計算機安全 HW4 Writeup

- Real name: 張瀚文
- Nickname on course website: Hwww
- Student ID: b07505027.

The Stupid Content Tracker

解法

利用scrable ()還原source code，可以發現有admin_protal_non_production這個位置，連上的話就可以看到FLAG，但是這個路徑被.htaccess設置了權限，需要帳號密碼登入才能看到。另外有個 `.gitignore` 檔案，裡面可以看到 `.htpasswd` 被忽略了，若是可以看到這個檔案，就可以知道帳號密碼（如果密碼沒有被好好加密），這裡猜測 `.htpasswd` 有可能在被寫入 `.gitignore` 之前被git紀錄下來，所以 `git log` 看一下commit紀錄，有關於password的紀錄，直接 `git show` 看 `commit 2577a... Add password` 這筆，帳號跟密碼就會出來了，連上 `/admin_portal_non_production` 就拿到FLAG了～

心得

沒想到還原後連記錄都有，真的是The Stupid Content Tracker

Zero Note Revenge

解法

這題跟LAB的Zero Note類似，一樣是XSS，但因為cookie被設定為HttpOnly，所以沒辦法透過 `document.cookie` 獲得，根據提示，試試看連上不存在的note（/note/${noteHash}），會發現server會把request的資訊回傳，其中包含cookie，所以如果讓admin帶著cookie前往這個頁面，再想辦法把這個頁面傳給我們，就有機會拿到HttpOnly的cookie。現在要設計怎麼在XSS中將admin的頁面傳給我們，我們可以利用fetch在不轉跳頁面的情況下直接fetch /note/${notehash} 並把response再用一次fetch傳給我們的webhook，但因為response很長，所以改用POST，把內容放在body。XSS的內容請見 `code/Zero Note Revenge/xss.html` 。

把note report to admin之後就可以在webhook看到cookie了～

心得

這題滿好想的～不存在的note其實在LAB時就有戳到，那時候還覺得怎麼會有一個沒用到的頁面，原來是用在這題。

Zero Meme

解法

先研究Update your favorite Meme那個框能夠幹嘛，發現他雖然有驗證輸入的開頭是不是http，但卻沒有過濾特殊字元，因此能夠簡單利用injection來XSS，把cookie傳出去，但現在問題是，怎麼讓admin “Update your favorite Meme”。這裡先看一下network，紀錄一下Update meme的路徑，是POST /me，formdata放intro。

要讓admin自己帶著cookie來POST /me，就會用到csrf。雖然這裡是用POST，cookie又預設是Lax，一般來說只會透過top-level GET才會帶著cookie，但因為Lax + POST政策延緩了這項規則，讓cookie在設立的兩分鐘可以跟著POST一起傳出去，也因為題目有說admin每次點連結前都會重新登入，因此可以達成這項條件，就可以成功Lax + Post了

詳細流程：

準備好自己的server及html，比如https://8787.com/csrf.html (https://8787.com/csrf.html) ，裡面寫了form，form裡面的intro填入了XSS的script，POST給 edu-ctf.csie.org (http://edu-ctf.csie.org)
->
分享https://8787.com/csrf.html 給admin
->
admin點擊連結進入https://8787.com/csrf.html 會看到form
->
利用js自動submit form，admin就會帶著他的edu-ctf.csie.org的cookie去POST /me
->
這時admin會被跳轉到表單回傳的結果，也就是edu-ctf.csie.org/me () ，其中含有剛剛的XSS，admin讀取頁面的時候就會自動執行，把cookie送給我們～

程式碼請參考 `code/Zero Note Revenge/csrf.html`

心得

這題滿複雜的，資訊又算是很新，閱讀英文不是很好懂，想了很久。