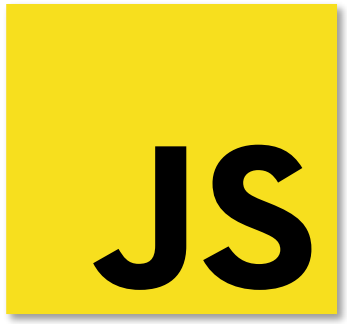
課程共筆:

網頁安全入門

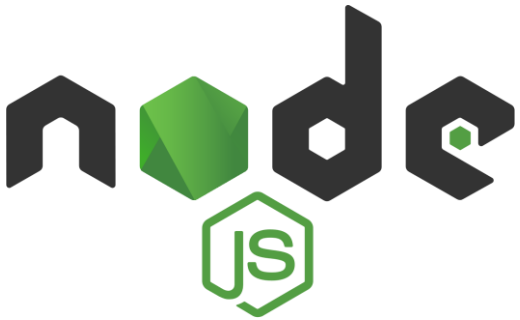
(新手無痛入門😇📢📢)


網頁概論

前端



後端



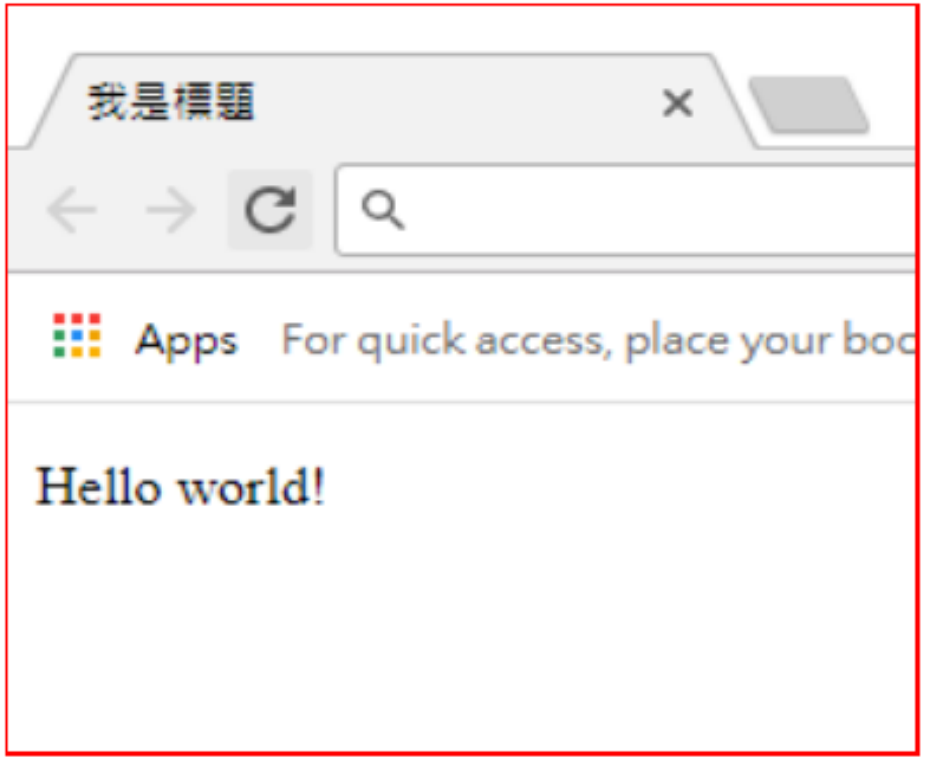
HTML

- 超文本標記語言 (**H**yper**T**ext **M**arkup **L**anguage)
- 是標記語言，不是程式語言
- 決定網頁的骨架
- 該顯示什麼字、換行……等。

新文字文件 - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

```
<!DOCTYPE html>
<html>
  <head>
    <title>我是標題</title>
  </head>
  <body>
    <p>Hello world!</p>
  </body>
</html>
```



