Project 2024/2025

Please, refer to the Moodle page of the Project 2024/2025 for the complete description
This ppt is intended only for a brief overview of the task and documents required

Project 2024/2025 - presentation

Project course Security Testing 2024/2025

The project concerns vulnerabilities detection and exploitation in two applications by using security testing tools. Details, requirements, and schedule instruction below. Please, carefully read and follow the project instructions.

This project is indented to be for students who passed / has to pass the written test of the academic year 2024/2025.

Project instructions

- Project description, requirements, and schedule

Templates

- Template for the PDF report (Conventional Project Submission)
- Template for the PDF report (In-Course Project Submission)
- Template for the XLS with collected data

Applications

- Introduction and Installation of applications
  - Preliminary installation of MySQL
  - Preliminary installation of Tomcat in Eclipse (already done in the Lab)
  - Install app tourism
  - tourism Eclipse project (ZIP) : it contains the Eclipse project of the application, the DB driver jar connector and the SQL files for the application DB

General Rules

In the following list some rules and answers to (typical) questions. The list is not intended to be exhaustive, rules can be extended and refined, in case it is needed.

Moodle

- Project instructions (what to do… how…)
- Templates (PDF and XLS files)
- Rules (submission, grades, typical FAQs …)

Please, refer to the Moodle page for the complete description

Project 2024/2025 (1)

- Context
  - DEVELOPERS: developers of a Java Servlet app (name: tourism)
  - SECURITY TESTERS: you
- Goal: realistic security testing experience
- Task:
  1. Pre-task questionnaire
  2. Install the app locally
  3. Test the app: Static Analysis
  4. Test the app: Dynamic Analysis
  5. Test the app: Manual Analysis (not identified vulnerabilities)
  6. Post-task questionnaire
- Output to produce (expected documents)
  - PDF report (template is provided): details the testing process, steps, tools, results
  - XLS report (template is provided): details all potential and real vulnerabilities

Please, refer to the Moodle page for the complete description

Project 2024/2025 (1)

- Context
  - DEVELOPERS: developers of a Java Servlet app (name: tourism)
  - SECURITY TESTERS: you
- Goal: realistic security testing experience
- Task:
  1. Pre-task questionnaire
  2. Install the app locally
  3. Test the app: Static Analysis
  4. Test the app: Dynamic Analysis
  5. Test the app: Manual Analysis (not identified vulnerabilities)
  6. Post-task questionnaire
- Output to produce (expected documents)
  - PDF report (template is provided): details the testing process, steps, tools, results
  - XLS report (template is provided): details all potential and real vulnerabilities

One or two person teams

Step3 SpotBugs+FindSecBugs
Step4 ZAP
Step5 No specific tools, but you are free to use other tools that can support your manual test

Step3/4/5 It not required to inspect all the types of vulnerability discovered by the tool, you could focus only on the ones we have seen in the course. But additional effort could be appreciated

Not copy&paste the output of the tool

The quality of the conducted analysis and of the reports produced is more important than just listing a high number of vulnerabilities

Please, refer to the Moodle page for the complete description

Project 2024/2025 (1)

- Context
  - DEVELOPERS: developers of a Java Servlet app (name: tourism)
  - SECURITY TESTERS: you
- Goal: realistic security testing experience
- Task:
  1. Pre-task questionnaire
  2. Install the app locally
  3. Test the app: Static Analysis
  4. Test the app: Dynamic Analysis
  5. Test the app: Manual Analysis (not identified vulnerabilities)
  6. Post-task questionnaire
- Output to produce (expected documents)
  - PDF report (template is provided): details the testing process, steps, tools, results
  - XLS report (template is provided): details all potential and real vulnerabilities

Request:
1. Run at least two testing tools (SpotBugs and ZAP)
2. Document all tool-provided vulnerabilities
3. Inspect at least 5 different tool-provided vulnerabilities (TP/FP, attack vector, etc)
4. Conduct an extensive manual test

Accepted:
1. Run only SpotBugs and ZAP
2. Document only the tool-provided vulnerabilities of the types we have seen in the course (e.g., XSS, SQLinjection, etc)
3. Inspect at least 3 different tool-provided vulnerabilities (TP/FP, attack vector, ..)
4. Conduct manual test

Please, refer to the Moodle page for the complete description

Project 2024/2025 (1)

- Context
  - DEVELOPERS: developers of a Java Servlet app (name: tourism)
  - SECURITY TESTERS: you
- Goal: realistic security testing experience
- Task:
  1. Pre-task questionnaire
  2. Install the app locally
  3. Test the app: Static Analysis
  4. Test the app: Dynamic Analysis
  5. Test the app: Manual Analysis (not identified vulnerabilities)
  6. Post-task questionnaire
- Output to produce (expected documents)
  - PDF report (template is provided): details the testing process, steps, tools, results
  - XLS report (template is provided): details all potential and real vulnerabilities

The PDF must describe all steps, tools, and results obtained
The PDF must report your critical analysis
The XLS file must contain the raw data about the vulnerabilities (both potential and real ones).

