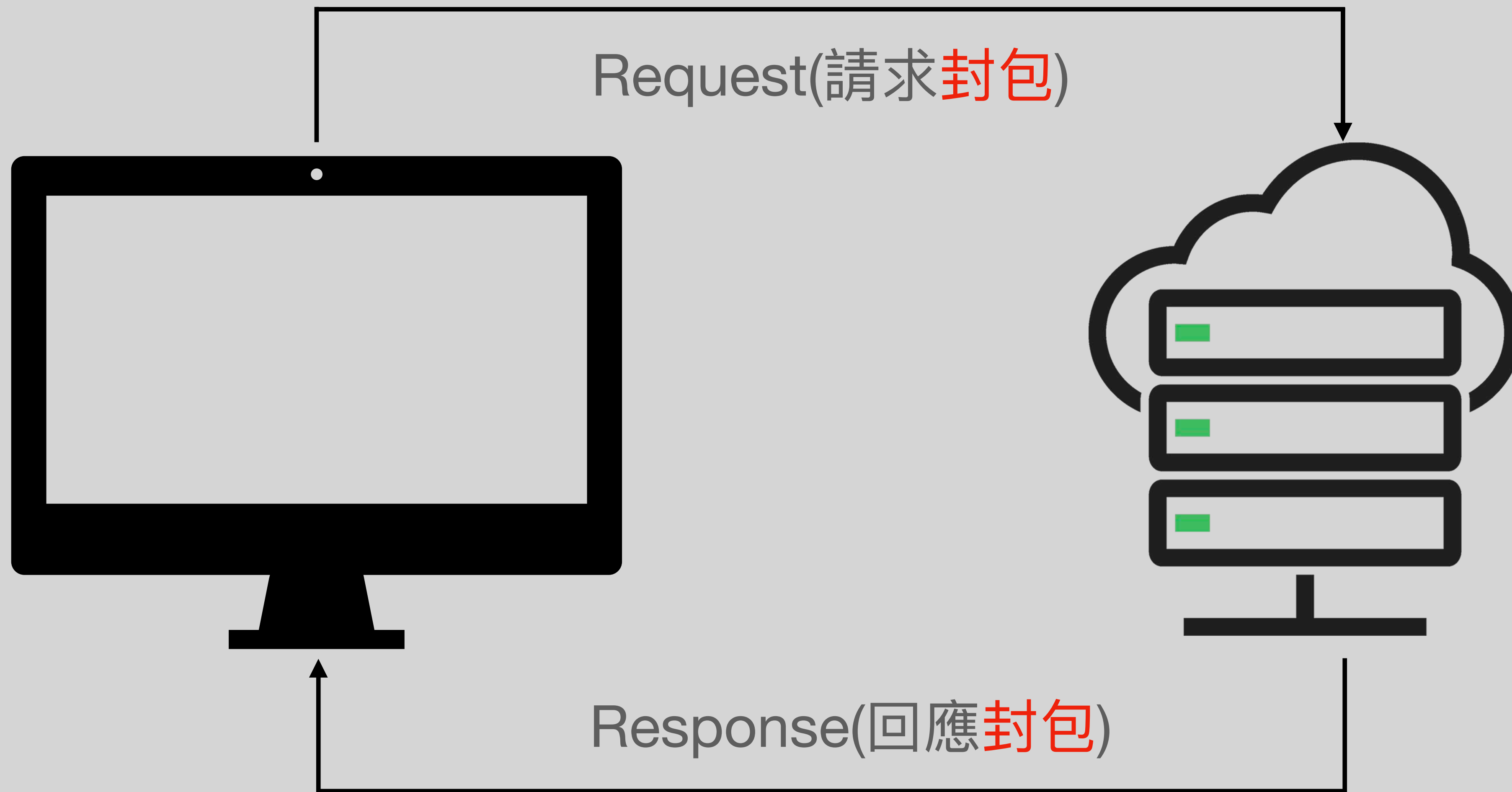
網頁三兄弟



網頁三兄弟

	HTML	CSS	JavaScript
負責項目	網頁的架構	網頁的美化	網頁的互動模組
房子來比喻	房子的水泥	房子的裝潢	房子的水電

網站運作原理



思考一下 Web 也會說中文嗎？



Request封包怎麼讀？

```
1 GET / HTTP/2
2 Host: scaict.org
3 Cache-Control: max-age=0
4 Sec-Ch-Ua: "Not:A-Brand";v="99",
  "Chromium";v="112"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "macOS"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0;
  Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/112.0.5615.50 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/x
  ml;q=0.9,image/avif,image/webp,image/apng,*/*
  ;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
15 Accept-Language:
  zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7
```

➡ 使用GET方法請求

➡ 請求的路徑(這裡是/)

➡ 搭配HTTP 2協定

Request封包怎麼讀？

```
1 GET / HTTP/2
2 Host: scaict.org
3 Cache-Control: max-age=0
4 Sec-Ch-Ua: "Not:A-Brand";v="99",
  "Chromium";v="112"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "macOS"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0;
  Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/112.0.5615.50 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/x
  ml;q=0.9,image/avif,image/webp,image/apng,*/
  ;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
15 Accept-Language:
  zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7
```

➡ 請求的目的是 scaict.org

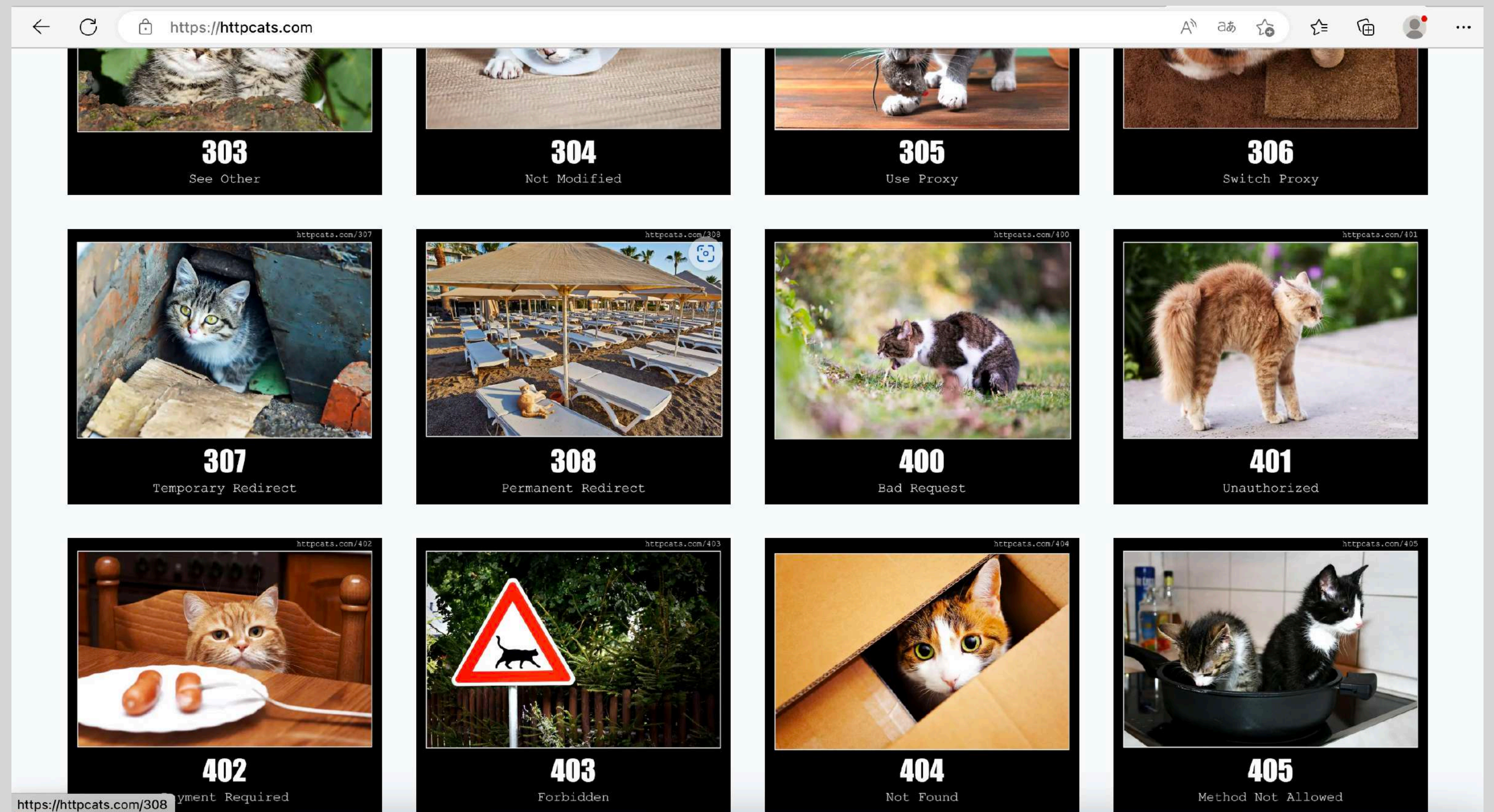
Response 封包怎麼讀？

```
1 HTTP/2 200 OK
2 Content-Type: text/html
3 Last-Modified: Sat, 11 Feb 2023 16:22:03 GMT
4 Accept-Ranges: bytes
5 Vary: Accept-Encoding
6 Content-Length: 10003
7 Date: Wed, 31 May 2023 06:44:03 GMT
8 Server: LiteSpeed
9 Alt-Svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000,
h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000,
h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"
```

➡ 使用http 2請求/, 回傳成功狀態碼(200)

常見回應狀態碼

- 200 - OK
- 400 - Bad Request
- 403 - Forbidden
- 404 - Not Found
- 405 - Method Not Allow
- 500 - Internal Server Error



常見回應狀態碼類別

資訊回應	成功回應	重定向	用戶端錯誤	伺服器端錯誤
100~199	200~299	300~399	400~499	500~599
https://httpcats.com/ https://http.dog/				

Response封包怎麼讀？

```
1 HTTP/2 200 OK
2 Content-Type: text/html
3 Last-Modified: Sat, 11 Feb 2023 16:22:03 GMT
4 Accept-Ranges: bytes
5 Vary: Accept-Encoding
6 Content-Length: 10003
7 Date: Wed, 31 May 2023 06:44:03 GMT
8 Server: LiteSpeed
9 Alt-Svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000,
h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000,
h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"
```

➡ 回傳檔案類型為文字檔的html檔案

Response 封包怎麼讀？

```
1 HTTP/2 200 OK
2 Content-Type: text/html
3 Last-Modified: Sat, 11 Feb 2023 16:22:03 GMT
4 Accept-Ranges: bytes
5 Vary: Accept-Encoding
6 Content-Length: 10003
7 Date: Wed, 31 May 2023 06:44:03 GMT
8 Server: LiteSpeed
9 Alt-Svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000,
h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000,
h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"
```

➡ 這份檔案的最後修改時間

Response 封包怎麼讀？

```
1 HTTP/2 200 OK
2 Content-Type: text/html
3 Last-Modified: Sat, 11 Feb 2023 16:22:03 GMT
4 Accept-Ranges: bytes
5 Vary: Accept-Encoding
6 Content-Length: 10003
7 Date: Wed, 31 May 2023 06:44:03 GMT
8 Server: LiteSpeed
9 Alt-Svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000,
h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000,
h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"
```

➡ 這份資料有10003個字元

Response 封包怎麼讀？

```
1 HTTP/2 200 OK
2 Content-Type: text/html
3 Last-Modified: Sat, 11 Feb 2023 16:22:03 GMT
4 Accept-Ranges: bytes
5 Vary: Accept-Encoding
6 Content-Length: 10003
7 Date: Wed, 31 May 2023 06:44:03 GMT
8 Server: LiteSpeed
9 Alt-Svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000,
  h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000,
  h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"
```