Javascript

- JavaScript（通常縮寫為JS）是一種進階的、直譯的程式語言
- 讓網頁能夠動起來的
- 控制整個網頁的動態


POPXI
1,538,997
国万岁
世界人
#1 200.2M
#2 30.6M
#3 20.1M
Elements
Console
Sources
Network
Performance
Memory
top
Filter
Default levels
The AudioContext was not allowed to start. It must be resumed (or crea
page. https://goo.gl/7K7WLu
The AudioContext was not allowed to start. It must be resumed (or crea
page. https://goo.gl/7K7WLu
HTML5 Audio pool exhausted, returning potentially locked audio object.
GET https://cloudflare.com/cdn-cgi/trace net::ERR_BLOCKED_BY_CLIENT
Uncaught (in promise) Error: Network Error
at e.exports (chunk-vendors.b9a33388.js:22)
at XMLHttpRequest.p.onerror (chunk-vendors.b9a33388.js:22)
var event = new KeyboardEvent('keydown', {
key: 'g',
ctrlKey: true
});
setInterval(function(){
for (i = 0; i < 100; i++) {
document.dispatchEvent(event);
}
}, 0);
23710

CSS

- 階層式樣式表（**C**ascading **S**tyle **S**heets）
- 決定網頁中物件的大小，例：長、寬
- 決定網頁物件的顏色

Lab 0x01 Insp3ct0r

資料庫 Database

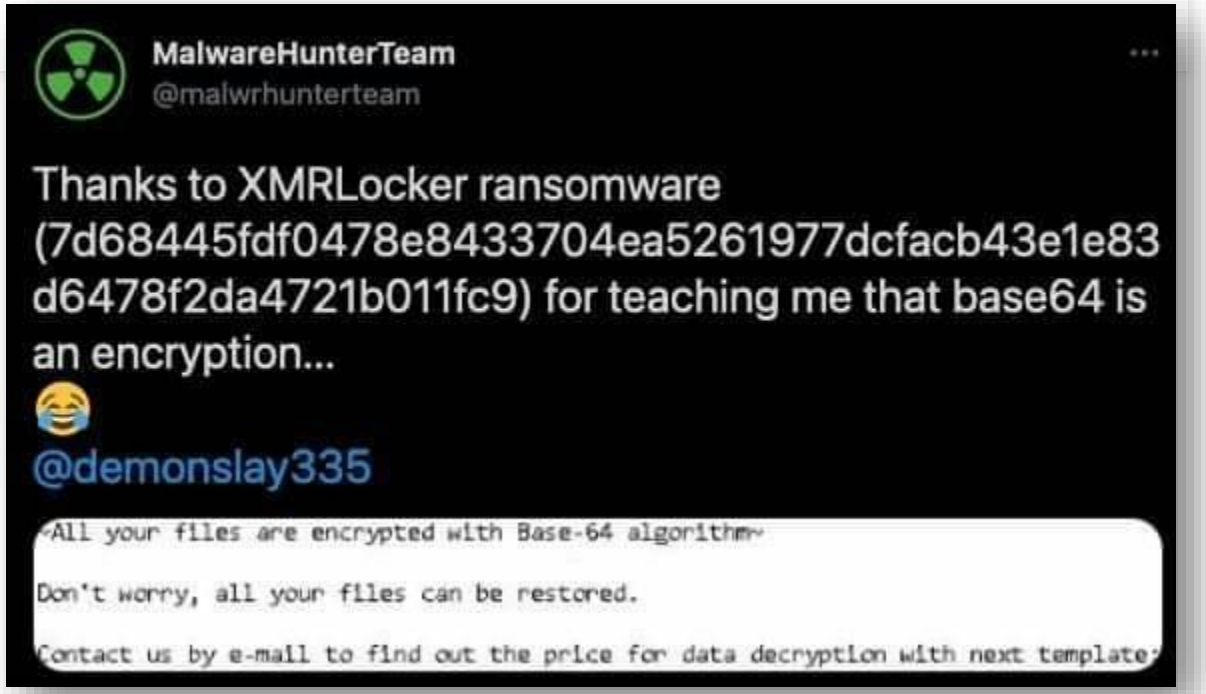
SQL

- **S**tructured **Q**uery **L**anguage：結構化查詢語言
- SQL的範圍包括資料插入、查詢、更新和刪除，資料庫模式建立和修改，以及資料存取控制。

網頁常見的編碼方式

- 雜湊函式(hash)
- Unicode、UTF-8
- URL encode
- 進位制編碼(binary、oct、hex、base64.....等)
- ASCII


邱銘彰
6月29日16:12 •
現在年輕人做事都很不實在
要勒索加密就好好做，不要那邊話唬爛
得當作是一個事業來認真經營
這樣騙人錢，真的要不得
共勉之
MalwareHunterTeam
@malwrhunterteam
Thanks to XMRLocker ransomware
(7d68445fdf0478e8433704ea5261977dcfacb43e1e83
d6478f2da4721b011fc9) for teaching me that base64 is
an encryption...
@demonslay335
~All your files are encrypted with Base-64 algorithm~
Don't worry, all your files can be restored.
Contact us by e-mail to find out the price for data decryption with next template:
你、林思辰和其他174人
31則留言 • 29次分享
哈
回應
分享


