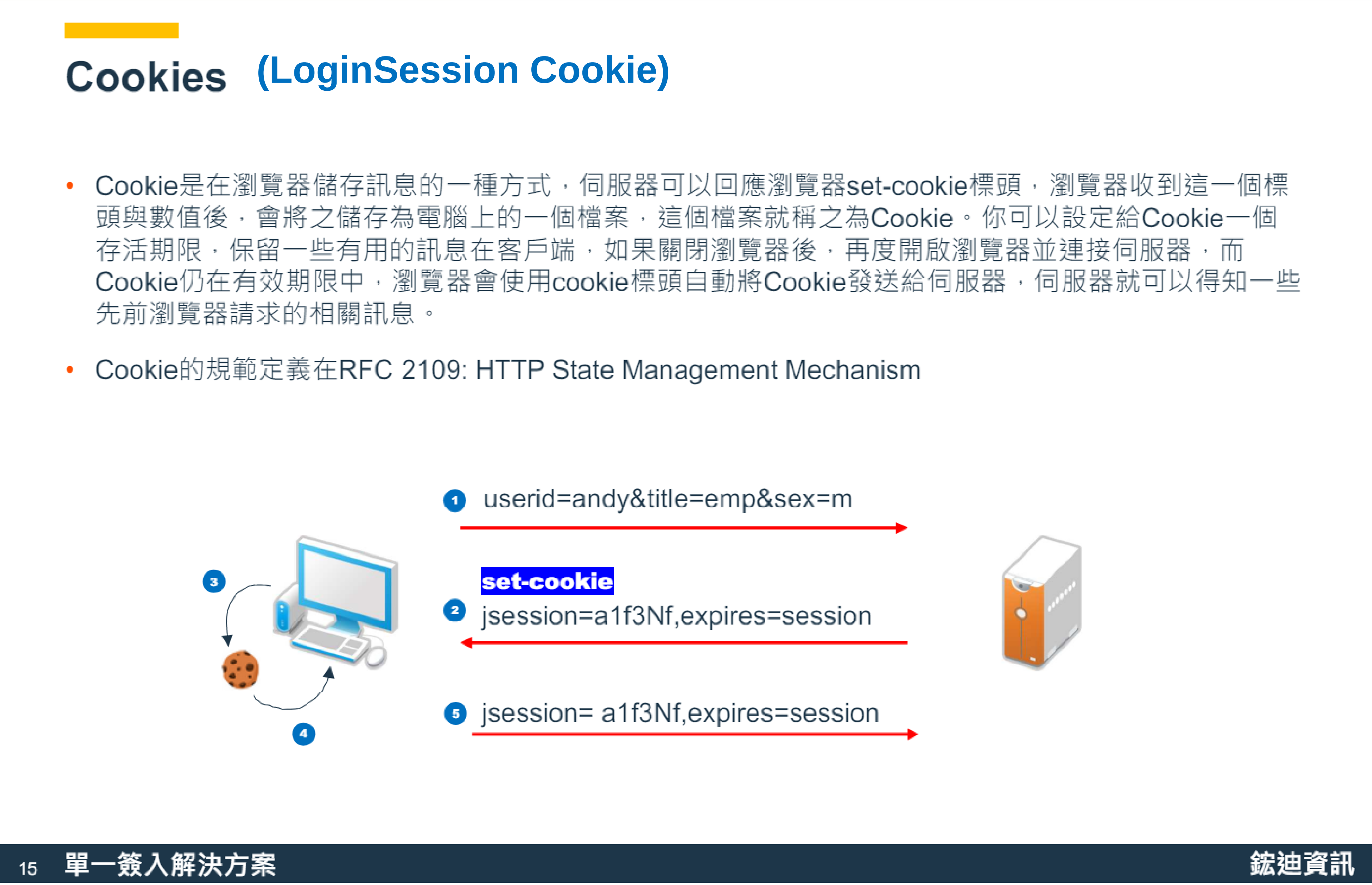
Why Cookie?

台大計中網路組
游子興
davisyou@ntu.edu.tw
02-33665008

Stateful vs. Stateless

- Telnet/SSH(Stateful) vs. HTTP(Stateless)



Cookies (LoginSession Cookie)

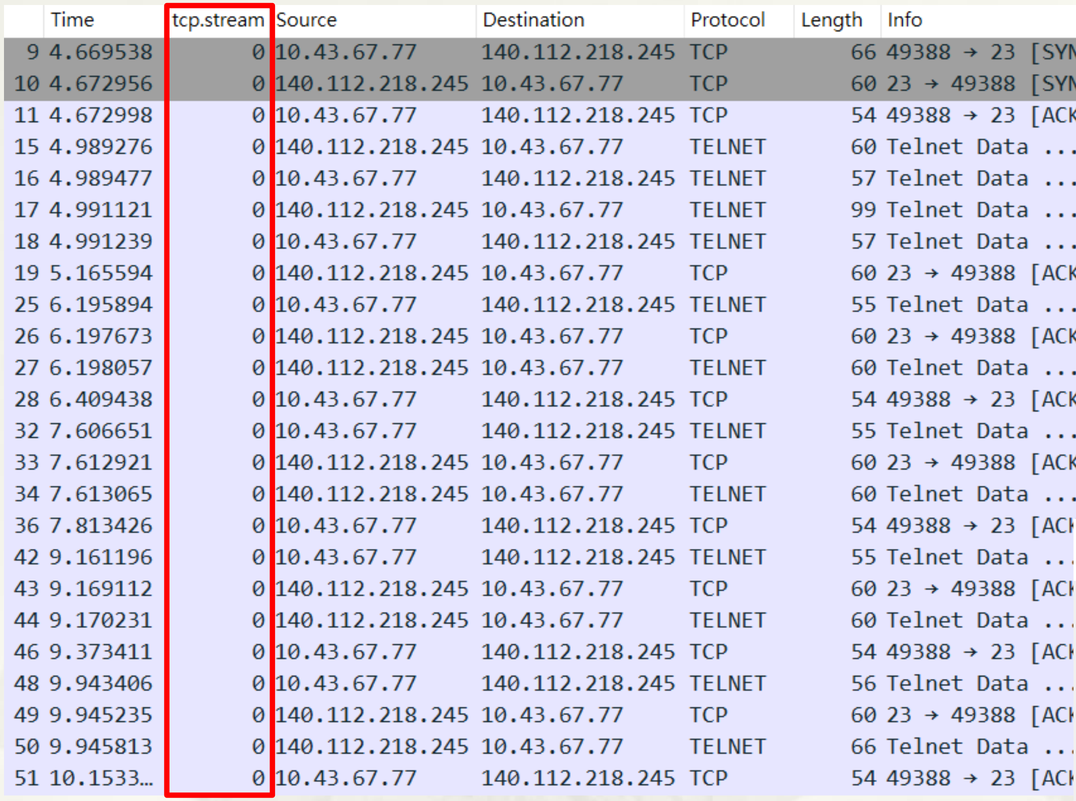
- Cookie是在瀏覽器儲存訊息的一種方式，伺服器可以回應瀏覽器set-cookie標頭，瀏覽器收到這一個標頭與數值後，會將之儲存為電腦上的一個檔案，這個檔案就稱之為Cookie。你可以設定給Cookie一個存活期限，保留一些有用的訊息在客戶端，如果關閉瀏覽器後，再度開啟瀏覽器並連接伺服器，而Cookie仍在有效期限中，瀏覽器會使用cookie標頭自動將Cookie發送給伺服器，伺服器就可以得知一些先前瀏覽器請求的相關訊息。
- Cookie的規範定義在RFC 2109: HTTP State Management Mechanism

1 userid=andy&title=emp&sex=m

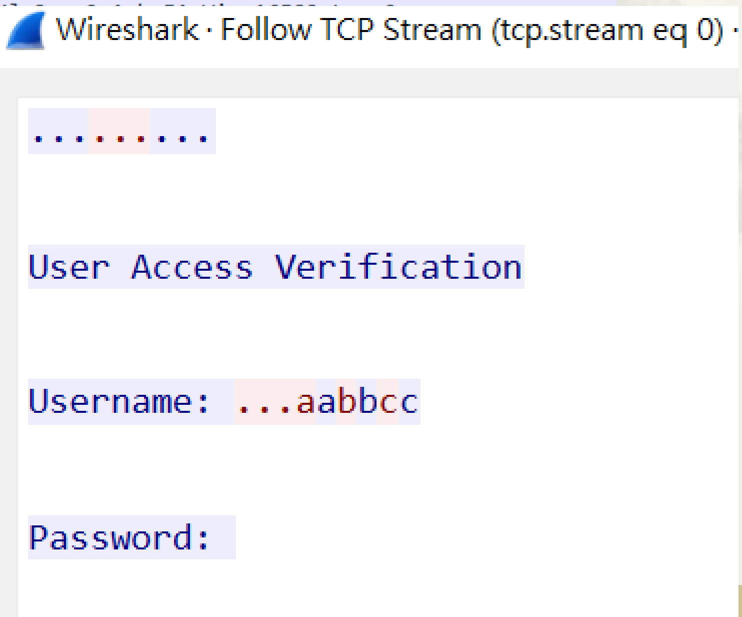
2 **set-cookie**
jsession=a1f3Nf,expires=session

5 jsession= a1f3Nf,expires=session

Telnet



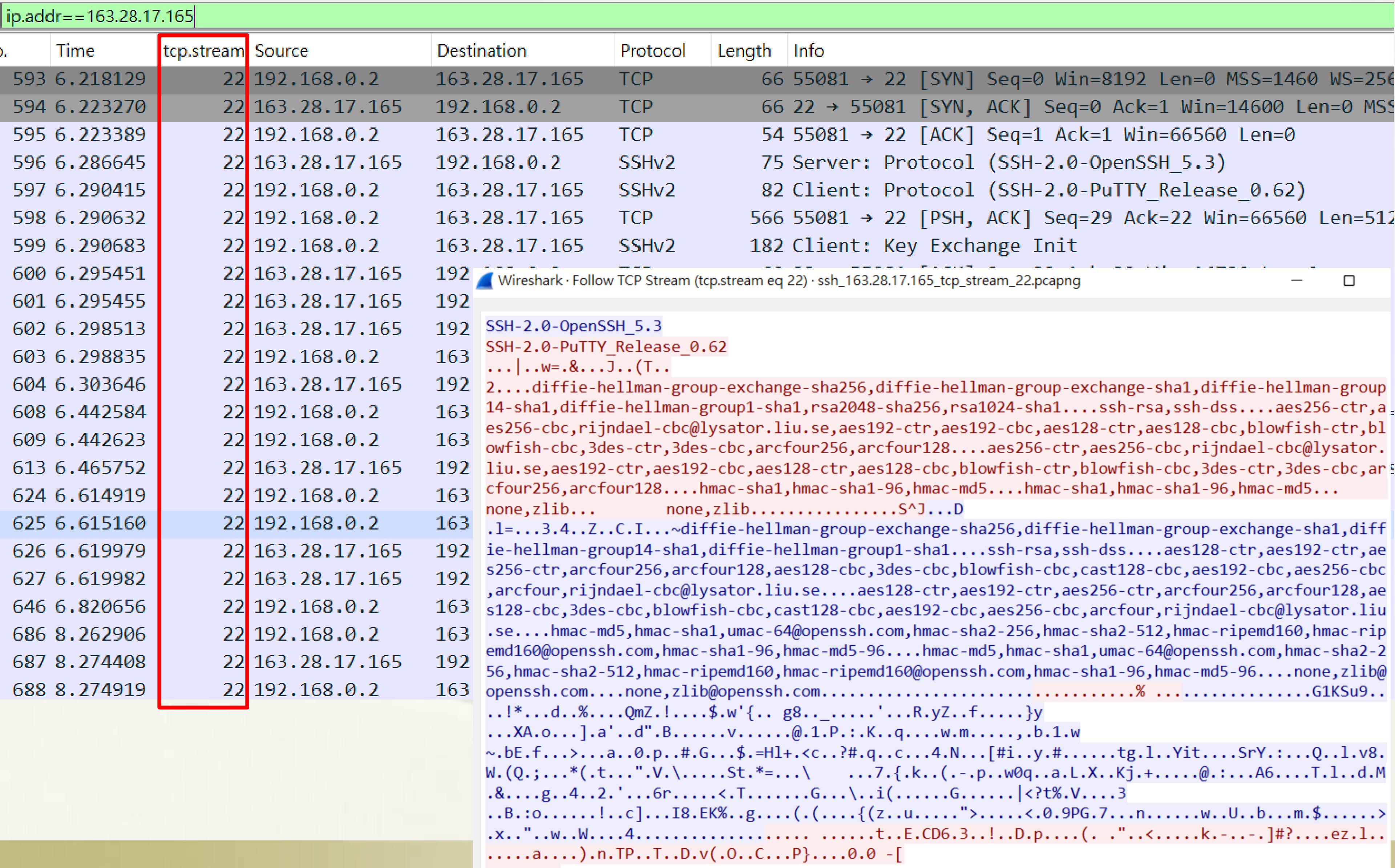
	Time	tcp.stream	Source	Destination	Protocol	Length	Info
9	4.669538	0	10.43.67.77	140.112.218.245	TCP	66	49388 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
10	4.672956	0	140.112.218.245	10.43.67.77	TCP	60	23 → 49388 [SYN, ACK] Seq=0 Ack=1 Win=40960 Len=0 MSS=1386
11	4.672998	0	10.43.67.77	140.112.218.245	TCP	54	49388 → 23 [ACK] Seq=1 Ack=1 Win=16632 Len=0
15	4.989276	0	140.112.218.245	10.43.67.77	TELNET	60	Telnet Data ...
16	4.989477	0	10.43.67.77	140.112.218.245	TELNET	57	Telnet Data ...
17	4.991121	0	140.112.218.245	10.43.67.77	TELNET	99	Telnet Data ...
18	4.991239	0	10.43.67.77	140.112.218.245	TELNET	57	Telnet Data ...
19	5.165594	0	140.112.218.245	10.43.67.77	TCP	60	23 → 49388 [ACK] Seq=49 Ack=7 Win=40960 Len=0
25	6.195894	0	10.43.67.77	140.112.218.245	TELNET	55	Telnet Data ...
26	6.197673	0	140.112.218.245	10.43.67.77	TCP	60	23 → 49388 [ACK] Seq=49 Ack=8 Win=40960 Len=0
27	6.198057	0	140.112.218.245	10.43.67.77	TELNET	60	Telnet Data ...
28	6.409438	0	10.43.67.77	140.112.218.245	TCP	54	49388 → 23 [ACK] Seq=8 Ack=50 Win=16583 Len=0
32	7.606651	0	10.43.67.77	140.112.218.245	TELNET	55	Telnet Data ...
33	7.612921	0	140.112.218.245	10.43.67.77	TCP	60	23 → 49388 [ACK] Seq=50 Ack=9 Win=40960 Len=0
34	7.613065	0	140.112.218.245	10.43.67.77	TELNET	60	Telnet Data ...
36	7.813426	0	10.43.67.77	140.112.218.245	TCP	54	49388 → 23 [ACK
42	9.161196	0	10.43.67.77	140.112.218.245	TELNET	55	Telnet Data ...
43	9.169112	0	140.112.218.245	10.43.67.77	TCP	60	23 → 49388 [ACK
44	9.170231	0	140.112.218.245	10.43.67.77	TELNET	60	Telnet Data ...
46	9.373411	0	10.43.67.77	140.112.218.245	TCP	54	49388 → 23 [ACK
48	9.943406	0	10.43.67.77	140.112.218.245	TELNET	56	Telnet Data ...
49	9.945235	0	140.112.218.245	10.43.67.77	TCP	60	23 → 49388 [ACK
50	9.945813	0	140.112.218.245	10.43.67.77	TELNET	66	Telnet Data ...
51	10.1533…	0	10.43.67.77	140.112.218.245	TCP	54	49388 → 23 [ACK



```
.........


User Access Verification


Username: ...aabbcc


Password:
```

- Demo
  - telnet 140.112.218.254

SSH



```
ip.addr==163.28.17.165
```

```
o.   Time      tcp.stream Source         Destination     Protocol  Length Info
 593 6.218129         22 192.168.0.2    163.28.17.165   TCP         66 55081 → 22 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
 594 6.223270         22 163.28.17.165  192.168.0.2     TCP         66 22 → 55081 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS
 595 6.223389         22 192.168.0.2    163.28.17.165   TCP         54 55081 → 22 [ACK] Seq=1 Ack=1 Win=66560 Len=0
 596 6.286645         22 163.28.17.165  192.168.0.2     SSHv2       75 Server: Protocol (SSH-2.0-OpenSSH_5.3)
 597 6.290415         22 192.168.0.2    163.28.17.165   SSHv2       82 Client: Protocol (SSH-2.0-PuTTY_Release_0.62)
 598 6.290632         22 192.168.0.2    163.28.17.165   TCP        566 55081 → 22 [PSH, ACK] Seq=29 Ack=22 Win=66560 Len=512
 599 6.290683         22 192.168.0.2    163.28.17.165   SSHv2      182 Client: Key Exchange Init
 600 6.295451         22 163.28.17.165  192
 601 6.295455         22 163.28.17.165  192
 602 6.298513         22 163.28.17.165  192
 603 6.298835         22 192.168.0.2    163
 604 6.303646         22 163.28.17.165  192
 608 6.442584         22 192.168.0.2    163
 609 6.442623         22 192.168.0.2    163
 613 6.465752         22 163.28.17.165  192
 624 6.614919         22 192.168.0.2    163
 625 6.615160         22 192.168.0.2    163
 626 6.619979         22 163.28.17.165  192
 627 6.619982         22 163.28.17.165  192
 646 6.820656         22 192.168.0.2    163
 686 8.262906         22 192.168.0.2    163
 687 8.274408         22 163.28.17.165  192
 688 8.274919         22 192.168.0.2    163
```

