**系統與網路安全實驗 lab5-2**

B04902103 資工四 蔡昀達

**Code**

* Python3
* Flask
* requests
* urllib
* python3 app.py
* http://127.0.0.1:5000/login

**Report**

1. Which grant type does the authorization flow follow?.

Authorization code grant

1. If your app is designed to read user’s private repo only, is your request scope over-privileged. Why or why not?

Yes, the repo scope grants full access including write access instead of read access only.

1. Find at least one possible security vulnerability or weakness of GitHub OAuth2 implementation.
2. The access token is passed as a get parameters.
3. The access token can be reused by many different client.
4. The scope is over-privileged.
5. How can you exploit the vulnerability or weakness?

When the access token is passed as a get parameters, the access token ends up being logged in access.log files (being the access token part of the URI). There is a risk of access token leakage through the referrer. An HTTP referrer is a special HTTP header field that browsers attach when surfing from a page to another. In this way the new webpage can see where the request originated. if a document contains a link and if the victim clicks on the link the above mentioned referrer will leak the access token.

- The attacker craft a special Word document containing a link to a website he owns (MUST be https though)

- The attacker upload the file to the PARTNER\_WEBSITE

- The attacker shares this document with the victim

- The attacker waits for the victim to access the document and click to the link

1. What are the possible defense mechanisms?

Don’t use GET.