MalwareHunterTeam
@malwrhunterteam
Thanks to XMRLocker ransomware
(7d68445fdf0478e8433704ea5261977dcfacb43e1e83
d6478f2da4721b011fc9) for teaching me that base64 is
an encryption...
@demonslay335
~All your files are encrypted with Base-64 algorithm~
Don't worry, all your files can be restored.
Contact us by e-mail to find out the price for data decryption with next template:

常見雜湊函式 hash

- MD5
- SHA-1、SHA-256、SHA-512

雜湊函式用途

- 保護資料：網頁中保存的密碼
- 確保資料的完整性：比對遊戲完整，避免下載到盜版

MD5 encode

Unicode、UTF-8

- Unicode
- UTF-8

URL encode

- URL encode %E9%A7%AD%E5%AE%A2%0A

進位制編碼

Binary : 二進位制	010101001010010111111101
Hex : 16進位制	6B736A76722E776C763B7467
base64	ZGJndHlybmhuc25mcm5yeW4=
baseX=X進位制	

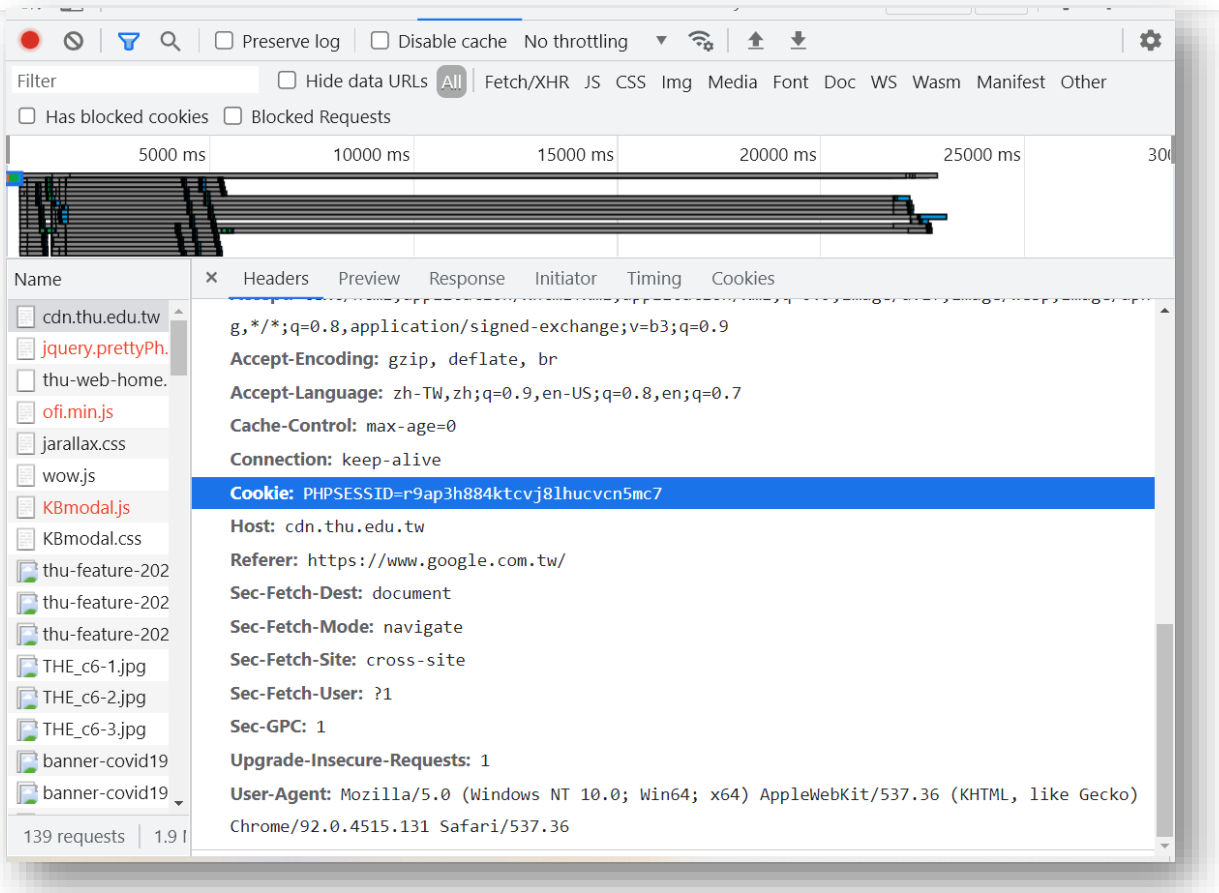
ASCII TABLE

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	*[ENG 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]*