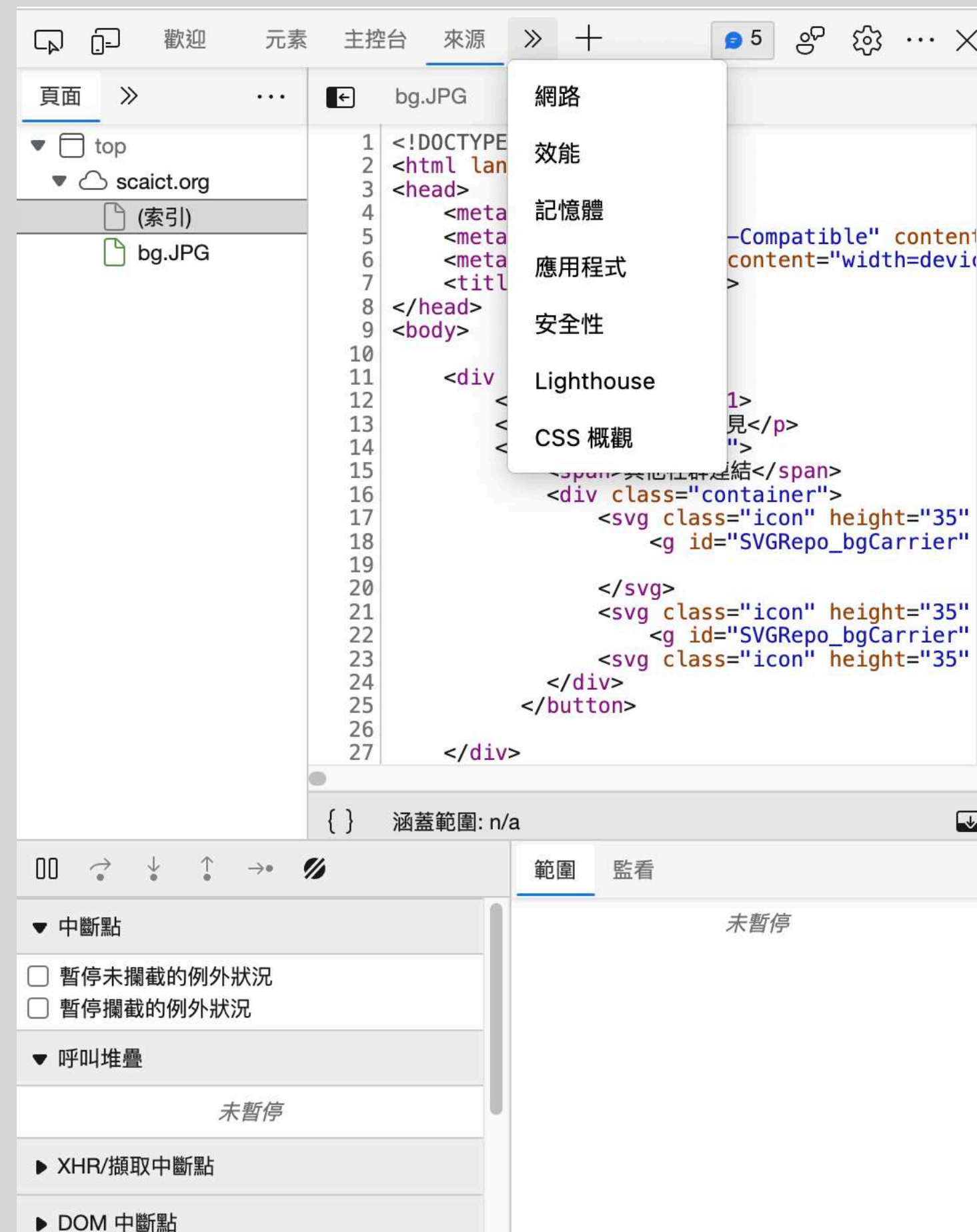
➡ 請求時間

瀏覽器 - 開發者模式

← 上一頁	⌘[
↻ 重新整理	⌘R
📄 另存新檔...	⌘S
🖨 列印...	⌘P
傳送索引標籤到您的裝置	
📱 建立此頁面的 QR 代碼	
A🔊 大聲朗讀	⇧⌘U
🌐 翻譯成 中文 (繁體)	
📄➕ 新增頁面至側邊欄	
📁➕ 將頁面新增至集錦	>
🔗 分享	
📄 網頁選取	⇧⌘X
📄 網頁擷取	⇧⌘S
🔍 檢視頁面來源	⇧⌘U
🔍 檢查	⇧⌘I

瀏覽器 - 開發者模式

- 程式碼編排
- 檔案來源
- 封包傳遞
- Cookie
- ...很多很多資訊



URL資源定位

你可能會看過...

<https://scaict.org:8080/login.php>

也會看過

<https://scaict.org:8080/tw/login.php?name=123#1>

這麼長到底表達什麼？

URL資源定位

https://scaict.org:8080/tw/login.php?name=123#1

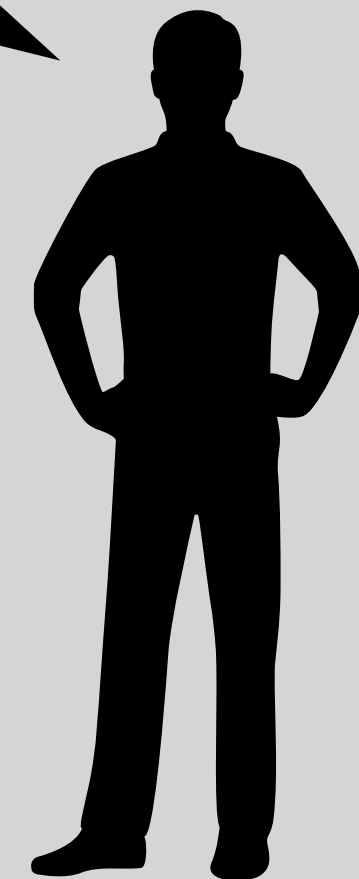
協定類型	網域	端口(:)	檔案路徑	檔案	查詢(?)	定位(#)
https://	scaict.org	:8080	/tw/	login.php	?name=123	#1

URL百分號編碼

想一想 如果對方看不懂中文怎麼辦

<https://scaict.org:8080/登入頁面.php>

我看不懂中文啊！



URL百分號編碼

URL Encode online

登入頁面.php

%E7%99%BB%E5%85%A5%E9%A0%81%E9%9D%A2.php

URL百分號編碼

URL Decode online

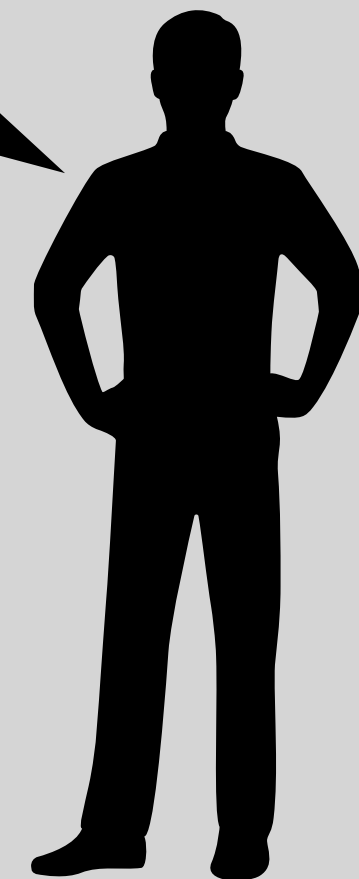
%E7%99%BB%E5%85%A5%E9%A0%81%E9%9D%A2.php|

登入頁面.php

URL百分號編碼

<https://scaict.org:8080/%E7%99%BB%E5%85%A5%E9%A0%81%E9%9D%A2.php>

用全世界都懂的數字解決看
不懂某些國家語言的問題



ASCII對照表

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	\$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[END OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

常見攻擊手法

30 mins



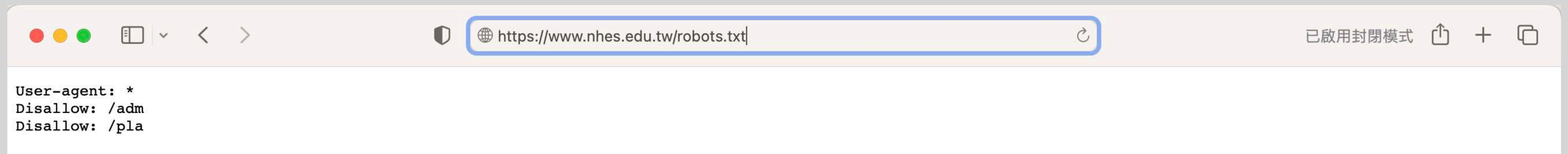
Boom! Leak Password

- 貼心提醒：不要使用過於簡單(短)的帳號和密碼

Demo: 密碼爆破

/robots.txt

- 危險目錄，存在的原因是要告訴搜尋引擎禁止自動化腳本訪問



SQL Injection

- 漏洞原理：利用資料庫語言(SQL)在前端Web上和後端資料庫互動
- 漏洞成因：後端邏輯未對使用者輸入的內容進行驗證, 因此使用者可以輸入惡意程式碼帶入資料庫

台大平台成績全被改87分 原是資工系學生抓漏洞

有機化學

課程資訊
教師資訊
公佈欄
課程內容
學習成績
登出

語言 Language
中文(Chinese)
更新: 2017-03-01
訪客: 4241

學習成績

項目列表

項目	比重	子項目	評分方式	說明	得分	評語	成績公布
第一次期中考	25%	無	百分制		87		公布個人
第二次期中考	25%	無	百分制		87		公布個人
第三次期中考	25%	無	百分制		87		公布個人
期末考	25%	無	百分制				
學期成績	100%		等第制				

有剛畢業的台大校友回報，成績真的全被改成87分。（擷取自 ptt）

看到教授終於願意對莘莘學子
高抬貴手 我感到充實而欣慰

有剛畢業的台大校友回報，成績真的全被改成87分。（擷取自 ptt）

2019/11/08 12:09

〔記者吳柏軒／台北報導〕台灣大學教務處的數位教學平台（CEIBA）6日被人發現，學生全部的平時成績都被改成87分，經查是校內資工系學生進行資訊安全漏洞研究，不小心修改，當晚立即電郵校

Structured Query Language



RDBMS

Structured Query Language

[illegible]

Structured Query Language

Table: items

ID	Fruit	Price
1	Apple	35
2	Banana	35
3	Orange	20
4	Pineapple	35
5	Peach	50
6	Grapes	80

Structured Query Language

```
SELECT * FROM Items WHERE Price = '35'
```

SELECT

*

FROM

Items

WHERE

Price = '35'

查詢

全部東西

從

Items這個
table

條件為

Price = '35'

Structured Query Language

Table: items

ID	Fruit	Price
1	Apple	35
2	Banana	35
3	Orange	20
4	Pineapple	35
5	Peach	50
6	Grapes	80

Structured Query Language

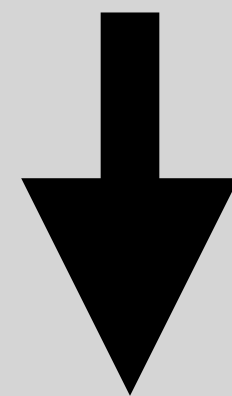
註解		
資料庫	符號	範例
Microsoft	-- /**/	admin--1234
Mysql	# -- /**/	admin--1234 admin#1234 admin/*1234*/
Oracle	--	admin--1234
PostgreSql	-- /**/	admin--1234 admin/*1234*/

Structured Query Language

運算子	意義
ALL	如果一組比較全為 TRUE，便是 TRUE。
AND	如果兩個布林運算式都是 TRUE 時，便是 TRUE。
ANY	如果一組比較中的任何一項是 TRUE，便是 TRUE。
BETWEEN	如果運算元在範圍內，便是 TRUE。
EXISTS	如果子查詢包含任何資料列，便是 TRUE。
IN	如果運算元等於運算式清單中的某個運算式，便是 TRUE。
LIKE	如果運算元符合某個模式，便是 TRUE。
NOT	反轉任何其他布林運算子的值。
OR	如果任一個布林運算式是 TRUE，便是 TRUE。
SOME	如果一組比較部分為 TRUE，便是 TRUE。

SQL Injection

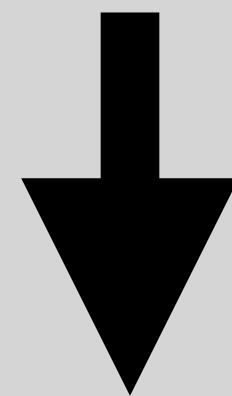
```
SELECT * FROM users WHERE ACCOUNT = '{username}' AND PASSWORD = '{password}'
```



```
SELECT * FROM users WHERE ACCOUNT = '{username}'--' AND PASSWORD = '{password}'
```

SQL Injection

```
SELECT * FROM users WHERE ACCOUNT = '{username}' AND PASSWORD = '{password}'
```



```
SELECT * FROM users WHERE ACCOUNT = '{username}' OR 1=1--' AND PASSWORD = '{password}'
```


Union SQL Injection

```
SELECT * FROM fruit WHERE Price= '{Price}'
```

這個查詢只能查水果...？

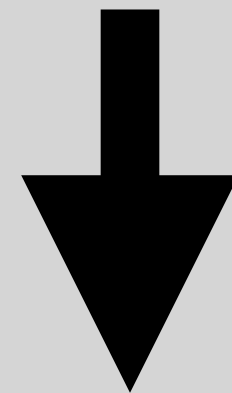
Union Structured Query Language

```
SELECT {???} FROM {TABLE}  
UNION  
SELECT {???} FROM {TABLE}
```

- 查詢欄位數量要相同
- 查詢對應的資料型態要相同
- 需有前後方的table

Union SQL Injection

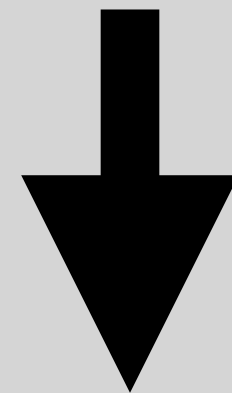
```
SELECT * FROM fruit WHERE Price= '{Price}'
```



```
SELECT * FROM fruit WHERE Price= " UNION SELECT * FROM users--'
```


Union SQL Injection

```
SELECT id, fruit, price FROM fruit WHERE Price= '{Price}'
```



```
SELECT id, fruit, price FROM fruit WHERE Price= " UNION SELECT {NULL}, {NULL}, {NULL} FROM users--'
```

Server Side Template Injection

- 漏洞原理：利用網站樣版引擎解析惡意參數
- 漏洞成因：後端邏輯未對使用者輸入的內容進行驗證, 讓樣版引擎解析惡意輸入的參數

程式語言	樣版引擎
Python	Jinja
PHP	Smarty、Twig
Ruby	Liquid
Java	Free marker、Velocity

Server Side Template Injection

PHP

```
$output = $twig->render("你好". $GET[name]);
```

```
name = ${2 * 2}
```

```
$output = $twig->render("你好". 4);
```

Server Side Template Injection - 預防

- 不將使用者的輸入作為被模板解析的字串
- 驗證使用者輸入

Cross Site Script(XSS)

