**郭又嘉**

**AosoraKuo**

**B06705020**

**TinyURL**

從看完app.py檔案之後

發現他會在你輸入一個網址之後

把你的網址紀錄進他的redis資料庫裡面

然後隨機產生一個縮網址

你要造訪縮網址時他會在從資料庫裏面拿檔案出來

然後GET那個網址拿Title

所以我們可以用SSRF把他的資料庫裡面塞我們的shellcode(類似gopher+redis)

然後再讓他自己拿資料庫裏面的我們塞進去的東西

拿出來執行

首先是先在自己虛擬機開的docker上開一個redis測試

發現每次自己的TinyURL在收到一個網址的時候都會留下一個session

裡面內容是\x00\x00之類的

經過查詢覺得他是python3的序列化後的code

也就表示我們要塞到session裡面的shellcode也需要經過python3序列化

所以寫了一個tinyurl.py幫忙

再來就用curl去訪問TinyURL

然後用在要POST的東西裡面塞我們的序列化後的shellcode加上設成session時要用到的程式碼

大概是長這樣:

curl -X POST --data “url=~~~Set Session:…~~shellcode~~” <https://edu-ctf~~~>

設定完之後就把TinyURL的session改成剛剛我們設定好的session再讓他去跑

就可以再我們提前監聽的外網port上面收到shell囉