IFS4103: Graded Lab Tasks 2
(Burp Suite's Scanner – 3 marks)

For this GLT 2, please use the shared **Burp Suite Pro license** to utilize **Burp Scanner**. You can refer to **Lab 3** for scanning a target site and selected URLs. Additionally, you can refer to this "Complementing your manual testing with Burp Scanner" short video to see the difference between "Scan", "Do passive scan" and "Do active scan" options when conducting you scanning.

To perform the tasks given below, you need to run **DVWA** as your target web app. DVWA v1.8 is included in the shared OWASP Broken Web Applications (BWA). You can refer to **Lab 2** for running OWASP BWA. Note that the default credential for DVWA v1.8 is: **username="admin"** and **password="admin"** (instead of password="`password`" in the previous DVWA versions, e.g. v1.0.7).

Please perform the following two tasks:

- **Task 2-1 (1.5 marks)**: Visit the DVWA's page for **"XSS reflected"** (<*ip-address*>/dvwa/vulnerabilities/xss_r). In your Burp Proxy's HTTP history, select the recorded request entry, right-click on it, then perform "**Do active scan**". Attach a screenshot (must be *in colour*) of your **Burp's Dashboard** showing its **Issue activity** panel with Cross-site scripting (reflected) entry shown. Additionally, check the scan request sent by Burp Scanner as shown in the **"Request" tab** at the bottom of the Issue activity panel. Which HTTP request's parameter carries the injected PoC script?
- **Task 2-2 (1.5 marks)**: In your Burp **Target's site map**, find an entry for "dvwa". In the **Contents** panel, you should be able to check that its URL is "/dvwa/". Do right-click on it, then select "**Scan**". In the shown New scan window, do select "**Crawl and audit**" scan type, with URLs to scan set as

"http://<*ip-address*>/dvwa/". You can just use a preset scan mode named "**Fast**". After the launched crawl and audit are finished (as shown in the Dashboard's **Event log** panel), do attach a screenshot (must be *in colour*) of your Burp's Dashboard which also shows its **Issue activity** panel. How many High and Medium issues are reported by using the scan mode? (You can simply select "High" and "Medium" buttons in the Issue activity panel's filter section to get only High and Medium issues shown.)

Like GLT 1, please follow these **instructions** for your submission:

- Please put the requested screenshots in a self-contained **PDF file** by using your **name and matric number** as part of your file name, e.g. JackLee-A012345-**GLT2**.pdf. Your report PDF should also contain your name and matric number on its first page.
- Upload your PDF file via "**`Graded Lab Tasks 2`**" Canvas Assignment by **Wednesday, 21 February 2024, 23:59 SGT**. Note that this deadline is a ***firm & final*** **deadline**. There will be ***no*** deadline extensions given. As such, you are advised to submit **well before** the cut-off time so as to avoid any technical issues with Canvas access or your uploading!

Happy scanning!