Assignment 210

This assignment is worth 15% of your final mark for COMP 210. Please submit your work as a PDF file using the link provided on Blackboard (click the Assignment 1 title above) by 5:00 p.m. on Friday August 27

You may work individually or in pairs for this assignment. If you do not have a strong technical background in computing/IT, you are encouraged to team up with someone who does. Conversely, if you are technically experienced, consider offering to pair up with someone less experienced. Only one member of the pair needs to submit (but make sure that both contributors are clearly identified).

Your report must be submitted in PDF format (use the Export or Print to File function of your word processor), and **should include the following:**

- Your name(s) and student ID number(s)
- A brief summary of the system, in terms of function and technology
- Identification of security flaws. For each:
  - Identify and briefly describe the flaw
  - Provide the relevant CVE number
  - Describe how the flaw was detected (in enough detail that someone else could replicate it)
  - A reflective conclusion/summary

You should investigate at least the following potential security vulnerabilities:

- Weaknesses in password policy or enforcement
- Password storage and management
- Network-level security (e.g. unencrypted HTTP)
- SQL injection
- JavaScript injection
- Path-traversal flaws

See the lectures, demonstrations, and lab work for details on how to proceed. We will also provide help as required during the lab sessions. Running the Virtual Machine

We recommend that you use the Linux lab computers (North CAL, OBS3.27) for this assignment, since all the demonstrated tools will be available, and you might not wish to download a half-gigabyte VM file at home. If you choose to use your own computer, you will need to install VirtualBox first.

To run VirtualBox in the Linux lab, open the Applications menu, go to System and run VirtualBox.

To import the virtual machine image:

- Download the (big!) OVA file from the Assignment 1 item on Blackboard, saving it to your home folder.
- Run VirtualBox and in the File menu choose Import Appliance.
- In the Import dialog, click the folder icon (by the File text field) and select the OVA file you downloaded.
- Click Next.
- Click Import.
- Keep the OVA file you downloaded in case you mess up the virtual machine!

To run the VM:

- Select the COMP 210 VM image at left.
- Click the big green Start button in the toolbar.
- If prompted by a dialog box to switch to Scale mode, click Cancel.
- The VM has started up completely when you see “Web Console server running...” and “TCP server running...”.

You will also need to know the following:

The virtual machine runs in headless mode (no GUI/windowing system). VirtualBox will capture the mouse when you click in the main window. When this happens, the mouse pointer will vanish. Use the Host Key (Right Ctrl) to release the mouse.

The system is running a Web application using Java Servlets and JSPs in the Tomcat Web server. To connect to the application, point your Web browser to http://localhost:8080/catalogue/.

```
The system is also running an H2 database service, which is used as a
storage back-end by the application. You can connect to the H2 console
to run SQL queries via http://localhost:8081. Select the COMP210
profile, use the default sa user, and the password is “spitfire
dogfight bulletin weekend”.
```

To shut down the virtual machine:

```
In the main VirtualBox Manager window, right-click the COMP 210 VM
entry at left, and choose Close > ACPI Shutdown.
In the dialog that opens, choose ACPI Shutdown.
```

COMP210_Audit_System.ova