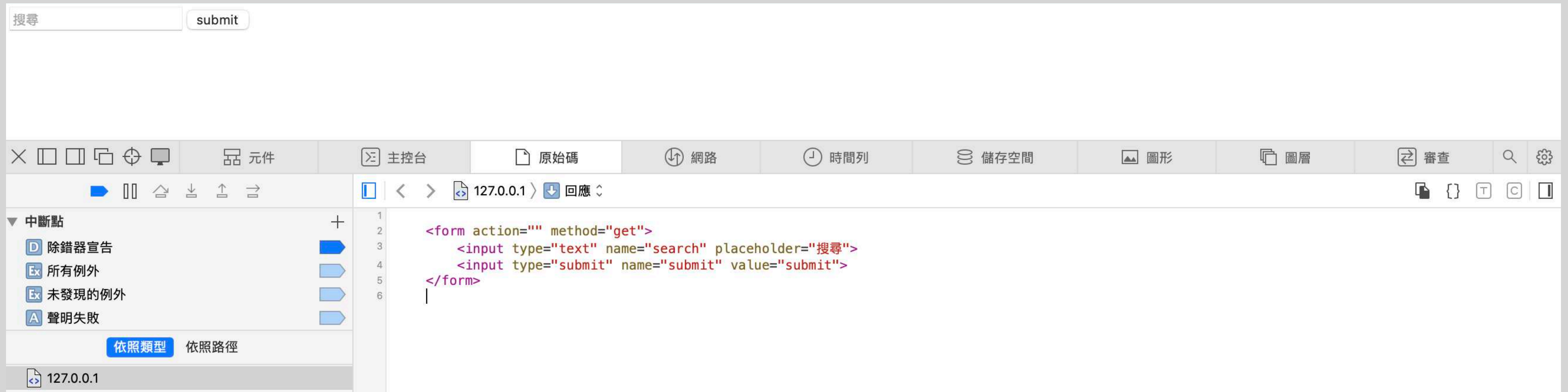
- 漏洞原理：前端將使用者輸入的惡意資訊解析
- 漏洞成因：後端邏輯未對使用者輸入的內容進行驗證, 使前端解析惡意程式碼
- 小知識：之所以縮寫不叫CSS是因為CSS已代表前端Web的語言(Cascading Style Sheets)

	Cross Site Script(XSS)		
Type	Reflect XSS	Store XSS	DOM XSS
危害程度	★	★★	★★★

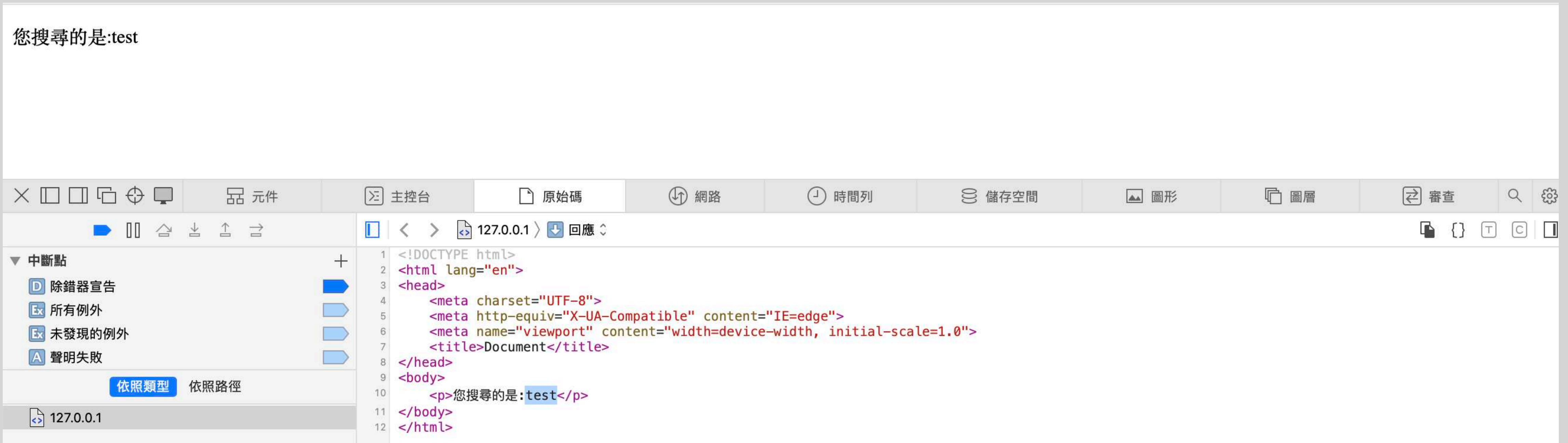
Reflect XSS

- 漏洞原理：前端將使用者輸入的惡意資訊解析
- 攻擊時效：非持續
- 原理解說：攻擊者透過前端輸入惡意程式碼(通常是JavaScript、HTML)使後端邏輯將惡意程式碼解析
- 組合技：搭配Social Engineering釣出cookie

Reflect XSS



Reflect XSS



如果輸入HTML tag會怎樣...

Reflect XSS

您搜尋的是:

這個網站存在xss

您搜尋的是:

這個網站存在xss

127.0.0.1

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta http-equiv="X-UA-Compatible" content="IE=edge">
6   <meta name="viewport" content="width=device-width, initial-scale=1.0">
7   <title>Document</title>
8 </head>
9 <body>
10  <p>您搜尋的是 <h1 style="color:red">這個網站存在xss</h1></p>
11 </body>
12 </html>
```

Reflect XSS



這個網站存在 xss

關閉

Reflect XSS

您搜尋的是:<script>alert("這個網站存在xss")</script>

✕

□

□

□

⊕

🖥

🧩 元件

🖱 主控台

📄 原始碼

🌐 網路

🕒 時間列

💾 儲存空間

🖼 圖形

📁 圖層

🔍 審查

🔍

⚙

▶

||

🏠

⬇

⬆

↔

📄

<

>

📄 127.0.0.1

>

⬇

回應

⌵

📄 {} T C I

▼ 中斷點

+

D 除錯器宣告

Ex 所有例外

Ex 未發現的例外

A 聲明失敗

依照類型

依照路徑

📄 127.0.0.1

1 <!DOCTYPE html>

2 <html lang="en">

3 <head>

4 <meta charset="UTF-8">

5 <meta http-equiv="X-UA-Compatible" content="IE=edge">

6 <meta name="viewport" content="width=device-width, initial-scale=1.0">

7 <title>Document</title>

8 </head>

9 <body>

10 <p>您搜尋的是:<script>alert("這個網站存在xss")</script></p>

11 </body>

12 </html>

Store XSS

- 漏洞原理：將惡意資訊寫入Database
- 攻擊時效：持續性
- 原理解說：在有連線資料庫的輸入框寫入惡意程式使每次將資料釣出時觸發攻擊
- 常見地方：留言板、和資料庫有串接的地方

Store XSS



Store XSS

第一則訊息:('這個網站有xss漏洞嗎',)

✕

📏

📐

📄

🔍

🖥

🧩 元件

🔧 主控台

📄 原始碼

🌐 網路

🕒 時間列

💾 儲存空間

🖼 圖形

📁 圖層

🔍 審查

🔍

⚙

▶

⏏

🏠

⬇

⬆

➡

▼ 中斷點

D

除錯器宣告

Ex

所有例外

Ex

未發現的例外

A

聲明失敗

依照類型

依照路徑

📄

127.0.0.1

📄

<

>

📄

127.0.0.1

>

⬇

回應

📄

}

T

C

📄

1

<!DOCTYPE html>

2

<html lang="en">

3

<head>

4

<meta charset="UTF-8">

5

<meta http-equiv="X-UA-Compatible" content="IE=edge">

6

<meta name="viewport" content="width=device-width, initial-scale=1.0">

7

<title>Document</title>

8

</head>

9

<body>

10

<p>第一則訊息:('這個網站有xss漏洞嗎',)</p>

11

</body>

12

</html>

Store XSS



Store XSS

第一則訊息:('這個網站有xss漏洞嗎')

第二則訊息:(")



這個網站有 xss 嗎

關閉

Cross Site Script - 預防

- 過濾html tag
- 驗證使用者輸入
- 將敏感符號改成其他東西代替

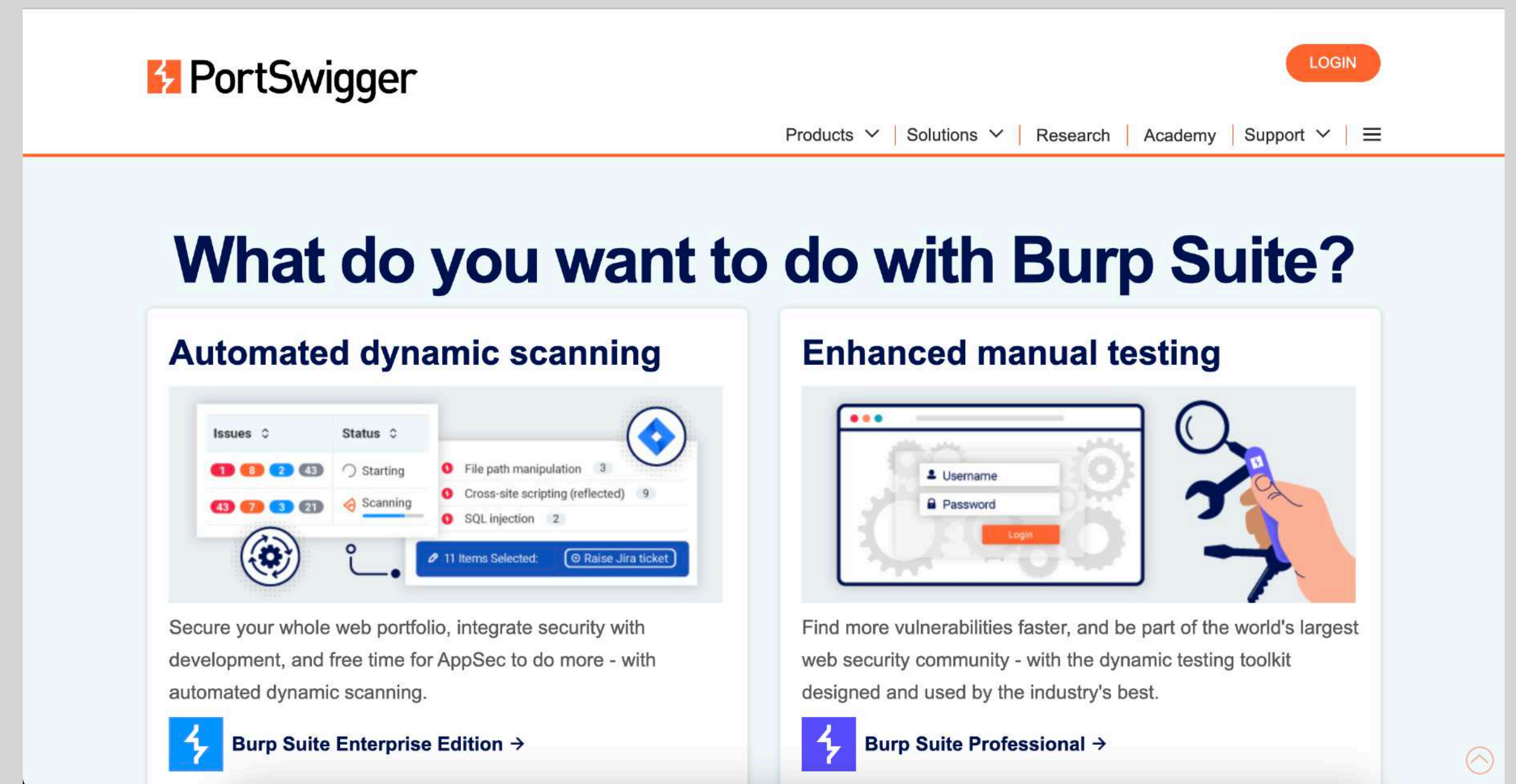
資安常見Tools / Packet

10 mins



Software - Burp Suite

- 開發商：Portswigger
- 常見使用情境：滲透測試、找漏洞
- 功能：攔截封包、爆破、資訊收集、繞過驗證..等



The screenshot displays the PortSwigger website's landing page for Burp Suite. The header features the PortSwigger logo, a 'LOGIN' button, and a navigation menu with links to Products, Solutions, Research, Academy, and Support. The main heading asks 'What do you want to do with Burp Suite?'. Below this, two primary use cases are highlighted: 'Automated dynamic scanning' and 'Enhanced manual testing'. The 'Automated dynamic scanning' section includes a screenshot of the Burp Suite interface showing a list of issues (File path manipulation, Cross-site scripting, SQL injection) and a 'Raise Jira ticket' button. The 'Enhanced manual testing' section features a screenshot of a login form and a hand using a magnifying glass. Both sections conclude with a call to action to purchase Burp Suite Enterprise Edition or Burp Suite Professional.

PortSwigger

Products Solutions Research Academy Support

What do you want to do with Burp Suite?

Automated dynamic scanning

Secure your whole web portfolio, integrate security with development, and free time for AppSec to do more - with automated dynamic scanning.

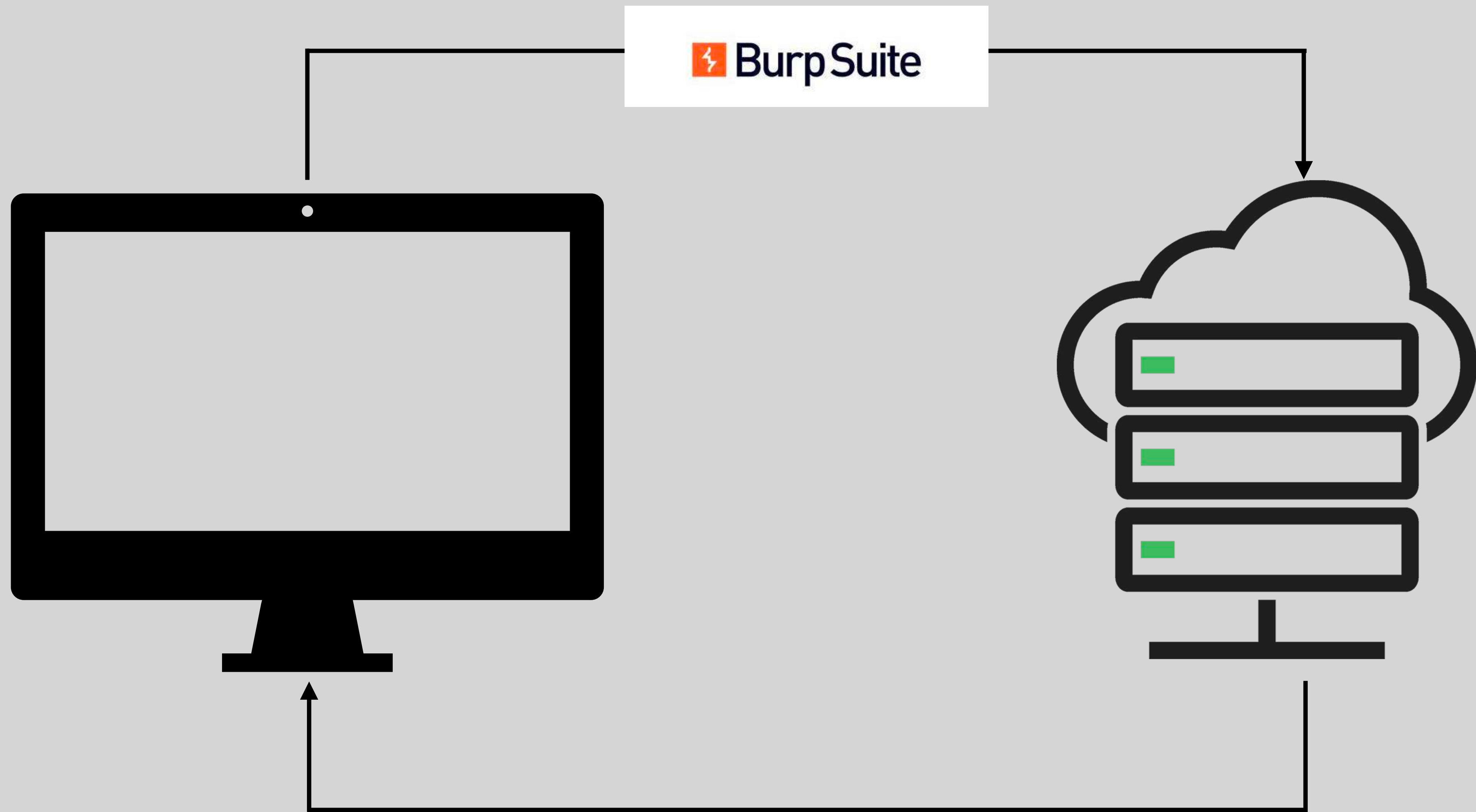
Burp Suite Enterprise Edition →

Enhanced manual testing

Find more vulnerabilities faster, and be part of the world's largest web security community - with the dynamic testing toolkit designed and used by the industry's best.

Burp Suite Professional →

運作原理



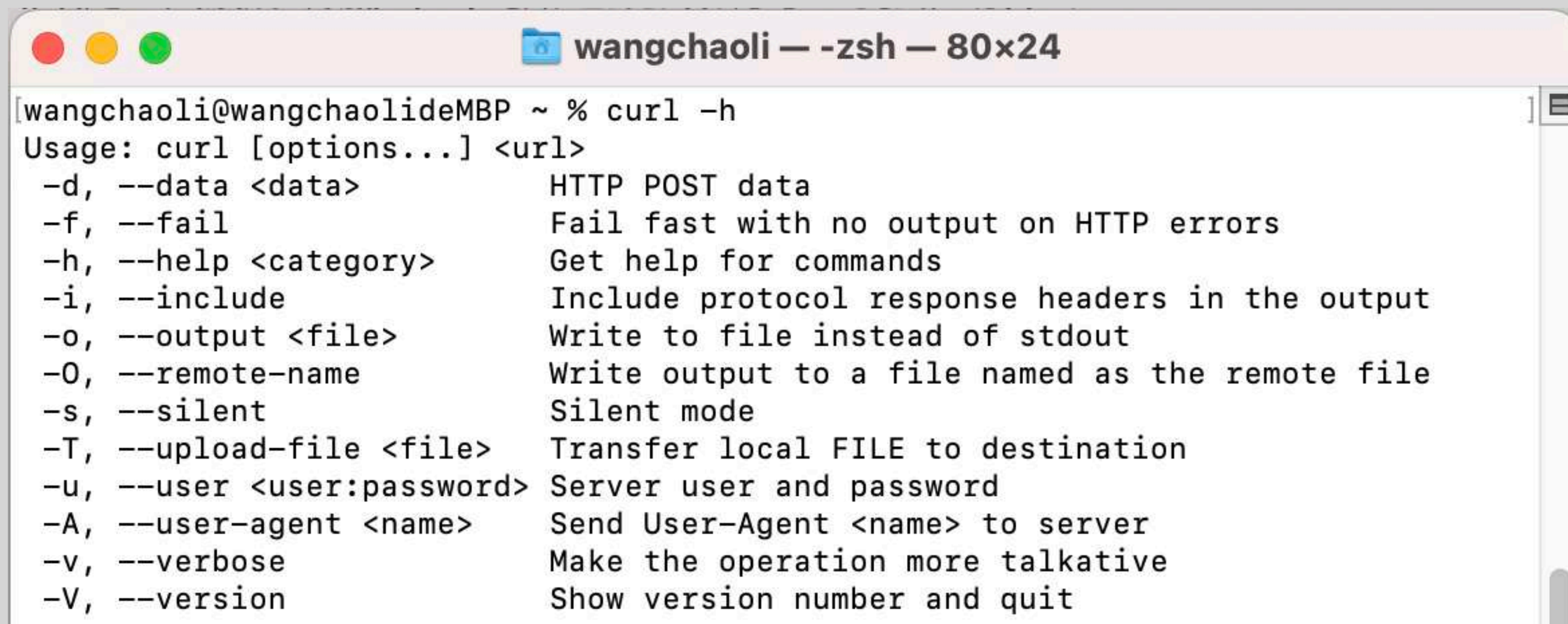
Command - dirb

- 介紹：自動化路徑掃描工具