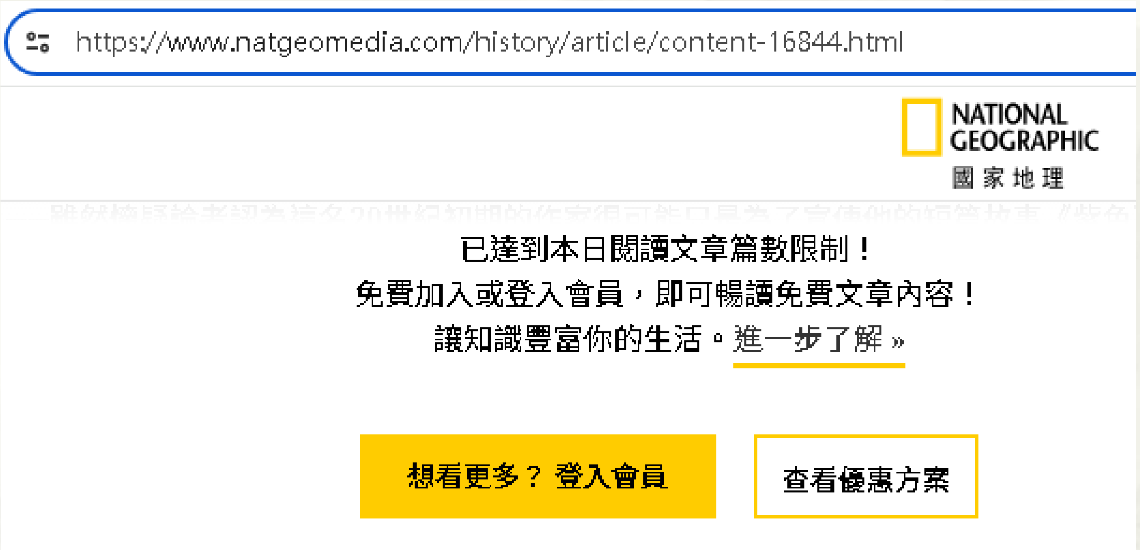
Wireshark · Follow TCP Stream (tcp.stream eq 22) · ssh_163.28.17.165_tcp_stream_22.pcapng

```
SSH-2.0-OpenSSH_5.3
SSH-2.0-PuTTY_Release_0.62
...|..w=.&...J..(T..
2....diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group
14-sha1,diffie-hellman-group1-sha1,rsa2048-sha256,rsa1024-sha1....ssh-rsa,ssh-dss....aes256-ctr,a
es256-cbc,rijndael-cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,blowfish-ctr,bl
owfish-cbc,3des-ctr,3des-cbc,arcfour256,arcfour128....aes256-ctr,aes256-cbc,rijndael-cbc@lysator.
liu.se,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,blowfish-ctr,blowfish-cbc,3des-ctr,3des-cbc,ar
cfour256,arcfour128....hmac-sha1,hmac-sha1-96,hmac-md5....hmac-sha1,hmac-sha1-96,hmac-md5...
none,zlib...        none,zlib................S^J...D
.l=...3.4..Z..C.I...~diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diff
ie-hellman-group14-sha1,diffie-hellman-group1-sha1....ssh-rsa,ssh-dss....aes128-ctr,aes192-ctr,ae
s256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc
,arcfour,rijndael-cbc@lysator.liu.se....aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,ae
s128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu
.se....hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160,hmac-rip
emd160@openssh.com,hmac-sha1-96,hmac-md5-96....hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-sha2-2
56,hmac-sha2-512,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96....none,zlib@
openssh.com....none,zlib@openssh.com.................................% .................G1KSu9..
..!*...d..%....QmZ.!....$.w'{.. g8.._.....'...R.yZ..f.....}y
...XA.o...].a'..d".B......v......@.1.P.:.K..q....w.m.....,.b.1.w
~.bE.f...>...a..0.p..#.G...$.=Hl+.<c..?#.q..c...4.N...[#i..y.#......tg.l..Yit....SrY.:...Q..l.v8.
W.(Q.;...*(.t...".V.\.....St.*=...\    ...7.{.k..(.-.p..w0q..a.L.X..Kj.+.....@.:...A6....T.l..d.M
.&....g..4..2.'...6r.....<.T.......G...\..i(......G......|<?t%.V....3
..B.:o......!..c]...I8.EK%..g....(.(....{(z..u.....">.....<.0.9PG.7...n......w..U..b...m.$......>
.x..."..w..W....4...................... ......t..E.CD6.3..!..D.p....(. ."..<.....k.-..-.]#?....ez.l..
.....a....).n.TP..T..D.v(.O..C...P}....0.0 -[
```

Cookie 功用之一
記錄用戶資訊

國家地理雜誌
每天只能看一篇?

- https://www.natgeomedia.com/



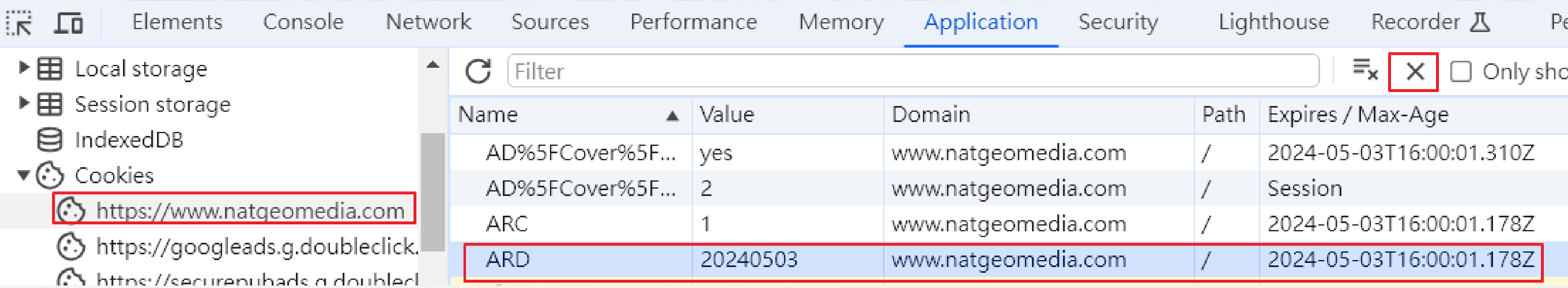
https://www.natgeomedia.com/history/article/content-16844.html

已達到本日閱讀文章篇數限制！

免費加入或登入會員，即可暢讀免費文章內容！

讓知識豐富你的生活。進一步了解 »

F12



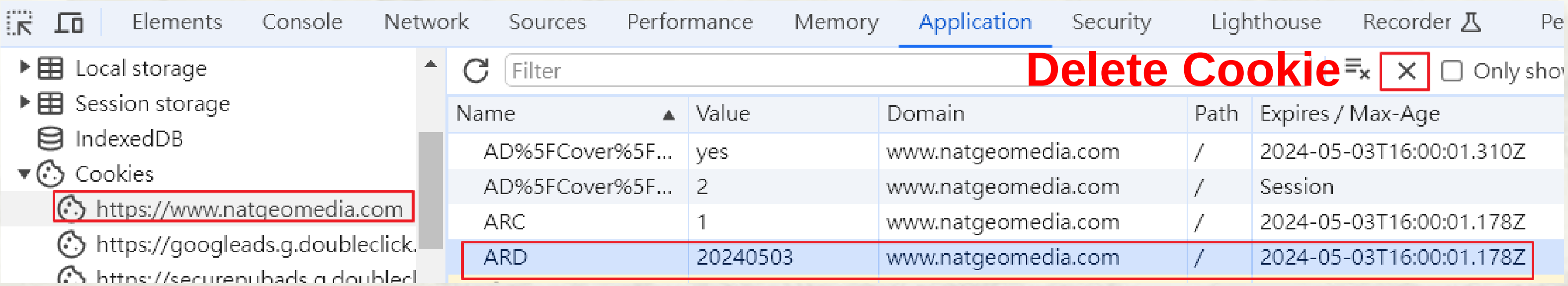
Name	Value	Domain	Path	Expires / Max-Age
AD%5FCover%5F...	yes	www.natgeomedia.com	/	2024-05-03T16:00:01.310Z
AD%5FCover%5F...	2	www.natgeomedia.com	/	Session
ARC	1	www.natgeomedia.com	/	2024-05-03T16:00:01.178Z
ARD	20240503	www.natgeomedia.com	/	2024-05-03T16:00:01.178Z

2024-05-03T16:00:00.390Z → UTC

2024-05-03 24:00:00 -> +8= 台北時間

每天只能看一篇
破解方法

- 方法1: 全部視窗關閉再打看
  - 無效.
  - 因為網站使用 Persistent Cookie
- 方法2:
  - Delete Cookie



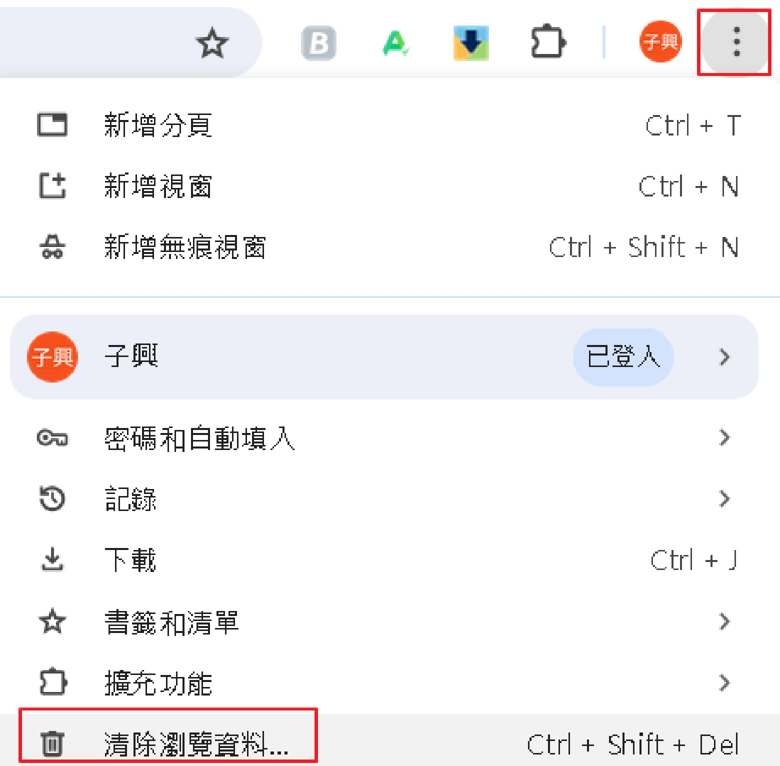
Delete Cookie

Name	Value	Domain	Path	Expires / Max-Age
AD%5FCover%5F...	yes	www.natgeomedia.com	/	2024-05-03T16:00:01.310Z
AD%5FCover%5F...	2	www.natgeomedia.com	/	Session
ARC	1	www.natgeomedia.com	/	2024-05-03T16:00:01.178Z
ARD	20240503	www.natgeomedia.com	/	2024-05-03T16:00:01.178Z

- 方法3: 新增無痕視窗
  - OK
  - 因為無痕視窗不會記錄 Persistent Cookie

每天只能看一篇
破解方法

- 方法4: 清除瀏覽資料
  - OK
  - 刪除 all Cookies



子興

新增分頁 Ctrl + T

新增視窗 Ctrl + N

新增無痕視窗 Ctrl + Shift + N

子興 子興 已登入 ›

密碼和自動填入 ›

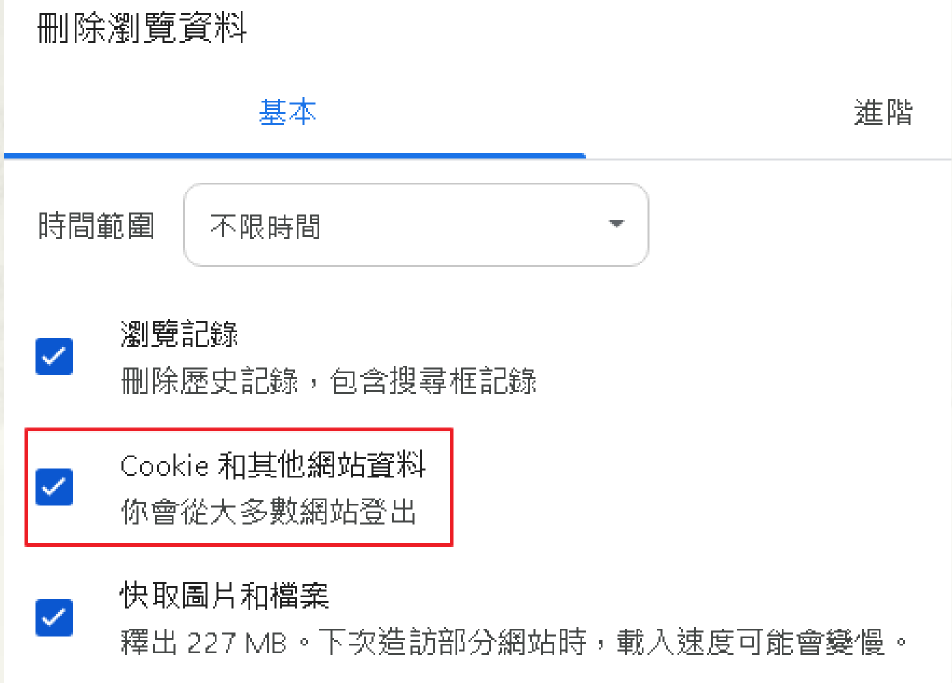
記錄 ›

下載 Ctrl + J

書籤和清單 ›

擴充功能 ›

清除瀏覽資料... Ctrl + Shift + Del



刪除瀏覽資料

基本 進階

時間範圍 不限時間

☑ 瀏覽記錄
刪除歷史記錄，包含搜尋框記錄

☑ Cookie 和其他網站資料
你會從大多數網站登出

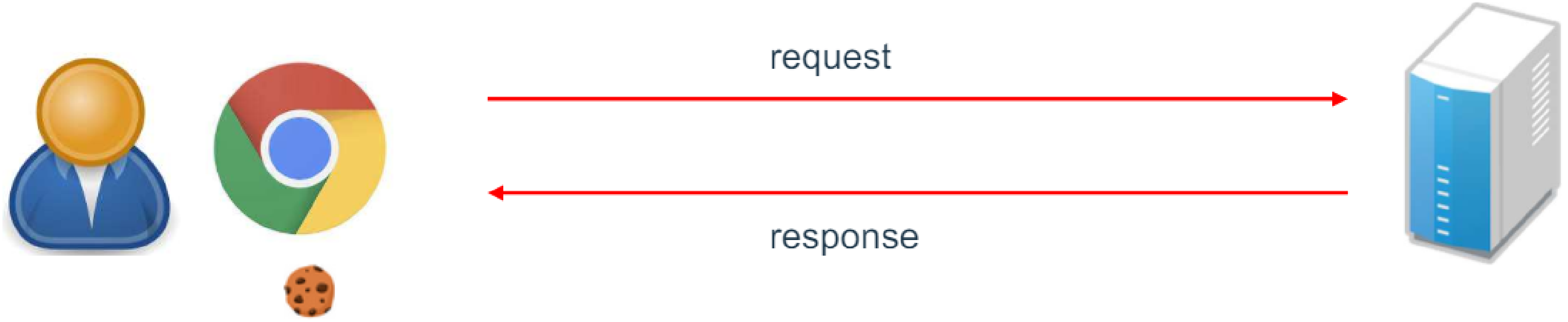
☑ 快取圖片和檔案
釋出 227 MB。下次造訪部分網站時，載入速度可能會變慢。

Cookie 功用之二
權限控管 帳號登入

LoginSession Cookie

Session

- Session是在伺服器端保存的一個數據結構，用來追蹤用戶的狀態，這一個數據可以是任何類別的數。每一個用戶都會有一個獨立的session。當程序需要為某個客戶端的請求創建一個session的時候，服務器首先檢查這個客戶端的請求裡是否已包含了一個session標識 - 稱為 session id，如果已包含一個session id則說明以前已經為此客戶端創建過session，服務器就按照session id把這個 session檢索出來使用。
- 在談論session機制的時候，常常聽到這樣一種誤解「只要關閉瀏覽器，session就消失了」。其實這並不完全正確，當使用者直接關閉瀏覽器時，其實後端伺服器並不知道，所以使用者的session id依舊存在伺服器端，直到session time out才會回收。



LoginSession Cookie

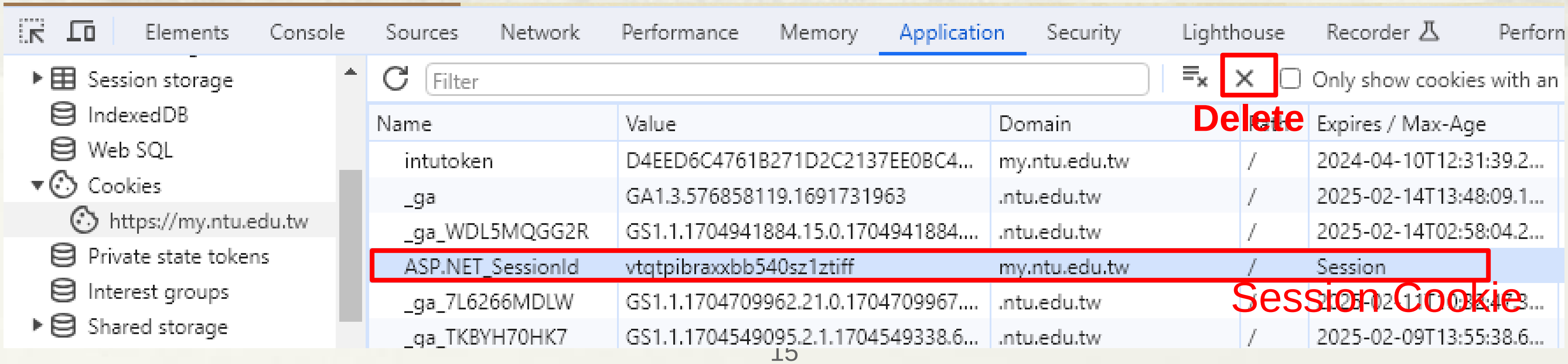
- For Login Credentials.
- One and Only One.
- Server 端之 Cookie 驗證僅比對其值，Cookie Attributes 僅是設定 Browser 如何控管 Cookie，與驗證無關
- 同一個 Cookie 可同時在多個裝置登入
  - 除非有額外加上限制條件，例如: Client IP, User Agent …
- 可記錄多組 Key Pairs 來辨識使用者身分
  - User ID
  - Client IP
  - Browser: User Agent
  - ….

