مینی پروژه شماره ۱

درس: مبانی امنیت شبکه‌های کامپیوتری

استاد: دکتر مهسا سعیدی

دستیاران آموزشی: علی عابدینی، علی دارابی و محمدرضا ولی

نیمسال اول سال تحصیلی ۰۵-۱۴۰۴

در این تمرین شما با OAuth 2.0 که یک پروتکل برای Authorization کاربران می‌باشد آشنا خواهید شد. پس از مطالعه کافی در مورد پروتکل OAuth و چگونگی کارکرد آن، دستورالعمل مربوطه را انجام داده، گزارش خود را تهیه کردن و در انتها به سوالات مطرح شده پاسخ دهید. توصیه می‌شود لینک‌های موجود در بخش منابع را قبل از انجام مراحل دستورالعمل مطالعه کرده و همچنین بخش نکات را پیش از شروع مراحل مد نظر قرار دهید.

1) دستورالعمل

در طی این دستورالعمل لازم است یک برنامه تحت وب ساده که از سیستم احراز هویت سرویس Github.com برای Authorization استفاده می‌کند را تولید نمایید. این برنامه با استفاده از پروتکل OAuth اطلاعات پروفایل کاربر را پس از ورود موفق نمایش خواهد داد. در این تمرین استفاده از روش Authorization Code Grant Type مورد نظر می‌باشد.

فرآیند Authorization در این روش شامل 4 مرحله خواهد بود:

1. انتقال کاربر به صفحه احراز هویت سایت Github پس از فشردن دکمه ورود در صفحه برنامه ایجاد شده
2. ارجاع کاربر پس از احراز هویت توسط Github به برنامه ایجاد شده توسط شما و دریافت کد ارجاع
3. دریافت Access token با استفاده از کد ارجاع دریافت شده و پارامترهای کلاینت
4. استفاده از Access token دریافت شده برای درخواست اطلاعات پروفایل کاربر از API سرویس Github

برای پیاده‌سازی مراحل زیر را طی کنید:

1. ابتدا باید با استفاده از راهنمای موجود در این لینک یک OAuth app را در اکانت Github خود ایجاد کنید. در فیلد callback url لازم است آدرس ارجاع پس از احراز هویت توسط Github را وارد کنید. به عنوان نمونه در این تمرین لینک ارجاع برابر http://localhost:8589/oauth/redirect خواهد بود.
2. پس از ساختن OAuth app، فایل سروری که در اختیار شما قرار گرفته است (server.py) را با استفاده از دستورات زیر (در مسیر دایرکتوری server) اجرا نمایید. در صورتی که سرور با

موفقیت اجرا شود، پیغامی مبنی بر فعالیت سرور روی پورت 8589 نمایش داده می‌شود. همچنین شما می‌توانید به راحتی پورت مربوط به سرور را در فایل server.py تغییر دهید. لازم به ذکر است در صورت تغییر پورت سرور، مقدار callback url در OAuth app خود را نیز با توجه به مقدار پورت مربوطه به‌روزرسانی کنید.

```
$ pip3 install fastapi

$ pip3 install uvicorn

$ python3 server.py
```

3. در این مرحله لازم است تا یک صفحه قابل اجرا و ساده با فرمت HTML و با نام login.html را طراحی کنید. این صفحه شامل یک دکمه با نام login بوده که با کلیک کاربر بر روی آن به صفحه احراز هویت سایت Github منتقل می‌گردد. توجه داشته باشید که درخواست مربوط به انتقال به صفحه احراز هویت Github باید شامل پارامترهایی که اطلاعات مربوط به آن‌ها در این لینک موجود است باشد.
4. کاربر پس از احراز هویت موفقیت‌آمیز در سایت Github به آدرس درج شده در callback url ارجاع داده می‌شود. همراه با این ارجاع پارامتری با نام code نیز تامین خواهد شد. سرور server.py با دریافت این ارجاع، پارامتر code را در کنسول در حال اجرا چاپ خواهد کرد و همچنین مقدار آن را در پاسخ برخواهد گرداند.
5. در این مرجله با در دست داشتن مقدار پارامتر code و همچنین مقایدر client_id و client_secret باید از سرویس Github درخواست Access token مربوطه را انجام دهید. این درخواست را به صورت دستی و توسط ابزارهای ارسال درخواست HTTP (نظیر cURL یا Postman) ارسال کرده و پاسخ را دریافت کنید. توجه داشته باشید که در گزارش خود حتما مقادیر مربوطه را ذکر کرده و تصاویر مربوط به انجام مراحل کار را درون گزارش الحاق کنید.
6. پس از دریافت Access token امکان استفاده از API سرویس Github برای شما مقدور خواهد بود. در این مرحله اطلاعات پروفایل کاربر (مانند نام، ایمیل و ...) را با استفاده از API دریافت کرده و نمایش دهید. این درخواست را به صورت دستی و توسط ابزارهای ارسال درخواست HTTP ارسال کرده و پاسخ را دریافت کنید. در این بخش نیز مقادیر مربوطه به همراه تصاویر دقیق از فرمت، محتوا و چگونگی مراحل ارسال و دریافت اطلاعات از API را در