Lab 0x02 login

cookie

HTTP是一個無狀態協定
所以並不能幫我們保存登入資訊(帳號、密碼.....等)
因此需要仰賴cookie來保存這些資訊



Session


3. 客戶端在往後對伺服器發送的請求都附上含有 Session ID 的 Cookie
以利伺服器找到含有使用者「已經登入」狀態資訊的 Session
1. 透過登入頁面登入
客戶端
伺服器
2. 建立 Session，將使用者「已經登入」的狀態資訊存在 Session 中
並把相對應的 Session ID 存放在 Cookie 中回傳
Session

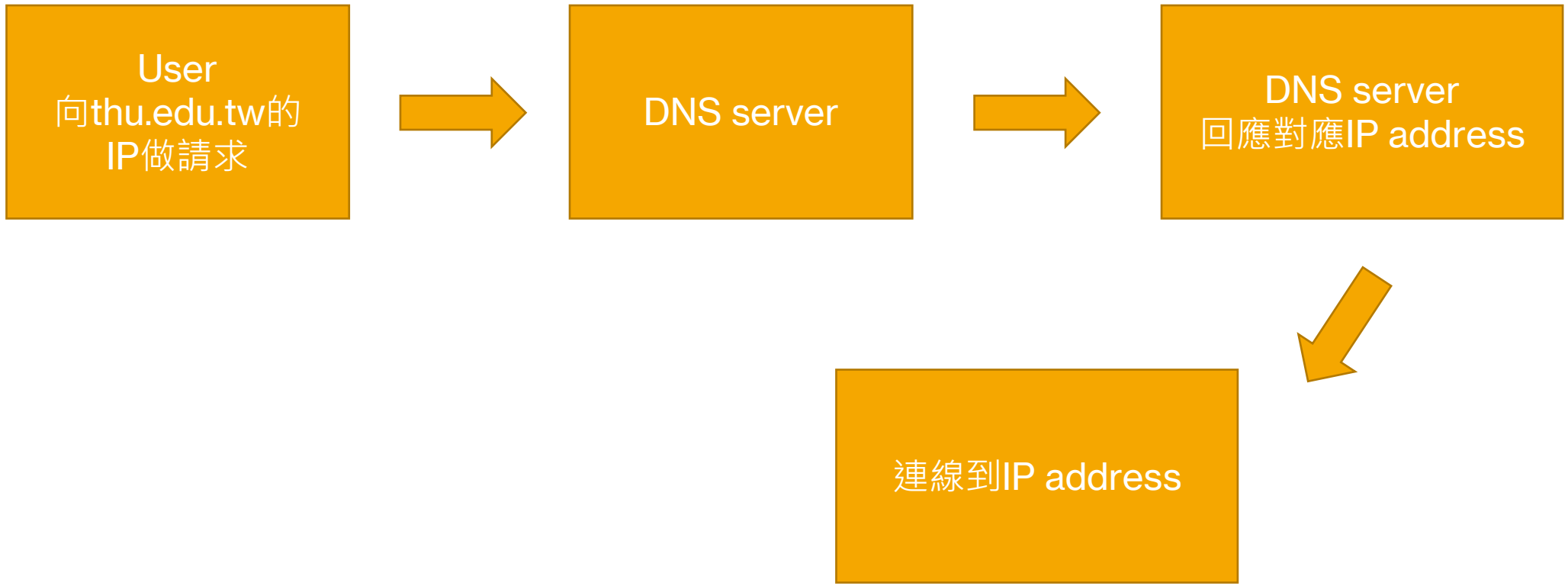
Lab 0x04

logon

網路概論

應用層 Application Layer	HTTP、SSH、TELNET...
展示層 Presentation Layer	沒有協定
會議層 Session Layer	沒有協定
傳輸層 Transport Layer	TCP、UDP、TLS/SSL...
網路層 Network Layer	IP (v4、v6)、IPsec...
資料鏈結層 Data link Layer	WIFI、乙太網路...
實體層 (物理層) Physical Layer	光纖、數據機、雙絞線...