```
charlie@DESKTOP-AO1MV95: ~  
charlie@DESKTOP-AO1MV95:~$ dirb https://ncves.net  
  
-----  
DIRB v2.22  
By The Dark Raver  
-----  
  
START_TIME: Sun Jun 18 00:25:02 2023  
URL_BASE: https://ncves.net/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
-----  
  
GENERATED WORDS: 4612  
  
---- Scanning URL: https://ncves.net/ ----  
=> DIRECTORY: https://ncves.net/assets/  
=> DIRECTORY: https://ncves.net/css/  
=> DIRECTORY: https://ncves.net/fonts/  
=> DIRECTORY: https://ncves.net/images/  
+ https://ncves.net/index (CODE:200|SIZE:21071)  
+ https://ncves.net/index.html (CODE:200|SIZE:21071)  
=> DIRECTORY: https://ncves.net/js/  
=> DIRECTORY: https://ncves.net/mail/  
+ https://ncves.net/rule (CODE:200|SIZE:0)  
=> DIRECTORY: https://ncves.net/uploads/
```


Command - curl

- 介紹：一個從終端機或腳本中發起網路請求的強大指令

A screenshot of a macOS terminal window titled "wangchaoli — -zsh — 80x24". The terminal shows the command "curl -h" being executed, which displays the usage and options for the curl command. The output lists various flags and their descriptions, such as "-d, --data" for HTTP POST data and "-v, --verbose" for making the operation more talkative.

```
wangchaoli@wangchaolideMBP ~ % curl -h
Usage: curl [options...] <url>
  -d, --data <data>           HTTP POST data
  -f, --fail                   Fail fast with no output on HTTP errors
  -h, --help <category>       Get help for commands
  -i, --include                 Include protocol response headers in the output
  -o, --output <file>          Write to file instead of stdout
  -O, --remote-name             Write output to a file named as the remote file
  -s, --silent                  Silent mode
  -T, --upload-file <file>     Transfer local FILE to destination
  -u, --user <user:password>   Server user and password
  -A, --user-agent <name>      Send User-Agent <name> to server
  -v, --verbose                 Make the operation more talkative
  -V, --version                 Show version number and quit
```

Command - curl

% curl [url]

```
wangchaoli — -zsh — 80x24
[wangchaoli@wangchaolideMBP ~ % curl https://scaict.org]
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
</head>
<body>
  <div class="box">
    <h1>🚧 網站施工中 </h1>
    <p>全新網站即將與您相見</p>
    <button class="btn">
      <span>其他社群連結</span>
      <div class="container">
        <svg class="icon" height="35" width="35" fill="#000000" viewBox=
"0 0 48 48" version="1.1" xmlns="http://www.w3.org/2000/svg" fill="#000000">
          <g id="SVGRepo_bgCarrier" stroke-width="0"></g><g id="SVGRepo_tracerCarrier" stroke-linecap="round" stroke-linejoin="round"></g><g id="SVGRepo_iconCarrier"> <title>Facebook-color</title> <desc>Created with Sketch.</desc>
          <defs> </defs> <g id="Icons" stroke="none" stroke-width="1" fill="none" fill-rule="evenodd"> <g id="Color-" transform="translate(-200.000000, -160.000000)" fil
```


Command - nmap

- 介紹：功能強大的開源網路掃描工具
- 常見使用情境：滲透測試、資訊搜集、入侵網站
- 常掃描：主機探測、端口、操作系統、漏洞掃描...等

```
(user@kali)-[~]  
$ nmap scaict.org  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-17 23:51 CST  
Nmap scan report for scaict.org (211.23.95.246)  
Host is up (0.035s latency).  
rDNS record for 211.23.95.246: ns8.dnsonic.com  
Not shown: 989 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
110/tcp   open  pop3  
143/tcp   open  imap  
443/tcp   open  https  
465/tcp   open  smtps  
587/tcp   open  submission  
993/tcp   open  imaps  
995/tcp   open  pop3s  
  
Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
```


Command - binwalk

- 功能：分析檔案、找出隱藏檔案

```
(user@kali)-[~]
$ binwalk -h

Binwalk v2.3.3
Craig Heffner, ReFirmLabs
https://github.com/ReFirmLabs/binwalk

Usage: binwalk [OPTIONS] [FILE1] [FILE2] [FILE3] ...

Signature Scan Options:
  -B, --signature          Scan target file(s) for common file signatures
  -R, --raw=<str>          Scan target file(s) for the specified sequence of bytes
  -A, --opcodes            Scan target file(s) for common executable opcode signatures
  -m, --magic=<file>       Specify a custom magic file to use
  -b, --dumb               Disable smart signature keywords
  -I, --invalid            Show results marked as invalid
  -x, --exclude=<str>     Exclude results that match <str>
  -y, --include=<str>     Only show results that match <str>

Extraction Options:
  -e, --extract            Automatically extract known file types
  -D, --dd=<type[:ext[:cmd]]> Extract <type> signatures (regular expression), give the files an extension of <ext>, and execute <cmd>
  -M, --matryoshka        Recursively scan extracted files
  -d, --depth=<int>       Limit matryoshka recursion depth (default: 8 levels deep)
  -C, --directory=<str>   Extract files/folders to a custom directory (default: current working directory)
  -j, --size=<int>         Limit the size of each extracted file
  -n, --count=<int>        Limit the number of extracted files
  -0, --run-as=<str>       Execute external extraction utilities with the specified user's privileges
  -1, --preserve-symlinks Do not sanitize extracted symlinks that point outside the extraction directory (dangerous)
  -r, --rm                Delete carved files after extraction
  -Z, --carve              Carve data from files, but don't execute external utilities
  -V, --subdirs            Extract into sub-directories named by the offset

