CMPUT 404 Lab 9

November 2, 2016

Overview

- Understand the basics of authentication for web-based applications.
- Understand what HTTP Basic, HTTP Token, and HTTP Session Authentication are.
- Understand what OAuth and OAuth2 are.
- Understand the security implications of authentication schemes.

Steps

1. Clone this repository

2. Create a Python virtual environment and install the requirements.

   ```
   virtualenv venv
   source venv/bin/activate
   pip install -r requirements.txt
   ```

3. Navigate to the `leopard` application, migrate the Django application.

   ```
   cd leopard
   python manage.py migrate
   ```

4. Navigate to the `iguana` application, migrate the Django application.

   ```
   cd ../iguana
   python manage.py migrate
   ```

5. Within the `iguana` application, create a superuser.

   ```
   python manage.py createsuperuser
   ```

6. Run the `iguana` application on port 8000.

   ```
   python manage.py runserver 8000
   ```

7. Open a new terminal, activate the virutalenv and run the `leopard` application on a port 9000.

   ```
   source venv/bin/activate
   cd leopard
   python manage.py runserver 9000
   ```

8. Use the `leopard` application to query the `iguana` application's user API using the three authentication methods: no authentication, HTTP Basic, and HTTP Token. Use the username and password for the superuser you created for the `iguana` application.

Hints

Examine the source of the `leopard` app! Particularly `consumer/views.py`.

Questions

Remember to cite your sources!

1. Provide an example HTTP **request** header(s) for authentication with HTTP Basic Authentication. Use username `cmput404` and password `skruntskrunt`.
2. Briefly explain the actors (end-user, user-agent(s), server(s)), involved in HTTP Token Authentication, and a sequence of how an end-user will authenticate (like a UML sequence diagram, but you do not need to draw or submit a diagram).
3. Provide example HTTP **response** header(s) for authentication with HTTP Session Authentication.
4. What is OAuth and OAuth2? Name one OAuth2 provider.
5. Assume a client and a server are using HTTP over an unencrypted connection. Explain how you would hijack the client's authentication if they are using HTTP basic authentication, HTTP token authentication, and HTTP session authentication.
6. What type of authentication did you use to login to eClass?