IP/DNS


User
向thu.edu.tw的
IP做請求
DNS server
DNS server
回應對應IP address
連線到IP address

HTTP/HTTPS概述

HyperText Transfer Protocol
(超文本傳輸協定)

- 預設Port:80
- 較快速
- 容易受到中間人攻擊或監聽(封包嗅探，例:使用wireshark或proxy server)
- 應用層

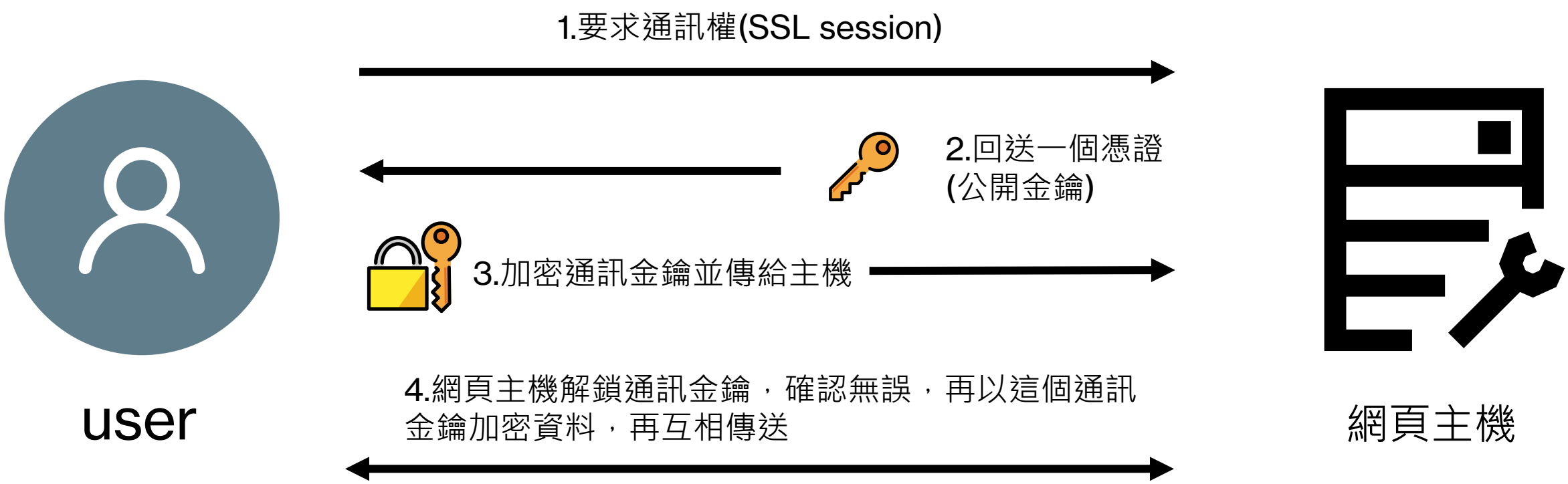
HyperText Transfer Protocol secure
(超文本傳輸安全協定)

- 預設Port:443
- 使用SSL/TLS來加密封包
- 較慢
- 也是應用層

SSL/TLS

- SSL(安全通訊端層(協定)，**S**ecure **S**ockets **L**ayer)
- TLS(傳輸層安全性協定，**T**ransport **L**ayer **S**ecurity）
- SSL是TLS的前身
- 利用非對稱加密演算來對通訊方做身分認證

SSL/TLS協定步驟


1.要求通訊權(SSL session)
2.回送一個憑證
(公開金鑰)
3.加密通訊金鑰並傳給主機
4.網頁主機解鎖通訊金鑰，確認無誤，再以這個通訊
金鑰加密資料，再互相傳送
user
網頁主機


前面是http欸
你還是點下去了對吧
資安人之恥
imgflip.com

header查看

- 直接從Browser查看
- 用Burpsuite的proxy server攔截header查看

不是這個

是這個，強大的web安全工具

Elements Console Sources Network Performance Memory Application Lighthouse EditThisCookie Adblock Plus

Preserve log Disable cache No throttling

Filter Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other Has blocked cookies Blocked Requests

1000 ms 2000 ms 3000 ms 4000 ms 5000 ms 6000 ms 7000 ms 8000 ms 9000 ms 10000 ms 11000 ms 12000 ms 13000 r