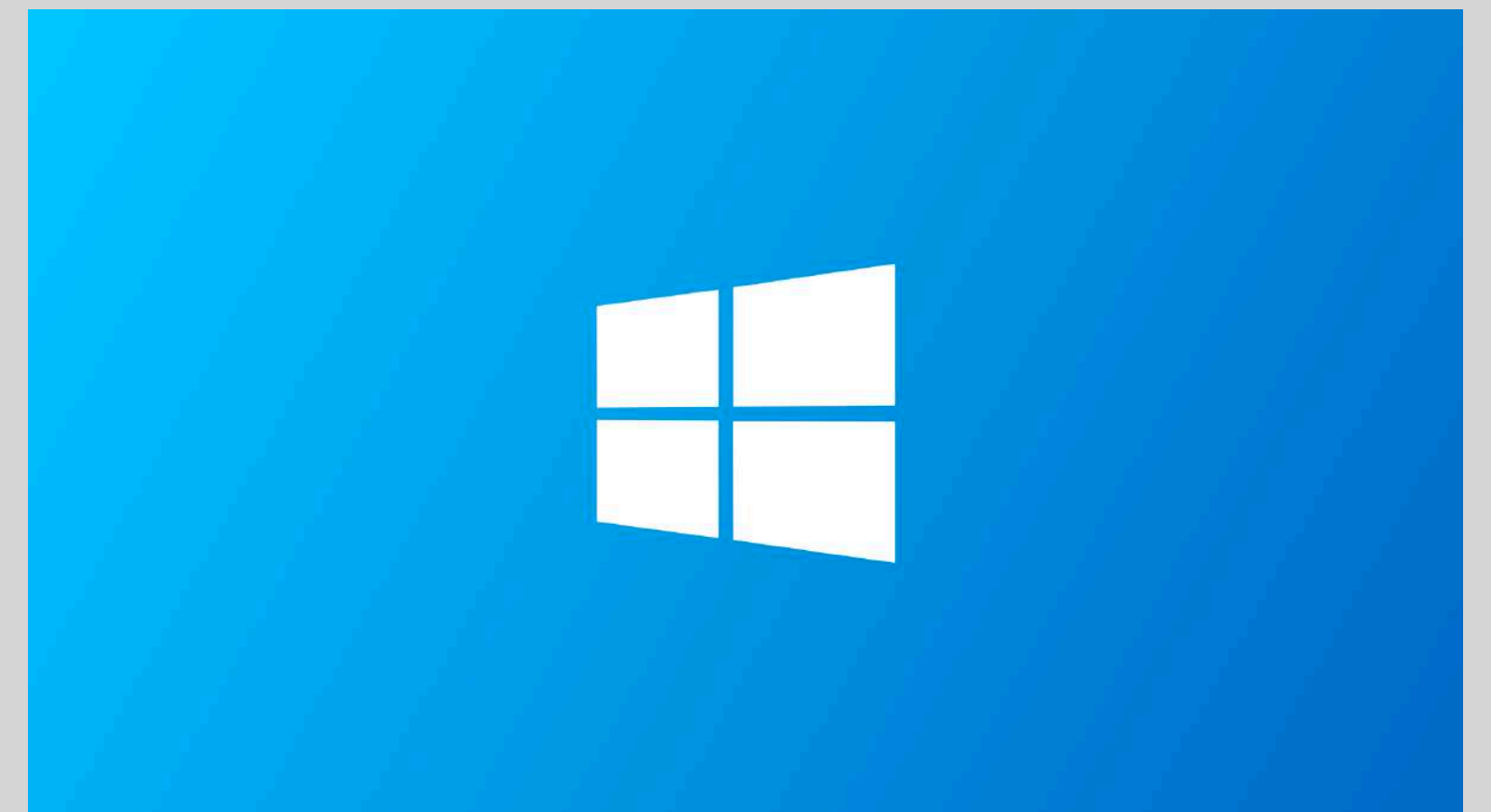
Entropy Options:
  -E, --entropy            Calculate file entropy
  -F, --fast               Use faster, but less detailed, entropy analysis
  -J, --save               Save plot as a PNG
  -Q, --nlegend            Omit the legend from the entropy plot graph
  -N, --nplot              Do not generate an entropy plot graph
  -H, --high=<float>       Set the rising edge entropy trigger threshold (default: 0.95)
  -L, --low=<float>        Set the falling edge entropy trigger threshold
```

Linux基礎指令

40 mins



認識一下！三大作業系統



作業系統的延伸

OS	說明
Linux	UNIX改版 開源 OS
Android	Google改版Linux給智慧型手機使用之OS
MacOS	Apple改版UNIX之OS
iOS	Apple改版MacOS給智慧型手機專用之OS

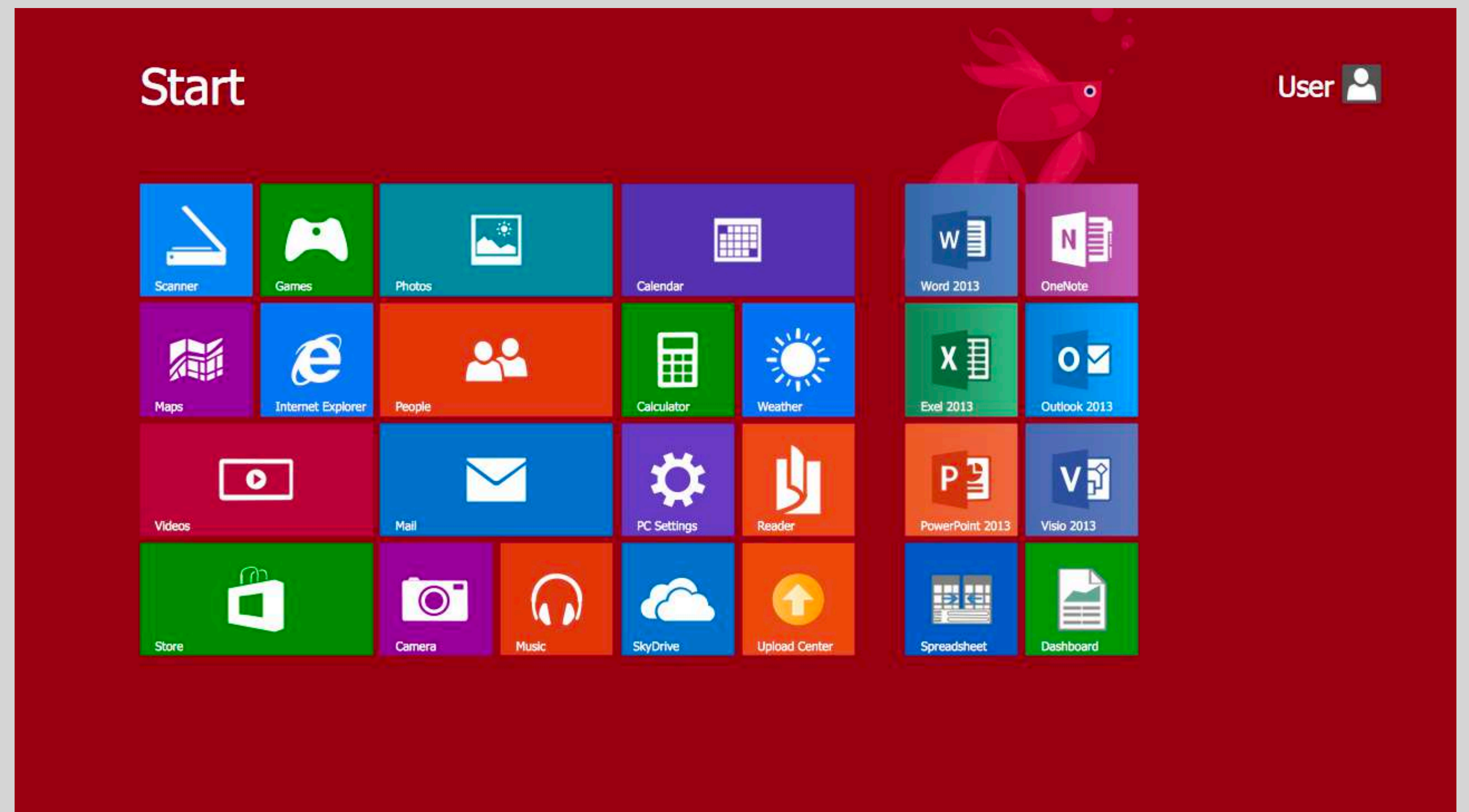
所以...Linux到底是什麼？他的特點？

Linux就是一個作業系統(OS), 它具有以下特點：

- 支援大量網路存取
- 速度快
- 非常穩定可靠
- 沒有授權問題(例：最高同時X台連線問題)
- 性價比極高(例：一台設備及可架設許多服務)
- 易維護
- 完全免費

Graphical User Interface, GUI

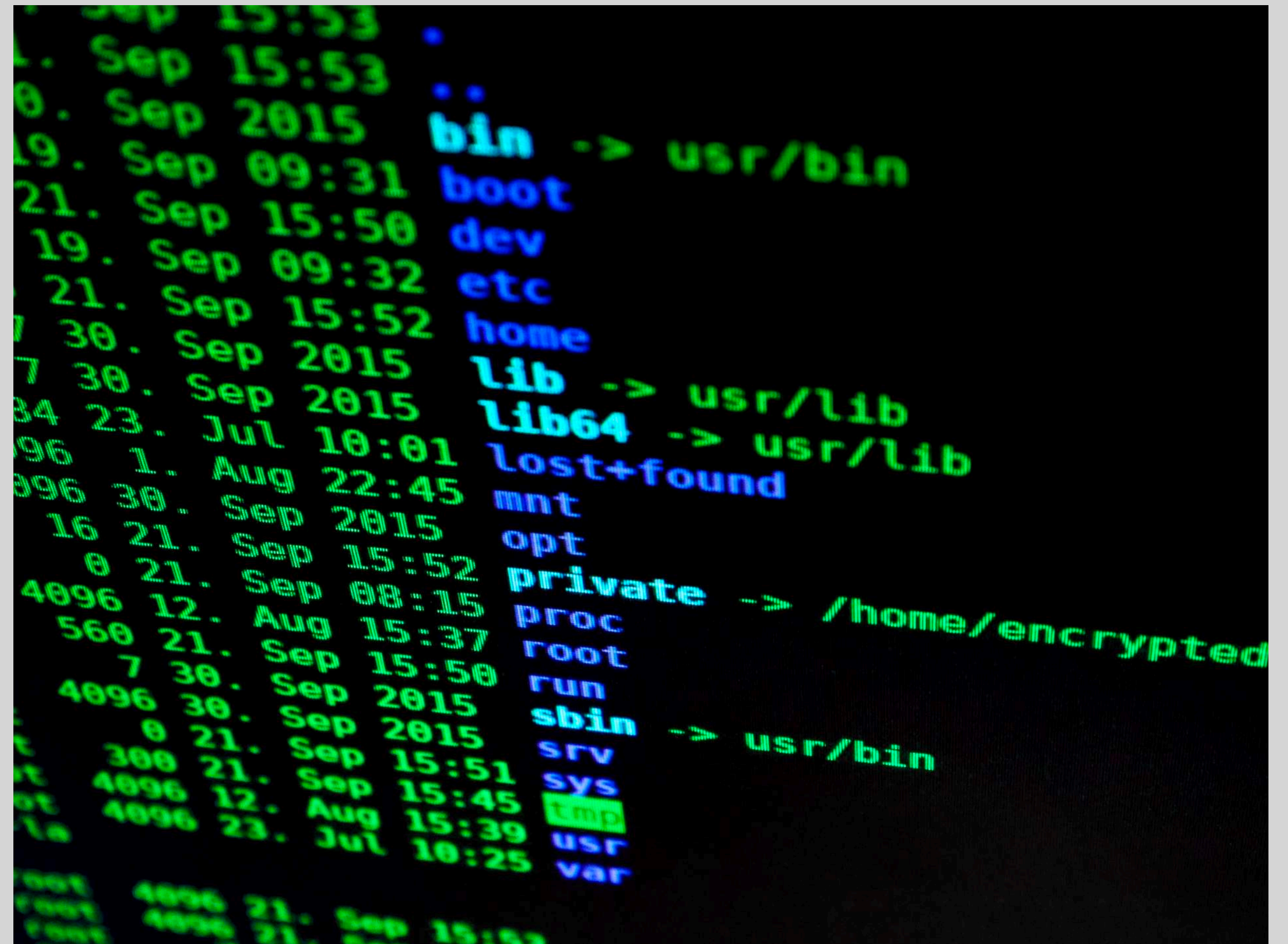
- 使用者介面中的豪華版
- 有圖、文字搭配
- 可搭配滑鼠使用



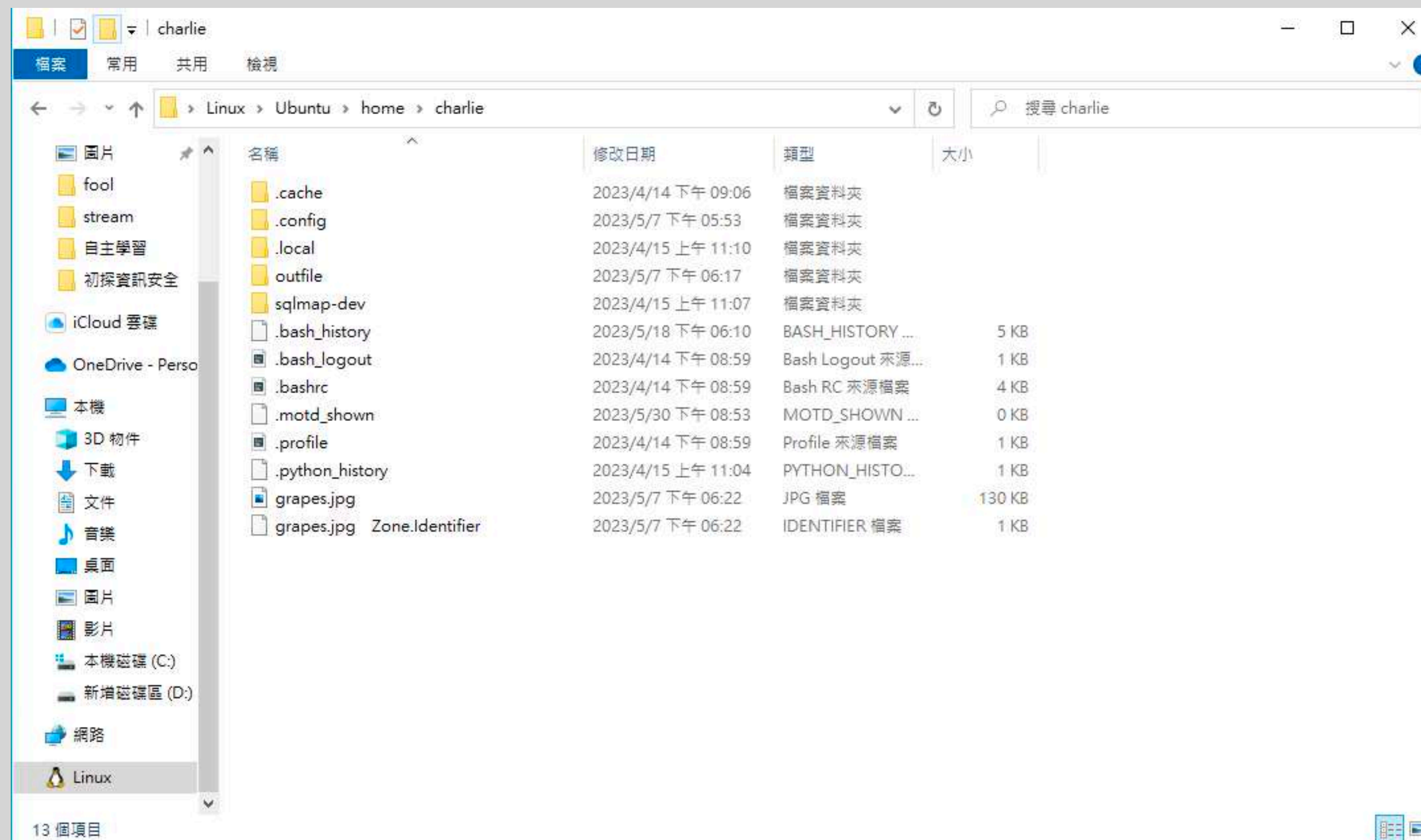
Character User Interface, CUI

Command-Line Interface, CLI

- 使用者介面中的陽春版
- 僅有文字介面
- 不可搭配滑鼠使用



Which do you prefer?

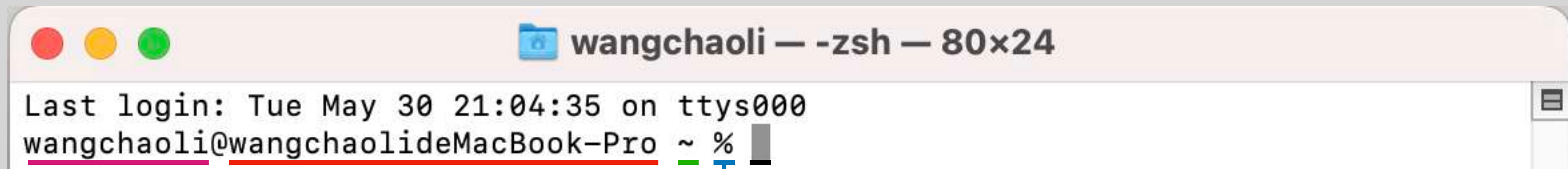


▲ Windows GUI

