NGWN-P1

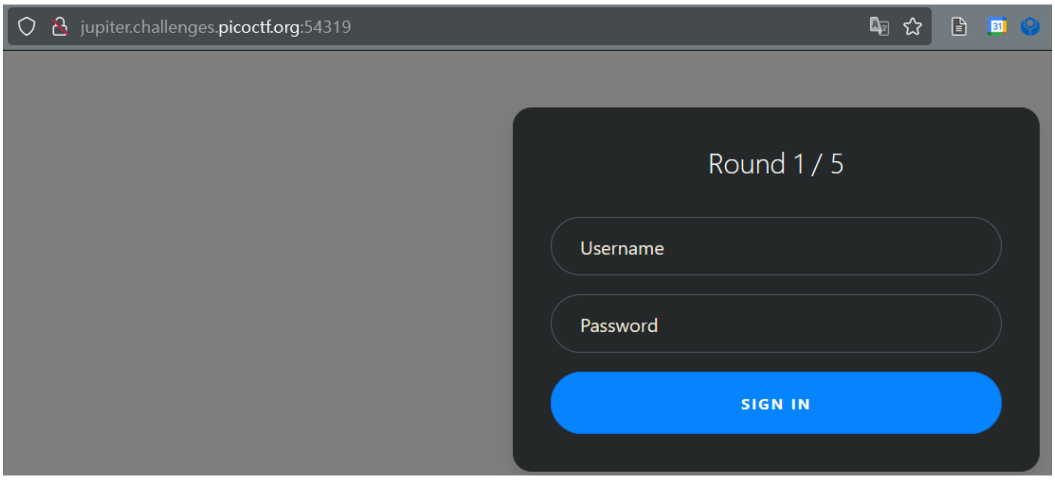
B10932017 張祐禎

Part 1

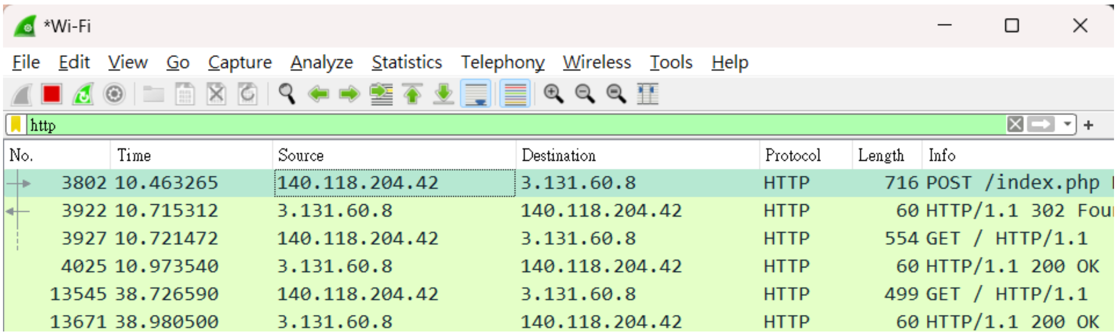
1. URL: http://jupiter.challenges.picoctf.org:54319/ (Web Gauntlet)