How to Find LoginSession Cookie?

- Cookie Attributes
  - Naming Rule
    - ASP.NET_SessionId, PHPSESSID, *SID, *SESSION_ID
  - Attribute
    - HttpOnly, Secure, Samesite
  - Path: /
- When to Create
  - Create by WebServer (HTTP Response)
  - Method1. 登入畫面，輸入帳密並送出
  - Method2. 使用已登入 URL 連結
    - https://my.ntu.edu.tw/assetManagement/consumables.aspx
- Try & Error
  - 刪除 or 更改 Cookie 值，Reload 頁面, 看是否會被登出

如何登出 myNTU？

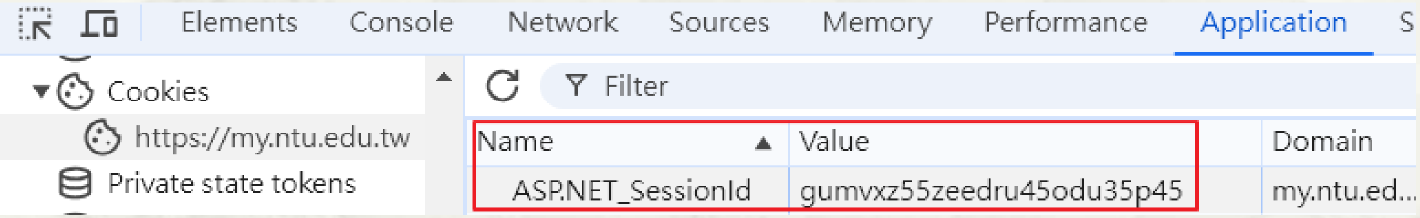
- 帳號簽到退 https://my.ntu.edu.tw/mattend/ssi.aspx
  - Find LoginSession Cookie: ASP.NET_SessionId
- 方法1: Click “登出”
  - LoginSession Cookie 在 Server 刪除
- 方法2: 關閉”所有” Browser視窗 (僅關閉當前視窗無效)
  - LoginSession Cookie 仍保留在 Server
- 方法3:
  - 刪除 Browser Cookie
  - LoginSession Cookie 仍保留在 Server



Name	Value	Domain	Path	Expires / Max-Age
intutoken	D4EED6C4761B271D2C2137EE0BC4...	my.ntu.edu.tw	/	2024-04-10T12:31:39.2...
_ga	GA1.3.576858119.1691731963	.ntu.edu.tw	/	2025-02-14T13:48:09.1...
_ga_WDL5MQGG2R	GS1.1.1704941884.15.0.1704941884....	.ntu.edu.tw	/	2025-02-14T02:58:04.2...
ASP.NET_SessionId	vtqtpibraxxbb540sz1ztiff	my.ntu.edu.tw	/	Session
_ga_7L6266MDLW	GS1.1.1704709962.21.0.1704709967....	.ntu.edu.tw	/	[illegible]
_ga_TKBYH70HK7	GS1.1.1704549095.2.1.1704549338.6...	.ntu.edu.tw	/	2025-02-09T13:55:38.6...

登出 vs. 關閉所有視窗 (LoginSession Cookie 是否仍保留在 Server)

- Step1.登入”帳號簽到退”
  - https://my.ntu.edu.tw/mattend/ssi.aspx
  - 保留 LoginSession Cookie 資訊



Name	Value	Domain
ASP.NET_SessionId	gumvxz55zeedru45odu35p45	my.ntu.ed...

- Step2.關閉所有視窗
- Step3.開啟”帳號簽到退”視窗
  - 按下”登入” (不需輸入帳密)
  - 回到上一頁
  - F12 貼上保留之 ASP.NET_SessionId 值
  - Reload 後可順利登入

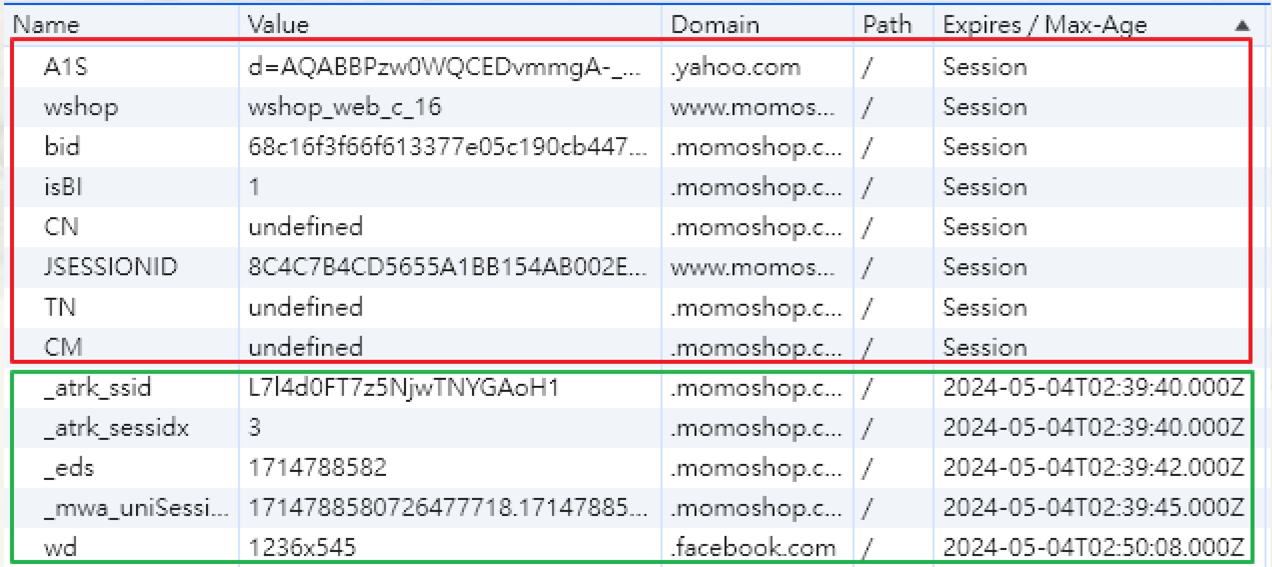
為何關閉所有 **Browser** 視窗 有時可登出、有時卻不行**?**

Demo

- 關閉所有 Browser 視窗後，需重新登入
  - myNTU
    - https://my.ntu.edu.tw/
  - 網路銀行
- 關閉所有 Browser 視窗後，不需重新登入
  - Google
    - https://www.google.com/
  - PChome 24H
    - https://24h.pchome.com.tw/
  - MOMO 購物網
    - https://www.momoshop.com.tw/

原因 : Expire Attribute of Cookie

- Session Cookie(Temporary)
  - 無 Expires日期， Browser 全部關閉就會消失.
- Persistent Cookie
  - 有 Expires 日期(預設GMT時區)，Browser 全部關閉或重開機後仍會存在。



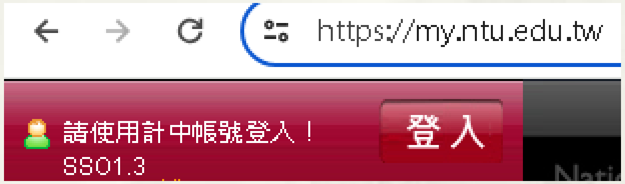
Name	Value	Domain	Path	Expires / Max-Age
A1S	d=AQABBPzw0WQCEDvmmgA-_...	.yahoo.com	/	Session
wshop	wshop_web_c_16	www.momos...	/	Session
bid	68c16f3f66f613377e05c190cb447...	.momoshop.c...	/	Session
isBI	1	.momoshop.c...	/	Session
CN	undefined	.momoshop.c...	/	Session
JSESSIONID	8C4C7B4CD5655A1BB154AB002E...	www.momos...	/	Session
TN	undefined	.momoshop.c...	/	Session
CM	undefined	.momoshop.c...	/	Session
_atrk_ssid	L7l4d0FT7z5NjwTNYGAoH1	.momoshop.c...	/	2024-05-04T02:39:40.000Z
_atrk_sessidx	3	.momoshop.c...	/	2024-05-04T02:39:40.000Z
_eds	1714788582	.momoshop.c...	/	2024-05-04T02:39:42.000Z
_mwa_uniSessi...	1714788580726477718.17147885...	.momoshop.c...	/	2024-05-04T02:39:45.000Z
wd	1236x545	.facebook.com	/	2024-05-04T02:50:08.000Z

Session Cookie

Persistent Cookie

Session Cookie

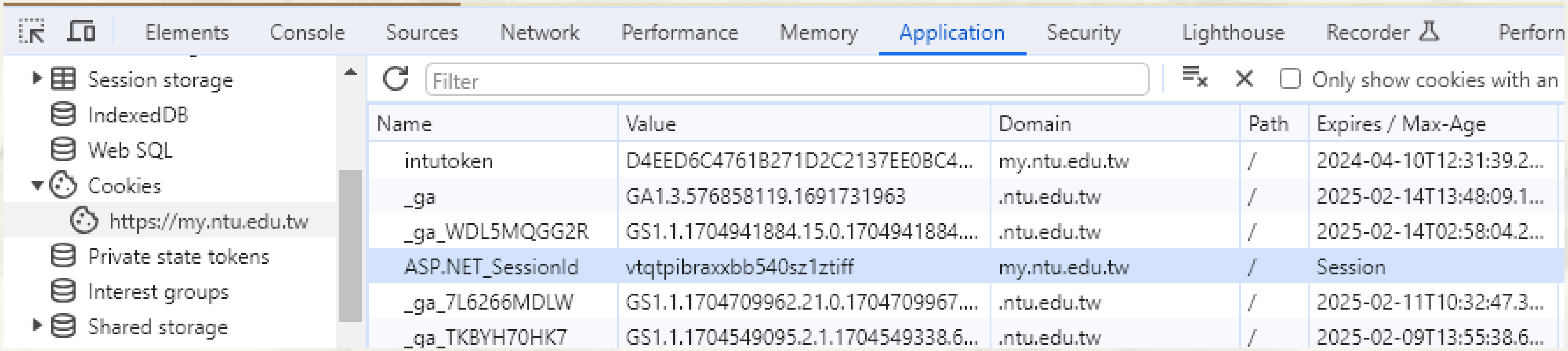
- myNTU



https://my.ntu.edu.tw

請使用計中帳號登入！

SSO1.3

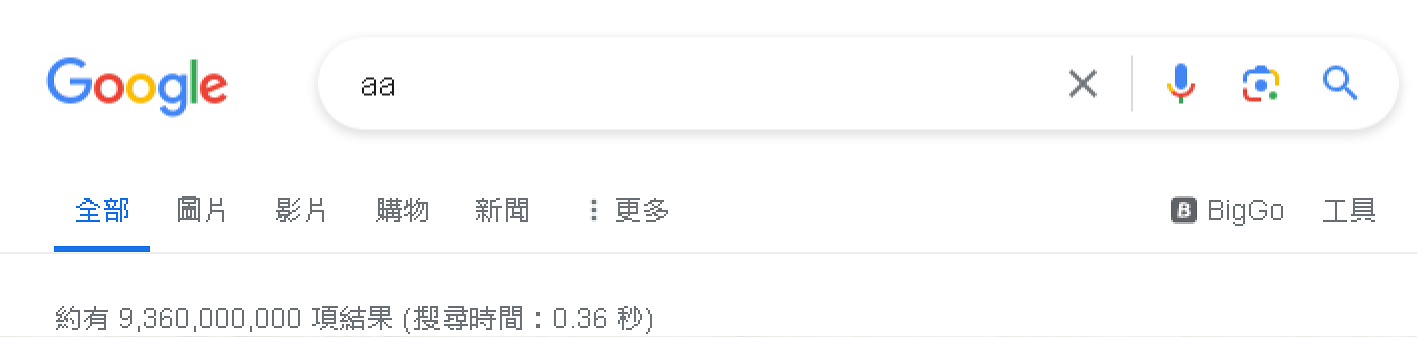


Name	Value	Domain	Path	Expires / Max-Age
intutoken	D4EED6C4761B271D2C2137EE0BC4...	my.ntu.edu.tw	/	2024-04-10T12:31:39.2...
_ga	GA1.3.576858119.1691731963	.ntu.edu.tw	/	2025-02-14T13:48:09.1...
_ga_WDL5MQGG2R	GS1.1.1704941884.15.0.1704941884....	.ntu.edu.tw	/	2025-02-14T02:58:04.2...
ASP.NET_SessionId	vtqtpibraxxbb540sz1ztiff	my.ntu.edu.tw	/	Session
_ga_7L6266MDLW	GS1.1.1704709962.21.0.1704709967....	.ntu.edu.tw	/	2025-02-11T10:32:47.3...
_ga_TKBYH70HK7	GS1.1.1704549095.2.1.1704549338.6...	.ntu.edu.tw	/	2025-02-09T13:55:38.6...

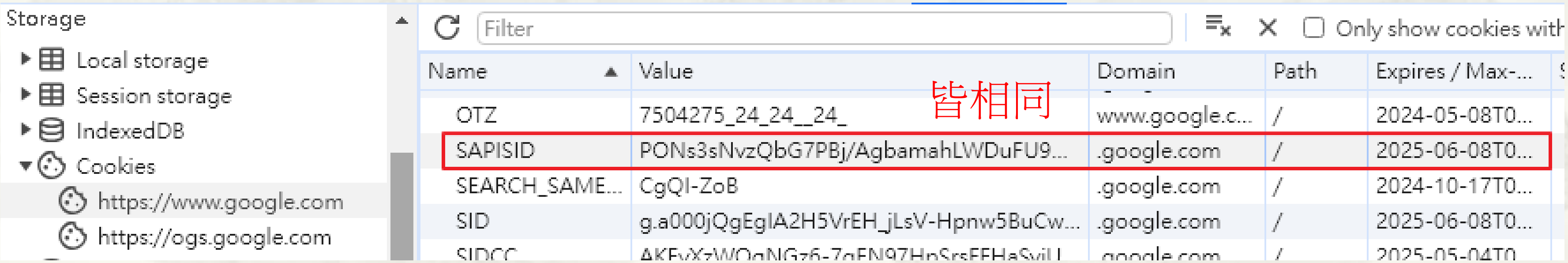
Session Cookie

Persistent Cookie

- www.google.com



約有 9,360,000,000 項結果 (搜尋時間：0.36 秒)

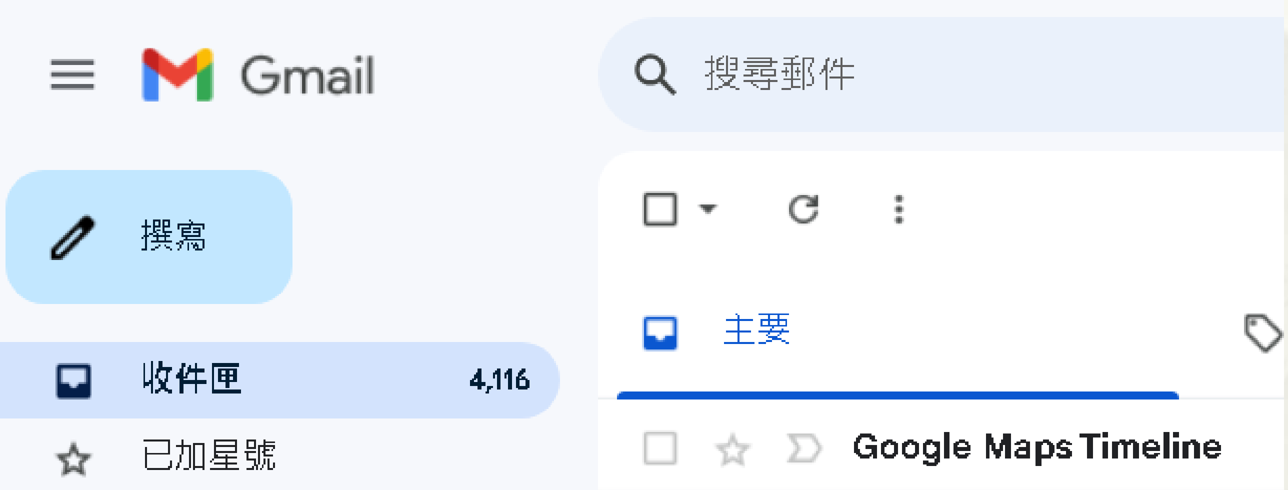


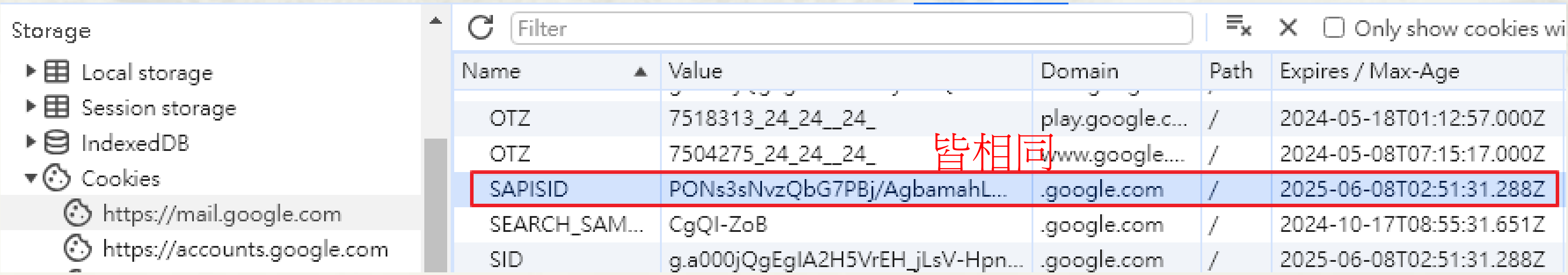
Name	Value	Domain	Path	Expires / Max-...
OTZ	7504275_24_24__24_	www.google.c...	/	2024-05-08T0...
SAPISID	PONs3sNvzQbG7PBj/AgbamahLWDuFU9...	.google.com	/	2025-06-08T0...
SEARCH_SAME...	CgQI-ZoB	.google.com	/	2024-10-17T0...
SID	g.a000jQgEgIA2H5VrEH_jLsV-Hpnw5BuCw...	.google.com	/	2025-06-08T0...
SIDCC	AKEyXzWQqNGz6-7qFN97HpSrsFFHaSvjLL	.google.com	/	2025-05-04T0