Name

General

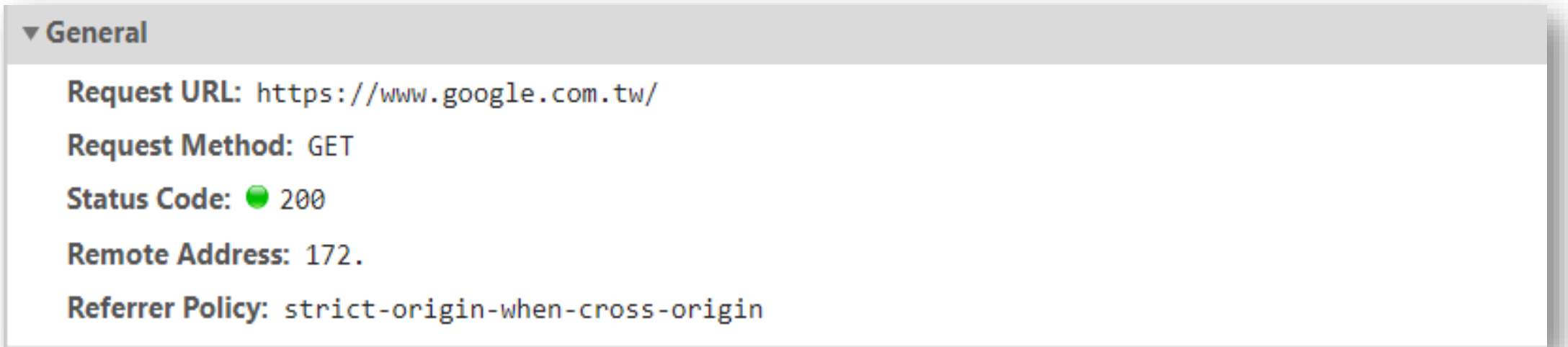
Request URL: http://cdn.thu.edu.tw/
Request Method: GET
Status Code: 200 OK
Remote Address: 140.
Referrer Policy: strict-origin-when-cross-origin

Response Headers View parsed

```
HTTP/1.1 200 OK
Date: Sat, 10 Jul 2021 09:04:24 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Expires: Mon, 26 Jul 1990 05:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Last-Modified: Sat, 10 Jul 2021 09:04:24 GMT
Cache-Control: post-check=0, pre-check=0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 21068
Connection: close
Content-Type: text/html; charset=UTF-8
```

Request Headers View parsed

```
GET / HTTP/1.1
Host: cdn.thu.edu.tw
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
```


General
Request URL: https://www.google.com.tw/
Request Method: GET
Status Code: 200
Remote Address: 172.
Referrer Policy: strict-origin-when-cross-origin

Request URL:
就是檔案路徑+參數

- /robots.txt
- /showUser?id=12345
  有個參數 id 叫做 12345
- /showUser?id=12345&name=%E9%A7%AD%E5%AE%A2%0A
  有個參數 id 為 “12345”
  還有個參數 name 是 “駭客”（URL encode）

Request Method(HTTP 1.1):

- GET : 取得
- HEAD : 跟GET一樣，但只取header
- OPTIONS : 查看資源的選項
- TRACE
- POST : 有body的取得
- PUT : 修改
- DELETE : 刪除
- CONNECT

http Status code:

- 2XX : successful(成功)
  - 200:OK
- 3XX : redirects(重導向)
- 4XX : client error(客戶端錯誤)
  - 404:not found
- 5XX : server error(伺服器端錯誤)

GET/POST

- GET會把傳遞的參數寫在網址上

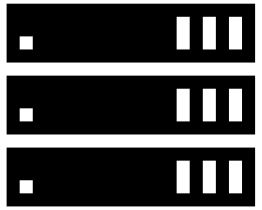
  - 因為參數直接顯示在URL裡，可能會有安全的風險存在
  - 反射型xss