Part 2

1. Your selected URL => screenshot_1

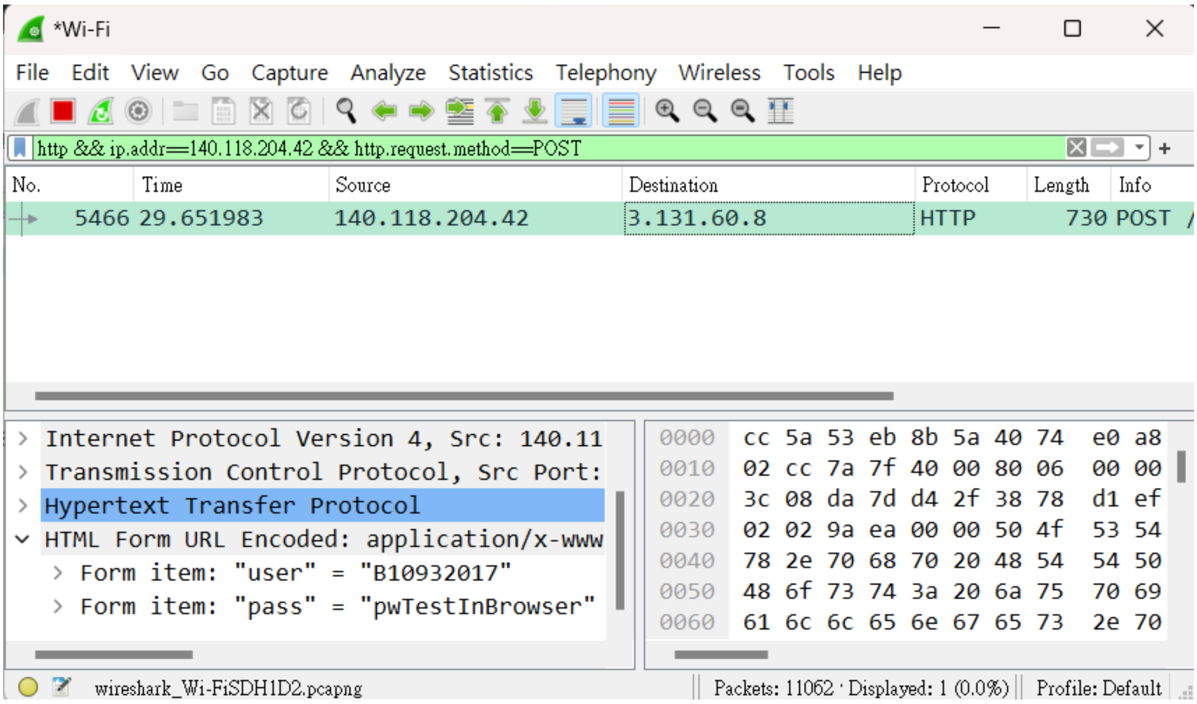


2. Wireshark sniffing => screenshot_2


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
No.    Time       Source          Destination     Protocol Length Info
 3802 10.463265   140.118.204.42  3.131.60.8      HTTP      716 POST /index.php
 3922 10.715312   3.131.60.8      140.118.204.42  HTTP       60 HTTP/1.1 302 Fou
 3927 10.721472   140.118.204.42  3.131.60.8      HTTP      554 GET / HTTP/1.1
 4025 10.973540   3.131.60.8      140.118.204.42  HTTP       60 HTTP/1.1 200 OK
13545 38.726590   140.118.204.42  3.131.60.8      HTTP      499 GET / HTTP/1.1
13671 38.980500   3.131.60.8      140.118.204.42  HTTP       60 HTTP/1.1 200 OK
```

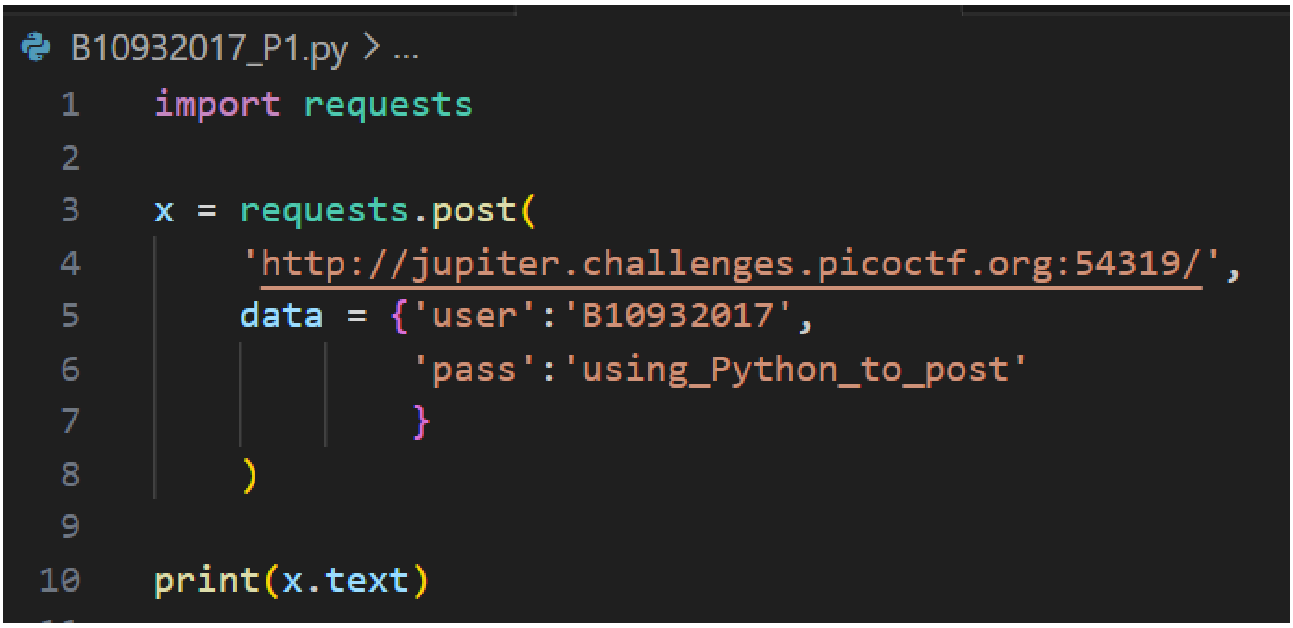
3. Wireshark packet part, including the account and password => screenshot_3


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http && ip.addr==140.118.204.42 && http.request.method==POST
No.   Time       Source          Destination  Protocol  Length Info
5466 29.651983   140.118.204.42  3.131.60.8   HTTP       730 POST /

> Internet Protocol Version 4, Src: 140.11
> Transmission Control Protocol, Src Port:
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www
    > Form item: "user" = "B10932017"
    > Form item: "pass" = "pwTestInBrowser"

0000  cc 5a 53 eb 8b 5a 40 74  e0 a8
0010  02 cc 7a 7f 40 00 80 06  00 00
0020  3c 08 da 7d d4 2f 38 78  d1 ef
0030  02 02 9a ea 00 00 50 4f  53 54
0040  78 2e 70 68 70 20 48 54  54 50
0050  48 6f 73 74 3a 20 6a 75  70 69
0060  61 6c 6c 65 6e 67 65 73  2e 70

wireshark_Wi-FiSDH1D2.pcapng    Packets: 11062 · Displayed: 1 (0.0%)    Profile: Default
```

