IFS4103:
Penetration Testing Practice

Lecture 6:
Pen-Testing Reporting & Management, Project 2

Outline

- Pen-testing reporting
- Useful collaborative tools & template files
- Project 2 (NUS app pen-testing)
- Lab 6
- *Free discussion (for both Projects 1 & 2)*

Pen-Testing Reporting

Reporting: Common Sections

- As mentioned, different templates are available
- **Standard/common sections** are as follows:
  - **Executive Summary**:
    - Describes to **your client's executive management** in **layman's terms** about **important findings** and **how they affect the business**
    - Briefly mentions:
      - Background
      - Timeline
      - Methodology
      - Issues encountered (if any)
      - Overall security posture
      - General findings: high-level or significant findings
      - Remediation/recommendation summary
      - Suggested strategic road map

Reporting: Common Sections (Cont.)

- **Project Scope**: Relevant points taken from RoE document
- **Environment Tested**
- **Methodology & Approach**:
  Infrastructure (various methodologies are available), **web app (*OWASP web security testing guide*)**, mobile app, IoT (OWASP IoT) attack testing
- **Testing Conducted**
- **Testing Limitations**
- **Tools Used**
- **Findings Overview**:
  - Overall security posture
  - No of vulnerabilities of different severity levels **(critical, high, medium, low, information)**
  - High-level or significant findings
  - Finding classification/segmentation used, and risk calculation method used

Reporting: Common Sections (Cont.)

- **Findings Details**: each mentioning:
  - Finding ID (reference no)
  - Title (issue name)
  - CWE/OWASP ID
  - **Target(s) affected**
  - **Risk/severity rating**: CVSS metrics and score *(please refer to Lecture 2)*
  - **Issue description**
  - Screenshot file(s)
  - **Impact summary**
  - **Steps to reproduce**
  - **Proof-of-Concept file(s)**

Reporting: Common Sections (Cont.)

- Suggested **remediation** measures (recommendations)
- Status: open/closed/…
- **References**

- **Testing-Environment Cleaning Up**
- **Conclusion**
- **Appendices**

- Some other relevant **references/resources**:
  - PTES's **Reporting**: http://www.pentest-standard.org/index.php/Reporting
  - Sample **pen-testing report** from Offensive Security (uploaded to Canvas): *for infra pen-testing?*

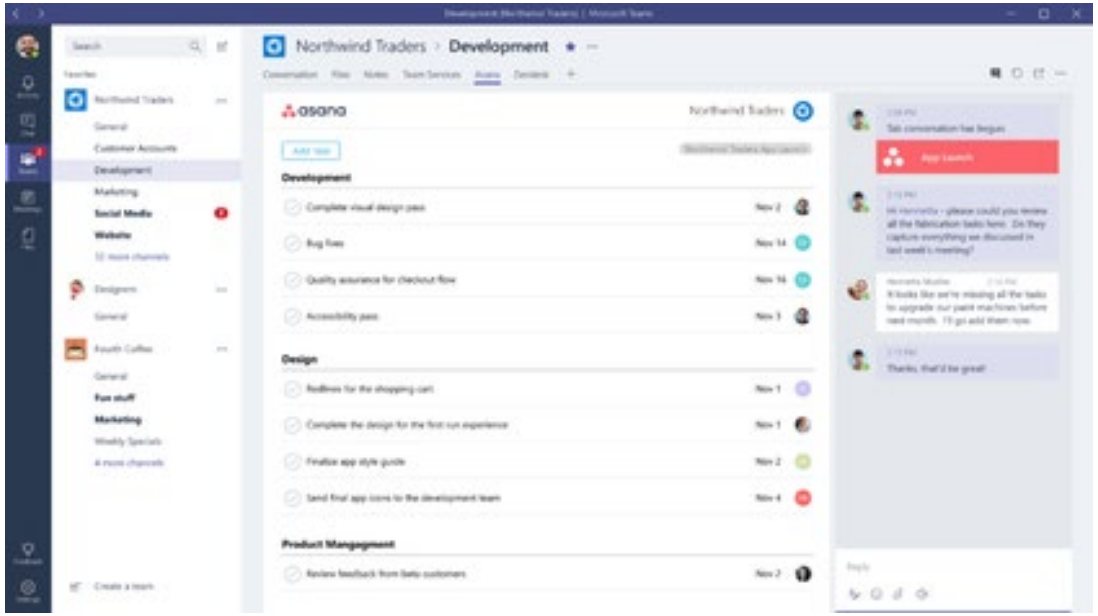
Useful Collaborative Tools & Template Files

