# Ethical Hacking

| **Deadline Date:** | **Contribution:** |
| --- | --- |
| **April 26th, 2024 - 23:30 UK Time** | **100% of course assessment** |

Plagiarism is presenting somebody else's work as your own. It includes copying information directly from the Web or books without referencing the material; submitting joint coursework as an individual effort; copying another student's coursework; stealing coursework from another student and submitting it as your own work. Suspected plagiarism will be investigated and if found to have occurred will be dealt with according to the procedures set down by the University. Please see your student handbook for further details of what is/isn't plagiarism.

**All material copied or amended from any source (e.g., internet, books) must be referenced correctly according to the Harvard reference style.**

**Your work will be submitted for plagiarism checking. Any attempt to bypass our plagiarism detection systems will be treated as a severe Assessment Offence.**

## Coursework Requirements

- **Attempt ONLY one of the given two coursework tasks.**
- **An electronic copy of your work for this coursework must be fully uploaded by the deadline date and time or before that.**
- **For this coursework you must submit a single PDF file.**
- **Make sure that any files you upload are virus-free and NOT protected by a password or corrupted otherwise they will be treated as null submissions.**

## DETAILED DESCRIPTION

This coursework contributes to 100% of your grade of the course Ethical Hacking. This coursework can be submitted **either individually or in a group of up to 3 students**. The coursework will include the submission and evaluation of the report. The assessment of the coursework report will be based on its completeness, correctness, readability, and conformance to the expected format. Please attempt any of the following two given tasks.

## Task 1

The aim of the task is to analyze security of software in general and mobile applications in particular by testing the open-source mobile applications by the provided tools developed in the frame of OWASP Mobile Application Security Testing Guide (MASTG) whose details are accessible at https://mas.owasp.org/MASTG/.

First familiarize yourself with the MASTG introduction and theory as provided on the abovementioned web page. Then perform the following steps for the analysis:

1. Choose any two tests (accessible via https://mas.owasp.org/MASTG/tests/) for both the Android or the iOS based on the following 8 control groups for security testing as provided by OWASP Mobile Application Security Verification Standard (MASVS) - https://mas.owasp.org/MASVS/
    a. Storage
    b. Crypto
    c. Authentication
    d. Network
    e. Platform
    f. Code
    g. Resilience
    h. Privacy
2. Choose and test any number of techniques and tools from https://mas.owasp.org/MASTG/techniques/ and https://mas.owasp.org/MASTG/tools/ to test the previously chosen controls each for
    a. Android or
    b. iOS applications - https://mas.owasp.org/MASTG/apps/
3. Discuss the differences of the tests for the controls for Android or iOS applications. You may highlight the underlying techniques used by the corresponding tools for handling the test for Android or iOS.
4. Create a table showing the mapping of each demonstrated test to three known vulnerabilities from https://cve.mitre.org that can be potentially tested by the test.

### Assessment guidelines

For the project report, you are asked to adhere to ALL the following rules:

- The report should be written using Calibri font size 11.
- The paper length should not exceed **8 pages double-column** according to the template (loosely based on the IEEE paper format), which can be seen on the next page. This is an upper limit to give you the flexibility to write an appropriate paper.
- The table of content of the report should include the following sections:
  - Introduction [05 marks]
    - This section should be a brief explanation to what the coursework is about, what you did for the coursework, and how the report is organized.
  - Background [05 marks]
    - This section should explain a table that shows what tests you have chosen and what are their testing goals.
  - Experiment [12 marks = 4 marks for each explaining techniques, tools, and applications]
    - This section should explain the related details of the chosen techniques, tools, and applications. A table can be prepared to show the description of the each of the chosen techniques, tools, and applications.
  - Demonstration [24 marks = 8 marks for each test + 4 marks for proposed fix of each test]
    - This section should explain the outcome of each test. You can also prepare a table showing test, its testing goals, configuration details of the testing, and outcome of the testing. Importantly, you should provide a short description of how to fix the detected insecurity by the corresponding tests, if any.
  - Analysis [20 marks = 7 marks for each Android or iOS tests + 3 marks for each test limitation]
    - This section should explain differences of the tests for the same control for Android and iOS applications. You may prepare a table highlighting underlying features of the techniques used by the corresponding tools to handle the same test for Android and iOS. Importantly, you should highlight limitations and weaknesses of each test.
  - Vulnerabilities [24 marks = 4 marks for each vulnerability]
    - This section should explain a table that maps the demonstrated tests to the vulnerabilities that may also be identified by these tests. Specifically, you should explain how each test may detect the mapped vulnerability by highlighting those features of the vulnerabilities that can be captured by the corresponding tests.
  - Conclusions [05 marks]
    - The conclusion based on analysis and implementation.
  - Presentation style [05 marks]
    - The presentation includes structure and contents of the report. The contents of the report should be adequate supported by reasonable justification.