皆相同

Persistent Cookie

- mail.google.com



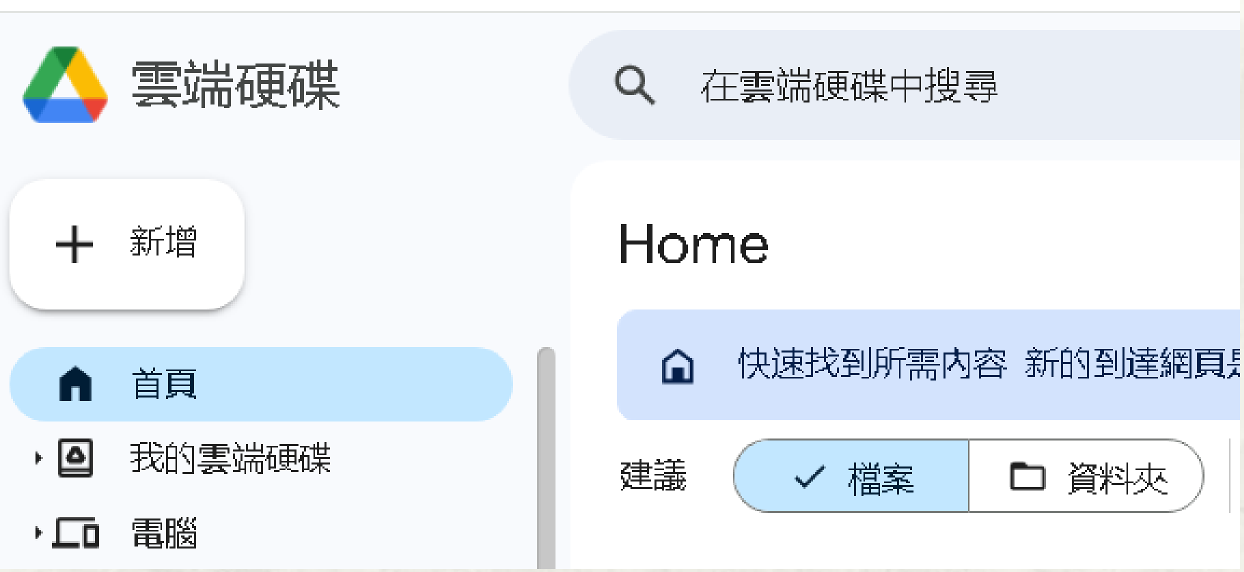


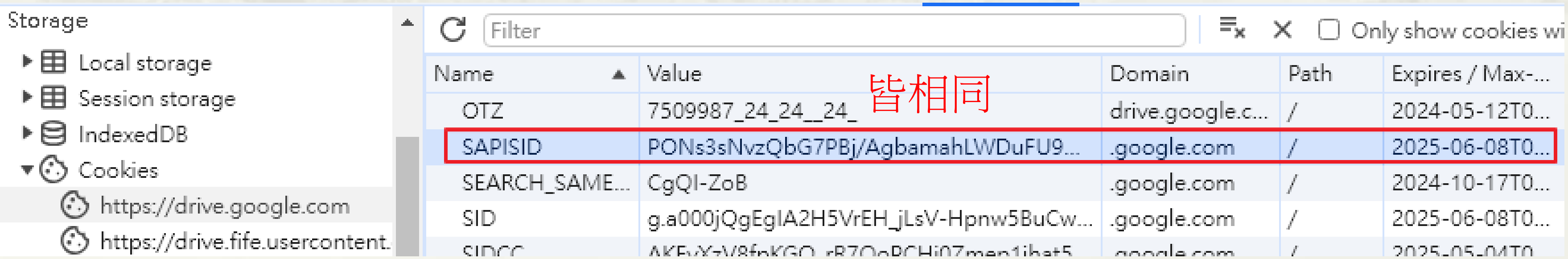
Name	Value	Domain	Path	Expires / Max-Age
OTZ	7518313_24_24__24_	play.google.c...	/	2024-05-18T01:12:57.000Z
OTZ	7504275_24_24__24_	www.google....	/	2024-05-08T07:15:17.000Z
SAPISID	PONs3sNvzQbG7PBj/AgbamahL...	.google.com	/	2025-06-08T02:51:31.288Z
SEARCH_SAM...	CgQI-ZoB	.google.com	/	2024-10-17T08:55:31.651Z
SID	g.a000jQgEgIA2H5VrEH_jLsV-Hpn...	.google.com	/	2025-06-08T02:51:31.288Z

皆相同

Persistent Cookie

- drive.google.com



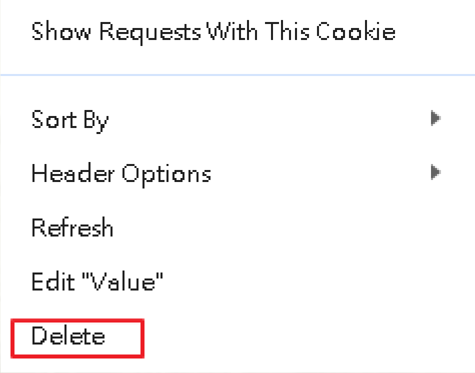


皆相同

Name	Value	Domain	Path	Expires / Max-...
OTZ	7509987_24_24__24_	drive.google.c...	/	2024-05-12T0...
SAPISID	PONs3sNvzQbG7PBj/AgbamahLWDuFU9...	.google.com	/	2025-06-08T0...
SEARCH_SAME...	CgQI-ZoB	.google.com	/	2024-10-17T0...
SID	g.a000jQgEgIA2H5VrEH_jLsV-Hpnw5BuCw...	.google.com	/	2025-06-08T0...
SIDCC	AKEyXzV8fpKGO_rB7OoRCHi0Zmep1ibat5	.google.com	/	2025-05-04T0

Google 所有服務

- 刪除 Cookie: SAPISID
  - 全部登出



Show Requests With This Cookie

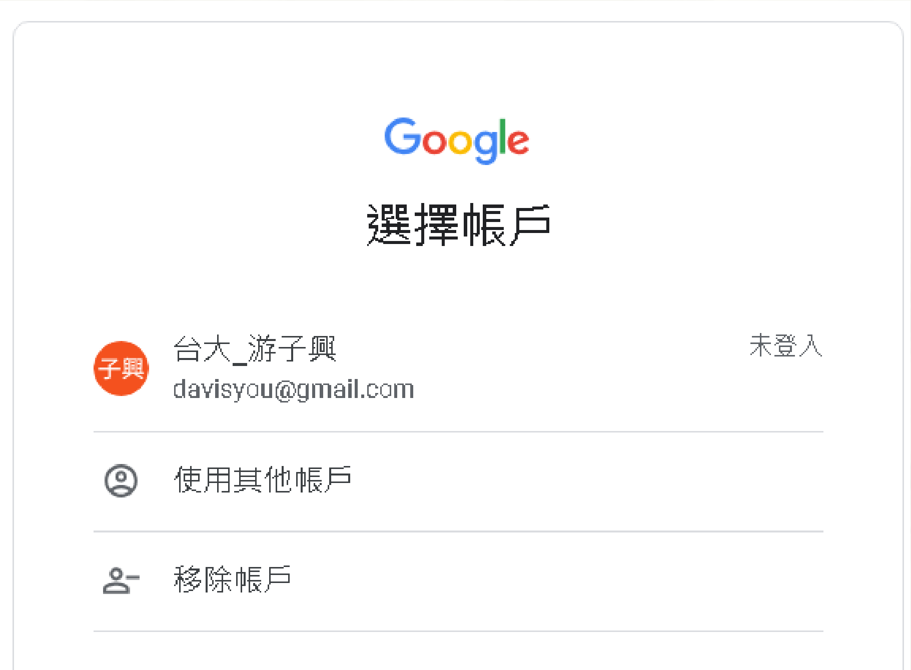
Sort By ▸

Header Options ▸

Refresh

Edit "Value"

Delete



Google

選擇帳戶

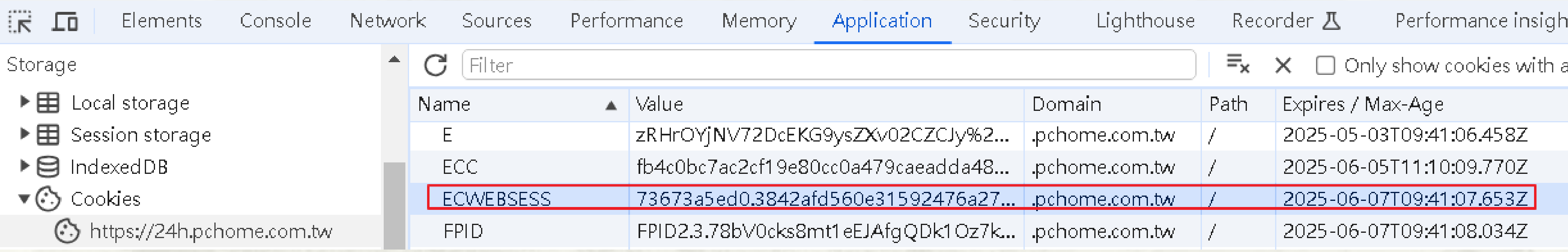
子興 台大_游子興 davisyou@gmail.com 未登入

使用其他帳戶

移除帳戶

Persistent Cookie

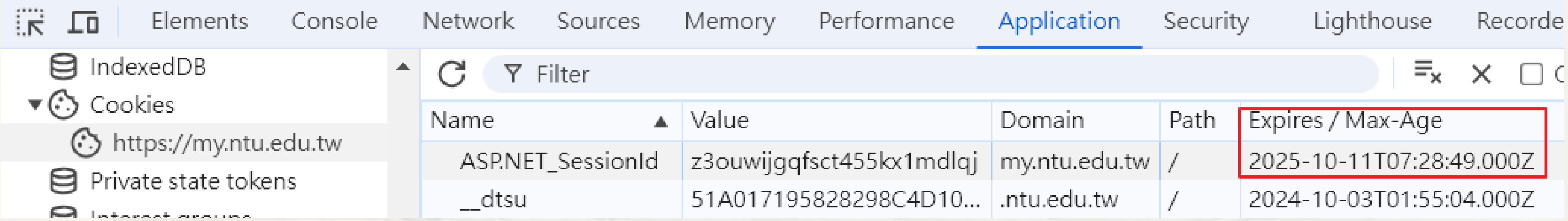
- PChome 24H
  - https://24h.pchome.com.tw/



Name	Value	Domain	Path	Expires / Max-Age
E	zRHrOYjNV72DcEKG9ysZXv02CZCJy%2...	.pchome.com.tw	/	2025-05-03T09:41:06.458Z
ECC	fb4c0bc7ac2cf19e80cc0a479caeadda48...	.pchome.com.tw	/	2025-06-05T11:10:09.770Z
ECWEBSESS	73673a5ed0.3842afd560e31592476a27...	.pchome.com.tw	/	2025-06-07T09:41:07.653Z
FPID	FPID2.3.78bV0cks8mt1eEJAfgQDk1Oz7k...	.pchome.com.tw	/	2025-06-07T09:41:08.034Z

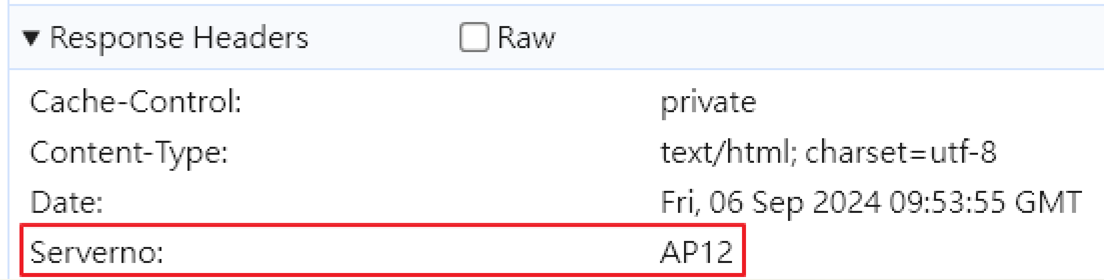
Change “Session Cookie” to “Persistent Cookie” ??

- myNTU 帳號簽到退
  - https://my.ntu.edu.tw/mattend/ssi.aspx



Name	Value	Domain	Path	Expires / Max-Age
ASP.NET_SessionId	z3ouwijgqfsct455kx1mdlqj	my.ntu.edu.tw	/	2025-10-11T07:28:49.000Z
__dtsu	51A017195828298C4D10...	.ntu.edu.tw	/	2024-10-03T01:55:04.000Z

- 可以，但是
  - LoginSession Cookie 真正 Timeout 是由伺服器端控制
  - 重複登入必須都是登入相同 AP Server

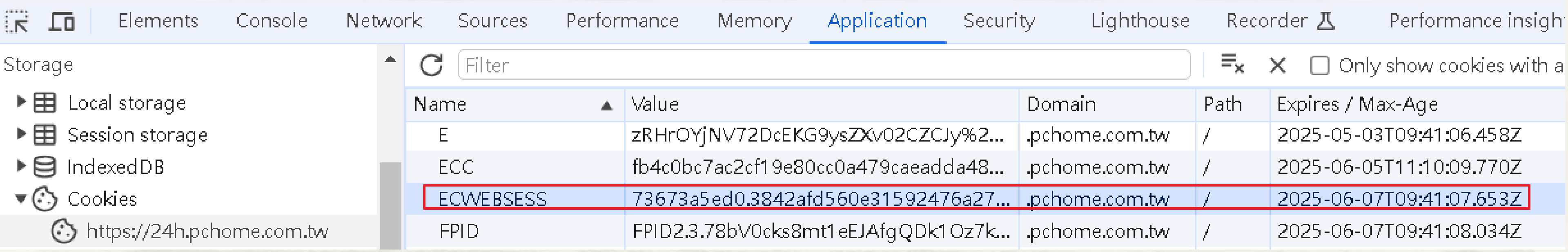


Cache-Control:	private
Content-Type:	text/html; charset=utf-8
Date:	Fri, 06 Sep 2024 09:53:55 GMT
Serverno:	AP12

使用 LoginSession Cookie 免帳密登入

Demo
使用 Cookie 免帳密登入

- PChome 24H
  - https://24h.pchome.com.tw/
  - Find LoginSession Cookie



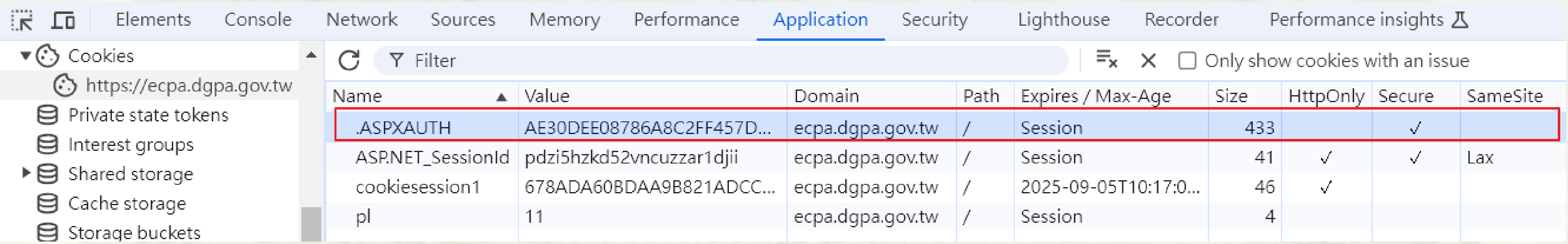
Name	Value	Domain	Path	Expires / Max-Age
E	zRHrOYjNV72DcEKG9ysZXv02CZCJy%2...	.pchome.com.tw	/	2025-05-03T09:41:06.458Z
ECC	fb4c0bc7ac2cf19e80cc0a479caeadda48...	.pchome.com.tw	/	2025-06-05T11:10:09.770Z
ECWEBSESS	73673a5ed0.3842afd560e31592476a27...	.pchome.com.tw	/	2025-06-07T09:41:07.653Z
FPID	FPID2.3.78bV0cks8mt1eEJAfgQDk1Oz7k...	.pchome.com.tw	/	2025-06-07T09:41:08.034Z