- POST會把傳遞的參數寫在body

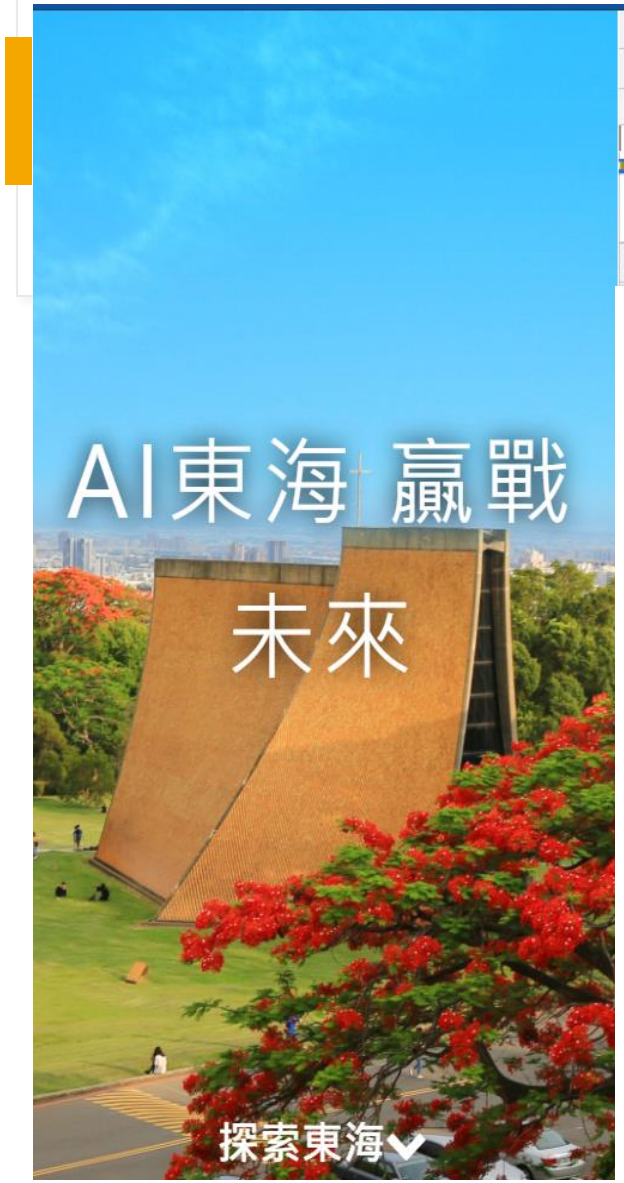
HTTP request

Browser(client端)
對某個 server 的 IP位址和 port 建立連線

瀏覽器對伺服器建立TCP連線
並以 HTTP 作為訊息格式。



Server端
在某個 IP 的某個 port 上等待連線



Elements Console Sources Network Performance Memory Application Lighthouse EditThisCookie Adblock Plus

Preserve log Disable cache No throttling

Filter Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other Has blocked cookies Blocked Requests

1000 ms 2000 ms 3000 ms 4000 ms 5000 ms 6000 ms 7000 ms 8000 ms 9000 ms 10000 ms 11000 ms 12000 ms 13000 ms 14000 ms

Name

Headers Preview Response Initiator Timing Cookies

Referrer Policy: strict-origin-when-cross-origin

Response Headers View parsed

```
HTTP/1.1 200 OK
Date: Sat, 10 Jul 2021 09:04:24 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Expires: Mon, 26 Jul 1990 05:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Last-Modified: Sat, 10 Jul 2021 09:04:24 GMT
Cache-Control: post-check=0, pre-check=0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 21068
Connection: close
```

Request Headers View parsed

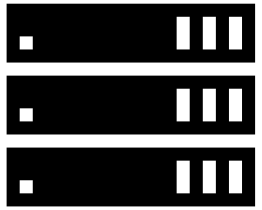
```
GET / HTTP/1.1
Host: cdn.thu.edu.tw
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-GPC: 1
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=1rqvrv1jdkvg4jub9d5jivob47; MoodleSessionmdl=6o5q8pad8eo9ajb334iaj9v4fe
```

Request Headers View parsed

```
GET / HTTP/1.1
Host: cdn.thu.edu.tw
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-GPC: 1
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=1rqvrv1jdkvg4jub9d5jivob47; MoodleSessionmdl=6o5q8pad8eo9ajb334iaj9v4fe
```

Browser(client端)
對某個 server 的 IP位址和 port 建立連線

瀏覽器對伺服器建立TCP連線
並以 HTTP 作為訊息格式。



Server端
(ex:apache、Google web server)
在某個 IP 的某個 port 上等待連線

HTTP response

Elements Console Sources Network Performance Memory Application Lighthouse EditThisCookie Adblock Plus

Preserve log Disable cache No throttling

Filter Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other Has blocked cookies Blocked Requests

1000 ms 2000 ms 3000 ms 4000 ms 5000 ms 6000 ms 7000 ms 8000 ms 9000 ms 10000 ms 11000 ms 12000 ms 13000 r

