Hardening an oTree Deployment on Heroku

Max R. P. Grossmann

If you run oTree on Heroku, please take a few minutes to apply the steps below. The default Heroku deployment is not configured the way you probably assume it is, and a routine upgrade on its own does not change that. Treat this as time-sensitive.

1. Set the environment variables

From a shell with the Heroku CLI authenticated and your app's git remote configured:

```
heroku config:set \
    OTREE_AUTH_LEVEL=STUDY \
    OTREE_ADMIN_PASSWORD='<a long random password>' \
    OTREE_PRODUCTION=1 \
    --app YOUR-APP-NAME
```

All three matter. `heroku config:set` restarts every dyno automatically, so both the `web` and `worker` processes pick up the new values on their next start. An empty string counts as "unset" — the value must literally be `STUDY`.

2. Verify the config landed

```
heroku config --app YOUR-APP-NAME | grep OTREE_
```

You should see all three variables present with the values you set.

3. Pin a current oTree

The default project skeleton ships a `requirements.txt` with a header comment saying oTree may overwrite the file. Remove that header first so your

pin survives, then pin a current release:

```
otree==5.11.5     # or otree==6.0.14 if you are on the 6.x line
psycopg2>=2.8.4
```

Older releases are not acceptable. If you are behind, update now.

4. Commit and deploy

```
git add requirements.txt
git commit -m 'Pin current oTree'
git push heroku main       # or: git push heroku master
```

If you deploy from a container or a private registry instead of `git push`, rebuild the image against the pinned version and re-release it — `heroku config:set` alone does not upgrade the oTree package.

5. Confirm in the admin UI

Log in to the admin interface and open `/server_check`. You want:

- A **green** *"Password protection is on. Your app's `AUTH_LEVEL` is `STUDY`"* alert.
- A **green** *"DEBUG mode is off"* alert.

If you see a red *"No password protection"* alert instead, the variable did not reach the process and the deployment is not yet hardened. Re-check step 1 and make sure the dynos have actually restarted.

A general note

Please also run oTree servers only for as long as the study strictly requires, and tear them down when you are done. Keeping an idle server reachable on the public internet is not free, even when nothing visible is happening on it.

If you have questions about any of the above, reply to me directly — please do not forward this note more widely for the time being.