Collaboration Tools and Files

- Some **collaborative tools**:
  - Founded issue library: ***private*** Github, Sharepoint, OneDrive, …
  - Microsoft Teams!
  - Discord?
- ***Finding table*** for collaborative access during pen-testing:
  - Record all the "**Findings Details**"
  - Some additional "**project housekeeping**" columns/fields:
    - *Finding Ownership*: date raised, issue founder, issue tester, client owner
    - *Follow-up*: follow-up date, issue tester #2
    - *Comments/remarks*: management comments, client remarks
  - Sample finding table's columns are uploaded to Canvas

Microsoft Teams

- **MS Teams** can be useful!
- The idea of a **team** as a **collaborative** platform with a **container** for file sharing, online document editing, online video call, …

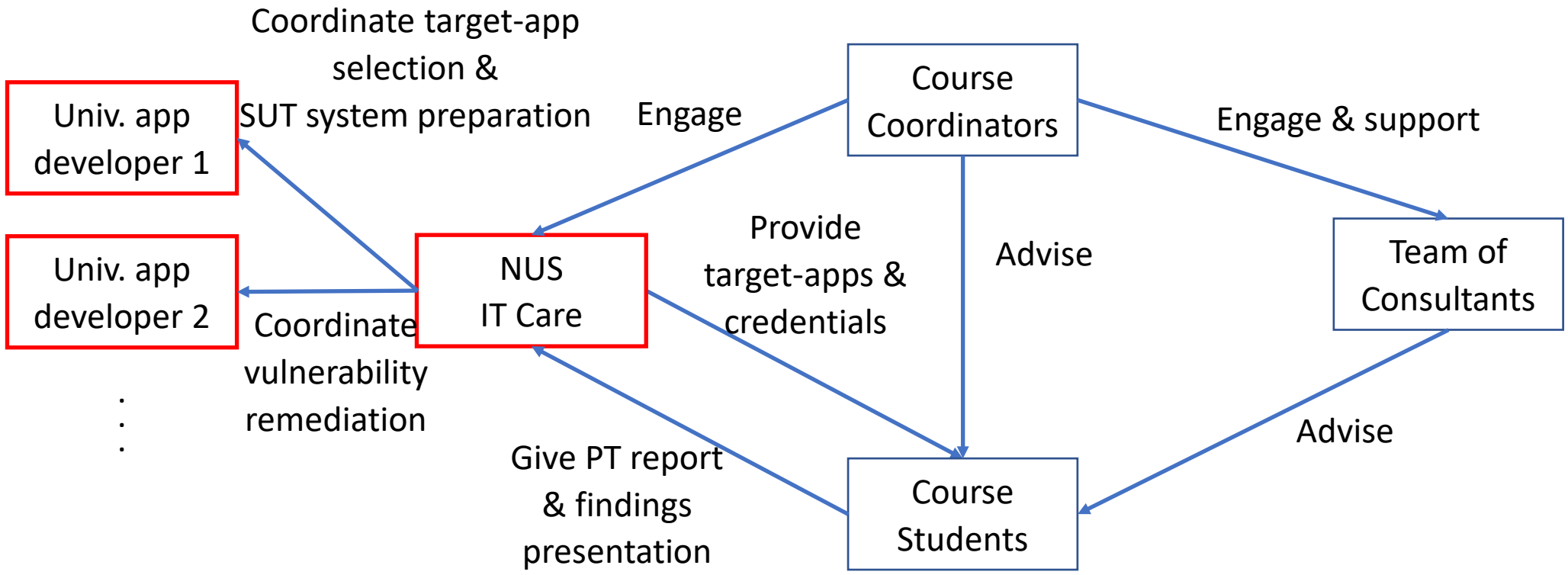


Source: Wikipedia

Project 2
(NUS App Pen-Testing)

