

IFS4103 Individual Assignment: Portswigger Lab Tasks (12 Marks)

1. Background & Grading Scheme

As explained in Lecture 1, there is an individual *lab-related* **assessment component** (worth 20% of your final marks) in our course. From your four **graded lab tasks**, which are based on the shared lab notes, you can obtain up to **8 marks**. The remaining **12 marks** will be based on several selected web pen-testing labs in Portswigger's Web Security Academy. This brief document explains the tasks that you need to do on the selected labs.

2. Selected Portswigger's Labs

The **purpose** of the assigned tasks is to facilitate your hands-on self-learning using good available resources provided by Portswigger's Web Security Academy. It has a number of useful **online labs** that you can go through in order to hone your web pen-testing skills using Burp Suite. To access the lab, as previously mentioned, you will need to have **an account** with Portswigger's Web Security Academy.

Please complete **all the following six labs** selected by Ensign:

1. Lab: CSRF vulnerability with no defenses:
<https://portswigger.net/web-security/csrf/lab-no-defenses>.
2. Lab: Insecure direct object references:
<https://portswigger.net/web-security/access-control/lab-insecure-direct-object-references>.
3. Lab: Web shell upload via obfuscated file extension:
<https://portswigger.net/web-security/file-upload/lab-file-upload-web-shell-upload-via-obfuscated-file-extension>.

4. Lab: File path traversal, validation of file extension with null byte bypass:
<https://portswigger.net/web-security/file-path-traversal/lab-validate-file-extension-null-byte-bypass>.
5. Lab: Exploiting a mass assignment vulnerability:
<https://portswigger.net/web-security/api-testing/lab-exploiting-mass-assignment-vulnerability>.
6. Lab: DOM-based open redirection:
<https://portswigger.net/web-security/dom-based/open-redirection/lab-dom-open-redirection>.

3. Tasks & Submission Instructions

For this assignment, please **complete** the six selected labs above, and **attach some screenshots** (must be *in colour*) for each lab as your sufficient proof of completion. You will obtain **2 marks** for each completed lab.

Note that the **solutions** to the labs are already given by Portswigger's Web Security Academy. Various **community solution videos** are also available online, including those listed by Portswigger in each of the labs. You just need to refer to the solutions and the shared solution steps. While the deadline has been pushed to the end of the reading week, you are *encouraged to finish the tasks earlier* so that you can be more prepared when pen-testing NUS apps in Project 2.

For your answer submission, please follow these **instructions**:

- Put the requested screenshots in a self-contained **PDF file** by using your **name and matric no** as part of your file name, e.g. JackLee-A012345-PLT.pdf.
Your report PDF should also contain your name & matric no on its first page.
- Upload your PDF file via "**Portswigger Lab Tasks**" Canvas Assignment by **Saturday, 27 April 2024, 23:59 SGT**.

There will be **no deadline extensions**, and there will be following **penalties for late submissions**:

- Late up to 12 hours: Maximum possible marks are capped at 90%.
- Later than 12 hours but no later than 1 day:
Maximum possible marks are capped at 80%.
- Later than 1 day (subject to approval only):
Maximum possible marks are capped at 70%.

4. Useful Resources

As mentioned above, various **community solution videos** are available online, including those listed by Portswigger in each of the labs. The following two **video authors** are particularly helpful:

- Intigriti:
<https://www.youtube.com/@intigriti/videos>.
- Rana Khalil:
<https://www.youtube.com/@RanaKhalil101/videos>.

Please feel free to refer to the videos uploaded by the two authors, among others, when completing the selected labs.

5. Queries & Contacts

Please send your queries to the course Instructor (dcssu@nus.edu.sg) by using email subject title: “IFS4103 Queries - Portswigger Lab Assignment”.

You can consult the Ensign consultant team on the assigned lab tasks during our lectures in the class.

All the best for your Portswigger’s lab tasks, and happy hacking!