گزارش خود بیان کنید. این تصاویر باید حداقل شامل یک بار انجام مراحل یک پروفایل کاربری Github خود شما باشد.

7. در انتها، در تمامی مراحل بالا که درخواست‌های خود را به صورت دستی ارسال می‌کردید، به صورت خودکار و در فایل server.py پیاده‌سازی کنید. برای این کار می‌توانید از کتابخانه پایتون Requests استفاده کنید. پیشنهاد می‌شود که پیش از پیاده‌سازی، مطالعه مختصری بر روی مستندات کتابخانه‌های FastAPI و Requests داشته باشید. در این تمرین از کتابخانه FastAPI برای سرویس‌دهی وب و از کتابخانه Requests برای سرویس‌گیری از وب استفاده می‌کنیم.

2) سوالات

1. مزیای استفاده از روش Authorization Code Grant چیست؟
2. در صورت استفاده از روش Client Credential Grant در یک نرم‌افزار تلفن همراه، چه ضعف(های) امنیتی متوجه این روش خواهد بود؟
3. آیا نوع Access token دریافتی از انواع شناخته شده (مانند JWT) می‌باشد؟ آیا می‌توان این Access token را Decode کرد؟ در مورد نوع و روش تولید Access token توضیح دهید.
4. با انتقال برنامه تولید شده توسط شما به محیط Production و استفاده از آن در محیط واقعی، حداقل یک مورد ضعف امنیتی برای برنامه شما وجود خواهد داشت. این ضعف امنیتی را شناسایی کرده و برای رفع آن راه حلی ارائه دهید.

ملاحظات تمرین

مهلت تحویل: 21 آذر ماه

- تمرین‌ها به صورت انفرادی انجام می‌شوند.
- لطفا پاسخ خود را در قالب یک فایل PDF با فرمت زیر در سامانه Elearn بارگذاری کنید:

StudentID_Lastname_MP1

- امکان ارسال تمرین نهایتاً با دو روز تاخیر با کسر ۱۰ درصد نمره به ازای هر روز وجود دارد.
- در صورت استفاده از منابعی غیر از کتاب مرجع در انجام تمرین، لطفاً حتماً نام منبع خود را ذکر کنید. در صورت مشاهده شباهت غیرمعمول میان پاسخ‌های دو نفر یا در صورتی که پاسخ‌ها برابر با محتوای منابعی غیر از کتاب مرجع باشد و نام منابع مورد استفاده ذکر نشده باشد، نمره‌ای برای شما منظور نخواهد شد.
- توصیه می‌شود برای انجام این تمرین از یک توزیع لینوکس مانند Ubuntu یا Debian استفاده کنید.
- برنامه شما فقط باید مجوز دسترسی به اطلاعات پروفایل کاربر را داشته باشد.
- در هر مرحله از انجام این تمرین، تصاویر مناسب از انجام عملیات را درون گزارش خود الحاق کنید.
- موارد تحویلی شما باید یک فایل فشرده شامل گزارش به صورت فایل pdf و همچنین یک دایرکتوری با نام server (حتما شامل فایل login.html و server.py) باشد.
- گزارش شما باید لازم و در عین حال کافی باشد. تعداد صفحات یک گزارش کیفیت آن را تعیین خواهد کرد.
- دقت داشته باشید که در انتهای این تمرین، OAuth app ساخته شده در Github را حذف کنید تا امکان سوء استفاده از آن به وجود نیاید.

- شما می‌توانید برای آشنایی با انواع OAuth Grant Type به این لینک، برای کسب اطلاعات دقیق در مورد API سرویس Github به این راهنما و برای آشنایی با مفهوم Scope و انواع آن در پروتکل OAuth سرویس Github به این لینک مراجعه کنید.
- می‌توانید سوالات خود را از طریق آیدی‌های تلگرام زیر یا گروه تلگرامی درس مطرح کنید:
  - abediniAli1@
  - Ali_819@
  - Jaxteler@

موفق باشید!