Our Pen-Testing Course Arrangement

- **Four parties** working **collaboratively** using **operational NUS apps**:
  - Students, pen-testing consultant (Ensign), NUS IT Care, CIT/SoC/…



Other Involved Parties

- **NUS IT Care** (Computer Centre):
  - Website: https://nusit.nus.edu.sg/itcare/
- **Two** operational **NUS target systems**:
  - Developed by **NUS app developers**, maintained/monitored by NUS IT Care
  - Fully deployed or customized in NUS
  - **SUT systems**: real systems *but* not the production systems
  - Access to SUT systems will be **regulated** during the pen-testing:
    - E.g. based on SoC IP address range (accessible from outside via NUS VPN)
    - Limited pen-testing window period
    - *TBD during the scoping meeting!*

Tentative Schedule

IFS4103 Tentative Schedule: Semester 2 AY2023/24 (January-April 2024)								
Week No	Date (Thur)	Agenda	Activity Type					
			Lecture	Consultation	Presentation	Lab	Client Meeting	
1	18-Jan	Introduction to pen-testing, course administration						
2	25-Jan	Pen-testing methodology & management, CVSS + lab tasks						
3	01-Feb	Web app pen-testing review, release of group assignment + lab tasks						
4	08-Feb	Burp & web pen-testing sharing + lab tasks						
5	15-Feb	Burp & web pen-testing sharing + lab tasks						
6	22-Feb	Scoping meeting of NUS apps (teams to possibly pen-test both apps)						
		Recess Week (29-Feb, Follow-up meeting of NUS apps for credential issuance matters if still needed)						
7	07-Mar	Group-based web vulnerability & exploitation sharing						
8	14-Mar	Group-based web vulnerability & exploitation sharing						
9	21-Mar	Pen-testing of NUS apps & consultation						
10	28-Mar	*NUS Well-Being Day (no class)*						
11	04-Apr	Pen-testing of NUS apps & consultation						
12	11-Apr	Internal-group presentation & discussion						
13	18-Apr	Final pen-testing presentation with clients, module wrap-up						
		Sessions conducted by SoC						
		Sessions conducted by Ensign						
		Session conducted together by SoC & Ensign						

Project 2: Weightage & Team Formation

Review

- **Total weightage: 50%**
  - Findings & report: **30%**
  - Presentation (Week 12): **10%**
  - Combined/delivered final report & client presentation (Week 13): **5%+5%**
- **Team formation:**
  - **Four teams** of 5-6: please refer to my Canvas announcement
  - **Teams 1 & 2**: each works on **NUS target system #1**, to form **Team A** for the final presentation
  - **Teams 3 & 4**: each works on **NUS target system #2**, to form **Team B** for the final presentation
  - ***Note***: depending on the 2 NUS apps, each team may pen-test both apps

Project 2 Report: Assessment Rubrics

Review

- The **total marks** possible for Project 2 report: **100**
- **Components/criteria**:
  - Vulnerability findings & validations reported: **50***
  - Report writing: **50***
    - Section completeness: **15**
    - Finding-details (including impact, mitigation) explanation writing & style: **20**
    - Report clarity/readability: **15**

Note: * The ratio can be adjusted *if needed*

Project 2 Presentation: Assessment Rubrics

Review

- The **total marks** possible for each project presentation: **100**
- **Components/criteria** & respective weightages:
  - Slide content, lay-out & design, clarity/readability: **50**
  - Presentation: **35**
  - Q&A: **15**

Projects 1 & 2: Team Diary

Review

- Each team keeps a **diary** (with shared editing)
- Could use Google Doc (requires Gmail IDs)
  or maybe Microsoft Teams (?)
- Record what each team member is doing:
  - Each team member should edit ***his/her own text*** only
  - Include **date** for each added entry
  - Use it as ***append-only*** **document**: even if you could re-edit past entries, just do it as a change-log while keeping the original past entries
- Free-format except for above rules

Notes on Group Marks

Review

- Group marks of each project are **to be shared**
- ***But***, with a **possible moderation/deduction** based on **your team's** peer-review feedback:
  - Group marks of those with **no** contribution at all or **minimal** contribution will be moderated
  - The moderation will be determined based on teammate's comments & the **team diary**
  - *How about negative feedback from **only 1 teammate**?*
- **The message is**: please work together, contribute what you can, help & support each other, perform together as a team

