楊力行 b06705001 b06705001

unexploitable:

在用chrome點開link時，顯示了警告的訊息，顯示了這個網站的憑證是來自[www.github.com，並且在網址的後面加上/.git時顯示的404頁面也有著github](http://www.github.com，並且在網址的後面加上/.git時顯示的404頁面也有著github)的圖標，因此我猜測這個網頁是用github生成的，所以到github搜索這個網址，到這裡時，理論上正確的步驟是點開CNAME的repo再去找他的刪除紀錄，最終找到flag，但是我在寫時，有人直接把如何找以及flag是多少寫了一個repo，所以點進去她的repo後直接就看到了flag。

safe R/W:

看程式碼後先發現了用strlen對\_GET[“c”]傳入的內容長度進行了限制，我利用strlen讀入數組會返回null來破解，在url的c= 改成c[]=，並且file\_get\_content時不能讀到<，但是沒有<?php include就不會把讀到的當作php程式碼執行，因此需要讓file\_get\_content和include讀到不同的東西，我使用data偽協議來處理，因為本題php://input不能使用，將f設成data:mydir，i為data:mydir/meow，根據本題的設定，file\_get\_content($i)時，會把它當成是偽協議來處理，而不是當成路徑，而在include中則是直接當成路徑讀取c的內容，也就是說可以在C中使用<了，接著在c中輸入<?php system("cd /;ls;"); 查看根目錄的檔案，發現有個flag\_is\_here，所以換成輸入<?php system("cd /;cat flag\_is\_here;");就可以得到flag

最終的url為[https://edu-ctf.csie.org:10155/?f=data%3Amydir&i=data%3Amydir%2Fmeow&c[]=%3C?php%20system(%22cd%20/;cat%20flag\_is\_here;%22);](https://edu-ctf.csie.org:10155/?f=data%3Amydir&i=data%3Amydir%2Fmeow&c%5b%5d=%3C?php%20system(%22cd%20/;cat%20flag_is_here;%22);)

兩題都沒有script