CSRF

Deliverable for this lab: briefly add the following information to the deliverable

- ***1.1: add a screenshot of the HTML code of the page you use to initiate a CSRF attack***
- ***1.2: explain briefly why the attack does not work anymore after the CSRF protection deployment***

1.1 CSRF attack

In this exercise you will attempt a CSRF attack. Make sure you understand the explanation of the token synchronizer pattern given on https://apwt.gitbook.io/software-security/access-control-basics/000introcsrf/002csrfprotection#without-the-synchronizer-token-pattern .

Take a look at the form at https://nodegoat-websec.herokuapp.com/profile (you need to be authenticated for that: the teacher has credentials for you), and investigate whether or not it is protected by a synchronizer token. If not, try to execute a CSRF attack.

If you are stuck, take a look at https://portswigger.net/web-security/csrf/lab-no-defenses for some inspiration.

1.2 CSRF protection

Wait until the teacher deploys a CSRF defense and retry your attack. Does it still work?