  - 允許 Client IP 變更，仍保持登入

Demo
使用 Cookie 免帳密登入

行政院人事行政總處
人事服務網 eCPA

- https://ecpa.dgpa.gov.tw/
- Find LoginSession Cookie



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite
.ASPXAUTH	AE30DEE08786A8C2FF457D...	ecpa.dgpa.gov.tw	/	Session	433		✓	
ASP.NET_SessionId	pdzi5hzkd52vncuzzar1djii	ecpa.dgpa.gov.tw	/	Session	41	✓	✓	Lax
cookiesession1	678ADA60BDAA9B821ADCC...	ecpa.dgpa.gov.tw	/	2025-09-05T10:17:0...	46	✓		
pl	11	ecpa.dgpa.gov.tw	/	Session	4			

- 允許 Client IP 變更，仍保持登入

免帳密登入
For Command Line Browser

- For 網頁測試程式需模擬帳密登入後頁面
- 案例展示
- Curl -b “cookie=xxxx”
  - myNTU 帳號簽到退: Cookie 正確 vs. 錯誤

```
~# curl -i https://my.ntu.edu.tw/mattend/ssi.aspx
```

```
~# curl -b "ASP.NET_SessionId=xxyyzz" -i https://my.ntu.edu.tw/mattend/ssi.aspx | grep -e 簽到時間 -e AP
```

- sqlmap
  - --cookie=xxxx

免帳密登入
For Command Line Browser

- ELK Heartbeat 網頁定時自動偵測
  - https://my.ntu.edu.tw/ 到勤差假系統 -> 差假統計查詢. (需帳密登入)
  - Config File

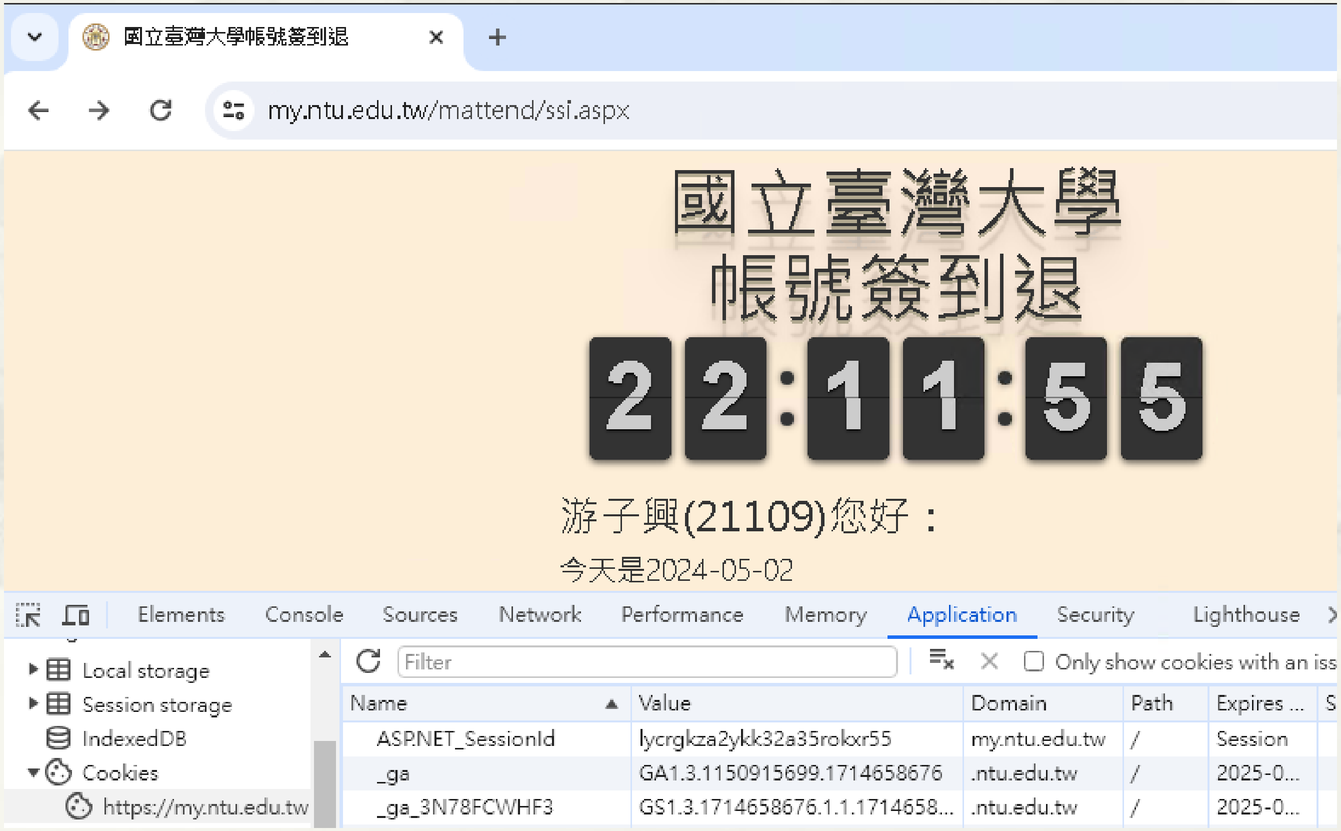
```
- type: http
  schedule: '@every 30s'
  urls: ["https://my.ntu.edu.tw/mattend/Handler.ashx?op=351&t=null&bid=351"]
  id: my.ntu.edu.tw_mattend
  check.request:
    method: POST
    headers:
      'Content-Type': 'application/x-www-form-urlencoded; charset=UTF-8'
      'Cookie': 'ASP.NET_SessionId=j5cq2yjk51pqk4pcsevhoa4d'
    body: "sY=2021&org1=&org2=&seqn=&yC=1&qM=p"
  check.response:
    status: [200]
```

Demo
使用 Cookie 免帳密登入

- myNTU
  - 帳號簽到退 https://my.ntu.edu.tw/mattend/ssi.aspx
  - 教室會議室借用系統 https://my.ntu.edu.tw/meetingroom/search.html
  - 財產物品管理 https://my.ntu.edu.tw/assetManagement/consumables.aspx
  - 到勤差假申請/簽核 https://my.ntu.edu.tw/attend2/
- 上述 Client IP 變更後被登出
  - Cookie 中有記錄 Client IP ??

Demo
使用 Cookie 免帳密登入

- 相同 IP 但不同電腦、不同 Browser
  - 可順利登入



國立臺灣大學
帳號簽到退

22:11:55

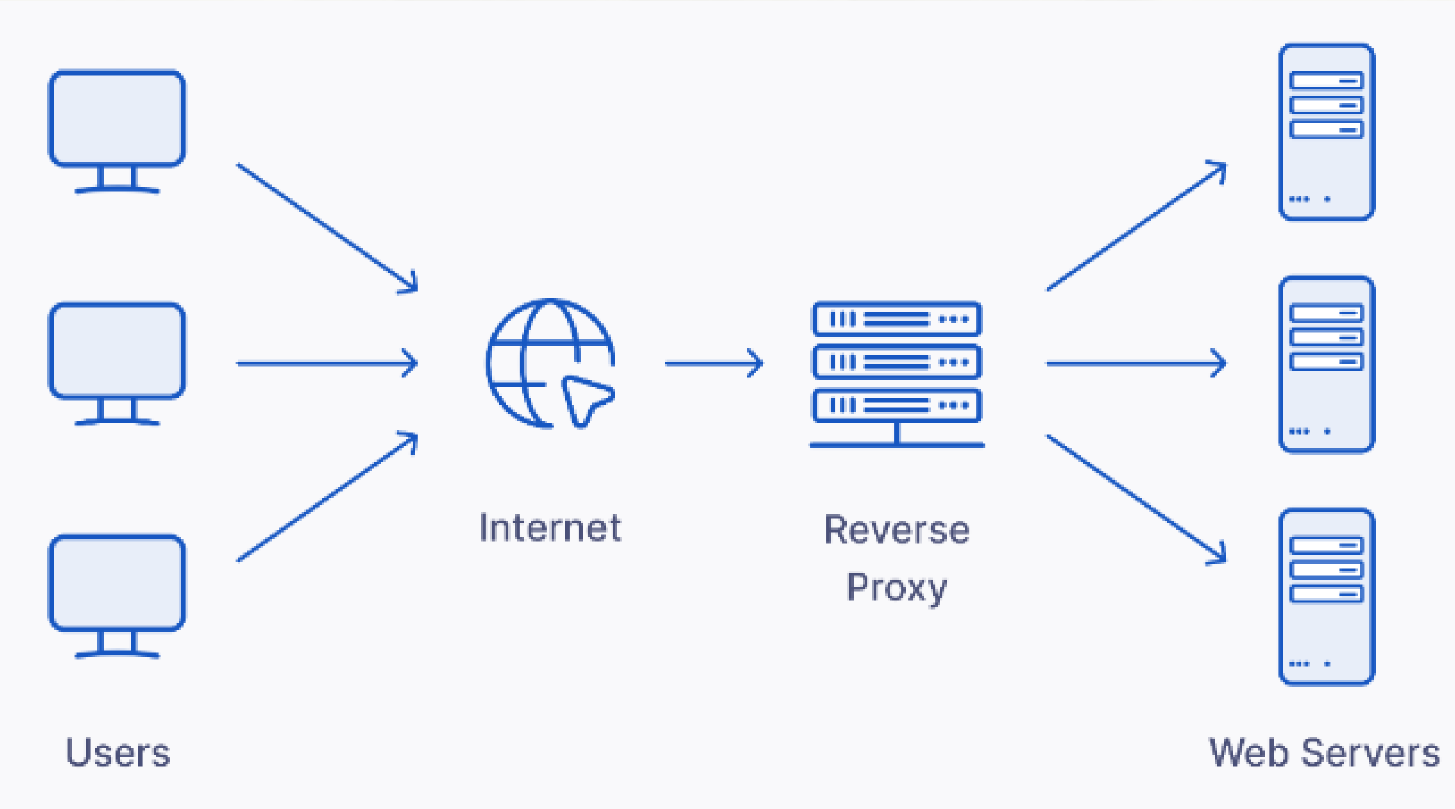
游子興(21109)您好：

今天是2024-05-02

Name ▲	Value	Domain	Path	Expires ...	S
ASP.NET_SessionId	lycrgkza2ykk32a35rokxr55	my.ntu.edu.tw	/	Session	
_ga	GA1.3.1150915699.1714658676	.ntu.edu.tw	/	2025-0...	
_ga_3N78FCWHF3	GS1.3.1714658676.1.1.1714658...	.ntu.edu.tw	/	2025-0...	

WAF(Reverse Proxy)
Load Balance

- 後端有多台 Web Server，而 LoginSession Cookie 由各台 Server 獨立儲存，無法跨 Server 共享.

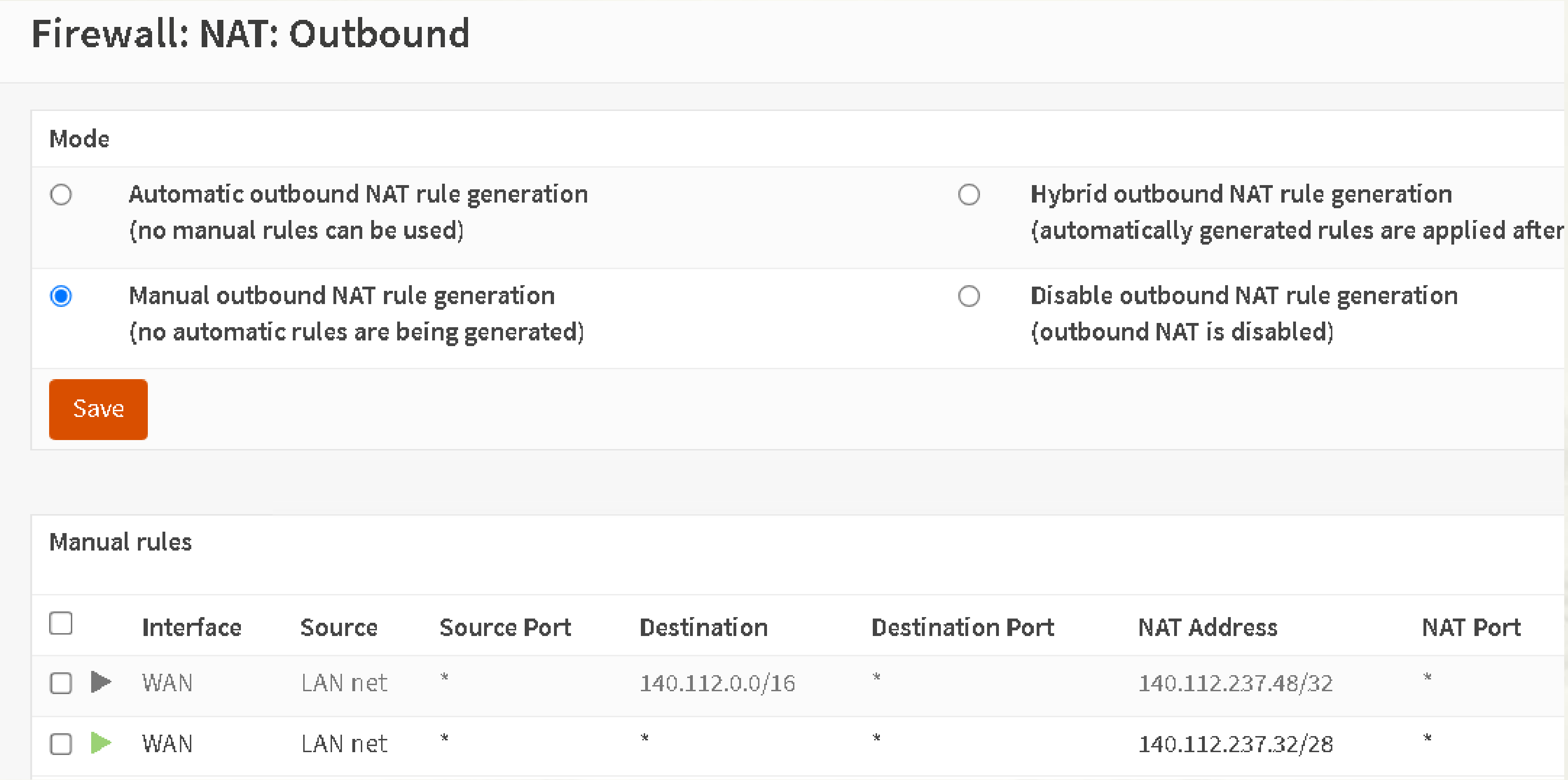


https://www.upguard.com/blog/reverse-proxy-vs-load-balancer

WAF Load Balance
Session Mapping Server 解決方法

- By Client IP: 一段時間內(30 Mins)
  - 缺點: NAT IP Pool 導致 SRC IP 無法固定
  - 案例: myNTU
- Insert an Extra Cookie
  - To track which server the user session belongs to.
  - Support: Citrix/NGINX
  - 優點:
    - 解決 Client IP 無法固定問題
    - 需 Match 兩個 Cookies(LoginSession + Extra Cookie) 才能驗證成功, 增加安全性

NAT IP Pool + Round Robin



Firewall: NAT: Outbound

Mode

○ Automatic outbound NAT rule generation
(no manual rules can be used)

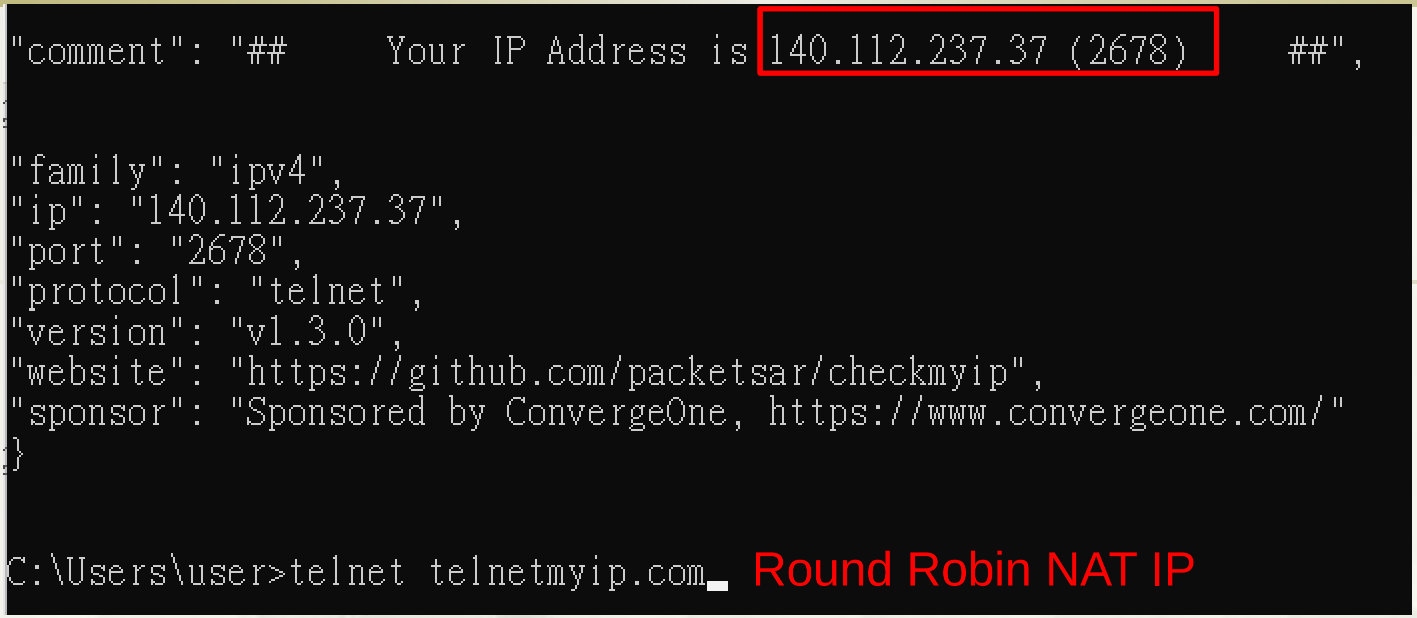
○ Hybrid outbound NAT rule generation
(automatically generated rules are applied after