Please, refer to the Moodle page for the complete description

Project 2024/2025 – PDF report (1)

Brief Introduction to the task, tested app, and used tools (max: 2 pages of text + figures)

*Briefly present **what has been done**, introduce the goal of the activity, **present the tested App**, and details the **used testing tools**. Detail problems encountered during the app and tool installation or use. Detail the used tool setup and configuration (e.g., list the plugins used for ZAP). In case of extra testing tools have been used, present and motivate their use.*

Explanation of the adopted process (max: 2/3 pages of text + figures)

*Describe the **testing process adopted** in the testing activity. In particular, report the overall process, detail each executed step and the tool used in each step. For each step, you could also make evident the input used and the output produced. It is also requested to explain the clearly explain **motivations and reasons** underlying any choices done (e.g., why a given process, why a given tool has been used in a step instead of another one, or why a tool has been used before another tool). Explain how the work has been **organized and splitted on the members of the testing team** and the single responsibilities.*

Please, refer to the Moodle page for the complete description

Project 2024/2025 – PDF report (2)

Summary of the collected data (max: 5/6 pages of text + figures + tables) - all data have to be reported in the related XLS file

*Present a **summary of the collected data**, with overall **statistics** (e.g., number of potential vulnerabilities discovered by the tools, among them the number of discovered vulnerabilities confirmed as **actual vulnerabilities** – True Positive, number of vulnerabilities discover only by the manual analysis – False Negative, total and average time spent for identifying and exploiting a vulnerabilities, most frequent type of vulnerability, etc.). Please, add references to the data in the filled XLS file. Details and **examples** on a few sample of vulnerabilities detected are appreciated.*

Brief discussion of the collected results (max: 4/5 pages of text + figures + tables)

Briefly discuss about the security degree if the tested application (did the developers followed the secure guidelines? Are the application enough secure?).
*Present also a brief discussion and a **critical analysis of the collected data** and of the overall statistics, as well as consideration about the **conducted experience**, and about the **use of the tools** (e.g., effort they require, their effectiveness, considering the spent effort, automatically identified vulnerabilities, missing vulnerabilities). Please, add references to the data in the filled XLS file.*
Finally, add some conclusions about your personal experience as security testers (e.g., time and knowledge required).

Please, refer to the Moodle page for the complete description

Project 2024/2025 – XLS report (1)

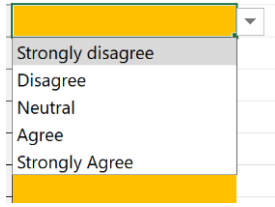
Id	st1
Name	...
Surname	...
Student ID/Matricola	...

Id	st2
Surname	...
Surname	...
Student ID/Matricola	...

APPLICATION TESTED	Tourism

Pre-Questionnaire

	Student Id	Question	Answer
1	st1	I have a strong experience as developer	
2	st1	I have a strong background and experience in programming with Java	
3	st1	I have a strong background and experience in programming Web apps with Java	
4	st1	I have a strong experience as tester (e.g., bug discovery and/or fixing)	
5	st1	I have a strong experience in security	
6	st1	The task that I have to do is clear enough	
7	st1	I agree that the anonymized report data can be used for research and teaching purposes	



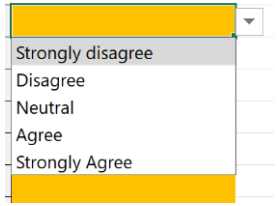
Both students in the team are asked to answer

Please, refer to the Moodle page for the complete description

Project 2024/2025 – XLS report (2)

Results (installation)

	Student Id	Question	Answer
1	st1	The installation of the application was easy	
2	st1	The provided documentation was useful	
3	st1	I had checked online for additional documentation	
4	st1	I have the application running in my computer	
5	st1	The steps needed for installing the application are now clear	
6	st1	I had previous experiences in installing applications based on: Java Servlet, Javscript, and MySQL	
7	st1	I have the following additional comment	...
1	st2	The installation of the application was easy	
2	st2	The provided documentation was useful	
3	st2	I had checked online for additional documentation	
4	st2	I have the application running in my computer	
5	st2	The steps needed for installing the application are now clear	
6	st2	I had previous experiences in installing applications based on: Java Servlet, Javscript, and MySQL	
7	st2	I have the following additional comment	...