```
charlie@DESKTOP-A01MV95:~$ ls -al
total 188
drwxr-x--- 7 charlie charlie 4096 May  7 18:22 .
drwxr-xr-x 3 root    root    4096 Apr 14 20:59 ..
-rw----- 1 charlie charlie 4117 May 18 18:10 .bash_history
-rw-r--r-- 1 charlie charlie  220 Apr 14 20:59 .bash_logout
-rw-r--r-- 1 charlie charlie 3771 Apr 14 20:59 .bashrc
drwxr-xr-x 3 charlie charlie 4096 Apr 14 21:06 .cache
drwxr-xr-x 3 charlie charlie 4096 May  7 17:53 .config
drwxr-xr-x 3 charlie charlie 4096 Apr 15 11:10 .local
-rw-r--r-- 1 charlie charlie   0 May 30 20:53 .motd_shown
-rw-r--r-- 1 charlie charlie  807 Apr 14 20:59 .profile
-rw----- 1 charlie charlie   32 Apr 15 11:04 .python_history
-rw-r--r-- 1 charlie charlie 132211 May  7 18:22 grapes.jpg
-rw-r--r-- 1 charlie charlie  249 May  7 18:22 grapes.jpg:Zone.Identifier
drwxr-xr-- 2 charlie charlie 4096 May  7 18:17 outfile
drwxr-xr-x 11 charlie charlie 4096 Apr 15 11:07 sqlmap-dev
```

▲ Ubuntu CUI / CLI

指令介面小小的知識

A screenshot of a macOS terminal window titled "wangchaoli — -zsh — 80x24". The window shows the login message "Last login: Tue May 30 21:04:35 on ttys000" and the prompt "wangchaoli@wangchaolideMacBook-Pro ~ %". The prompt is annotated with colored lines and labels: a pink line under "wangchaoli" points to the label "使用者名稱"; a red line under "@wangchaolideMacBook-Pro" points to the label "使用者裝置"; a green line under "~" points to the label "目錄"; and a blue line under "%" points to the label "游標位置(一直閃爍)".

```
wangchaoli — -zsh — 80x24
Last login: Tue May 30 21:04:35 on ttys000
wangchaoli@wangchaolideMacBook-Pro ~ %
```

使用者名稱

使用者裝置

目錄

游標位置(一直閃爍)

命令提示字元(每個使用者寫法不一樣)

知道指令卻不會用嗎？

```
% man [command]
```

```
% [command] --help
```

➡顯示指令使用手冊(man較複雜, --help較簡易)

基礎指令 - date

% date



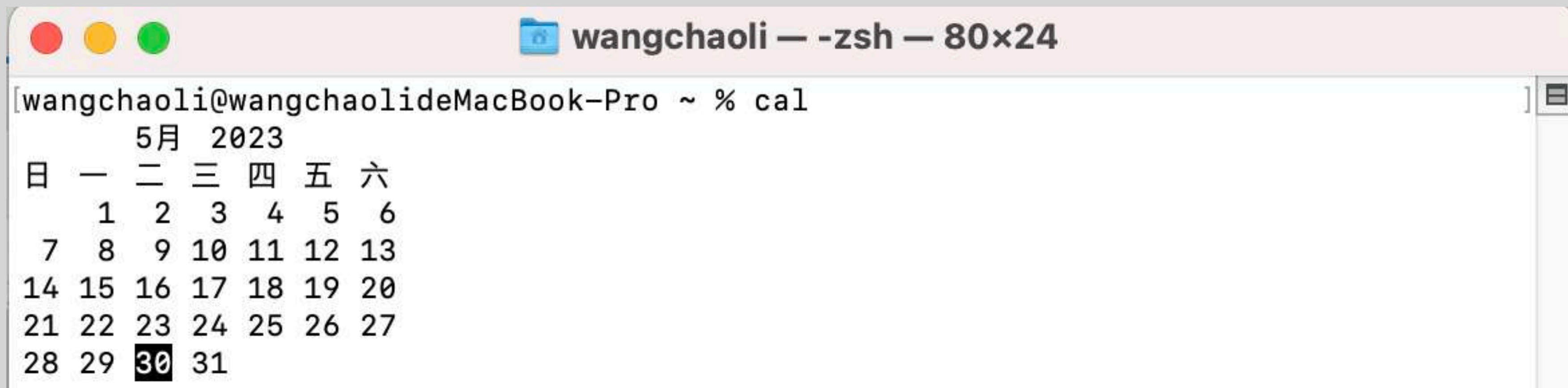
A screenshot of a macOS terminal window. The title bar shows the window name 'wangchaoli — -zsh — 80x24'. The terminal content shows the command '[wangchaoli@wangchaolideMacBook-Pro ~ % date' followed by its output '2023年 5月30日 週二 21時49分15秒 CST'. The window has standard macOS window controls (red, yellow, green buttons) on the top left.

```
wangchaoli@wangchaolideMacBook-Pro ~ % date
2023年 5月30日 週二 21時49分15秒 CST
```

➡ 顯示當天日期

基礎指令 - cal

% cal



```
wangchaoli — -zsh — 80x24
[wangchaoli@wangchaolideMacBook-Pro ~ % cal
      5月 2023
日 一 二 三 四 五 六
   1  2  3  4  5  6
  7  8  9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30 31
```

➡ 顯示當月日歷

常用參數介紹 - cal

% cal 2023

➡顯示2023整年日歷

% cal 5 2023

➡顯示2023 5月日歷

複習一下

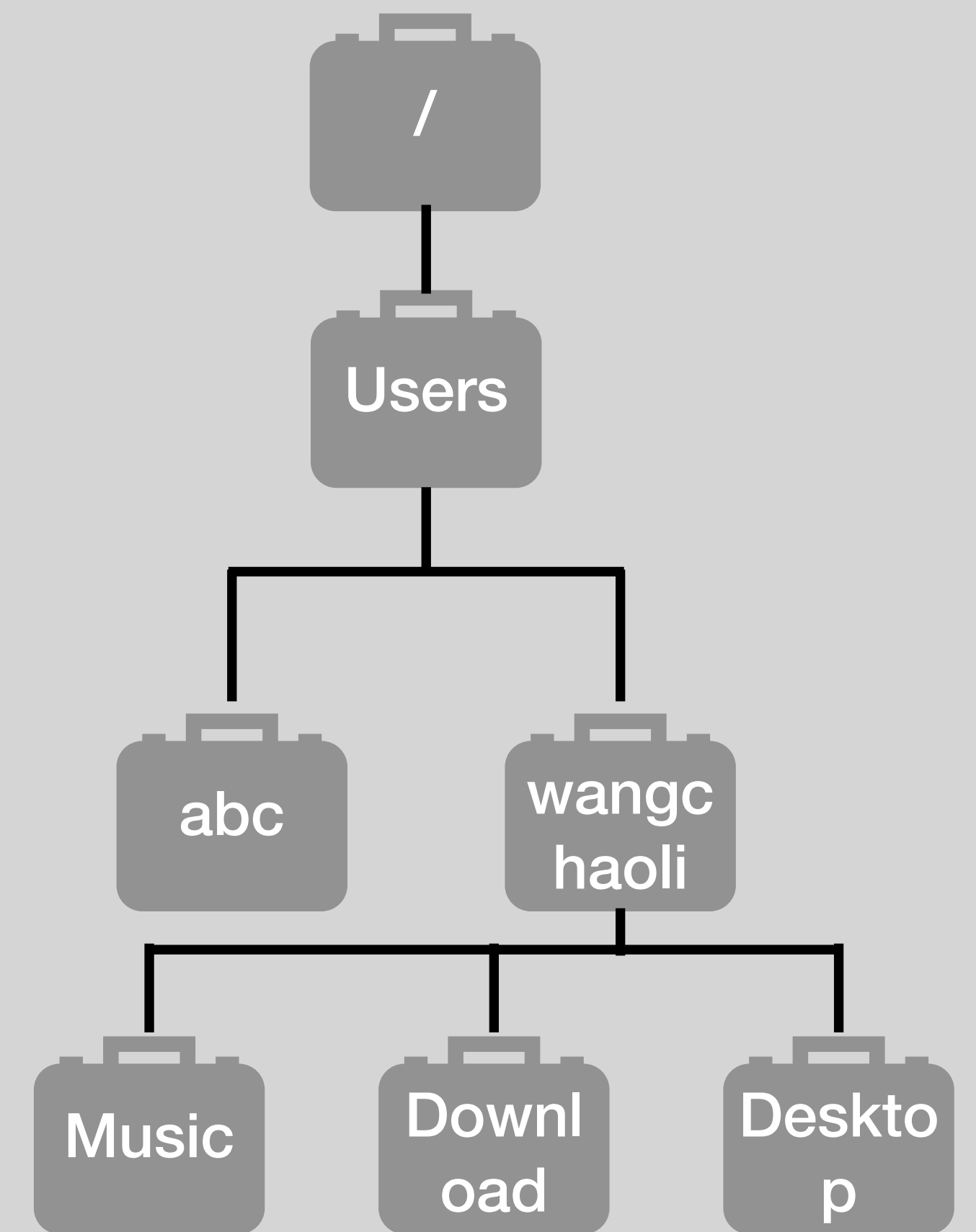
% cal --help
% man cal

基礎指令 - pwd

% pwd

```
wangchaoli — -zsh — 80x24  
[wangchaoli@wangchaolideMacBook-Pro ~ % pwd  
/Users/wangchaoli
```

➔ 顯示當前路徑



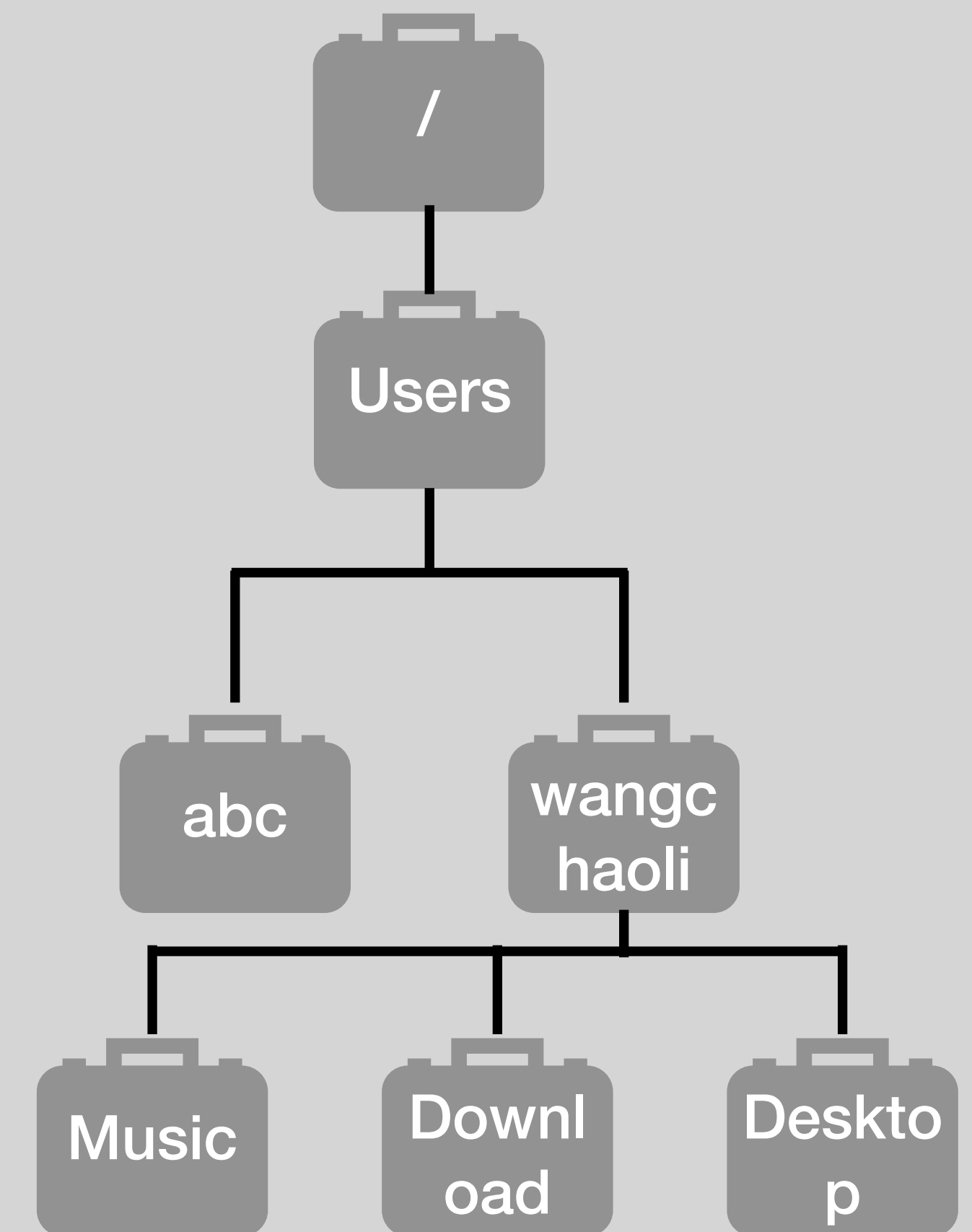
基礎指令 - cd

% pwd