Project 2: NUS App Pen-Testing

- Two assigned NUS apps this semester (**4 Mar to 12 Apr**):
  1. **Peer review system**: tentatively for **Team 1 & Team 2** (Joint-Team A later)
  2. **NUS Student Work Scheme – NSWS**:
     tentatively for **Team 3 & Team 4** (Joint-Team B later)
- **Before** the scoping meeting:
  - Please take a look at the uploaded **Scoping Questionnaire Forms**
  - Sign the **NDA form** from NUS IT
  - Note that NUS test-account **binding for 2FA** may be needed later
- *What if:*
  - The scopes of the apps are not balanced?
  - One assigned app is hard to pen-test (limited vulnerabilities to report)?

Tentative Schedule

IFS4103 Tentative Schedule: Semester 2 AY2023/24 (January-April 2024)								
Week No	Date (Thur)	Agenda	Activity Type					
			Lecture	Consultation	Presentation	Lab	Client Meeting	
1	18-Jan	Introduction to pen-testing, course administration						
2	25-Jan	Pen-testing methodology & management, CVSS + lab tasks						
3	01-Feb	Web app pen-testing review, release of group assignment + lab tasks						
4	08-Feb	Burp & web pen-testing sharing + lab tasks						
5	15-Feb	Burp & web pen-testing sharing + lab tasks						
6	22-Feb	Scoping meeting of NUS apps (teams to possibly pen-test both apps)						
		Recess Week (29-Feb, Follow-up meeting of NUS apps for credential issuance matters if still needed)						
7	07-Mar	Group-based web vulnerability & exploitation sharing						
8	14-Mar	Group-based web vulnerability & exploitation sharing						
9	21-Mar	Pen-testing of NUS apps & consultation						
10	28-Mar	*NUS Well-Being Day (no class)*						
11	04-Apr	Pen-testing of NUS apps & consultation						
12	11-Apr	Internal-group presentation & discussion						
13	18-Apr	Final pen-testing presentation with clients, module wrap-up						
		Sessions conducted by SoC						
		Sessions conducted by Ensign						
		Session conducted together by SoC & Ensign						

Important Dates (1/2)

- **Four** internal teams' **pen-testing report** submission:
  - Week 12: Thursday, **11 April, 2:00pm** (before our class)
  - Submit your PDF report to Canvas assignment: `Project-2-Report`
- **Four** internal teams' **findings presentation**:
  - Week 12: Thursday, **11 April, 2:00pm** (before our class)
  - Submit your slides to Canvas assignment: `Project-2-Slides`
  - Each presentation is **30 minutes** (including demo), followed by **15 minutes** of Q&A and feedback
  - **Presentation order**: *TBD*

Important Dates (2/2)

- Two joint-teams' **presentation dry-run** (*not* graded):
  - Week 12 or 13: on your own → *online?*
- Two joint-teams' final **pen-testing report** submission**:**
  - Please email me your joint team's PDF by **Tuesday, 16 April, 7:00pm**
  - I'll email back the commented PDF by **Tuesday**, **16 April, 11:59pm?**
  - Please email me your revised/final PDF by **Wednesday, 17 April, 2:00pm**
  - I'll email the final report to NUS IT by **Wednesday, 17 April, 3:00pm**
- The **findings presentation sessions** with NUS:
  - Week 13: Thursday, **18 April, 2:00-5:00pm** (during our class)

Lab 6 (Our Last Lab)

Lab 6 (Our Last Lab)

- The tasks on Burp Suite's **project files**, **options, Sequencer & Extender**:
  - To use Burp Suite's **project files**: https://www.youtube.com/watch?v=s3j1VvJlx9E
  - To configure Burp Suite's **project & user options**: https://www.youtube.com/watch?v=CdcJcdp-ObQ
  - To analyze session token randomness using **Burp Sequencer**: https://www.youtube.com/watch?v=kNSAhKiXctA
  - To add **extensions**: https://www.youtube.com/watch?v=C03EUbgRLNE

Questions?

Thanks!

After the scoping meeting today, enjoy your recess week!