● Manual outbound NAT rule generation
(no automatic rules are being generated)

○ Disable outbound NAT rule generation
(outbound NAT is disabled)

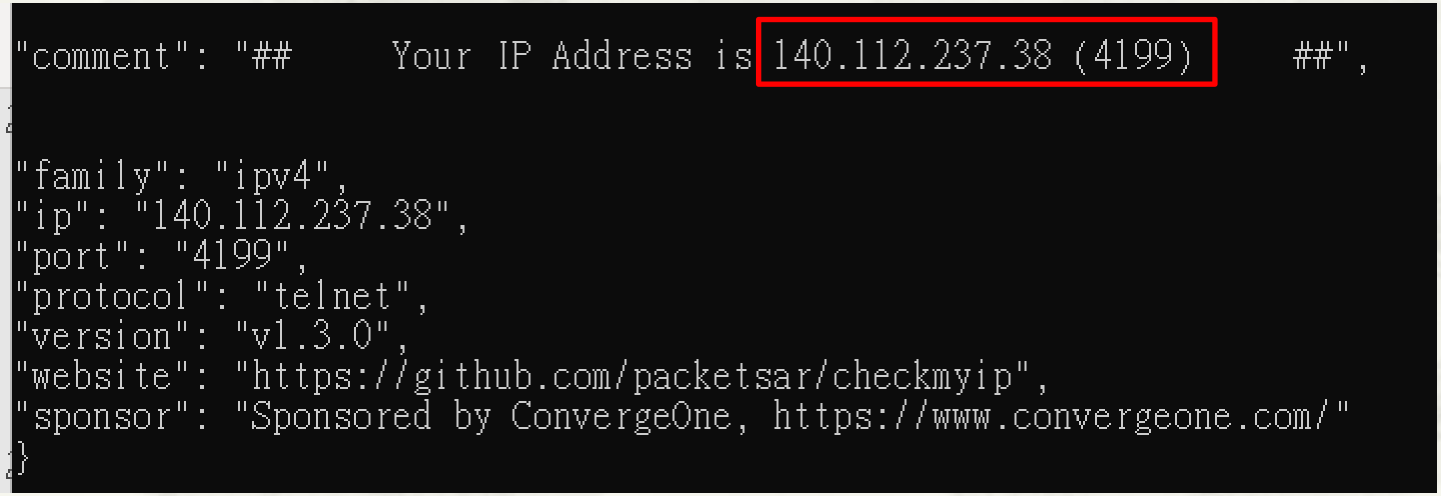
Manual rules

□		Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port
□	▶	WAN	LAN net	*	140.112.0.0/16	*	140.112.237.48/32	*
□	▶	WAN	LAN net	*	*	*	140.112.237.32/28	*

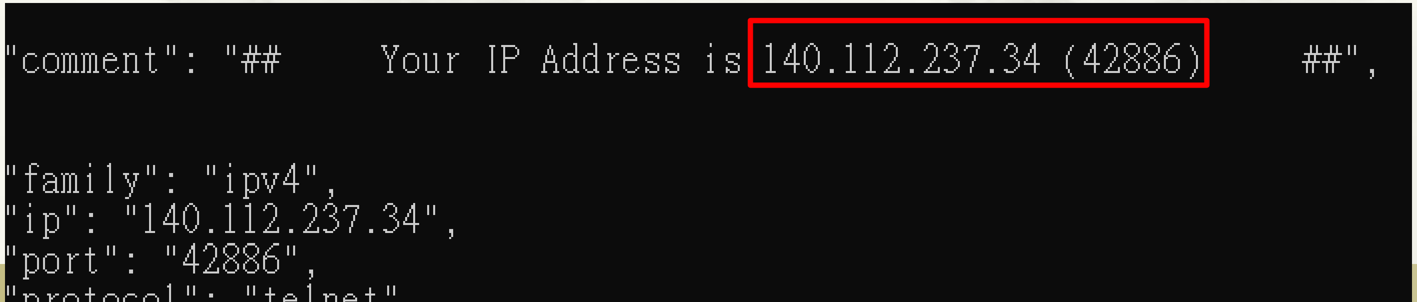


```
"comment": "##     Your IP Address is 140.112.237.37 (2678)     ##",

"family": "ipv4",
"ip": "140.112.237.37",
"port": "2678",
"protocol": "telnet",
"version": "v1.3.0",
"website": "https://github.com/packetsar/checkmyip",
"sponsor": "Sponsored by ConvergeOne, https://www.convergeone.com/"
}

C:\Users\user>telnet telnetmyip.com_
```

Round Robin NAT IP



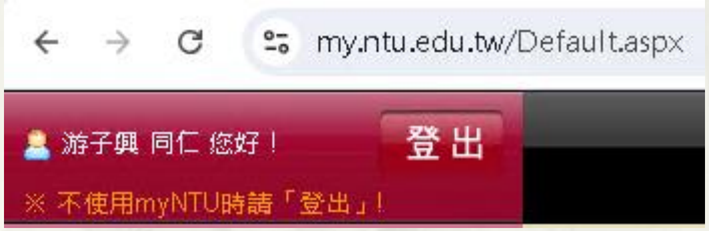
```
"comment": "##     Your IP Address is 140.112.237.38 (4199)     ##",

"family": "ipv4",
"ip": "140.112.237.38",
"port": "4199",
"protocol": "telnet",
"version": "v1.3.0",
"website": "https://github.com/packetsar/checkmyip",
"sponsor": "Sponsored by ConvergeOne, https://www.convergeone.com/"
}
```



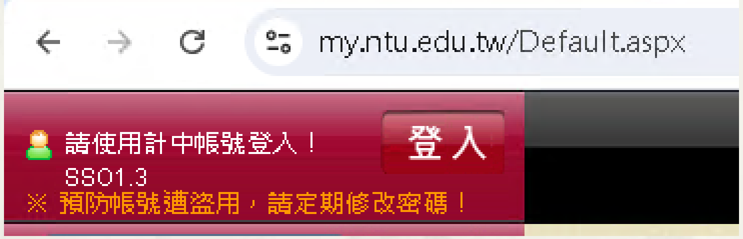
```
"comment": "##     Your IP Address is 140.112.237.34 (42886)     ##",

"family": "ipv4",
"ip": "140.112.237.34",
"port": "42886",
"protocol": "telnet",
```

Refresh 頁面更換 NAT IP
若分配至別台 AP Server，就會被登出

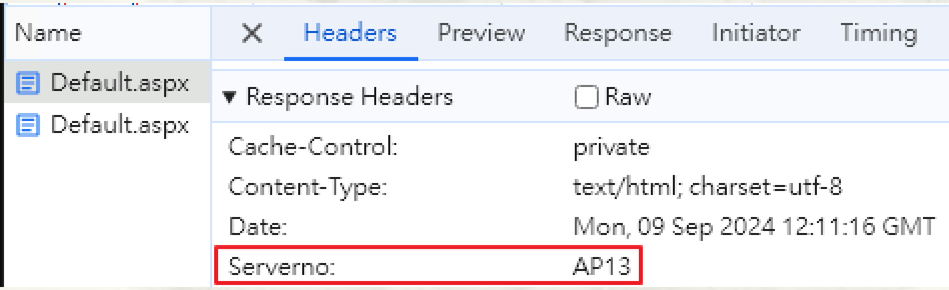
- https://my.ntu.edu.tw/Default.aspx



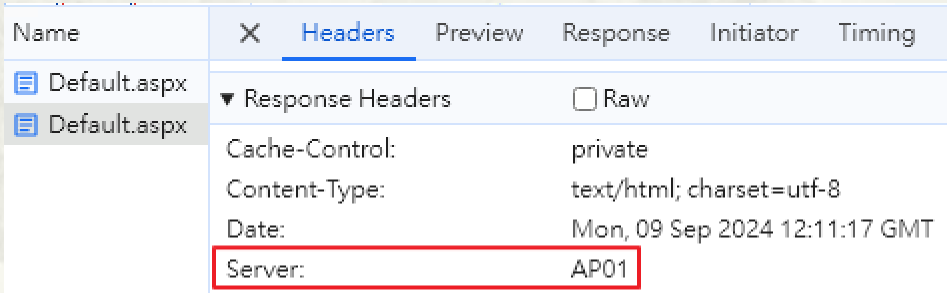
※ 不使用myNTU時請「登出」！



SSO1.3
※ 預防帳號遭盜用，請定期修改密碼！



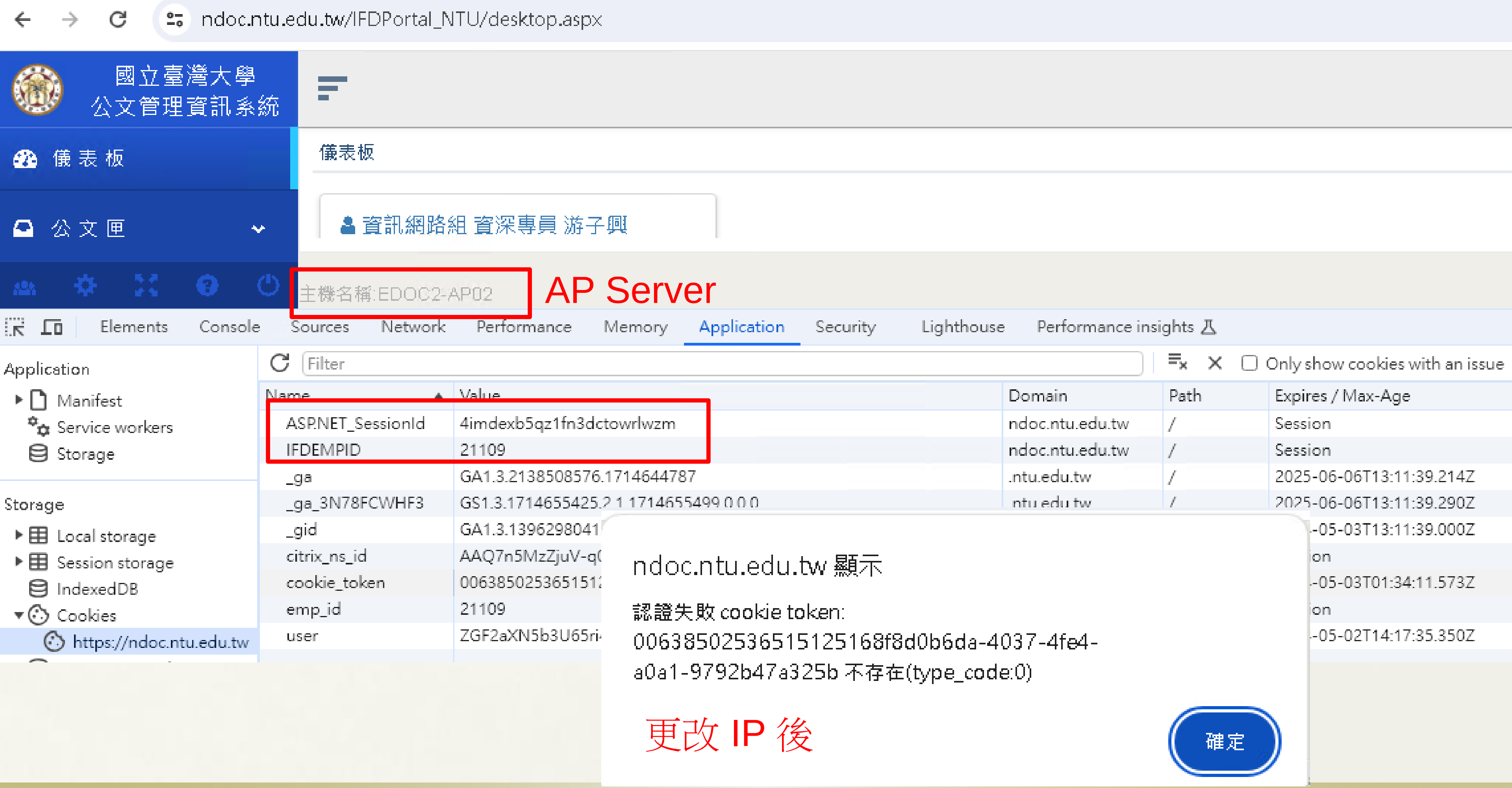
```
Cache-Control:      private
Content-Type:       text/html; charset=utf-8
Date:               Mon, 09 Sep 2024 12:11:16 GMT
Serverno:           AP13
```



```
Cache-Control:      private
Content-Type:       text/html; charset=utf-8
Date:               Mon, 09 Sep 2024 12:11:17 GMT
Server:             AP01
```

公文系統

- https://ndoc.ntu.edu.tw/IFDPortal_NTU/login.aspx



主機名稱:EDOC2-AP02

AP Server

Name	Value	Domain	Path	Expires / Max-Age
ASP.NET_SessionId	4imdexb5qz1fn3dctowrlwzm	ndoc.ntu.edu.tw	/	Session
IFDEMPID	21109	ndoc.ntu.edu.tw	/	Session
_ga	GA1.3.2138508576.1714644787	.ntu.edu.tw	/	2025-06-06T13:11:39.214Z
_ga_3N78FCWHF3	GS1.3.1714655425.2.1.1714655499.0.0.0	.ntu.edu.tw	/	2025-06-06T13:11:39.290Z
_gid	GA1.3.1396298041			-05-03T13:11:39.000Z
citrix_ns_id	AAQ7n5MzZjuV-q(			ion
cookie_token	006385025365151:			-05-03T01:34:11.573Z
emp_id	21109			ion
user	ZGF2aXN5b3U65ri			-05-02T14:17:35.350Z

ndoc.ntu.edu.tw 顯示

認證失敗 cookie token:
00638502536515125168f8d0b6da-4037-4fe4-a0a1-9792b47a325b 不存在(type_code:0)

更改 IP 後

確定

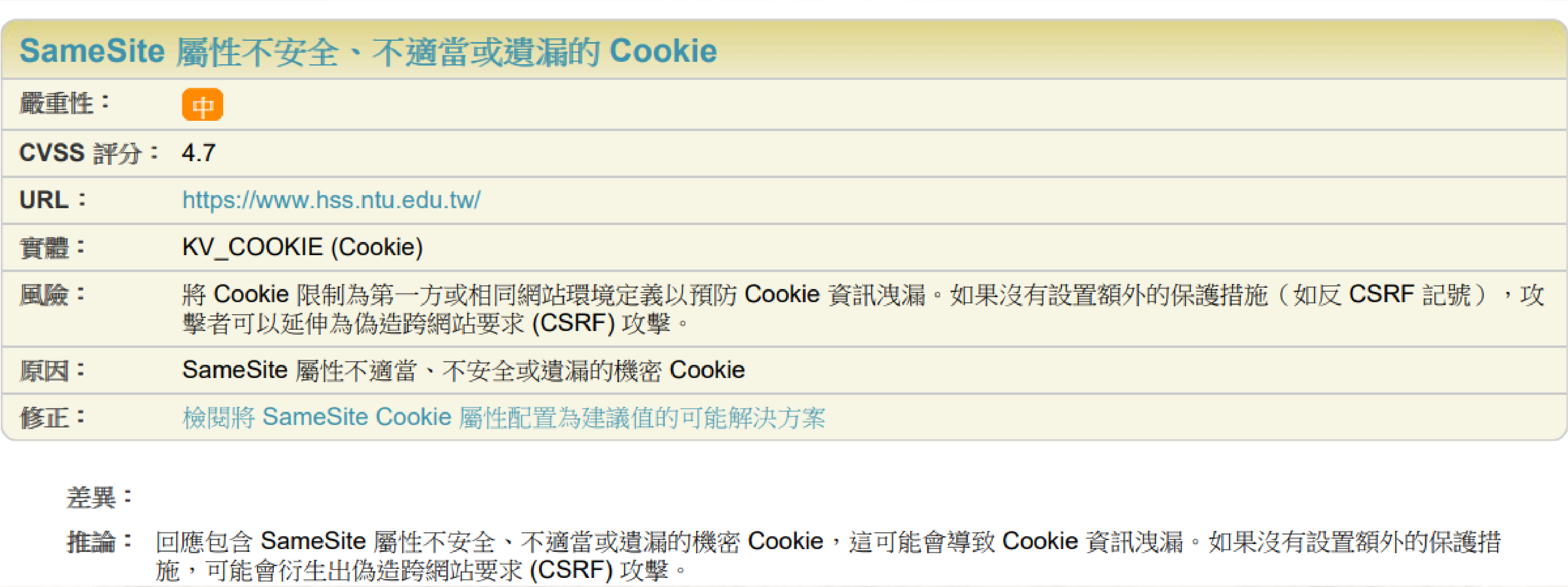
LoginSession vs. Normal Cookie

Cookie	Created by	Stored @	個數	Name(命名規則)	Value
LoginSession Cookie	Server	Both	One	By WebServer (SSID, SESSION_ID)	隱密 (值為亂數)
Normal Cookie	Server or Client	Client Only	1 or many	By User (無規則)	非隱密

Cookie	Path(預設值)	Expire Date	用途
LoginSession Cookie	/ (WebServer 設定)	Cookie Attr or Server Session TimeOut	Login Credential
Normal Cookie	目前檔案所在目錄	Cookie Attr	UI Friendly、Statistic

