Key term: CSRF, Cross site request forgery

**Refinement 1:**

Open link: https://efdsearch.senate.gov/search/home/
Agree to terms and conditions to collect validated CSRF token
Open search page and request for data using filters
Iterate through pagination to scrape all the data on the tables

**Refinement 2:**

Open link: https://efdsearch.senate.gov/search/home/

```
Get past terms of service
##When a person clicks the checkbox, the website sends a request to the server side validating CSRF token, so in our case we send the request ourself with our CSRF token which is given as a cookie in the beginning of the website

Collect validated CSRF token through the cookies of the website
##Once we validate the CSRF token we store in a variable so that we can have a validated CSRF token to implement future requests.

Open search page
Search for data based specific filters
Send a request to the resulting table
## Using the validated CSRF we can send a request to the search page, with a payload attached with all the preferred filters

Going through all the pages of the table, the table is paginated iteratively
## If there are is more than one page in the table we have to detect that and iterate through all the pages(POSSIBLY recursively)

loop through each row in table
        Open the link in each row which returns a html file

        Scrape all the data from the from each row iteratively as well
        ##We retrieve the html page from the previous request and parse the html file for a table
        ##Than we iterate through the table and store each row in our local database
```