Lab 9 - Authentication

Published on Wed, 20 Feb 2019 at 14:47 MST
Last Modified on Thu, 07 Mar 2019 at 18:17 MST

By Alexander Wong

Category: Lab
Tags: django authentication

Learn the basics of authentication for web applications. Explore the provided Django Rest Framework applications utilizing HTTP Basic, HTTP Token, and HTTP Session authentication. Understand the high-level intention behind OAuth/OAuth2 and the security implications behind these different authentication schemes.

Fork and clone the authentication lab repository.

- github.com/uofa-cmput404/authentication-lab

Follow the Getting Started instructions and run the application locally.

```
virtualenv venv --python=python3
source venv/bin/activate
pip install -r requirements
./manage.py migrate
./manage.py createsuperuser
./manage.py runserver
```

Navigate to the `/api` route and log into the browsable API. Create a new code snippet.

Question 1: What authentication scheme is used by default in Django Rest Framework's browsable API? How is this managed?

In a new terminal, use `httpie` to query the api endpoints.

```
http POST http://127.0.0.1:8000/api/snippets/ code="print(123)"

http -a username:password POST http://127.0.0.1:8000/api/snippets/ code="print(123)"
```

Question 2: What authentication scheme is used by `httpie` when querying with the `-a` or `--auth` option flag?

Configure Token Authentication

Official documentation can be found here.

Within `authlab/settings.py`, add `rest_framework.authtoken` into the `INSTALLED_APPS` setting. include `TokenAuthentication` in the Django Rest Framework settings.

```
INSTALLED_APPS = [
    # ...
    'rest_framework',
    'rest_framework.authtoken'
]

# ...
# Django Rest Framework
REST_FRAMEWORK = {
    'DEFAULT_PAGINATION_CLASS': 'rest_framework.pagination.PageNumberPagination',
    'PAGE_SIZE': 10,
    'DEFAULT_AUTHENTICATION_CLASSES': (
        'rest_framework.authentication.BasicAuthentication',
        'rest_framework.authentication.SessionAuthentication',
        'rest_framework.authentication.TokenAuthentication'
    )
}
```

Run `./manage.py migrate` after changing the settings.

Register the token model in the Django project admin dashboard. Update `client/admin.py` to be the following:

```
from rest_framework.authtoken.admin import TokenAdmin

TokenAdmin.raw_id_fields = ('user',)
```

Navigate to the Django admin dashboard and create a new token for your user.

Use `httpie` to create a new code snippet using token authentication.

Replace `YOUR_TOKEN` with your token in the following command:

```
http POST http://127.0.0.1:8000/api/snippets/ "Authorization:Token YOUR_TOKEN" code="print('Token works')"
```

For example, if your token is `56b9afcaccad879e5bd9b39fe622927f17163092`, then you should run the command:

```
http POST http://127.0.0.1:8000/api/snippets/ "Authorization:Token 56b9afcaccad879e5bd9b39fe622927f17163092" code="print('Token works')"
```

Question 3: What is the difference between `Session Authentication` and `Token Authentication`? How is `Token Authentication` an improvement over `Basic Authentication`?

Identity and Authentication

Identity management on the web can be a difficult problem. Consider the following features a good web application may have for identity management:

- Forgot Password/Forgot Username workflows
- Email verification
- Sign in with Google, Facebook, GitHub, etc.
- Password-less authentication (Medium, Slack, WhatsApp)
- Two Factor Authentication:
  - by sending a One Time Password (OTP) through voice to a phone number
  - by sending a OTP text message to a mobile number
  - utilizing a Time-based or HMAC-based OTP algorithm
  - using Hardware Tokens (YubiKey, Solo)

Question 4: Provide a high level summary of what happens during an OAuth2 authentication flow. For instance: `bitbucket.org` > `Log In` > `Log in with Google`. What happens when I click "Log in with Google"?

Question 5: Please provide a link to your code.

- Hint: DigitalOcean introduction to OAuth2

Optional: Configure your Django project and Django Rest Framework API to utilize OAuth2.

- Auth0 Django bindings and tutorial
- Additionally, you can use github.com/jazzband/django-oauth-toolkit to create an OAuth2 provider for others to use.
- *You are not expected to implement OAuth for your project!*