SameSite Attribute

AppScan 報告



SameSite 屬性不安全、不適當或遺漏的 Cookie

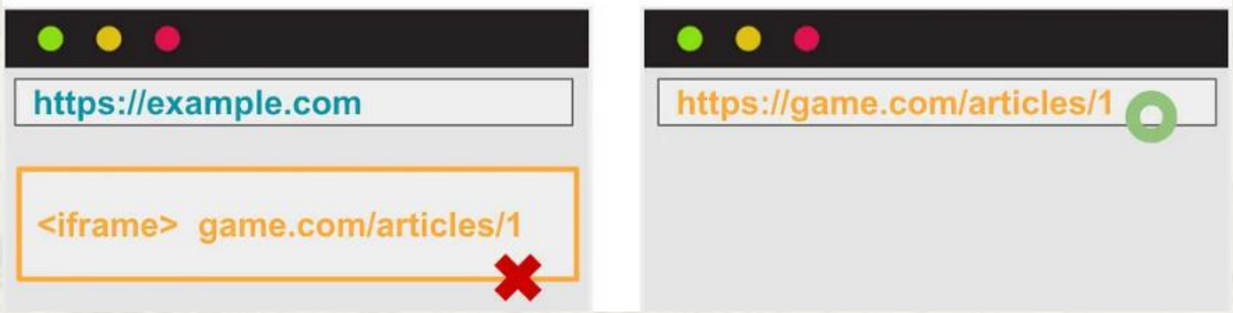
嚴重性：	中
CVSS 評分：	4.7
URL：	https://www.hss.ntu.edu.tw/
實體：	KV_COOKIE (Cookie)
風險：	將 Cookie 限制為第一方或相同網站環境定義以預防 Cookie 資訊洩漏。如果沒有設置額外的保護措施（如反 CSRF 記號），攻擊者可以延伸為偽造跨網站要求 (CSRF) 攻擊。
原因：	SameSite 屬性不適當、不安全或遺漏的機密 Cookie
修正：	檢閱將 SameSite Cookie 屬性配置為建議值的可能解決方案

差異：

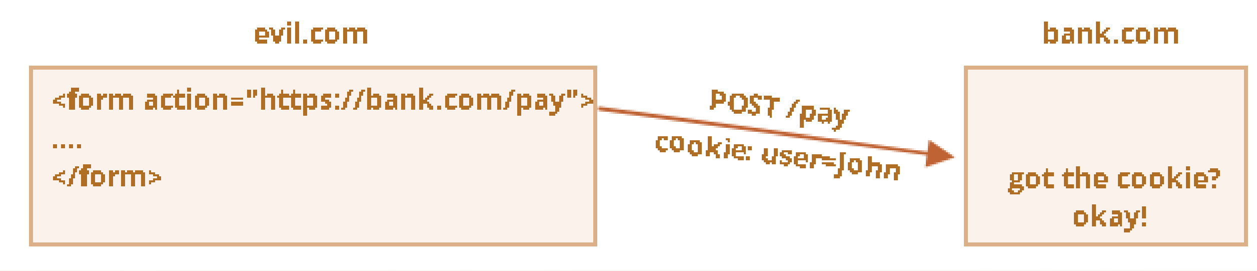
推論： 回應包含 SameSite 屬性不安全、不適當或遺漏的機密 Cookie，這可能會導致 Cookie 資訊洩漏。如果沒有設置額外的保護措施，可能會衍生出偽造跨網站要求 (CSRF) 攻擊。

SameSite Attribute

- Cookie 同源政策(Cookie Same Origin Policy)
  - 連上的網站其 Domain 與原 Cookie 一致，且符合 Path + Secure 之條件，Cookie 就會自動送出
- Chrome 51 版之後新增 SameSite Attribute
- 控制 Cookie 是否允許傳送至不同 Domain 網站
  - Allow or Not Send Cookie to Third-party WebSite

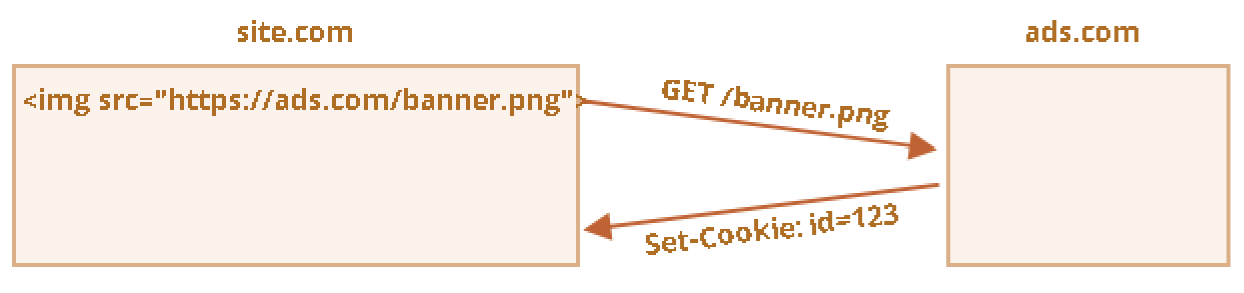


- 目的: 避免跨站請求偽造攻擊 CSRF/XSRF(Cross-Site Request Forgery) attack

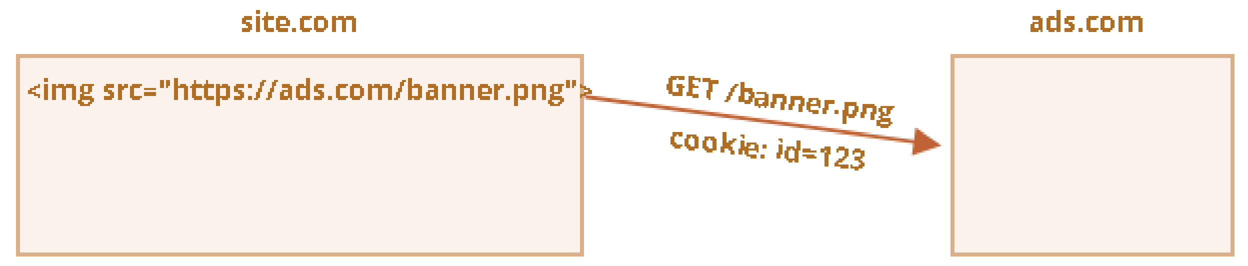


Third-party Cookies

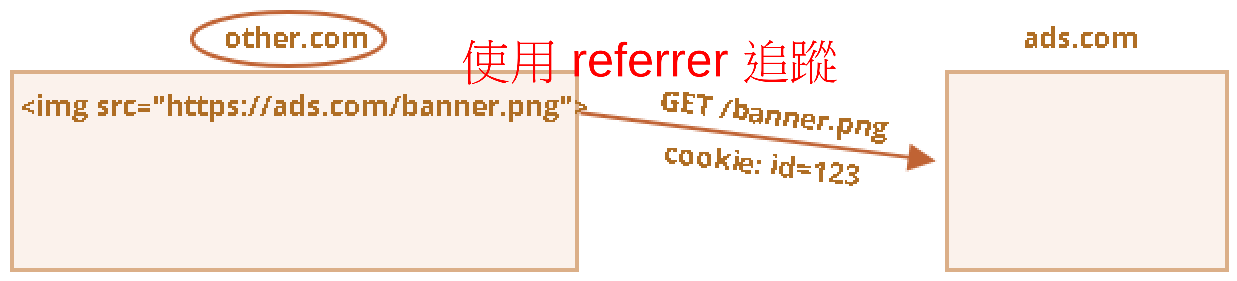
- It’s placed by a domain other than the page the user is visiting.
- First Time



- Next Time

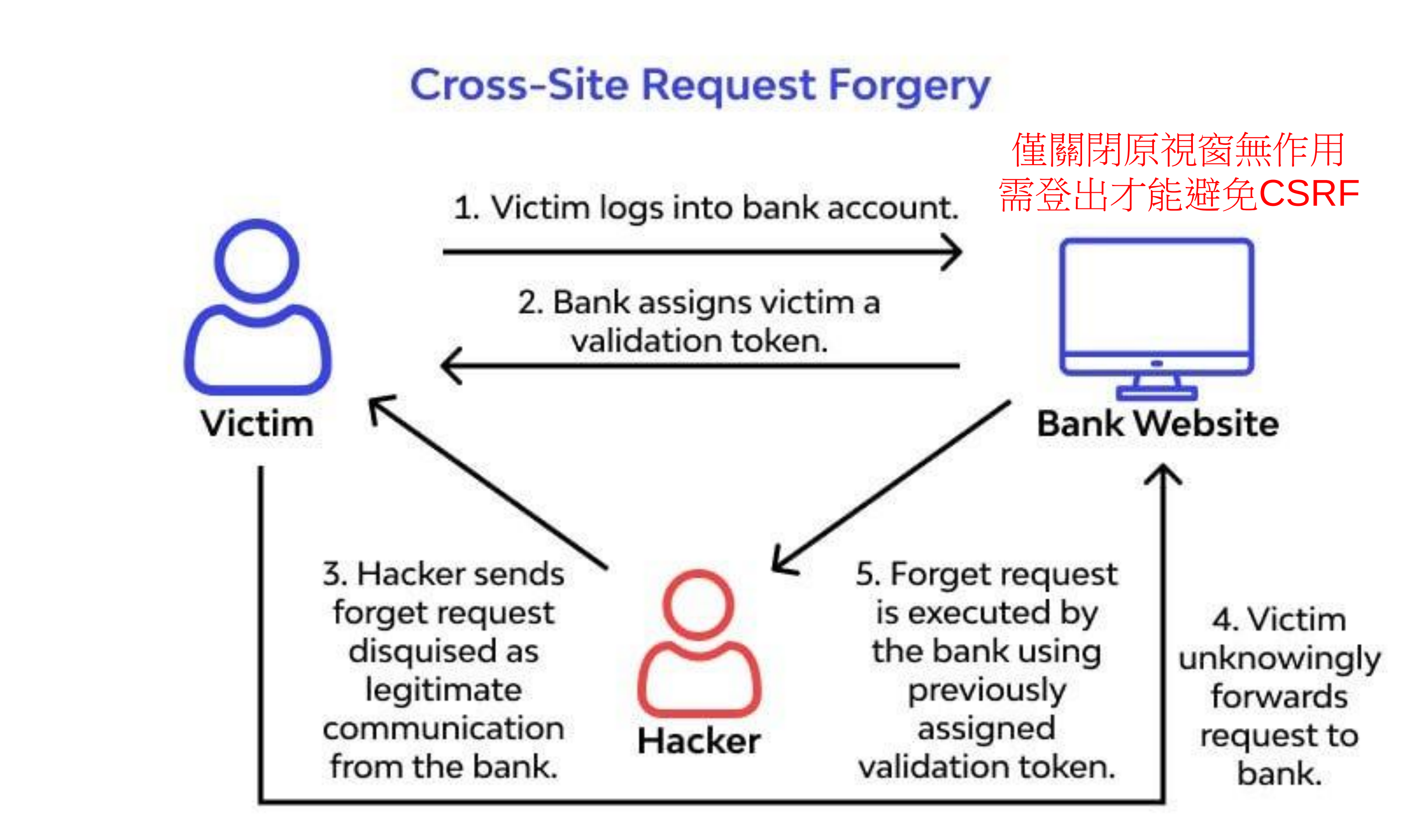


- Track user



使用 referrer 追蹤

跨站請求偽造攻擊
CSRF(Cross-Site Request Forgery) attack


Cross-Site Request Forgery
1. Victim logs into bank account.
2. Bank assigns victim a validation token.
Victim
Bank Website
3. Hacker sends forget request disquised as legitimate communication from the bank.
Hacker
5. Forget request is executed by the bank using previously assigned validation token.
4. Victim unknowingly forwards request to bank.

僅關閉原視窗無作用
需登出才能避免CSRF

https://medium.com/@rajeevranjancom/cross-site-request-forgery-csrf-attack-6949edb9e4

SameSite Attribute Value

- Strict
  - 與目前網頁網址一致，才允許傳送 Cookie
- Lax
  - For Third-party Domain Website: Use “HTTP GET”，才允許傳送 Cookie
- None
  - 無限制 Domain，但必需搭配 Secure=True
- NULL (未輸入)
  - 詳見後面說明
- ※不同瀏覽器可能有不同的結果

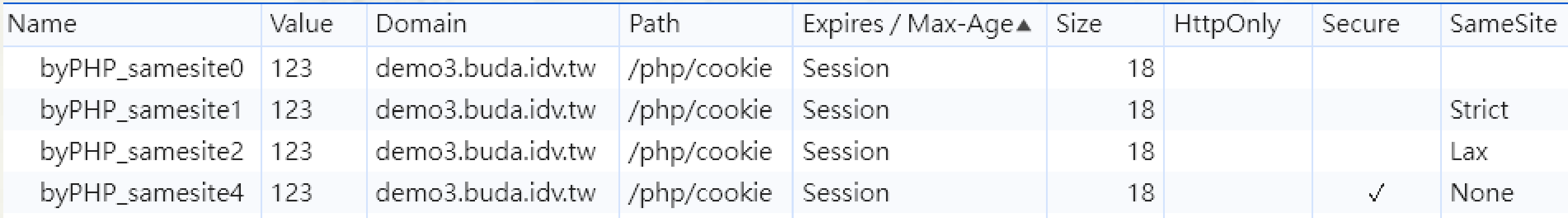
Samesite Attribute
Set Cookie by PHP

- Source Code for cookie_set_attr.php

```
<?php
$cookie_opt1 = array ('samesite' => 'Strict');
$cookie_opt2 = array ('samesite' => 'Lax');
$cookie_opt3 = array ('samesite' => 'None');
$cookie_opt4 = array ('samesite' => 'None','secure' => true);

setcookie(‘byPHP_samesite0’,‘123'); //未設定 samesite
setcookie('byPHP_samesite1','123', $cookie_opt1);
setcookie('byPHP_samesite2','123', $cookie_opt2);
setcookie('byPHP_samesite3','123', $cookie_opt3);
setcookie('byPHP_samesite4','123', $cookie_opt4);
?>
```

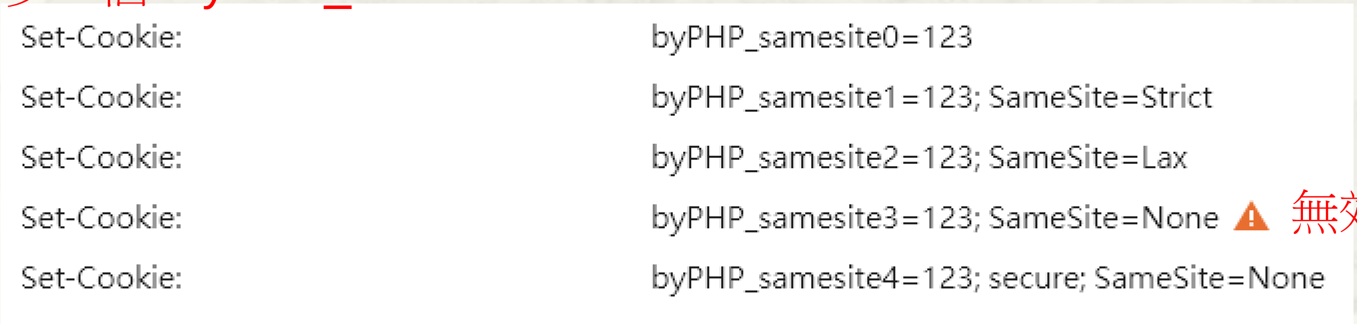
Samesite Attribute

- 測試 HTTPS
  - https://demo3.buda.idv.tw/php/cookie/cookie_set_attr_samesite.php
- Chrome F12



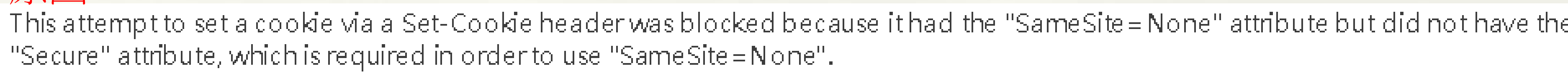
Name	Value	Domain	Path	Expires / Max-Age▲	Size	HttpOnly	Secure	SameSite
byPHP_samesite0	123	demo3.buda.idv.tw	/php/cookie	Session	18			
byPHP_samesite1	123	demo3.buda.idv.tw	/php/cookie	Session	18			Strict
byPHP_samesite2	123	demo3.buda.idv.tw	/php/cookie	Session	18			Lax
byPHP_samesite4	123	demo3.buda.idv.tw	/php/cookie	Session	18		✓	None

少一個: byPHP_samesite3



Set-Cookie:	byPHP_samesite0=123
Set-Cookie:	byPHP_samesite1=123; SameSite=Strict
Set-Cookie:	byPHP_samesite2=123; SameSite=Lax
Set-Cookie:	byPHP_samesite3=123; SameSite=None ⚠ 無效
Set-Cookie:	byPHP_samesite4=123; secure; SameSite=None

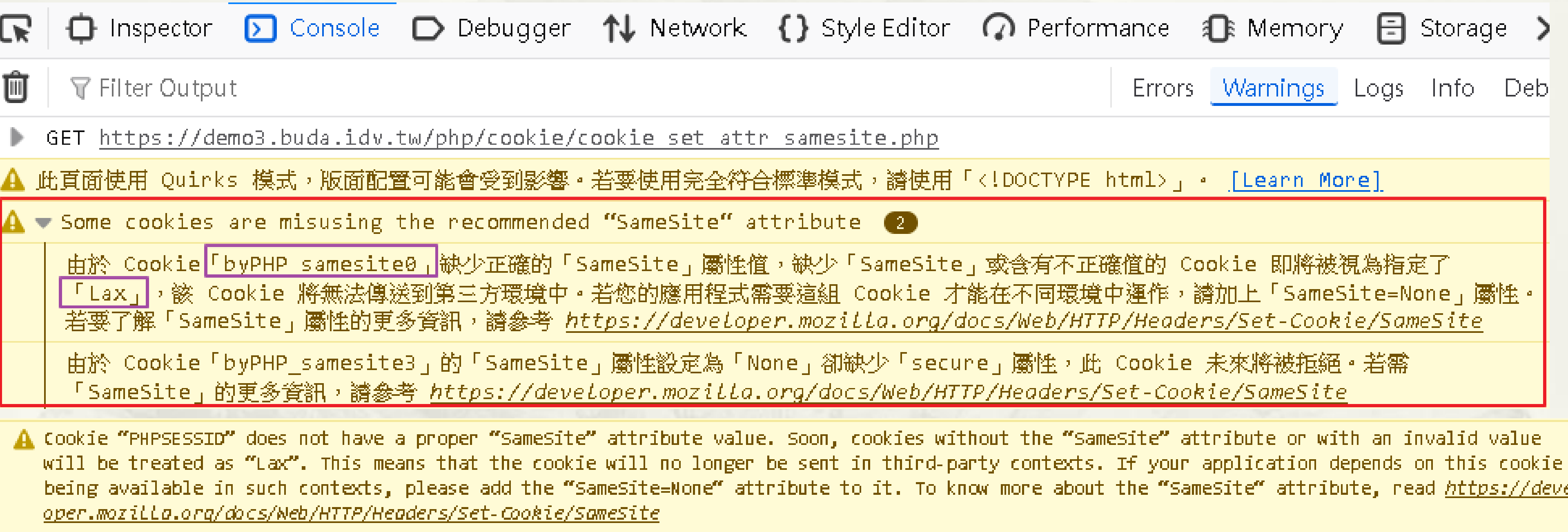
原因：



This attempt to set a cookie via a Set-Cookie header was blocked because it had the "SameSite=None" attribute but did not have the "Secure" attribute, which is required in order to use "SameSite=None".

