M10915027 石成峰 HW4

[Are You a Robot?]

1. 使用Firefox開啟題目網頁。
2. 將勾選框的節點整個刪除，將form中onsubmit的事件也刪除。
3. 將拉霸的數值調成2020，輸入框的長度限制取消。
4. 將id為flag的值設為true後送出獲得flag。

[Zero Note]

1. 先使用alert測試出網站有XSS。
2. 寫一個會傳出cookie的note。
3. 提交給admin開啟，執行裡面的JS傳出cookie並接收。
4. 將網站的cookie替換成admin的，被server當成admin後查看note裡的flag。

[The Stupid Content Tracker]

1. 透過GitHack的工具將伺服器上的.git整包抓下來。
2. 找到網站有admin\_portal\_non\_production目錄，發現需要登入。
3. 將git版本回捲到.htpasswd還在且還是明碼的狀態。
4. 在網站上使用.htpasswd的資訊登入後獲得flag。

[Zero Note Revenge]

1. 依照提示嘗試訪問不存在的note，發現會顯示debug的資訊，其中有包含所使用的cookie。
2. 使用XSS攻擊在note中寫入訪問不存在note的網頁並回傳資料。
3. 提交給伺服器開啟note網頁。
4. 在傳回的資料中找到admin的cookie中有flag。

[Zero Meme]

1. 先使用alert測試出網站有XSS。
2. 確認可以使用XSS讓meme網頁將使用者的cookie送出。
3. 需要讓admin在meme網頁上進行XSS，讓memem網頁把admin的cookie流出。
4. 測試如果送出連結網址，admin所做的操作相當於點開連結網站。
5. 確認admin方的流程為:收到連結後，先重新登入網站再點開連結。
6. 使用git架設一個簡易的跳板網站，功能為送出XSS的代碼到meme網站上。
7. 將git的網站連結傳給admin，admin會先登入拿到cookie後，進入跳板網站，自動送出XSS代碼讓meme網頁送出cookie。
8. 在webhook中接收到admin流出的cookie即為flag。