NUS IFS4103 Penetration Testing, Semester 2 AY2023/24
Pen-Testing Scope and Arrangement
(*App 1: Peer Review System*)

1. Kick-off/Scoping Meeting Information

Date : **Thursday, 22 February 2024**

Time : **4-5pm**

Venue : **F2F in COM3-01-22, SoC**

2. Target System Information

- What is the target system's accessible **domain name** or **IP address** (please also specify the applicable protocols, e.g. HTTP and/or HTTPS)?
  - https://qat-aces.nus.edu.sg/peerreview/

- Which **components/modules** of the system that need to be pen-tested? And which components/modules that are **out of scope** to be excluded?
  - **Initiate Review, Pending Reviews,**
  - **Processed Reviews, Reporting**
  - **[To be Excluded] - Configure approvers functionality**

- Is it a **production** or a **UAT system**?
  - **UAT System**

- Is there any **real data** contained in the application? Or only **dummy** data is contained?
  - **Dummy Data**

- Will the system be **backed up** and/or **snapshotted** before the pen-testing starts?
  - **Yes. QAT data will be backed up**

- Are there any open **URLs/links** about the target system's background information (e.g. online description, user guide, FAQ) or **any short description** that can be shared?
  - 

3. Penetration-Testing Method and Period

- Will the **target system's information** be given (e.g. source code, module design document, etc.), or a **black-box pen-testing** (+ only **additional credentials given**) is preferred?
  - **Black box with staff temporary ID**

- When is the agreed **pen-testing period**? Is the suggested **4 March (Monday) to 12 April 2024 (Friday)** testing period fine?
  - **Yes**

- Will the target system be available **24/7** during the pen-testing period?
  - **Non-office hours may have disruption for deployment, database or server maintenance and patching etc. especially over the weekend.**
- Are there any **time periods** where the pen-testing **should be avoided**, e.g. daily/nightly/weekly backup periods on the target system?
  - **Non-office hours may have disruption for deployment, database or server maintenance and patching etc. especially over the weekend.**
- Will the system be available **from outside** of NUS: is it **without or with** NUS VPN?
  - **Intranet Application, need VPN**

4. Target System's Credentials

- What are the system's **user types/roles** (including possibly its admin user) that need to be tested?
  - **Staff as Dept Admin, Reviewer, HOD, Dean, Reviewee**

- Can **12 different accounts** be created/assigned for ***each relevant user-type/role*** of the application's in-scope components, and be provided during the kick-off meeting?

  User Type 1:

  Note: [User Type and test accounts will be provided following the kick-off meeting and student grouping]

No	Account Name/ID	Password
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		

- Is the following note on **the NUS passwords shared by NUS IT Security** still relevant? "The given passwords are temporary passwords. The students need to change the password of each NUS account issued to a password of their choice before they can access NUS resources. To change the password, please go to https://exchange.nus.edu.sg/passwordportal/, and enter the provided temporary password as the "Old Password"."
  - **Yes**

- Are **2FA-related** authentication steps involved in accessing the target system?
    - ➢ **Yes, for Staff**

5. Deliverables

At the end of the penetration-testing exercise, the following deliverables are to be provided:

- **Penetration-testing report document (1 set):**
  will be emailed by **Wednesday, 17 April 2024 afternoon**.
- **Penetration-testing findings presentation**:
  is scheduled on **Thursday, 18 April 2024, 2-3 pm**.
  The meeting is to be held F2F in COM3-01-22, SoC.

Any found **critical vulnerabilities**, however, will be reported **immediately** by the penetration testing teams to the PoC information given in Part 7 below for immediate follow ups.

6. Confidentiality Agreement

- Will the enrolled students need to sign **an NDA e-form** prepared by NUS IT Security (Attn: Ma Huijuan, ma.huijuan@nus.edu.sg), which needs to be done using DocuSign?
    - ➢ **Yes, follow up by Huijuan**

7. Contact Information

- Can we know the **points of contact** (PoCs) for the pen-testing exercise:
    - Names:
        - ➢ **Amalraj Albina (albina@nus.edu.sg) , Jebamony Maneksha Babu (ccejmb@nus.edu.sg)**
    - The desired **mode** of contacts (e.g. email, phone SMS/messaging, phone call);
        - ➢ **Email**
    - **Contactable** days and hours?

- **Office Hours**

8. Document Notes

- Prepared by: Sufatrio, SoC, NUS, 5 February 2024
- Updated by: Amalraj Albina , NUSIT, NUS, 20 February 2024
- Acknowledged by: Amalraj Albina, NUSIT, NUS, 20 February 2024

_____