SameSite = NULL(未輸入) Firefox Console 警告訊息

- NULL(未設定) 未來將等同 “Lax” (非現在)



```
GET https://demo3.buda.idv.tw/php/cookie/cookie_set_attr_samesite.php
此頁面使用 Quirks 模式，版面配置可能會受到影響。若要使用完全符合標準模式，請使用「<!DOCTYPE html>」。 [Learn More]
Some cookies are misusing the recommended “SameSite“ attribute 2
由於 Cookie「byPHP_samesite0」缺少正確的「SameSite」屬性值，缺少「SameSite」或含有不正確值的 Cookie 即將被視為指定了
「Lax」，該 Cookie 將無法傳送到第三方環境中。若您的應用程式需要這組 Cookie 才能在不同環境中運作，請加上「SameSite=None」屬性。
若要了解「SameSite」屬性的更多資訊，請參考 https://developer.mozilla.org/docs/Web/HTTP/Headers/Set-Cookie/SameSite
由於 Cookie「byPHP_samesite3」的「SameSite」屬性設定為「None」卻缺少「secure」屬性，此 Cookie 未來將被拒絕。若需
「SameSite」的更多資訊，請參考 https://developer.mozilla.org/docs/Web/HTTP/Headers/Set-Cookie/SameSite
Cookie “PHPSESSID” does not have a proper “SameSite” attribute value. Soon, cookies without the “SameSite” attribute or with an invalid value
will be treated as “Lax”. This means that the cookie will no longer be sent in third-party contexts. If your application depends on this cookie
being available in such contexts, please add the “SameSite=None“ attribute to it. To know more about the “SameSite“ attribute, read https://deve
oper.mozilla.org/docs/Web/HTTP/Headers/Set-Cookie/SameSite
```

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie#samesitesamesite-value

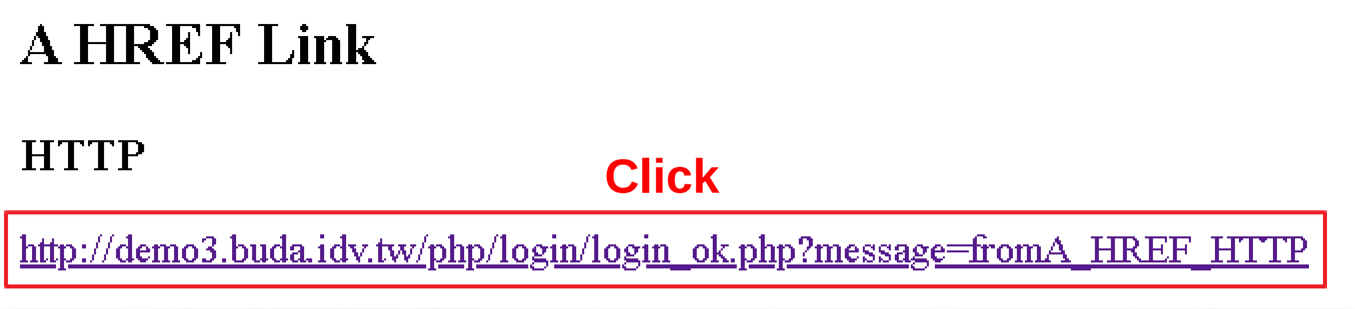
SameSite Attribute
是否傳送 Cookie to Third-party

- Chrome

	None (Secure=1)		Lax		Strict	NULL(未輸入)
	HTTP	HTTPs	HTTP	HTTPs	HTTP/HTTPs	HTTP/HTTPs
A HREF Link	V(bug?)	V	V	V		V
Form GET	V(bug?)	V	V	V		V
Form POST		V				V
IFRAME		V				
IMG Src	V(bug?)	V				
preconnect Link		V				
prefetch Link		V				
preload Link						
prerender Link	V(bug?)	V				V

Bugs: Chrome 會自動將 http 以 https 重送一次

補充:
Chrome 會自動將 http 以 https 重送一次

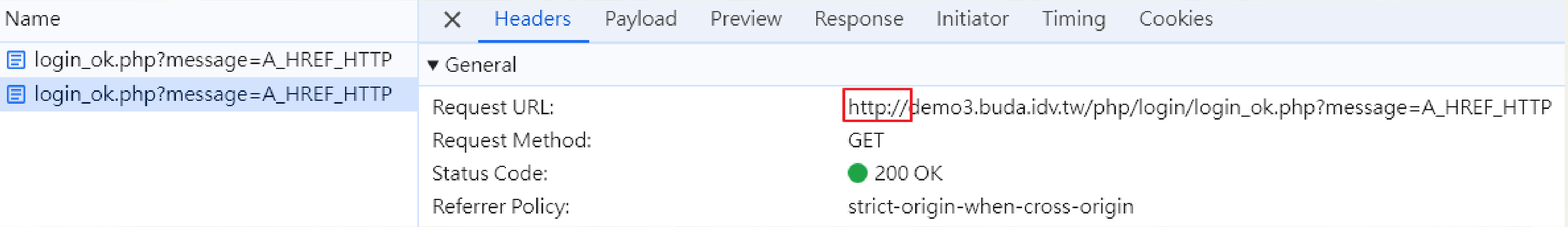


A HREF Link

HTTP

Click

http://demo3.buda.idv.tw/php/login/login_ok.php?message=fromA_HREF_HTTP



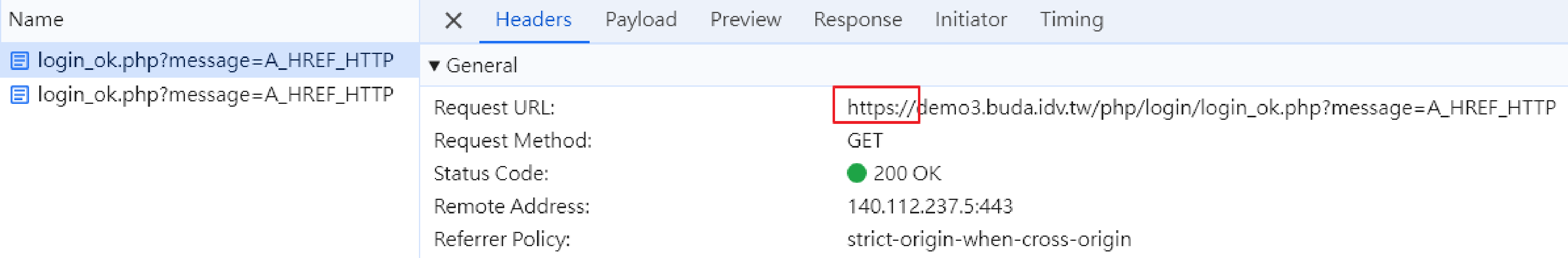
Name

login_ok.php?message=A_HREF_HTTP

login_ok.php?message=A_HREF_HTTP

▼ General

Request URL:	http://demo3.buda.idv.tw/php/login/login_ok.php?message=A_HREF_HTTP
Request Method:	GET
Status Code:	● 200 OK
Referrer Policy:	strict-origin-when-cross-origin



Name

login_ok.php?message=A_HREF_HTTP

login_ok.php?message=A_HREF_HTTP

▼ General

Request URL:	https://demo3.buda.idv.tw/php/login/login_ok.php?message=A_HREF_HTTP
Request Method:	GET
Status Code:	● 200 OK
Remote Address:	140.112.237.5:443
Referrer Policy:	strict-origin-when-cross-origin

SameSite Attribute
是否傳送 Cookie to Third-party

- Chrome (無痕視窗)

	None (Secure=1)		Lax		Strict	NULL(未輸入)
	HTTP	HTTPs	HTTP	HTTPs	HTTP/HTTPs	HTTP/HTTPs
A HREF Link	V(bug)	V	V	V		V
Form GET	V(bug)	V	V	V		V
Form POST		V				V
IFRAME						
IMG Src						
preconnect Link						
prefetch Link						
preload Link						
prerender Link						

SameSite Attribute
是否傳送 Cookie to Third-party

- Firefox

	None (Secure=1)		Lax		Strict	NULL(未輸入)
	HTTP	HTTPs	HTTP	HTTPs	HTTP/HTTPs	HTTP/HTTPs
A HREF Link		V	V	V		V
Form GET		V	V	V		V
Form POST		V				V
IFRAME						
IMG Src						
preconnect Link						
prefetch Link						
preload Link						
prerender Link						

SameSite Attribute
是否傳送 Cookie to Third-party

- Firefox (無痕視窗)

	None (Secure=1)		Lax		Strict	NULL(未輸入)
	HTTP	HTTPs	HTTP	HTTPs	HTTP/HTTPs	HTTP/HTTPs
A HREF Link	V(bug?)	V	V	V		V
Form GET		V	V	V		V
Form POST		V				V
IFRAME						
IMG Src						
preconnect Link						
prefetch Link						
preload Link						
prerender Link						

SameSite Testing

自架 login.php

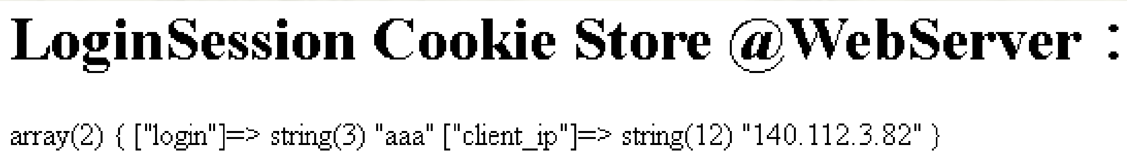
SameSite Testing 自架 login.php

- 登入
  - https://demo3.buda.idv.tw/php/login/login.php
- Test1 : 手動執行 (Form Method=GET or POST)
  - https://demo.davis.cc.ntu.edu.tw/csrf_manual_load.html
- Test2 : 開啟即自動執行 (Form Method= GET)
  - https://demo.davis.cc.ntu.edu.tw/csrf_auto_load.html

SameSite Testing
自架 login.php

- SameSite=“Strict”/”Lax”/”None”/NULL
  - 方法1: session.cookie_samesite   @Apache Server
    - Ubuntu 22.04: /etc/php/8.1/apache2/php.ini
    - Ubuntu 24.04: /etc/php/8.3/apache2/php.ini

    ~# systemctl restart apache2
  - 方法2: @Browser
    - F12 修改 Cookie Attribute (立即生效)
- Cookie 檢測
  - 方法1: F12 觀察, Request Header 是否送出 Cookie
  - 方法2: https://demo.davis.cc.ntu.edu.tw/csrf_cookie.html



LoginSession Cookie Store @WebServer：

```
array(2) { ["login"]=> string(3) "aaa" ["client_ip"]=> string(12) "140.112.3.82" }
```

CSRF Mitigation 傳統方法

- Check “HTTP Referrer” Header
- Use CSRF Token (一次性驗證碼)
  - Generate a special field called “CSRF Token”, that an evil page can’t generate from a remote page.

```
<form action=“run.do" method="post">
<input type="hidden" name="CSRFToken" value="123token123">
[...]
</form>
```

  - 當 User 發送請求給 Server 時，Server 會先確認 Token 的時間有效性和正確性.
  - 需注意取得 CSRF token 的 API 不能接受跨網域的請求，如果讓駭客有機會取得 CSRF token 一樣有風險。
  - 實作上可使用套件，如: nodejs csurf、OWASP CSRFGuard
  - 方法同上, 但 CSRF Token 放在 HTTP Header 自定義

LoginSession Cookie Best Practice

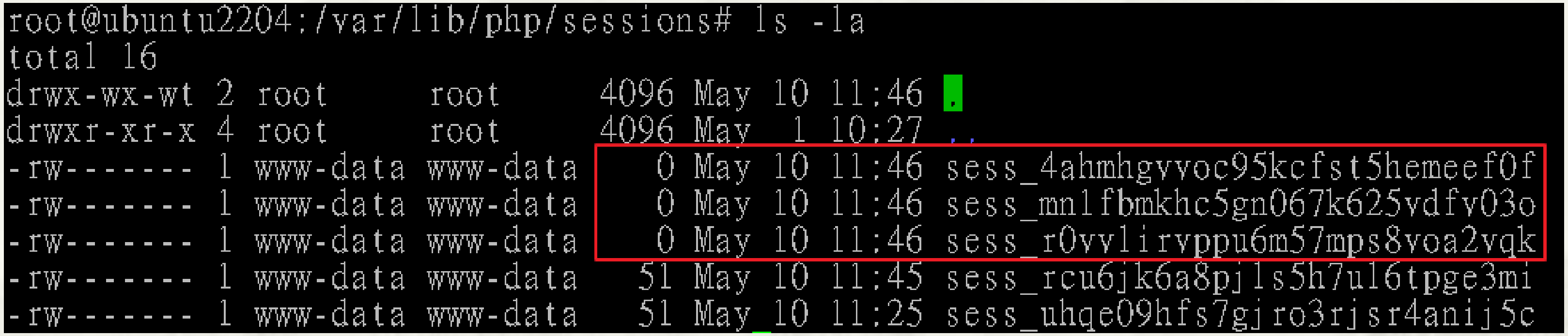
LoginSession Cookie Best Practice

- LoginSession Cookie Name 應避免使用預設名稱或有易於猜測之關鍵字
  - ASP.NET_SessionId, PHPSESSID, *SID, *SESSION_ID
- LoginSession Cookie Attributes 應設定如下值
  - HttpOnly= True, Secure= True, Samesite= Lax/Strict
  - 如下設定可能有 CSRF 漏洞
  - Samesite= NULL or None
  - Samesite= Lax 且支援 HTTP GET
- 提供”登出”功能，並應確實刪除伺服器端 LoginSession Cookie
- 應避免尚未登入時，就產生 LoginSession Cookie
  - 避免耗盡 Server 資源
  - 避免洩漏 LoginSession Cookie Name
- 不應使用其他 Cookie 儲存 “使用者 ID”，並作為使用者權限控管依據
  - “使用者 ID” 應直接儲存於 LoginSession Cookie
- 不應接受使用者提供之 LoginSession Cookie Value
  - 避免 Session Fixation/Adoption Vulnerability

應避免尚未登入時，就產生 LoginSession Cookie

- 何時產生 LoginSession Cookie？

  <? php session_start();?>



```
root@ubuntu2204:/var/lib/php/sessions# ls -la
total 16
drwx-wx-wt 2 root      root      4096 May 10 11:46 .
drwxr-xr-x 4 root      root      4096 May  1 10:27 ..
-rw------- 1 www-data www-data     0 May 10 11:46 sess_4ahmhgvvoc95kcfst5hemeef0f
-rw------- 1 www-data www-data     0 May 10 11:46 sess_mn1fbmkhc5gn067k625vdfv03o
-rw------- 1 www-data www-data     0 May 10 11:46 sess_r0vvlirvppu6m57mps8voa2vqk
-rw------- 1 www-data www-data    51 May 10 11:45 sess_rcu6jk6a8pjls5h7ul6tpge3mi
-rw------- 1 www-data www-data    51 May 10 11:25 sess_uhqe09hfs7gjro3rjsr4anij5c
```

應避免尚未登入時，就產生 LoginSession Cookie

尚未登入時，就產生 LoginSession Cookie

https://demo3.buda.idv.tw/php/login/login_check_v1.php

```
<?php
session_start();
if ($_SESSION['login']) {
   echo "已經登入";
} else {
   echo "尚未登入";
}
?>
```

避免未登入時，就產生 LoginSession Cookie

https://demo3.buda.idv.tw/php/login/login_check_v2.php

```
<?php
//Check "LoginSession Cookie" first.
If ($_COOKIE['PHPSESSID']){
   session_start();
   if ($_SESSION['login']) {
     echo "已經登入";
     exit();
   }
}
echo "尚未登入";
?>
```

簡報完畢

謝謝