```
wangchaoli — -zsh — 80x24  
[wangchaoli@wangchaolideMacBook-Pro ~ % pwd  
/Users/wangchaoli
```

% cd Desktop/

```
桌面 — -zsh — 80x24  
[wangchaoli@wangchaolideMacBook-Pro ~ % cd Desktop  
wangchaoli@wangchaolideMacBook-Pro Desktop %
```



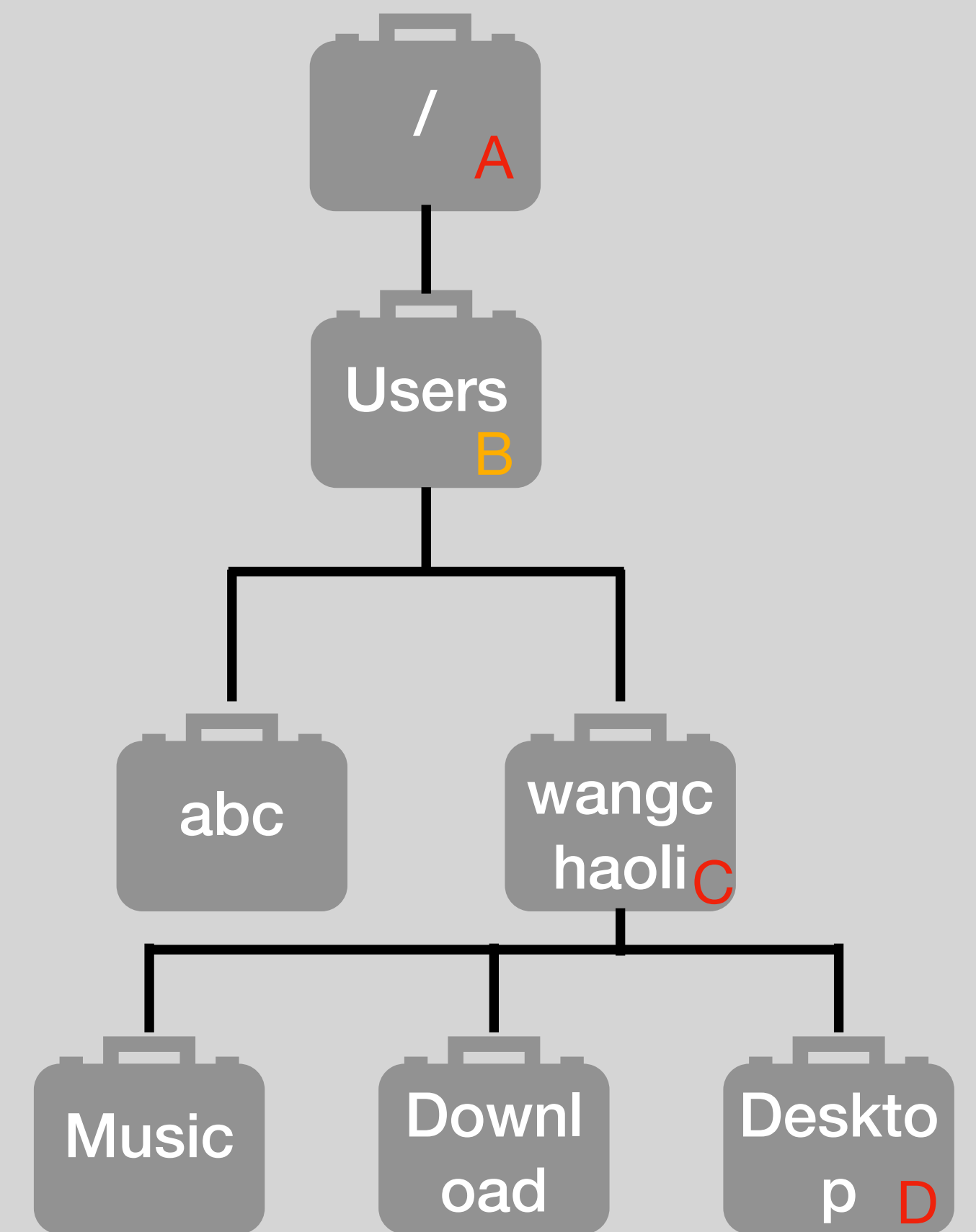
路徑快速表示法

% cd ~

➡ B → C (回到使用者目錄)

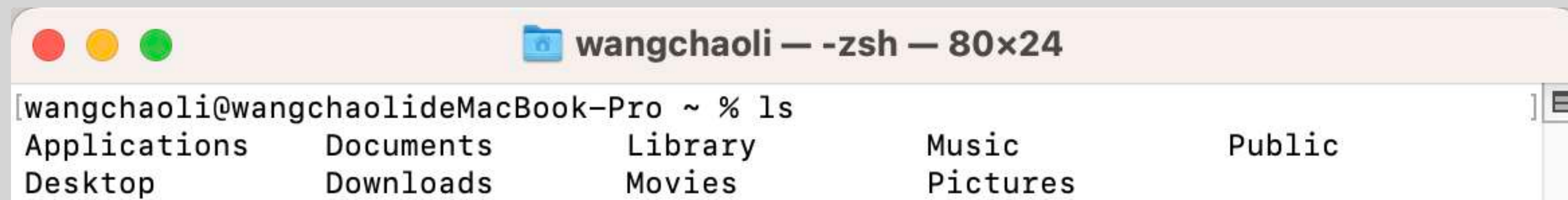
% cd ..

➡ B → A (上個目錄)



基礎指令 - ls

% ls



A screenshot of a macOS terminal window titled "wangchaoli — -zsh — 80x24". The terminal shows the command `% ls` being executed, resulting in a listing of the user's home directory. The output is as follows:

Applications	Documents	Library	Music	Public
Desktop	Downloads	Movies	Pictures	

➔ 顯示當前目錄的檔案

常用參數介紹 - ls

% ls -a

➡ 顯示隱藏檔案

% ls -l

➡ 顯示檔案詳細資訊

% ls -al

基礎指令 - cat

% cat [filename]

A screenshot of a macOS terminal window titled "桌面 — -zsh — 80x24". The terminal shows a user named wangchaoli at a MacBook-Pro Desktop. The user runs the command 'ls', which lists 'flag.txt'. Then, the user runs 'cat flag.txt', and the terminal displays the output 'You can get cat command%'.

```
wangchaoli@wangchaolideMacBook-Pro Desktop % ls  
flag.txt  
wangchaoli@wangchaolideMacBook-Pro Desktop % cat flag.txt  
You can get cat command%
```

➡ 讀取指定檔案的內容(文字檔)

基礎指令 - less

```
% less [filename]
```

- ➡ 讀取指定檔案的內容(文字檔)
- ➡ 與cat的功能幾乎一樣, 差別在less可以使用鍵盤進行互動, 常使用在長文章

基礎指令 - mkdir

% mkdir [dir]

➡ 創建資料夾

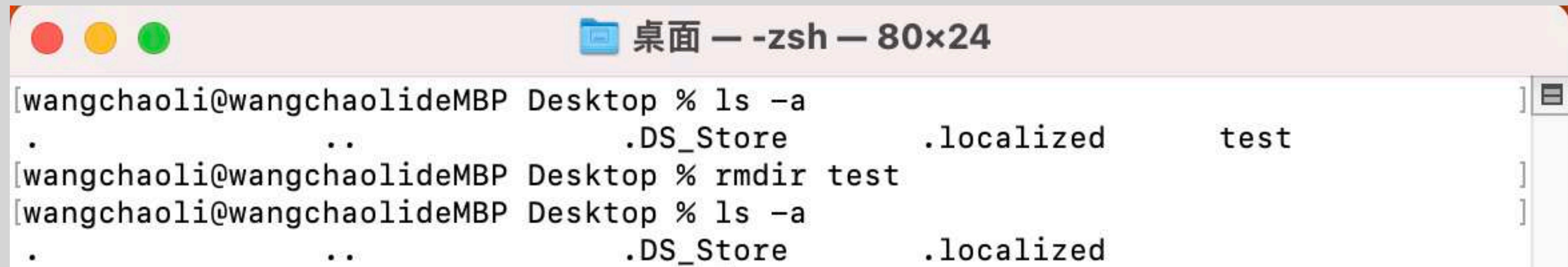
A screenshot of a macOS terminal window titled "桌面 — -zsh — 80x24". The window shows three lines of terminal output. The first line shows the result of 'ls -a' on the Desktop, listing hidden files like .DS_Store and .localized. The second line shows the command 'mkdir test' being executed. The third line shows the result of 'ls -a' after the command, now including 'test' in the list of files.

```
[wangchaoli@wangchaolideMBP Desktop % ls -a  
.  
..  
.DS_Store  
.localized  
[wangchaoli@wangchaolideMBP Desktop % mkdir test  
[wangchaoli@wangchaolideMBP Desktop % ls -a  
.  
..  
.DS_Store  
.localized  
test
```

基礎指令 - rmdir

% rmdir [dir]

➡ 刪除資料夾



```
桌面 — -zsh — 80x24
[wangchaoli@wangchaolideMBP Desktop % ls -a
.          ..          .DS_Store      .localized      test
[wangchaoli@wangchaolideMBP Desktop % rmdir test
[wangchaoli@wangchaolideMBP Desktop % ls -a
.          ..          .DS_Store      .localized
```


基礎指令 - nano

% nano [filename]

➔ 開啟文字編輯器



基礎指令 - file

% file [filename]

➡ 顯示檔案格式



```
test — -zsh — 80x24
[wangchaoli@wangchaolideMacBook-Pro test % file test
test: ASCII text
```

A screenshot of a macOS terminal window. The title bar shows three colored window control buttons (red, yellow, green) on the left, a folder icon and the text "test — -zsh — 80x24" in the center, and a close button on the right. The terminal content shows a prompt "[wangchaoli@wangchaolideMacBook-Pro test %]" followed by the command "file test". The output of the command is "test: ASCII text".

基礎指令 - wget

% wget [url]

```
(user@kali)-[~]  
$ wget https://github.com/Charlie28661/Password-validation/blob/main/main.py  
--2023-06-17 23:26:34-- https://github.com/Charlie28661/Password-validation/  
blob/main/main.py  
正在查找主機 github.com (github.com)... 20.27.177.113  
正在連接 github.com (github.com)|20.27.177.113|:443 ... 連上了。  
已送出 HTTP 要求，正在等候回應 ... 200 OK  
長度：未指定 [text/html]  
儲存到：「main.py」  
  
main.py [ ⇄ ] 184.38K --.-KB/s 於 0.1s  
  
2023-06-17 23:26:35 (1.21 MB/s) - 已儲存「main.py」 [188807]
```


使用者、群組、權限

% ls -al

```
wangchaoli — -zsh — 80x24
Last login: Tue May 30 23:44:39 on ttys000
[wangchaoli@wangchaolideMacBook-Pro ~ % ls -al
total 120
drwxr-x--- 25 wangchaoli staff 800 5 30 23:48 .
drwxr-xr-x  5 root      admin 160 5  5 19:38 ..
drwx----- 7 wangchaoli staff 224 5  2 01:01 .BurpSuite
-r-----  1 wangchaoli staff   8 9 20 2022 .CFUserTextEncoding
-rw-r--r--  1 wangchaoli staff 10244 5 30 23:38 .DS_Store
drwx----- 2 wangchaoli staff  64 5 28 01:16 .Trash
drwx----- 3 wangchaoli staff  96 10 13 2022 .cups
drwxr-xr-x  3 wangchaoli staff  96 11  2 2022 .idlerc
-rw-----  1 wangchaoli staff  37 11  2 2022 .python_history
drwx----- 4 wangchaoli staff 128  3 24 03:14 .ssh
drwxr-xr-x  5 wangchaoli staff 160  9 21 2022 .swiftpm
-rw-----  1 wangchaoli staff 532  5 30 23:44 .viminfo
drwxr-xr-x  4 wangchaoli staff 128  9 20 2022 .vscode
-rw-r--r--  1 wangchaoli staff 166 10 13 2022 .zprofile
-rw-----  1 wangchaoli staff 29388 5 30 23:44 .zsh_history
drwx----- 46 wangchaoli staff 1472 5 30 23:48 .zsh_sessions
drwx----- 3 wangchaoli staff   96  5  3 07:48 Applications
drwx----- 6 wangchaoli staff  192  5 30 23:45 Desktop
drwx----- 9 wangchaoli staff  288  5 27 22:27 Documents
drwx----- 25 wangchaoli staff  800  5 30 18:39 Downloads
drwx----- 90 wangchaoli staff 2880  5 28 09:49 Library
```


使用者、群組、權限

- 紅色：檔案模式
- 綠色：使用者姓名
- 藍色：群組名稱

