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 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);

兩題都沒有 script