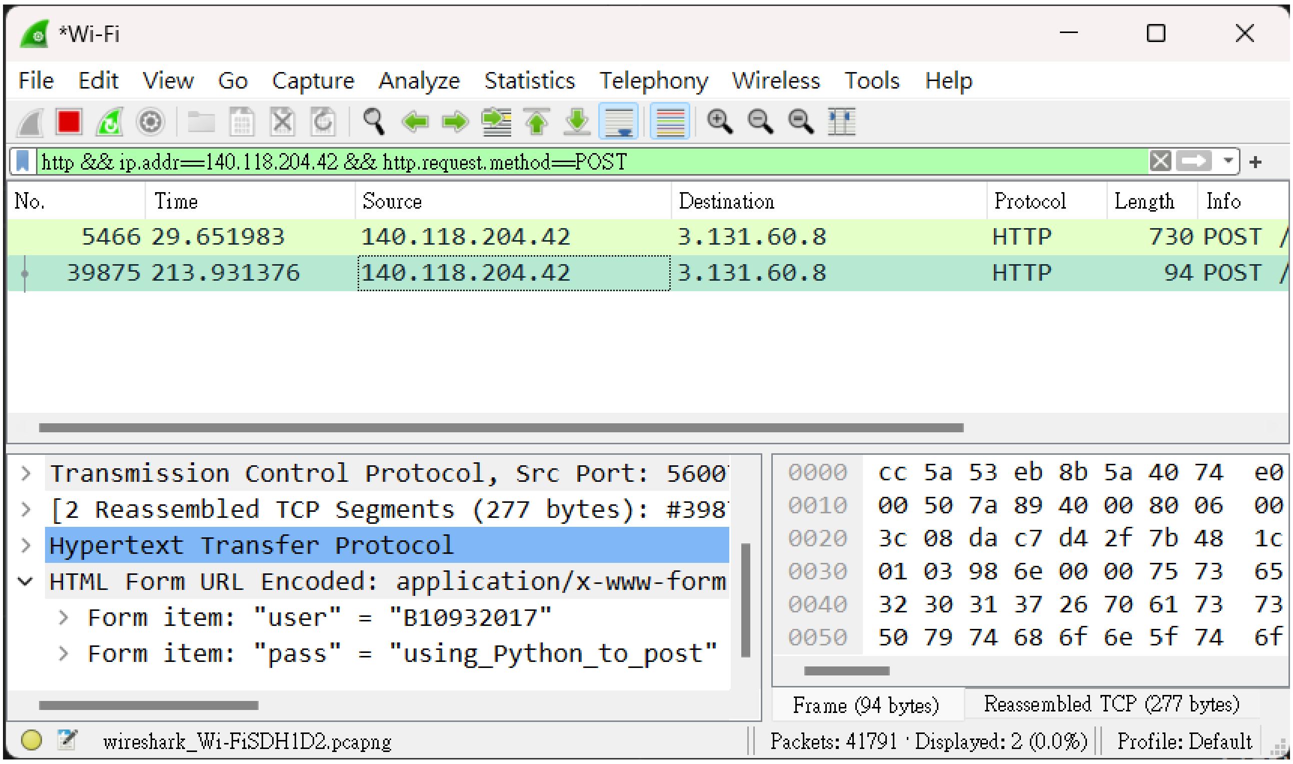
Part 3

1. Python program to send a packet to URL => screenshot_4.



```python
import requests

x = requests.post(
    'http://jupiter.challenges.picoctf.org:54319/',
    data = {'user':'B10932017',
            'pass':'using_Python_to_post'
            }
    )

print(x.text)
```

2. Packet sniffing by Wireshark => screenshot_5



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http && ip.addr==140.118.204.42 && http.request.method==POST

No.	Time	Source	Destination	Protocol	Length	Info
5466	29.651983	140.118.204.42	3.131.60.8	HTTP	730	POST /
39875	213.931376	140.118.204.42	3.131.60.8	HTTP	94	POST /

```
> Transmission Control Protocol, Src Port: 5600
> [2 Reassembled TCP Segments (277 bytes): #398
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form
  > Form item: "user" = "B10932017"
  > Form item: "pass" = "using_Python_to_post"
```

```
0000  cc 5a 53 eb 8b 5a 40 74  e0
0010  00 50 7a 89 40 00 80 06  00
0020  3c 08 da c7 d4 2f 7b 48  1c
0030  01 03 98 6e 00 00 75 73  65
0040  32 30 31 37 26 70 61 73  73
0050  50 79 74 68 6f 6e 5f 74  6f
```

Frame (94 bytes) Reassembled TCP (277 bytes)

wireshark_Wi-FiSDH1D2.pcapng Packets: 41791 · Displayed: 2 (0.0%) Profile: Default