Lab 3: PUT attack

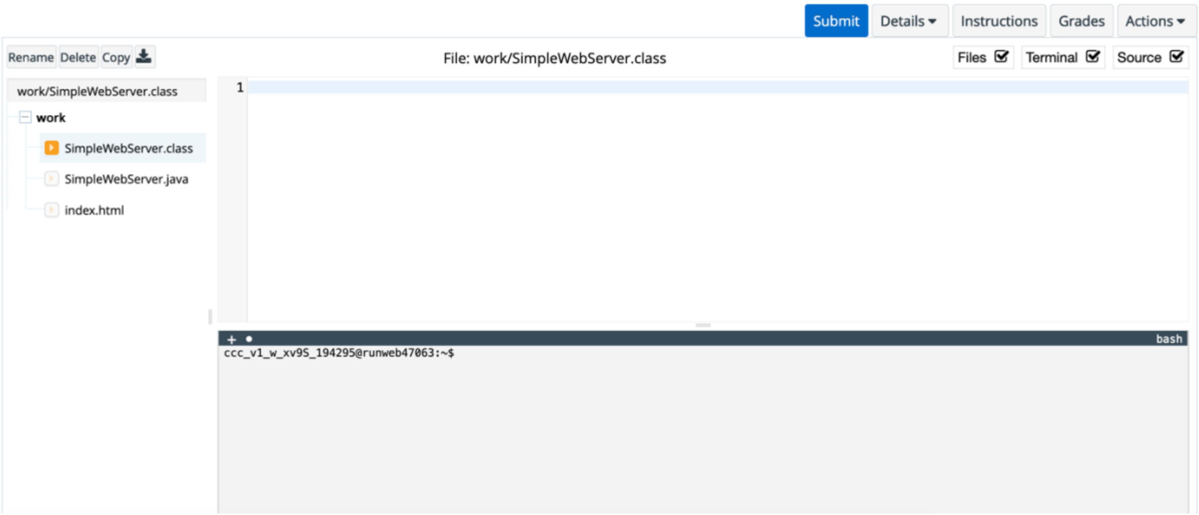
Objective and Set Up:

The goal of this assignment is to show you how an attack can change a web page. You will create a "malicious" index.html file and upload it by using the PUT method that you added to SimpleWebServer.java in the previous Lab 2.

NOTES:

- *In this exercise you need to change the index html file. The lab is completed by uploading the "bad" index.html to the web server.*
- *This assignment is optional and is not graded, but it is highly recommended you complete it.*
- *We encourage you to find a solution yourself. If you get stuck, you can use useful hints at the end of the guide.*

There should be three files in your work area on the left panel. You will see a preview of the files on the top right, and the terminal window on the bottom right.



```
ccc_v1_w_xv9S_194295@runweb47063:~$
```

This is a description of each file in your work area:

SimpleWebServer.java: The web server file that supports PUT (from Lab 2).

SimpleWebServer.class: This is the class file compiled from SimpleWebServer.java.

index.html: The original html file that displays a Hello World message.

PUT Attack Lab

Objective:

Your goal in this exercise is to deface the index web page. You will need to change the index.html with a bad message.

A successful attack means that you will see the defaced index page of SimpleWebServer. That is, instead of seeing a response message from SimpleWebServer

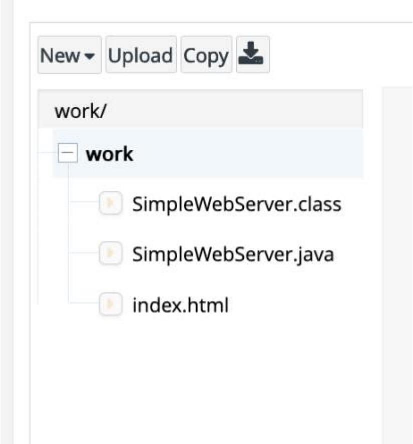
"Hello world"

You see a different message that you changed in a new index.html.

Instructions:

1. Create and edit a malicious index.html.

2. Upload your SimpleWebServer from Lab 2, which supports the PUT functionality. In the File pane select the work folder and click the 'Upload' button. In the popup dialog navigate to the SimpleWebServer.java and upload it.



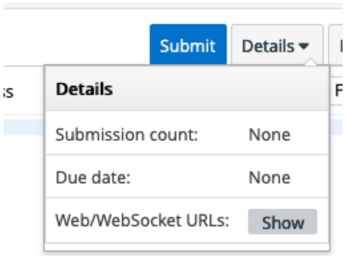
3. Compile the modified SimpleWebServer.java in a terminal by typing

```
javac SimpleWebServer.java
```

4. Start the SimpleWebServer by typing:

```
port=`voc_get_proxied_server_port`
java SimpleWebServer $port
```

5. Find "Details" on the upper navigation pane of the Lab Environment, and click on "Show" next to "Web/WebSocket URLs". This will open a new window. Copy the Web URL link (not the WebSocket) and paste it in a browser window on your computer.



Submission count:	None
Due date:	None
Web/WebSocket URLs:	Show

5. In a separate terminal window, upload the malicious index.html file to SimpleWebServer using PUT method. You can review an example in the Lab 2 Solutions to see how to upload a file to SimpleWebServer (curl or Postman).

6. Refresh the browser and access the index file, if the attack was successful, the newly uploaded index file will show.