Chapter 11: Web Application Vulnerability Scanning using OWASP ZAP

1. Start and login to your Kali Linux virtual machine as user kali with a password of **kali**.

2. Open a terminal windows and type sudo **ifconfig lo up**. This will ensure that the local loopback interface is up and running. We are doing this since by default Wireshark will not capture local traffic as you will be for testing purposes.

3. From the Kali Linux menu in the upper left, type in **wire** and click wireshark.

4. In the Wireshark interfaces list, double-click **Loopback:lo**. This begins a packet capturing session on the local loopback interface.

5. In a Kali Linux terminal window, type **sudo hping3 -S 127.0.0.1 -a 1.2.3.4 -c 5**. This will send five (-c 5)packets to 127.0.0.1 but will show the source IP address (-a) as being 1.2.3.4.

6. Switch back to Wireshark. Notice there are five packets from 1.2.3.4. Click the red stop button to stop the packet capture. Keep Wireshark open.

7. Back in a terminal, type cd and press ENTER to switch to the current user home directory.

8. Create a fake payload file by **typing echo "This is nothing but fake data" > fake_payload.txt**.

9. Type **cat fake_payload.txt** to view the file contents.

10. Back in Wireshark, from the File menu choose **File**, **Close**, **Continue without saving**, then double-click the **Loopback:lo** interface listing to begin a new packet capture.

11. Switch back to a terminal window.

12. To send a completely forged packet, type **sudo hping3 127.0.0.1 -a 1.2.3.4 -p 555 -d 500 --file fake_payload.txt**. This sends 500 byte packets with a destination port of 555 from 1.2.3.4 using our fake payload file as the packet data.

13. Switch back to Wireshark and stop the capture by clicking the red stop button. Click on any captured packet from 1.2.3.4. In the center panel next to **Transmission Control Protocol** (the TCP header), notice that the destination port is set to 555. Down in the bottom panel notice our fake payload showing up in the packet data.