```
wangchaoli — -zsh — 80x24
Last login: Tue May 30 23:44:39 on ttys000
[wangchaoli@wangchaolideMacBook-Pro ~ % ls -al
total 120
drwxr-x--- 25 wangchaoli staff 800 5 30 23:48 .
drwxr-xr-x  5 root      admin 160 5  5 19:38 ..
drwx----- 7 wangchaoli staff 224 5  2 01:01 .BurpSuite
-r-----  1 wangchaoli staff   8 9 20  2022 .CFUserTextEncoding
-rw-r--r--  1 wangchaoli staff 10244 5 30 23:38 .DS_Store
drwx----- 2 wangchaoli staff  64 5 28 01:16 .Trash
drwx----- 3 wangchaoli staff  96 10 13  2022 .cups
drwxr-xr-x  3 wangchaoli staff  96 11  2  2022 .idlerc
-rw-----  1 wangchaoli staff  37 11  2  2022 .python_history
drwx----- 4 wangchaoli staff 128 3 24 03:14 .ssh
drwxr-xr-x  5 wangchaoli staff 160 9 21  2022 .swiftpm
-rw-----  1 wangchaoli staff 532 5 30 23:44 .viminfo
drwxr-xr-x  4 wangchaoli staff 128 9 20  2022 .vscode
-rw-r--r--  1 wangchaoli staff 166 10 13  2022 .zprofile
-rw-----  1 wangchaoli staff 29388 5 30 23:44 .zsh_history
drwx----- 46 wangchaoli staff 1472 5 30 23:48 .zsh_sessions
drwx----- 3 wangchaoli staff  96 5  3 07:48 Applications
drwx----- 6 wangchaoli staff 192 5 30 23:45 Desktop
drwx----- 9 wangchaoli staff 288 5 27 22:27 Documents
drwx----- 25 wangchaoli staff 800 5 30 18:39 Downloads
drwx----- 90 wangchaoli staff 2880 5 28 09:49 Library
```

使用者、群組、權限

d**rwx****r**-**xr**-**x**

- 灰色：檔案類型(目錄會寫d, 檔案寫-)
- 紅色：擁有者權限
- 綠色：群組權限
- 藍色：其他使用者權限

使用者、群組、權限

`drwxr-xr-x`

r：讀取(4)

w：寫入(2)

x：執行(1)

➡ 此目錄權限為755

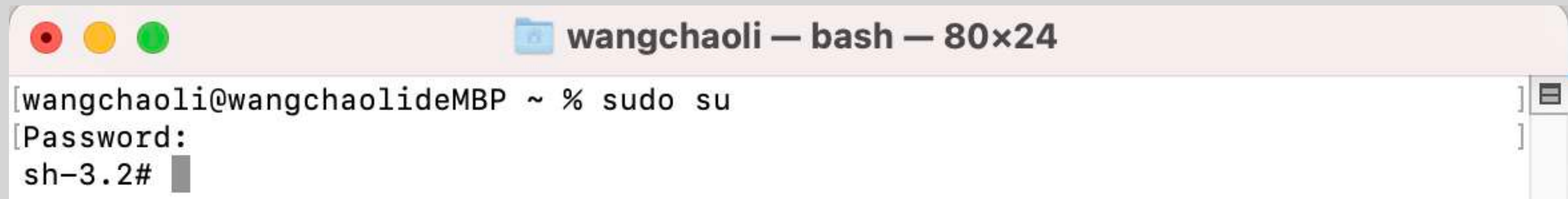
使用者、群組、權限

權限	數字	說明
rwXrwxrwx	777	所有使用者皆可讀、寫、執行
rw-r--r--	644	所有使用者皆可讀, 擁有者可寫入
rwXr-xr-x	755	所有使用者皆可讀、執行, 擁有者可寫入
rw-----	600	僅擁有者可讀、寫
-----	000	任何人都不能讀、寫、執行

基礎指令 - sudo

% sudo [command]

➡ 最高權限執行(需密碼)

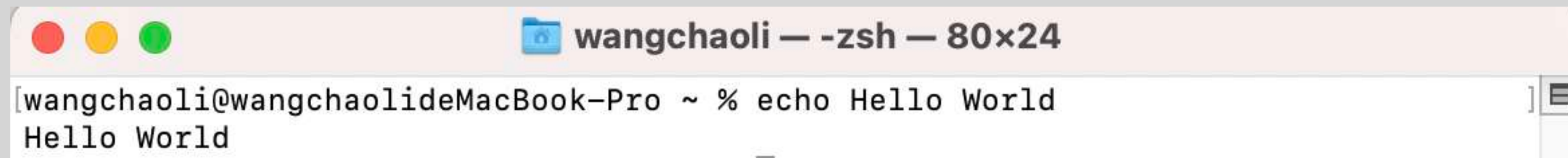


```
wangchaoli — bash — 80x24
[wangchaoli@wangchaolideMBP ~ % sudo su
[Password:
sh-3.2#
```

The image shows a terminal window titled "wangchaoli — bash — 80x24". The prompt is "[wangchaoli@wangchaolideMBP ~ %". The user has entered the command "sudo su". The prompt changes to "[Password:", indicating that a password is required for execution. The user has entered the password, and the prompt has changed to "sh-3.2#", indicating that the user is now in a shell with root privileges.

方便的指令 - echo

% echo [word]



A screenshot of a macOS terminal window. The title bar shows the name 'wangchaoli' and the shell '-zsh' with a size of '80x24'. The terminal content shows the command '[wangchaoli@wangchaolideMacBook-Pro ~ % echo Hello World]' followed by the output 'Hello World' on the next line.

```
wangchaoli — -zsh — 80x24  
[wangchaoli@wangchaolideMacBook-Pro ~ % echo Hello World]  
Hello World
```

➡ 輸出[word]

方便的指令 - wc

% wc [filename]

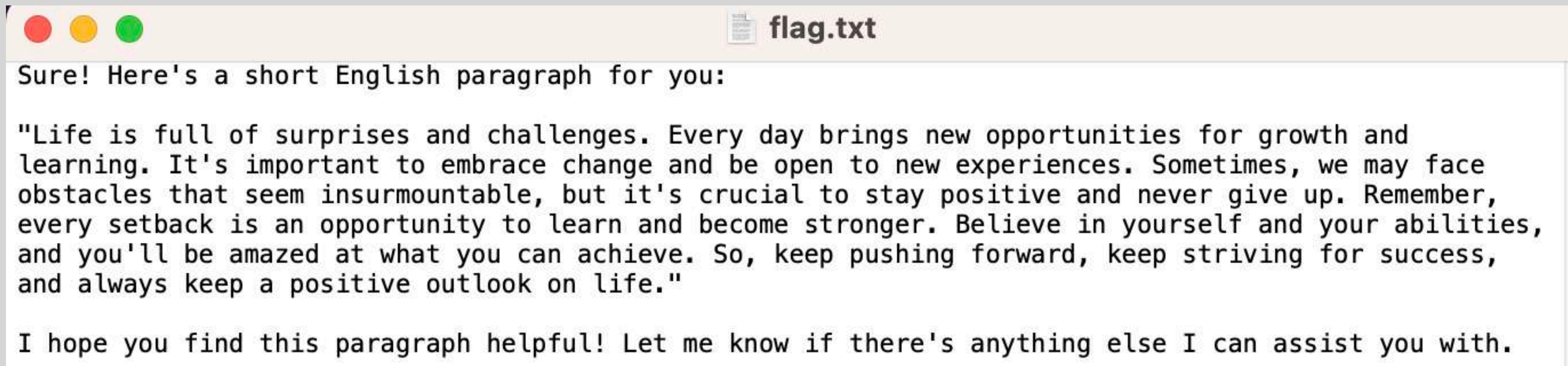


A terminal window titled "桌面 — -zsh — 80x24" showing the command `wc flag.txt` and its output. The output is displayed on a single line with four colored underlines: red for the line count (4), green for the word count (114), blue for the byte count (685), and black for the filename (flag.txt).

```
wangchaoli@wangchaolideMacBook-Pro Desktop % wc flag.txt
  4    114   685 flag.txt
```

- 紅色：列數
- 綠色：單字數
- 藍色：位元數
- 黑色：檔案名

方便的指令 - grep



A screenshot of a text editor window titled "flag.txt". The window contains the following text:

```
Sure! Here's a short English paragraph for you:  
  
"Life is full of surprises and challenges. Every day brings new opportunities for growth and learning. It's important to embrace change and be open to new experiences. Sometimes, we may face obstacles that seem insurmountable, but it's crucial to stay positive and never give up. Remember, every setback is an opportunity to learn and become stronger. Believe in yourself and your abilities, and you'll be amazed at what you can achieve. So, keep pushing forward, keep striving for success, and always keep a positive outlook on life."  
  
I hope you find this paragraph helpful! Let me know if there's anything else I can assist you with.
```

% grep [filter] [filename]



A screenshot of a terminal window titled "桌面 - -zsh - 80x24". The terminal shows the following command and output:

```
wangchaoli@wangchaolideMacBook-Pro Desktop % grep hope flag.txt  
I hope you find this paragraph helpful! Let me know if there's anything else I c  
an assist you with.
```

指令符號

	前面指令的輸出成為後面指令的輸入
	前面指令執行失敗才執行後面指令
&	讓前面的指令在背景執行
& &	前面指令執行成功才執行後面指令

駭客思維和相關網站

10 mins



駭客的種類



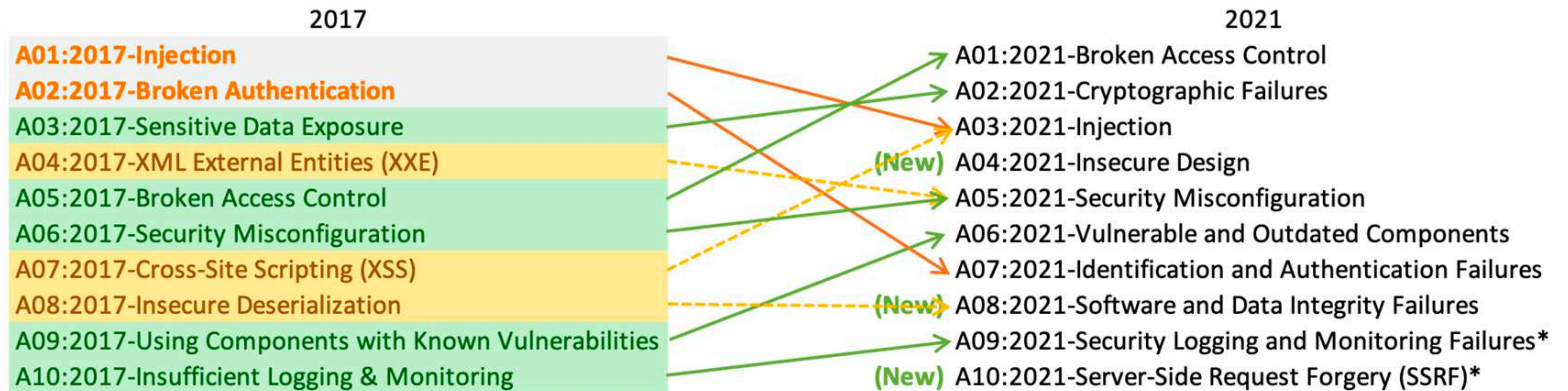
	黑帽	灰帽	白帽
行為	從事非法行為	與自身利益有關	擔任資安工程師
滲透測試中角色	紅隊		藍隊

白、灰帽駭客思維

Bug Bounty	提供獎勵計畫
提供獎勵計畫	所有現正提供 Bug Bounty 獎勵計畫的組織
狄卡科技股份有限公司	  
夯溫電地科論壇	 
Bilaxy Co.Ltd	 
現代財富科技有限公司	 
Matters Lab	  
泓科科技有限公司	 
Bitmark Inc. 英屬開曼群島商比特記號股份有限公司台灣分公司	
群暉科技股份有限公司	 

1 / 1

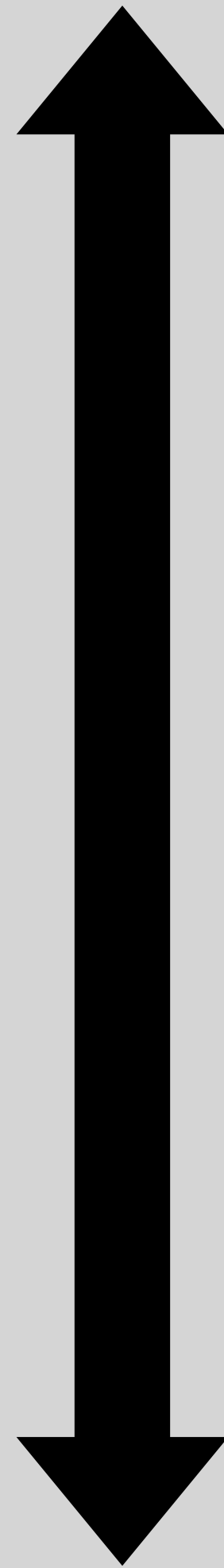
OWASP TOP 10



* From the Survey

這個漏洞有多嚴重？(CVSS)

10分(最嚴重)



0分(最不嚴重)

CTF TIME!!

40 mins

\$CAICT

What is CTF?

Capture the Flag(奪旗戰)

是一種常見的資訊安全競賽形式

在CTF比賽中，參賽者需要解決各種與資訊安全相關的問題，並尋找並奪取旗幟作為證明解題的標誌

常考分類

- Web Security(網頁安全)
- Pwn(code找漏洞)
- Reverse(逆向工程)
- Crypto(密碼學)
- Misc(雜項)

CTF禁忌

- 與他人共享flag
- 與他人共享解法

CTF Link

<http://ctf.scaict.org/>

感謝參與

2023/07/02

\$CAICT