## Task 2

The aim of the task is to report on the current state of the security, safety, and privacy vulnerabilities, risks, and threats in AI-based systems that are used in various application domains, e.g., robotics, autonomous systems, smart cities, smart agriculture, healthcare, and ecommerce systems.

Choose one of the following topics for vulnerabilities, risks, and threats:

- Privacy
- Security
- Safety

Choose any application domain for your study, including (but not limited to) the followings:

- Robotics
- Autonomous systems
- Smart cities
- Smart agriculture
- Healthcare
- Ecommerce systems

The report should discuss the following for your chosen topic in the chosen application domain:

- Workflow of the application target system in the domain
- Vulnerabilities, risks, and/or threats, and their corresponding:
    - Prevention,
    - Detection, and
    - Recovery techniques
- Strengths and weaknesses of the prevention, detection, and recovery techniques.

You must use Google Scholar (https://scholar.google.com/) to find state of the art literature about the given topics. You should use proper citation for using the contents from other papers or research material.

## Assessment guidelines

For the project report, you are asked to adhere to ALL the following rules:

- The report should be written using Calibri font size 11.
- The paper length should not exceed **8 pages double-column** according to the template (loosely based on the IEEE paper format), which can be seen on the next page. This is an upper limit to give you the flexibility to write an appropriate paper.
- The table of content of the report should include the following sections:
    - Introduction [05 marks]
        - This section should be a brief explanation of the application domain, and the impact of vulnerabilities, risks, and threats in such domains, what you did for the coursework, and how the report is organized.
    - Workflow [10 marks]
        - This section should
            - Explain the workflow of your chosen application domain highlighting its related components and resources, and
            - Provide a list of risks, threats, and/or vulnerabilities in the workflow.
    - Prevention Techniques [2 x 10 marks]
        - This section should discuss:
            - Techniques to prevent the identified vulnerabilities, risks, and threats, and
            - Strengths and weaknesses of these techniques.
    - Detection Techniques [2 x 10 marks]
        - This section should discuss:
            - Techniques to detect the identified vulnerabilities, risks, and threats, and
            - Strengths and weaknesses of these techniques.
    - Recovery Techniques [2 x 10 marks]

    - This section should discuss:
        - Techniques to recover from the detected vulnerabilities, risks, and threats, and
        - Strengths and weaknesses of these techniques.
- Discussion [3 x 5 marks]
    - This section should discuss the challenges in prevention, detection, and recovery of the risks, threats, and vulnerabilities.
- Conclusions [05 marks]
    - The conclusion based on the analysis and future work.
- Presentation style [05 marks]

The presentation includes structure and contents of the report. The contents of the report should be adequate supported by reasonable justification.

Note: There is a 20% penalty if the paper does not abide by all above rules. Furthermore, first the submission will be evaluated based on the above criteria. Later, marks for each group member will be calculated based on their submitted percentage of contribution. For instance, if a group of 2 students with equal contribution (i.e., 50% each) achieves 80%, then a member of the group who has 50% contribution will get full 80% but if someone had, for example, 25% contribution, he would get only 40% score.

## Assessment criteria

The assessment criteria for the technical task implementation and report are provided in a separate spreadsheet named “Rubrik.xlsx”.

# Title of the Task


## Author 1 name and Author 2 name and Author 3 name

Ethical Hacking
University of Ravensbourne
United Kingdom



***Abstract*—This is a very summary of the work produced, including a brief explanation of the topic and key results. This is the first piece of text that the reader will see. So, make sure it is well-written. A good length is one or two small paragraphs.**


## I. Introduction

This section should be a brief explanation to what the coursework is about, what you did for the coursework, and how the report is organized.

Note that it is important to follow this template from the beginning to the end. Do not change font (Calibri 11), sizes or anything else.

**This section worth 5% of the report.**

Note that the whole paper needs to be precisely up to 8 pages long. If you exceed the 8-page limit, you will lose marks.

## II. Background

This section should explain a table that shows what tests you have chosen and what are their testing goals.

**This section worth 5% of the report.**

## III. Experiment

This section should explain the related details of the chosen techniques, tools, and applications. A table can be prepared to show the description of the each of the chosen techniques, tools, and applications.

**This section worth 12% of the report.**

## IV. Demonstration

This section should explain the outcome of each test. You can also prepare a table showing test, its testing goals, configuration details of the testing, and outcome of the testing. Importantly, you should provide a short description of how to fix the detected insecurity by the corresponding tests, if any.

