Google Search

1. 前言:

將這篇SQL Injection報告分成兩個部分，第一個部分是手動SQL Injection的成果，另外一個是用程式去自動在google搜尋關鍵字後，把有相關有符合關鍵字的網頁標題跟網址下載下來。

2. 手動SQL Injection:

我依據關鍵字login.php, login.asp…等，去google搜尋並把每一個網址輸入跟SQL injection有相關的字詞。

輸入的字詞:

1. ‘or 1=1--

2. admin

3. admin’--

4. ‘HAVING1=1—

5. ‘ or 1=1 //

6. ‘or 1=1 /\*

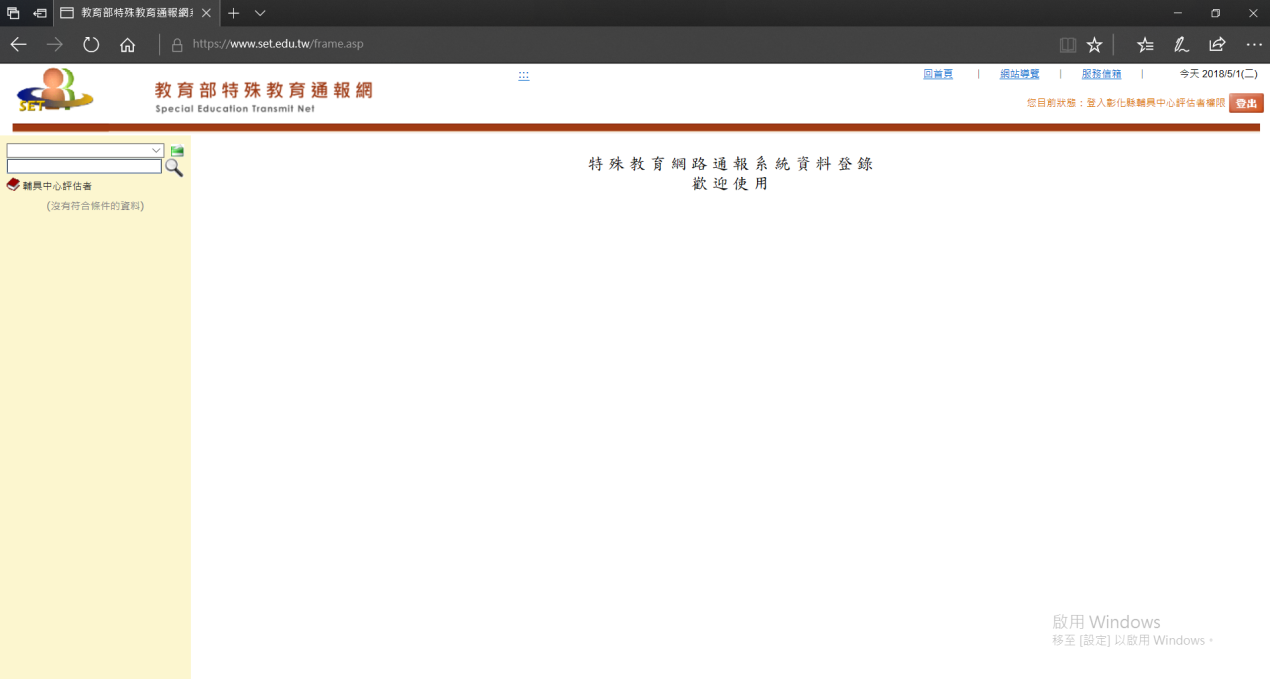
依據上述幾個再做一些相關變化之後，有找到以下幾個網址是可以成功進去的，除了可以進去的也有找到會有錯誤訊息的。

教育部特殊教育通報網:

https://www.set.edu.tw/setnet/reg/login.asp



帳號密碼皆為admin，之後會進去這網頁



不曉得是不是管理員沒有把admin關掉，雖然能登進去但是裡面什麼都沒有就是了。

小學數學新思維 : https://primarymaths.ephhk.com/login.php



帳號密碼皆為: 'or 1=1--



就可以成功登入使用，只是網頁好像都不能用就是了



教師版的帳號密碼也是: 'or 1=1--



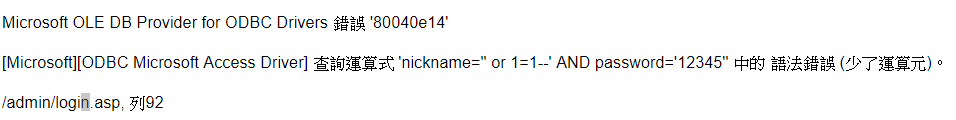
教師版的功能就都可以用



除此上述的兩個網站，也有發現一個會跳錯誤訊息的，可是經過很多種方式之後，發現還是沒辦法成功進去。



<http://www.yusw.org.tw/admin/login.asp>



有試過很多種方法，後來發現就算邏輯對了，但是只要有關鍵字or之類的，就還是會直接擋住，所以就沒成功破解。

3. 網頁爬蟲:

有鑑於一個一個找太麻煩了，所以寫了一個程式去把關鍵字丟到google搜尋之後，再把找到的資料的標題和網址存下來成為一個url.txt檔，以便之後使用。

1. 創立google網址:

有兩種方式可以去上google搜尋內容，一種是跟正常使用的方法一樣，在搜尋欄內，輸入關鍵字之後開始搜尋，另外一種是在google網址列輸入想要的內容之後案開始，而我是選擇第二種方式來做使用。

基本上要讓google搜尋東西時，讓網址欄變成這樣<https://www.google.com.tw/search?q>=

然後再q=之後輸入想要搜尋的內容之後，就可以開始搜尋，假設我要搜尋login.php我就讓網址變成<https://www.google.com.tw/search?q=login.php>

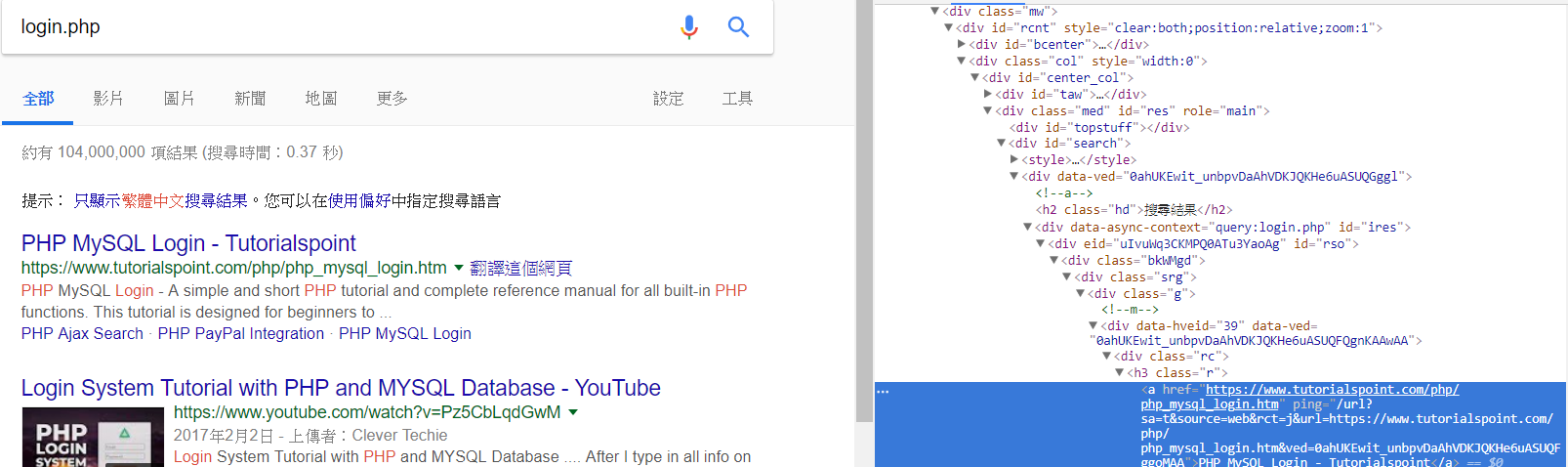
就可以進行搜尋了。

2. 找尋網址名稱跟網址

接下來我們進到搜尋畫面之後，可以看到每一個有我們所需要的標題和網址



這時我們再想要找的內容上右鍵→檢查，就會出現那一個內容在網頁的哪裡



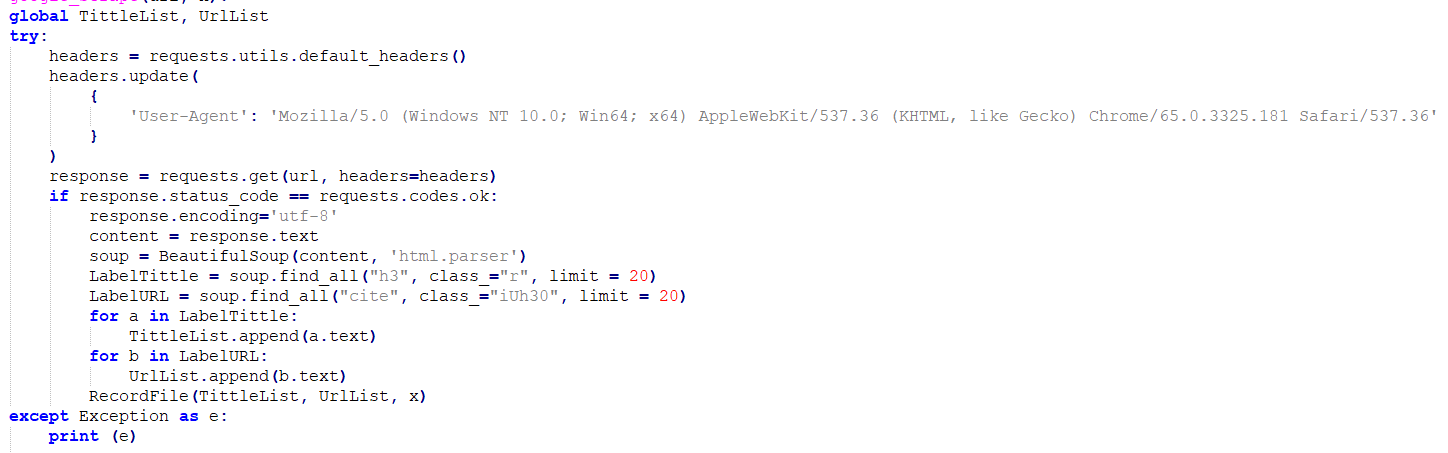
在這邊發現標題是在<h3 class “r”>的標籤裡面



然後我們再找網址，是在<cite class “iUH30”>



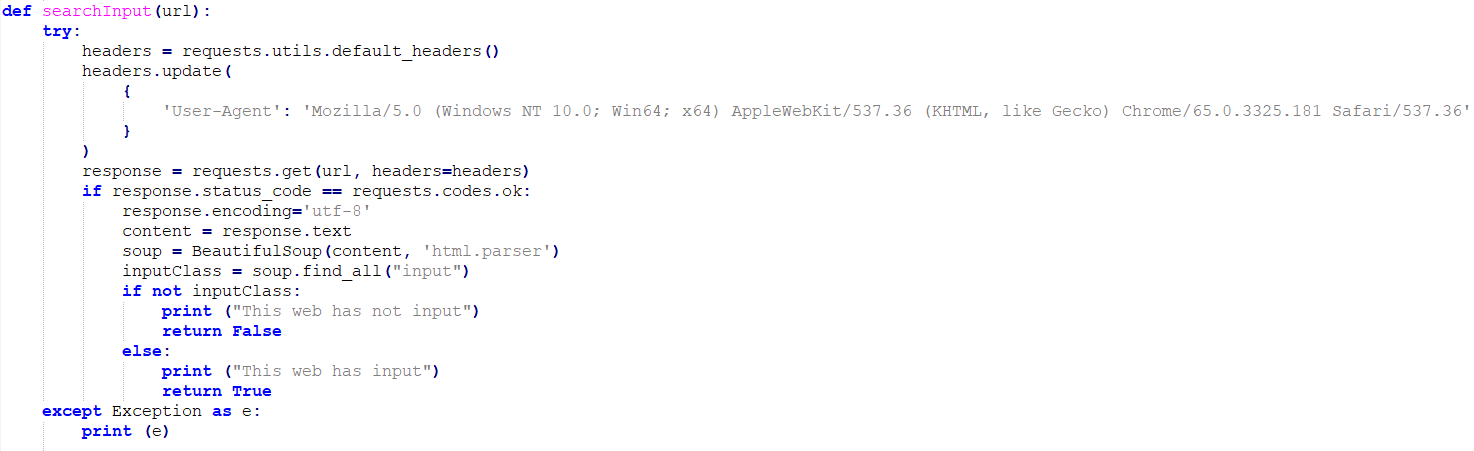
都知道內容之後就可以開始在程式裡面撰寫所需的內容



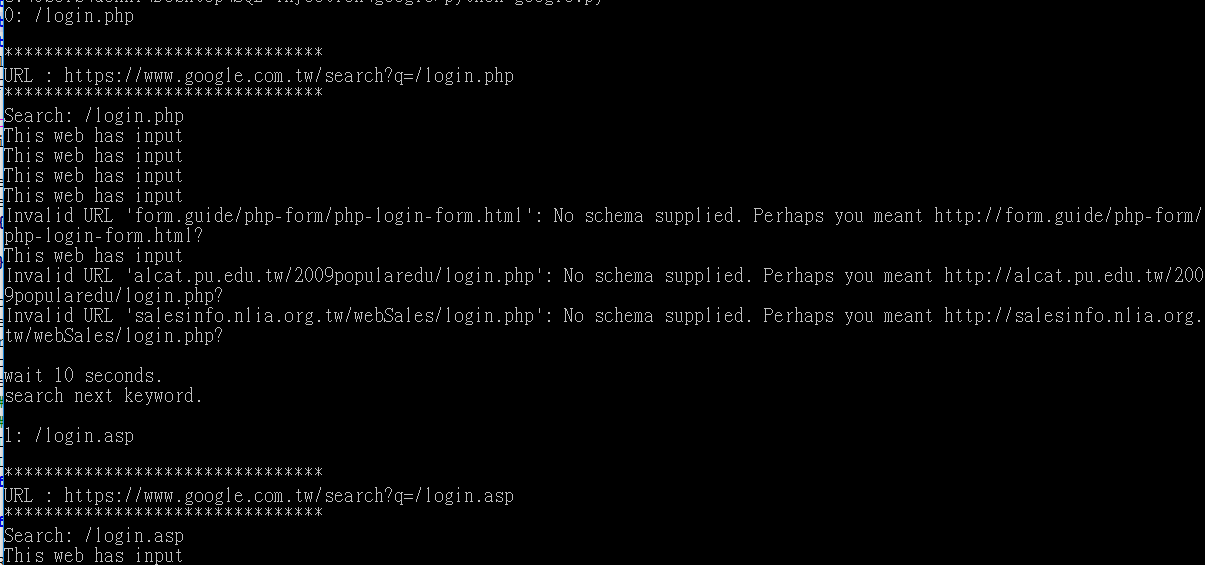
