

COLLEGE OF COMPUTER STUDIES AND MULTIMEDIA ARTS

**IT0005L**

**(Information Assurance & Security 1)**

**EXERCISE**

**10**

**Investigating IoT Security Requirements**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Student Name / Group Name:** |  | |  | |
| **Members (if Group):** |  | **Name** | **Role** |  |
|  |  |
|  |  |
|  |  |
| **Section:** |  | |  | |
| **Professor:** |  | |  | |

# I. PROGRAM OUTCOME/S (PO) ADDRESSED BY THE LABORATORY EXERCISE

• Analyze a complex problem and identify and define the computing requirements appropriate to its solution. [PO: B]

# II. COURSE LEARNING OUTCOME/S (CLO) ADDRESSED BY THE LABORATORY EXERCISE

• Explain the key factors involved in authentication and how they are used to verify identity and grant access to the system

# III. INTENDED LEARNING OUTCOME/S (ILO) OF THE LABORATORY EXERCISE

At the end of this exercise, students must be able to:

• Learn about IoT security requirements by investigating OWASP critical IoT security vulnerabilities

# IV. BACKGROUND INFORMATION

In this lab, you will review a list of the top 10 IoT security vulnerabilities as documented by the Open Web Application Security Project (OWASP). These vulnerabilities are generic weaknesses in IoT devices, communications, or applications that can be exploited by threat actors. The vulnerabilities are directly related to the IoT security requirements.

**V. GRADING SYSTEM / RUBRIC (please see separate sheet)**

# VI. LABORATORY ACTIVITY Step 1: Investigate OWASP

a. Visit the home page for [The OWASP Foundation.](https://www.owasp.org/index.php/Main_Page)

What is the purpose of the OWASP foundation?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

b. Visit the [OWASP Internet of Things Project](https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project) page.

c. Explore the resources that are available on the page and the tabs at the top of the page to answer the following questions. What is the purpose of the OWASP IoT Project?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For what specific IoT use cases does OWASP offer recommendations?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Look at the IoT Event Logging Project tab. Give three examples of the security events that OWASP recommends should be logged.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Step 2: Investigate the OWASP IoT Top 10 Vulnerabilities

Vulnerabilities are weaknesses in IoT systems that can be exploited by threat actors in various types of attacks. The goal of IoT security is the identification of vulnerabilities in system components before they are selected or deployed and during the operation of the IoT system. In 2014 OWASP collected the top 10 IoT vulnerabilities and documented how to identify and address the vulnerabilities. Although this list is due to be updated, it is still useful very for understanding IoT security.

1. Go to the [OWASP IoT Top 10 Vulnerabilities](https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10) page. Click several vulnerabilities in the list. Look at the linked page. What information is provided for each vulnerability?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. What is the first vulnerability? What needs to be checked to determine if this vulnerability is present in a system?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What are some of the things that can be done to verify that an IoT web interface is secure?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Step 3: Investigate Vulnerabilities, Vulnerability Assessment, and Mitigation Measures

Become familiar with the features of some of the other OWASP IoT Top 10 vulnerabilities.

Work in the table below, or in your notebook using the table as a guide. Investigate the other top 10 vulnerabilities. Select three and complete the table below. List the vulnerability, some of the vulnerability assessment questions, and some of the mitigation techniques for each.

Note: You are not expected to understand all of the information provided for each vulnerability. However, you should understand enough to provide a few entries for at least three of them. Take time to research some of the things that you don't currently understand, if possible.

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerability |  |  |  |
| Assessment |  |  |  |
| Mitigation |  |  |  |

# VII. QUESTION AND ANSWER

Briefly answer the questions below. Avoid erasures. For group activity, specify the name of GROUP MEMBER/s who answered the question. Do not forget to include the source for all NON-ORIGINAL IDEAS.

•

**VIII. REFERENCES**

* <https://owasp.org/www-project-internet-of-things/#tab=IoT_Top_10>
* <https://www.cs.utexas.edu/~byoung/cs361c/slides1-intro.pdf>