**This section worth 24% of the report.**

## V. Analysis

This section should explain differences of the tests for the same control for Android and iOS applications. You may prepare a table highlighting underlying features of the techniques used by the corresponding tools to handle the same test for Android and iOS. Importantly, you should highlight limitations and weaknesses of each test.

**This section worth 20% of the report.**

## VI. Vulnerabilities

This section should explain a table that maps the demonstrated tests to the vulnerabilities that may also be identified by these tests. Specifically, you should explain how each test may detect the mapped vulnerability by highlighting those features of the vulnerabilities that can be captured by the corresponding tests.

**This section worth 24% of the report.**

## VII. Conclusion

Here, you briefly summarise the work carried out and suggest possible future work. The conclusions section is like the abstract with the addition of the future work suggestion or perhaps more detail in the summarization of the results of the previous section.

**This section worth 5% of the report.**


### Acknowledgement

This is an optional section, where, if you want, you can thank colleagues or family that helped you or supported you in relation to this paper.

**References**

[List and number all references used in this paper following the Harvard Referencing style. It is not terribly important whether in each reference you place the issue number, page, publisher etc. What matters is that you are consistent, and you use precisely the same format in all your references.

An example list of references following the Harvard referencing style is shown below. Note the appropriate use of italics:]

Young, H.D., Freedman, R.A., Sandin, T. and Ford, A. (2000) *Sears and Zemansky's university physics*. 10th edn. San Francisco: Addison-Wesley.

Bell, J. (2005) *Doing your research project*. 4th edn. Maidenhead: Open University Press.

Jackson, G. (2000) 'Ports 1700-1840', in Clark, P. (ed.) *Cambridge urban history of Britain: Vol. 2 1540-1840*. Cambridge: Cambridge University Press, pp. 705-730.

***Abstract*—This is a very summary of the work produced, including a brief explanation of the topic and key results. This is the first piece of text that the reader will see. So, make sure it is well-written. A good length is one or two small paragraphs.**

## I. Introduction

This section should be a brief explanation of the application domain, and the impact of vulnerabilities, risks, and threats in such domains, what you did for the coursework, and how the report is organized.

Note that it is important to follow this template from the beginning to the end. Do not change font (Calibri 11), sizes or anything else.

**This section worth 5% of the report.**

Note that the whole paper needs to be precisely up to 8 pages long. If you exceed the 8-page limit, you will lose marks.

## II. Workflow

This section should explain the workflow of your chosen application domain highlighting its related components and resources, and provide a list of risks, threats, and/or vulnerabilities in the workflow.

**This section worth 10% of the report.**

## III. Prevention Techniques

This section should discuss the techniques to prevent the identified vulnerabilities, risks, and threats, and strengths and weaknesses of these techniques.

**This section worth 20% of the report.**

## IV. Detection Techniques

This section should discuss the techniques to detect the identified vulnerabilities, risks, and threats, and strengths and weaknesses of these techniques.

**This section worth 20% of the report.**

## V. Recovery Techniques

This section should discuss the techniques to recover from the detected vulnerabilities, risks, and threats, and strengths and weaknesses of these techniques.

**This section worth 20% of the report.**

## VI. Discussion

This section should discuss the challenges in prevention, detection, and recovery of the risks, threats, and vulnerabilities.

**This section worth 15% of the report.**

## VII. Conclusion

Here, you briefly summarise the work carried out and suggest possible future work. The conclusions section is like the abstract with the addition of the future work suggestion or perhaps more detail in the summarization of the results of the previous section.

**This section worth 5% of the report.**

**Acknowledgement**

This is an optional section, where, if you want, you can thank colleagues or family that helped you or supported you in relation to this paper.

**References**

[List and number all references used in this paper following the Harvard Referencing style. It is not terribly important whether in each reference you place the issue number, page, publisher etc. What matters is that you are consistent, and you use precisely the same format in all your references.

An example list of references following the Harvard referencing style is shown below. Note the appropriate use of italics:]

Young, H.D., Freedman, R.A., Sandin, T. and Ford, A. (2000) *Sears and Zemansky's university physics*. 10th edn. San Francisco: Addison-Wesley.

Bell, J. (2005) *Doing your research project*. 4th edn. Maidenhead: Open University Press.

Jackson, G. (2000) 'Ports 1700-1840', in Clark, P. (ed.) *Cambridge urban history of Britain: Vol. 2 1540-1840*. Cambridge: Cambridge University Press, pp. 705-730.