網址做好之後輸入給requests讓它進行訪問，再利用BeautifulSoup去找尋剛剛找到的規則，並將它串成list之後輸入到Url.txt

3. 確定是否有input

接下來為了確認我們找到的網頁有沒有Input Label來讓我們輸入，因此我們要檢查網頁沒有存在這個label，有鑑於剛剛可以找到tittle跟url，因此我們這邊也是用相同的方法來做使用，只是這次這邊找的關鍵字是input，有的話就寫入到url.txt，沒有就跳過。



4. 結果



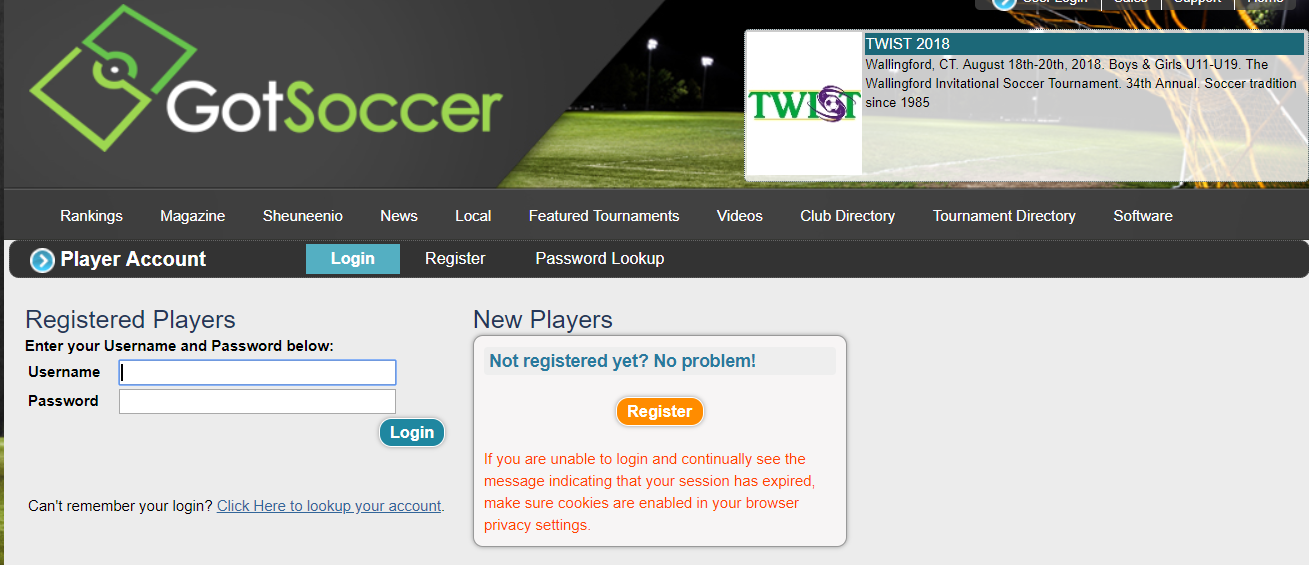
會看到有些存下來的網址不能直接用，還要再做處理。

接下來看看存下來的網址是不是都有input可以用



隨便找幾個來看看



確定都有欄位可以輸入。