CS3235 AY2021/22
Web Security Coding Assignment

Due Date : Friday, 22 April 2022, 23:59 pm SGT

1 Setting Up

We will be using Github Classroom for autograding this assignment. Please follow the instructions below to set it up.

1. Follow previous instructions to set up the Docker. Make sure that you can use the provided script to run the tutorial demos.
2. Download the assignment zip file (on Luminus) and extract it to a folder. We will use `ASSIGNMENT_FOLDER` in place of the folder you extract the files to.
3. In the `ASSIGNMENT_FOLDER`, execute `./init`. This will prompt you for your NUSNET ID. Once this is done, two folders `ASSIGNMENT_FOLDER/student/wsb` and `ASSIGNMENT_FOLDER/student/bad` will be present.
4. Visit `https://classroom.github.com/a/MkLG26Ni`. Choose your NUSNET ID from the list and accept the assignment.
5. Once you have joined the Github classroom and accepted the assignment, you will automatically get a Github repository for this assignment. Clone that repository to your local environment. We use `REPO_FOLDER` to represent your local repository folder.
6. Copy `ASSIGNMENT_FOLDER/.studentid` to `REPO_FOLDER/.studentid`:

```
$ cp ASSIGNMENT_FOLDER/.studentid REPO_FOLDER/
```

2 How to Submit

To submit, simply place the files to be submitted in `REPO_FOLDER`, commit and push to your Github repository (we explain what you need to submit and how you should name them in §5). A Github Action workflow will run to evaluate your submission, the results of which should be available within minutes. To see the evaluation progress and results, you can then go to the "Actions" tab of your Github repository.

For more information, take a look at the official documentations of Github Classroom.

- *You may find a folder named* `.github` *inside* `REPO_FOLDER`*. Please do not modify anything inside this folder. Evaluation results for commits with modified* `.github` *will be considered as invalid.*
- *The file* `.studentid` *should be included in your commits. Make sure that it contains your correct NUSNET ID.*

3 Local Evaluation

You can also evaluate your answers locally. In `ASSIGNMENT_FOLDER`, execute `./run-eval REPO_FOLDER`. It is expected that there should be no discrepancy between the local and the online evaluation results. In case you encounter a discrepancy, please ask the TAs for help.

NOTE: Local evaluation results are for your own reference only. The final marks you get for this assignment are decided by your submissions on Github.

4 Tasks

This assignment consists of 5 tasks, each requiring you to obtain a flag value (a random-looking hexadecimal string) either by printing it to the console (with `console.log(...)`) or making it appear in the HTTP response (the returned HTML).

In `ASSIGNMENT_FOLDER`, execute `./run`. It will open a built-in browser if you have a working X server (normally true on Linux-based systems). If it does not open a browser, please append the following two lines to the hosts file (`/etc/hosts` for Linux and macOS users, and `C:\windows\system32\drivers\etc\hosts` for Windows users), and use your own browser:

```
127.0.0.1 www.wsb.com
127.0.0.1 www.badsite.com
```

You have access to two websites, `www.wsb.com` and `www.badsite.com`. You may view their source files which are located in `ASSIGNMENT_FOLDER/student/wsb` and `ASSIGNMENT_FOLDER/student/bad` respectively.

Note: Along with the flag values, there are a few more randomly generated hexadecimal strings in this assignment. Unless otherwise stated, those values will change during each evaluation. For this reason, you should not rely on their values in your solutions.

Below, we omit the prefix `ASSIGNMENT_FOLDER/student` when talking about "relevant files".

Case 1 (6 points)

Relevant files: `wsb/case01.php`

Goal:

1. Open `http://www.wsb.com/case01.php` in browser;
2. Submit the form with your chosen data for up to 5 times;
3. Open `http://www.wsb.com/case01.php` in browser and the flag appears in the console output.

Case 2 (5 points)

Relevant files: `wsb/case02.php`

Goal:

1. Open `http://www.wsb.com/case02.php` in browser;
2. Submit the form with your chosen data. The flag appears in the HTTP response (on the page).

Note: There are two records in the database table. Do not rely on the data in the record that contains the flag. You may assume that the other record is fixed.

Case 3 (6 points)

Relevant files: `wsb/case03.php`

Goal:

1. Create a web page and place it at `http://www.badsite.com/case03.html`;
2. Open `http://www.badsite.com/case03.html` in browser. The flag appears in the console output.

Note: You may assume that the CSRF token does not change.

Case 4 (8 points)

Relevant files: `wsb/case04/login.php`, `wsb/case04/404.php`, `bad/cookie_thief.php`

Goal:

1. Open `http://www.wsb.com/case04/login.php` in browser;
2. Choose a URL in `www.wsb.com` (i.e., `http://www.wsb.com/<you_choose_this_part>`);
3. Open that URL, and the flag appears in the console output.

Note: You may assume that the CSRF token does not change.

Case 5 (8 points)

Relevant files: `wsb/case05/login.php`, `wsb/case05/index.php`, `wsb/case05/delete.php`

Goal:

1. Open `http://www.wsb.com/case05/login.php` in browser;
2. Open `http://www.wsb.com/case05/index.php` in browser;
3. Submit the form with your chosen data. The flag appears in the console output.

5 What to Submit

Please include the following files directly inside `REPO_FOLDER`, with the required file names (case-sensitive):

- **Case 1:** Place the "title" field and the "content" field for the first form submission in `case01.title1` and `case01.content1` respectively. As it might be necessary to make multiple form submissions, you may provide the contents for subsequent form submissions in files `case01.title2`, `case01.title3`, ... and `case01.content2`, `case01.content3`, ... Up to 5 form submissions are allowed.
- **Case 2:** Provide the content for the "search" field in `case02.search`
- **Case 3:** Provide the web page you constructed in `case03.html`
- **Case 4:** In `case04.path`, provide the path name of the URL you constructed (the part indicated in `<you_choose_this_part>`).
- **Case 5:** In `case05.say`, provide the content for the form submission.

6 Report

Aside from submitting the required files for each task to your Github repository, you also need to write a short report to describe your methods and submit it on Luminus before the deadline.

For every task you have finished, write a few sentences to briefly explain the sequence of events that lead to the appearance of the flag, including the part that your answer plays.

In the report, please also indicate the hash of the Github commit you want to use for the final grading.

7 Grading

This assignment is worth 33 points. We will use the evaluation results from Github Classroom.