Goal: feedback on installation

Please, refer to the Moodle page for the complete description

Project 2024/2025 – XLS report (2)

Results (static)

Id (incremental number)	Student Id (who did the task)	Type of analysis (Static)	Tool used	Reported vulnerability **(from the tool)**	Details about the vulnerability **(from the tool)**	OWASP Top-10	CWE	Overall Exploitation Time (minutes) (manual inspection of tool results)
1		Static	SpotBugs + Find-Sec-Bugs					

Is the vulnerability alert correct? (yes / no) (manual inspection of tool results)	Confidence (how much you are sure about the correctness of the alert)	Test case for vulnerability exploitation / Attack Vector		
		(URL, if any)	input data	exploitation actions

Bug location (file name, class, and line number of the vulnerability sink) (manual inspection of tool results)	Observations

Goal: feedback on static analysis

Please, refer to the Moodle page for the complete description

Project 2024/2025 – XLS report (2)

Results (static)

The student who mainly did the task

Definition of the vulnerability detected from the tool

Classification by the tool, validated by the student, of by the student

Time required (estimation)

Id (incremental number)	Student Id (who did the task)	Type of analysis (Static)	Tool used	Reported vulnerability **(from the tool)**	Details about the vulnerability **(from the tool)**	OWASP Top-10	CWE	Overall Exploitation Time (minutes) (manual inspection of tool results)
1		Static	SpotBugs + Find-Sec-Bugs					

The student can decide if the vuln is true or not

The confidence of the student in deciding if the vuln is true or not (I'm sure…)

The attack path identified to exploit the vulnerability, if the vuln is true then we need to have an attack path (inputs to raise the vuln.), if no attack pattern is identified some motivation are expect in the Observations field

Is the vulnerability alert correct? (yes / no) (manual inspection of tool results)	Confidence (how much you are sure about the correctness of the alert)	Test case for vulnerability exploitation / Attack Vector		
		(URL, if any)	input data	exploitation actions

Location of the bug in the code

Any additional observation or comment or note about the vuln or vuln. exploitation

Bug location (file name, class, and line number of the vulnerability sink) (manual inspection of tool results)	Observations

Goal: feedback on static analysis

Please, refer to the Moodle page for the complete description

Project 2024/2025 – XLS report (2)

Results (dynamic)

Id (incremental number)	Student Id (who did the task)	Type of analysis (Dynamic)	Tool used	Reported vulnerability **(from the tool)**	Entry points identified by the Scanner (URL, HTML element, etc)	Details about the vulnerability **(elaborated from the one provided from the tool)**	OWASP Top-10	CWE	Overall Exploitation Time (minutes) (manual inspection of tool results)
1		Dynamic	Zap web scanner						

Is the vulnerability alert correct? (yes / no) (manual inspection of tool results)	Confidence (how much you are sure about the correctness of the alert)	Test case for vulnerability exploitation / Attack Vector		
		(URL, if any)	input data	exploitation actions

Bug location (file name, class, and line number of the vulnerability sink) (manual inspection of tool results)	Observations

Goal: feedback on dynamic analysis

Please, refer to the Moodle page for the complete description

Project 2024/2025 – XLS report (2)

Results (dynamic)

The student who mainly did the task

Definition of the vulnerability detected from the tool

Classification by the tool, validated by the student, of by the student

Time required (estimation)

Id (incremental number)	Student Id (who did the task)	Type of analysis (Dynamic)	Tool used	Reported vulnerability **(from the tool)**	Entry points identified by the Scanner (URL, HTML element, etc)	Details about the vulnerability **(elaborated from the one provided from the tool)**	OWASP Top-10	CWE	Overall Exploitation Time (minutes) (manual inspection of tool results)
1		Dynamic	Zap web scanner						

The student can decide if the vuln is true or not

The confidence of the student in deciding if the vuln is true or not (I'm sure…)

The attack path identified to exploit the vulnerability, if the vuln is true then we need to have an attack path (inputs to raise the vuln.), if no attack pattern is identified some motivation are expect in the Observations field

Is the vulnerability alert correct? (yes / no) (manual inspection of tool results)	Confidence (how much you are sure about the correctness of the alert)	Test case for vulnerability exploitation / Attack Vector		
		(URL, if any)	input data	exploitation actions

