NUS IFS4103 Penetration Testing, Semester 2 AY2023/24
Pen-Testing Scope and Arrangement
(*App 2: NUS Student Work Scheme - NSWS*)

1. Kick-off/Scoping Meeting Information

Date : **Thursday, 22 February 2024**

Time : **3-4pm**

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-wws.nus.edu.sg/nswspt/app/login

- Which **components/modules** of the system that need to be pen-tested? And which components/modules that are **out of scope** to be excluded?
  - **NSWS : Job Posting, WBS Approval, Job application process (apply, offer , accept/reject) , Job Searching**
  - **RP : Research Posting, Research Searching**

scope until timesheet submission

OOS actual submit button

- 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?
  - **Data is randomized and masked**

- Will the system be **backed up** and/or **snapshotted** before the pen-testing starts?
  - **New instance for PT**

- 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?
    - https://nsws.nus.edu.sg//policies/ for user guide

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 student and 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 Job Poster/Job Supervisor, WBS approver**
    - **Student as applicant**

yellow vs blue login page

- yellow is nusstu
- blue is nus

private browsing to prevent SSO issue
, yellow might login of ours

- 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: Job Poster/Job Supervisor, WBS Approver

No	Account Name/ID	Password
1	ccetet01	
2	ccetet02	
3	ccetet03	
4	ccetet04	
5	ccetet05	
6	ccetet06	
7	ccetet07	
8	ccetet08	
9	ccetet09	
10	ccetet10	
11	ccetet11	
12	ccetet12	
13	ccetet13	
14	ccetet14	
15	ccetet15	
16	ccetet16	
17	ccetst72	
18	ccetst73	
19	ccetst74	
20	ccetst75	
21	ccetst76	
22	ccetst77	
23	ccetst80	
24	ccetst81	

CCET0056 CCET0057

User Type 2: Applicant

No	Account Name/ID	Password
1	t0923418	
2	t0923419	
3	t0923420	
4	t0923421	
5	t0923422	
6	t0923423	

7	t0923424	
8	t0923439	
9	t0923440	
10	t0923441	
11	t0923417	
12	t0923404	
13	t0923405	
14	t0923406	
15	t0923407	
16	t0923408	
17	t0923409	
18	t0923410	
19	t0923411	
20	t0923412	
21	t0923413	
22	t0923414	
23	t0923415	
24	t0923416	

- 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, 3-4pm**.
  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:
    - **Yow Chea Keng (cceyowck@nus.edu.sg) , Darmawi (darmawi@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: Yow Chea Keng, NUSIT, NUS, 19 February 2024
- Acknowledged by: Yow Chea Keng, NUSIT, NUS, 19 February 2024
