Лабораторна робота – Дослідження вимог до безпеки IoT

1. Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Objectives

У цій лабораторній роботі ви дізнаєтеся про вимоги безпеки IoT, досліджуючи критичні вразливості безпеки OWASP.

• **Дослідження OWASP.**

**• Дослідження 10 найпопулярніших вразливостей OWASP IoT.**

**• Дослідження вразливостей, оцінка вразливостей та заходи пом’якшення наслідків**.

1. Background / Scenario

У цій лабораторній роботі ви розглянете перелік 10 найбільших уразливостей безпеки IoT, задокументованих Open Web Application Security Project (OWASP). Ці вразливості є загальними слабкими місцями в пристроях, комунікаціях або програмах Інтернету речей, якими можуть скористатися зловмисники. Уразливості безпосередньо пов’язані з вимогами безпеки IoT.

1. Required Resources

* ПК з доступом до Інтернету.
  + 1. Дослідження OWASP.
       1. Відвідайте сторінку [The OWASP Foundation](https://www.owasp.org/index.php/Main_Page).

Які цілі OWASP foundation?

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

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

* + - 1. Відвідайте сторінку [OWASP Internet of Things Project](https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project)
      2. Перегляньте ресурси, доступні на сторінці та вкладки у верхній частині сторінки, щоб відповісти на наведені нижче запитання.

Яка мета проекту OWASP IoT?

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

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

Для яких конкретних випадків використання IoT пропонує рекомендації OWASP?

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

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

Подивіться на вкладку IoT Event Logging Project. Наведіть три приклади подій безпеки, які OWASP рекомендує реєструвати.

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

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

* + 1. Дослідження 10 найпопулярніших уразливостей OWASP IoT.

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.

Вразливості — це слабкі місця в системах ІоТ, які можуть використовуватися суб’єктами загрози в різних типах атак. Метою безпеки IoT є виявлення вразливостей у компонентах системи до їх вибору або розгортання, а також під час роботи систем IoT. У 2014 році та у 2018 році OWASP зібрав 10 найпоширеніших вразливостей Інтернету речей і задокументував, як визначити та усунути вразливості. Хоча цей список має бути оновлено, він все ще дуже корисний для розуміння безпеки IoT.

З оновленим на 2024 рік переліком ІоТ вразливостей можна ознайомитись тут:

<https://www.wattlecorp.com/owasp-iot-top-10/#2_Insecure_Network_Services>

* + - 1. Перейдіть на сторінку [OWASP IoT Top 10 Vulnerabilities](https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10) . Клацніть на кілька вразливостей у списку. Дослідіть сторінку, на яку веде посиланням. Яка інформація надається для кожної вразливості?

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

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

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

* + - 1. Яка перша вразливість? Що потрібно перевірити, щоб визначити, чи присутня ця вразливість у системі?

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

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

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

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

Що можна зробити, щоб переконатися, що веб-інтерфейс ІоТ безпечний?

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

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

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

* + 1. Дослідження вразливостей, оцінка вразливостей та заходи пом’якшення наслідків

Ознайомтеся з іншими топ-10 уразливостями OWASP IoT.

Виберіть три вразливості та заповніть таблицю нижче. Перелічте уразливі місця, оцінку вразливостей і деякі методи пом’якшення для кожної.

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