Location of the bug in the code

Any additional observation or comment or note about the vuln or vuln. exploitation

Bug location (file name, class, and line number of the vulnerability sink) (manual inspection of tool results)	Observations

Goal: feedback on dynamic analysis

Please, refer to the Moodle page for the complete description

Project 2024/2025 – XLS report (2)

Results (manual)

Id (incremental number)	Student Id (who did the task)	Type of analysis (fully manual, manual+extra tool)	Tool used (if any)	Discovered Vulnerability	Details about the vulnerability	OWASP Top-10	CWE	Overall Exploitation Time (minutes)
1								

Confidence (how much you are sure about the correctness of the alert)	Test case for vulnerability exploitation / Attack Vector		
	(URL, if any)	input data	exploitation actions

Bug location (file name, class, and line number of the vulnerability sink)	Brief Vulnerability description

Goal: feedback on the manual and final analysis

Please, refer to the Moodle page for the complete description

Project 2024/2025 – XLS report (2)

Results (manual)

The student who mainly did the task

Tool used to support the manual analysis, if any

Definition of the vulnerability detected from the tool

Classification by the tool, validated by the student, of by the student

Time required (estimation)

Id (incremental number)	Student Id (who did the task)	Type of analysis (fully manual, manual+extra tool)	Tool used (if any)	Discovered Vulnerability	Details about the vulnerability	OWASP Top-10	CWE	Overall Exploitation Time (minutes)
1								

The confidence of the student in deciding if the vuln is true or not (I'm sure…)

The attack path identified to exploit the vulnerability, if the vuln is true then we need to have an attack path (inputs to raise the vuln.), if no attack pattern is identified some motivation are expect in the Observations field

Confidence (how much you are sure about the correctness of the alert)	Test case for vulnerability exploitation / Attack Vector		
	(URL, if any)	input data	exploitation actions

Location of the bug in the code

Any additional observation or comment or note about the vuln or vuln. exploitation

Bug location (file name, class, and line number of the vulnerability sink)	Brief Vulnerability description

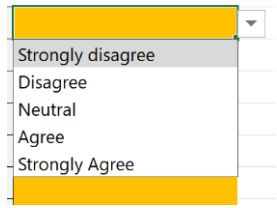
Goal: feedback on the manual and final analysis

Please, refer to the Moodle page for the complete description

Project 2024/2025 – XLS report (3)

Post-Questionnaire

	Student Id	Question	Answer
		In my opinion, …	
1	st1	the task of the project was easy	
2	st1	the task was too expensive, i.e., it required too much time	
3	st1	the tool used for the static analysis has been effective in discovering vulnerabilities	
4	st1	the tool used for the static analysis has been helpful for vulnerability exploitation	
5	st1	the tool used for the dynamic analysis has been effective in discovering vulnerabilities	
6	st1	the tool used for the dynamic analysis has been helpful for vulnerability exploitation	
7	st1	overall the tools have been helpful in vulnerability identification and exploitation	
8	st1	the tested application is enough secure	
9	st1	the tested application seems to be developed adequately following secure coding rules	
10	st1	the overall experience has been interesting	
11	st1	the overall experience has been useful	
12	st1	I have the following comment	…



Goal: feedback on the overall activity

Please, refer to the Moodle page for the complete description

Project 2024/2025 – Rules (summary)

- Conventional Submission
  - Submission: PDF and XLS files, via Moodle (check the page)
  - Any time in the year but, in any case, at the latest one week before the exam session, e.g., Exam: Jan.24, 2024 → first option deadline: Jan.17, 2024
- In-course Submission
  - Submission: PDF and XLS files, via Moodle (check the page)
  - Participants must register by means of a Moodle link or a Google form shared by the teacher via Moodle
  - Three mandatory milestone to submit three parts:
    1. Installation + static analysis;
    2. Dynamic analysis;
    3. Manual analysis (+ opt. refinement of previous parts)
    - Milestone schedule Tentative: Nov.6, Dec.01, Dec.19
- Grade
  - Expressed in /30, and sufficient if both >= 18
  - Average with written part (65% -written test and 35% - project).
  - No fixed execution order between written test and project
  - Both valid for the academic year 2024/2025
- Others:
  - Maximum 2 submissions (in any case, if the first one is not sufficient or if you want to increase the grade)
  - The sufficient score valid for 2 written tests
  - In case of re-submission, a delta is expected (otherwise -1)