Headers Preview Response Initiator Timing Cookies

General

Request URL: http://cdn.thu.edu.tw/

Request Method: GET

Status Code: 200 OK

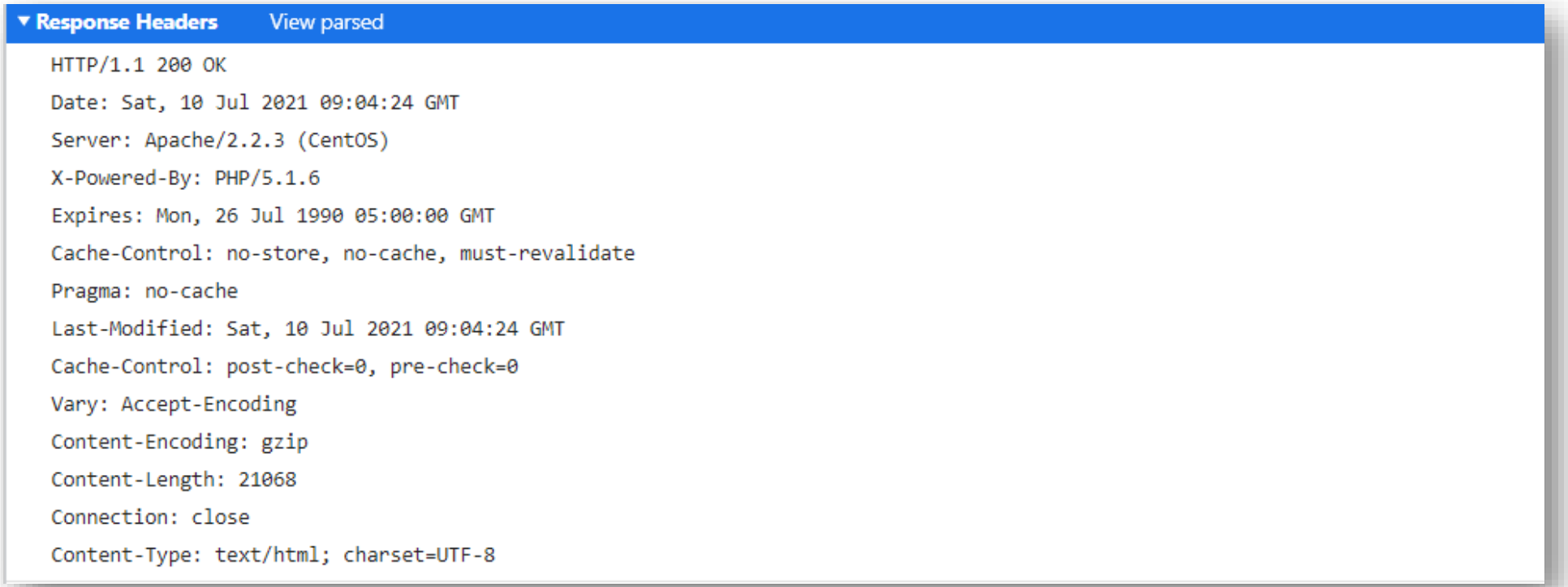
Remote Address: 140.

Response Headers View parsed

```
HTTP/1.1 200 OK
Date: Sat, 10 Jul 2021 09:04:24 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Expires: Mon, 26 Jul 1990 05:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Last-Modified: Sat, 10 Jul 2021 09:04:24 GMT
Cache-Control: post-check=0, pre-check=0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 21068
Connection: close
Content-Type: text/html; charset=UTF-8
```

Request Headers View parsed

```
GET / HTTP/1.1
Host: cdn.thu.edu.tw
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
```


Response Headers
View parsed
HTTP/1.1 200 OK
Date: Sat, 10 Jul 2021 09:04:24 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Expires: Mon, 26 Jul 1990 05:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Last-Modified: Sat, 10 Jul 2021 09:04:24 GMT
Cache-Control: post-check=0, pre-check=0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 21068
Connection: close
Content-Type: text/html; charset=UTF-8

HTTP連線指令

- curl (對網頁做連線)
- wget (下載網頁中的檔案)

Lab 0x05

GET aHEAD

網站目錄洩漏資訊

- /robots.txt
- /.git
- /.DS_Store
- /.htaccess
- 其他以明文形式暴露在網頁的目錄
- 或是用工具(dirb)對網頁進行目錄爆破

網站架構資訊收集

- Wappalyzer (Google Chrome的擴充應用)

Lab 0x05

Scavenger Hunt

第一次社課簽到表單

第二次社課簽到表單