Password for lesson1按右鍵找原始碼

gtVrDuiDfck831PqWsLEZy5gyDz1clto

password for lesson 2 按F12，找網頁原始碼

ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi

Password for lesson3 打出/files

sJIJNW6ucpu6HPZ1ZAchaDtwd7oGrD14

password for lesson 4 打出robots.txt

Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ

Password for lesson 5

iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq

方法：下載一個叫做burp的程式並對referer亂搞

原理：因為上面寫的是access disallowed can only come from natas5，所以就要讓網站以為我們是從natas5過來的。

Burp不會用~~

Password for lesson 6

一張含有 螢幕擷取畫面 的圖片

自動產生的描述aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1

這一章節要介紹的是cookie，cookie是一種在網路上的小檔案，目的是貯存使用者在網路上的帳號密碼和其他使用者做過的事情(像是購物網站中的購物籃)，所以在清除瀏覽資料時，同時會問要不要清除cookie中的資料。原本我沒有在管這些，只是覺得每次清除瀏覽資料後，facebook之類的網站都要重登一遍，後來才知道原來是因為cookie被清除了，其實說真的，cookie真的挺方便的，而且名字很可愛。

所以這個才會出現🡪🡪

方法：

Chrome中有一個外掛程式，叫做”Edit this cookie”，安裝後，把”logged in”的值從0改成1，按一下下面的勾勾，重新整理，就可以取得密碼了！！！也可以用burp啦。

Password for lesson 7

7z3hEENjQtflzgnT29q7wAvMNfZdh0i9

這一個部分是利用觀察力~~

首先先看網頁原始碼(首頁就有說View source code了，應該很明顯)，裡面可以發現includes/secret.inc(如下)

了解之後，在網址後方打上一張含有 螢幕擷取畫面 的圖片

自動產生的描述/includes/secret.inc，找到secret的檔案，輸入秘密，即可得到密碼。

Password for lesson 8

DBfUBfqQG69KvJvJ1iAbMoIpwSNQ9bWe

好的，這關我很傻眼的過了，其實大概猜的到它要甚麼。

它在網頁原始碼中有寫<!-- hint: password for webuser natas8 is in /etc/natas\_webpass/natas -->一張含有 螢幕擷取畫面 的圖片

自動產生的描述

恩亨，這就表示這一串東西就是解答所在，在查詢過網路後，這一題要介紹的是page=…，反正就是在page後打上所要的東西，就可以找到密碼了，這一個部分所要的東西是/etc/natas\_webpass/natas，所以只要在page=後打上這串，就可以找到解答了。

Password for lesson 9

W0mMhUcRRnG8dcghE4qvk3JA9lGt8nDl

這段我有點看不太懂，它剛開始裡面放了一個被鎖住的密碼，下面給了解開密碼的演算法，我覺得這一題的重點要知道加密跟解密的順序是相反的，就可以將密碼解出來。但其實我不知道要在哪裡跑這個程式阿。TAT

Password for lesson 10

nOpp1igQAkUzaI1GUUjzn1bFVj7xCNzu

這一題的原理是利用原始碼中的passthru()的一個小漏洞，passthru()有一個致命的缺點，就是你輸入什麼字，它會不經思索的把整個字串放入程式碼，所以，只要在網頁中的search欄打入; cat /etc/natas\_webpass/natas10 #，就可以讓程式自己吐出答案。

Password for lesson 11

U82q5TCMMQ9xuFoI3dYX61s7OZD9JKoK

這一題想法跟上一題差不多，但是不能用許多符號，例如：’;’，所以，可想而知，上一題的; cat /etc/natas\_webpass/natas10 #，就不能用了，要想想新方法了，就試試看用grep吧，grep就是一個可以將想要找的字串找出來的一群指令元，因此，我們就把前面的;改成.\*。(變成.\* cat /etc/natas\_webpass/natas11 #)欸嘿嘿，出來了耶~~~

Password for lesson 12