SCRIPT OF EPISODE 1

Episode 1 – Buggy's first hack:

In the first episode, the participants will meet Buggy. A young, funny (and a bit cocky) hacker who tells us the story of one of his big hacks. Buggy uses an incorrect implementation of an access control mechanism in a web application to get to the administrator's function. This function allows him to load licenses and send them in an XML format. Incorrect parser configuration proves vulnerable to an XXE attack, which due to the lack of proper control on outgoing connections, ultimately allows Buggy to steal the organisation's internal files.

The episode is based on a kill-chain with the following vulnerabilities:

1. Incorrect implementation of access control mechanism.
2. Faulty XML parser configuration allowing XEE attack.
3. Lack of control on outgoing connections.

Issues covered in episode 1?

1. **Access control flaws**
    - Access control vulnerabilities - what are they and what do they look like?
    - What is authentication and what is authorization?
    - What are the risks of access control vulnerabilities?
    - Differences between function and resource access control bugs.
    - Examples of the most common access control vulnerabilities.
    - Examples of the most common incorrect fixes.

- What you should pay attention to in order to correctly implement access control.

2. **XML vulnerabilities**

   - An XML External Entity (XXE) attack - what is it and what does it look like?
   - What is an XML Bomb attack and what does it look like?
   - What are the risks of XXE and XML Bomb attacks?
   - How do attackers exploit incorrect implementations of XML parsers?
   - Default parser configurations are not always properly configured
   - What should a safe XML parser configuration contain?

3. **Outgoing connections**

   - Consequences of not checking outgoing connections.
   - Correct configuration of outgoing connections.

4. **Introduction to threat modelling**

   - What is threat modeling and what are its benefits?
   - Example of basic threat modeling.
   - A set of sample questions to consider during threat modeling.

The episode also includes exercises that help understand the raised issues and enable better knowledge assimilation:

EXERCISE 1: Access control bugs related to functions and resources

An exercise in which the participants - on the basis of e.g. a description of a situation, sample HTTP requests or HTTP responses that we encountered during the tests - will have to decide whether a given example concerns vulnerability related to a function or to resources.

Purpose of this exercise:

·See a real example of an access control vulnerability.

·Understand how access control errors are exploited and what they are.

·Distinguishing between function and resource access control bugs.

EXERCISE 2: Review of sample payloads used by an attacker to take advantage of incorrect XML parser configuration

An exercise in which the participants will have to choose one of the prepared payloads that allows an attacker to perform a specific action, e.g. download a file, make the server unavailable.

Purpose of this exercise:

·Increased awareness of the consequences of incorrect XML parser configuration.

·Contact with a real example of XXE, XML BOMB.

·Understand how invalid XML parser configurations can be used.

EXERCISE 3: Identifying invalid XML parser configurations

An exercise in which the participants, seeing a sample XML parser configuration, will have to decide whether it is vulnerable or secure.

Purpose of this exercise:

·Realizing that not every available configuration is safe with default settings.

·Understanding the key elements that affect security of an XML parser.

·Ability to recognize unsafe XML parser configurations.

EXERCISE 4: Introduction to threat modeling

An exercise in which the participants learn the basics of threat modeling and see what short threat modeling may looks like. Then they will try to perform such modeling using prepared sample questions.

Purpose of the exercise:

·To understand the basics, purpose, and how threat modeling works.

·To become familiar with the basic terms.

·To encourage reflection on the designed components within the company

At the end of the episode, a summary Quiz will allow students to repeat the most important issues raised in the first module.

SUMMARY:

After episode 1, the participants should:

1. Understand and be able to identify the risks associated with access control vulnerabilities.

2. Understand and be able to identify threats related to incorrect XML configuration.

3. Understand the basics of threat modeling.

4. Know key security principles of access control, XML parsers, and outbound connections.