Faculty of Computing and Information Technology
University of the Punjab
(Term Spring 25)

CC-403 Information Security Student ID:_____

Class Activity 03

Marks: 80

This activity is about **Penetration Testing of Web Application** related to Handout # 2.9 and 2.10. You should attempt the following tasks on your own laptops in the lab virtual environment. Need to submit a hand written document (1-2 pages for each task) to the TAs on the day of your viva-voce exam related to each task. TAs will evaluate the hand written task only if the related PoCs are running on your laptops as well. TAs need to collect and submit the handwritten documents to me. TAs of all the sections will announce the RV, day, and time of viva after coordinating with the CRs of their respective sections.
Happy Learning to all…

Task 01 (Overview of Tools): **[10]**
From your Kali Linux machine, use a browser, `curl` and `wget` utility to access the landing pages of following websites that should exist in the `/var/www/` directory of your Metasploitable2 (M2) machine. Meanwhile students should run `Burp Suite` to capture the network traffic (HTTP request/response objects) and get ready to answer the viva questions of the TAs regarding all the related concepts (Do look for cookies inside the DevTools of your browser and inside Burp).

- `http://<IP of M2>/dvwa/login.php`
- `http://<IP of M2>/books/index.html`

Task 02 (Brute Force Attacks): **[10]**
Use `hydra` and `burp` to launch Brute force attack on the following link (Note: Do this task with DVWA security level to low and medium)

- `http://<IP of M2>/dvwa/vulnerabilities/brute/index.php`

Task 03 (Command Injection Attacks): **[10]**
Exploit command injection vulnerability inside DVWA to perform the following tasks (Note: Do this task with DVWA security level to low and medium):

- Craft an input that will create a bind shell on M2, which you can connect from Kali.
- Craft an input that will create a reverse shell on M2, which can connect to a listener (`nc`) running on Kali.
- Write down all the steps/commands that you will follow to achieve a `meterpreter` shell on your Kali machine by exploiting command injection vulnerability inside DVWA.

Task 04 (SQLi Attacks): **[10]**
Practice performing classic SQLi attacks as discussed in HO#2.10 using DVWA SQLi page as well as using `SQLMap`. Be ready to perform any task mentioned by TAs during viva-voce and describe the payload that you have used to perform that task. (Note: Do this task with DVWA security level to low and medium).

Task 05 (Browser Exploitation): **[20]**
For this task, you need to have three machines: Kali (attacker), Windows10 (victim), and M2 running DVWA. The steps to perform this task are mentioned below (Note: Do this task with DVWA security level to low):

- From Kali, inject BeEF hook into DVWA (M2) via XSS, so that every visitor to the Guestbook page will now load `hook.js` from Kali. From Win10 visit the DVWA page on M2, the injected BeEF hook forces the victim's browser to connect back to BeEF running on Kali. Once you have successfully hooked the victim browser inside your BeEF running on Kali, you can perform lot of tasks as discussed in class, but for this task you need to get a `meterpreter` session of Win10 on Kali:
  - Generate an appropriate payload on Kali for Win10 machine (`payload.exe`)
  - Start apache2 on Kali and host the payload inside `/var/www/html/`
  - Use MSF, and set up a multi handler listener on Kali
  - Launch a Social Engineering attack by using a pop-up alert tricking user on Win10 to click it, and this should download the above payload on Win10 machine.
  - User on Win10 clicks link → Downloads/runs `payload.exe` → Meterpreter session opens on Kali ☺

Task 06 (Overview of Tools): **[20]**
Use the `setoolkit` (discussed in HO#2.10) and generate a pdf file with embedded payload in it. When a user opens the infected pdf file in his/her laptop or mobile phone, a reverse/meterpreter shell should be spawned on your Kali Linux machine. (To get full credit, use `ngrok` to make this work outside the virtual lab setup)