**郭又嘉**

**AosoraKuo**

**B06705020**

**Unexploitable**

先進到網站在網址後面接上一些東西例如 /flag

會跳出Github的404頁面

因此猜測網站是在Github上面架的

於是到Github搜尋unexploitable.kaibro.tw

發現叫Bucharesti的用戶

在Bucharesti的repositories裡面的紀錄找到delete secret file

Load之後就找到FLAG了

**Safe R/W**

看過程式碼之後發現繞過file\_get\_contents()可以觸發include()執行$i裡面的東西

而當file\_get\_contents()讀到data開頭的會把它當成偽協議

所以先讓$f = data:xxx

因為file\_put\_contents()把$c放在data:xxx下的meow裡面

所以$i = data:xxx/meow

當file\_get\_contents()吃到data:xxx/meow時他會發現沒有meow類別的xxx這種東西於是回傳NULL

就繞過了file\_get\_contents()

再來就可以在$c裡面放php code執行因為include()會直接把檔案裡面的東西拿出來跑

而$c不能超過20個字

要繞過strlen就先讓c不是string

先用?c[]=<?system("ls ~/");找到跟目錄下有flag\_is\_here

再用?c[]=<?system("cat ~/flag\_is\_here");就可以找到FLAG