Security requirements

**lesson 2 Abuse case**

# Developing Abuse Cases based on CAPEC Attack Patterns

**Lab Description:** To create secure and reliable software, developers must anticipate abnormal behavior. Misuse (or abuse) cases can help developers to think about negative or unexpected events.CAPEC is a comprehensive dictionary and classification taxonomy of known attacks that can be used by analysts, developers, testers, and educators to advance community understanding and enhance defenses [1]. The aim of this lab is to learn how to create abuse cases using CAPEC attack patterns for a software application.

**Lab Environment:** In this assignment, you will follow the method below to develop abuse cases for a given web application based on CAPEC attack patterns. Describe each abuse case using the given Abuse Case Template. The requirements specification of the web application including use cases are provided to you. A website for TrAP (Tool for Retrieving Relevant Attack Patterns) to search for CAPEC Attack Patterns is shown below. Username: **comp727** Password: **comp727** (<http://cstrap.ncat.edu/attackpatterns/logintotrap.html> )

**Lab Files that are Needed:**

1. Abuse Case Template and Instruction.

Describe each abuse case using the given Abuse Case Template.

1. Apparel and Footwear Online Shopping System Requirements Specification.

Requirements specification of the web application including use cases.

### **Lab Exercise/step 1**

For each use case, select words from the use case description that will be used for searching attack patterns from CAPEC. Record these words.

**LAB EXERCISE/STEP 2**

For each of the word selected, use TrAP (Tool for Retrieving Relevant Attack Patterns) to search for CAPEC Attack Patterns. Select the attack patterns that are relevant to the Abuse Case. The TrAP tool can be accessed from: <http://cstrap.ncat.edu/attackpatterns/logintotrap.html> username: **comp727** password: **comp727**. Once logged in, you will be redirected to the TrAP page.

* Please note that to search for an attack pattern by “keyword”, only one word may be entered to get any result(s). TrAP will match the keyword entered with the description of the attack pattern in the database. All attack patterns that include the keyword (s) in their description will be returned. Also, not all attack patterns will have all the information needed for describing the abuse cases.
* Use the search by keyword function (see Figure 1). From the List of Attack Patterns returned, select the ones that are relevant to the Abuse Case (see Figure 2). The selection can be based on the attack pattern’s Name, and the description of the attack pattern. The description of the attack pattern can be found by following the link associated with the attack patterns returned by TrAP (see Figure 3). To view a detailed description of the attack pattern, select Complete for Presentation Filter (see Figure 4).

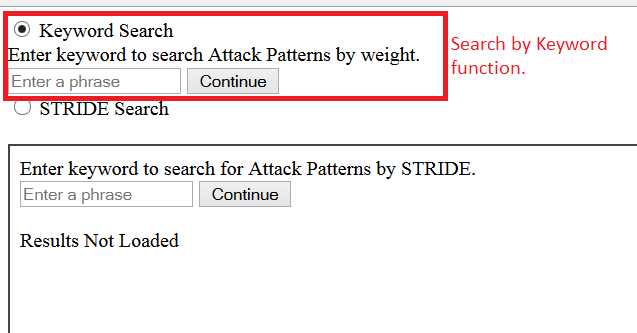


Figure 1: Keyword search for attack patterns

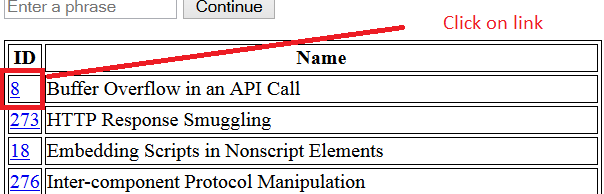


Figure 2: Results

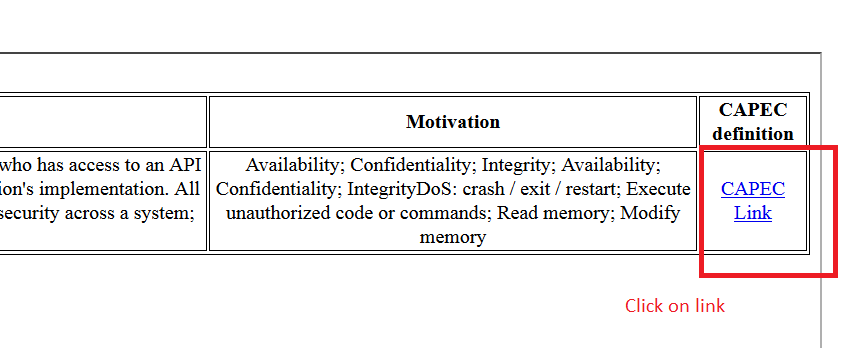


Figure 3: Link to CAPEC website for information about the attack pattern.

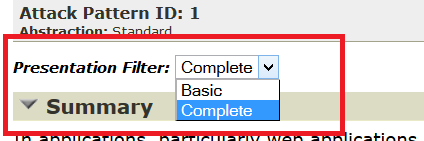


Figure 4: To view a detailed attack pattern.

As an alternative, you can also use the “Search CAPEC” function on the CAPEC website.

**LAB EXERCISE/STEP 3**

Use the information from the attack pattern to fill out the *Abuse Case Template (See Abuse Case Template Instruction for the mapping of attack pattern information to Abuse Case information)*.  Use the mitigation information from the CWE, if provided by the attack pattern, to add more solution(s) & mitigation(s) for the abuse case. **Please Note:** If some of the fields/information are missing from an attack pattern, use your best judgement to fill out the *Abuse Case Template* and make a note of it in you abuse case template. For example, if there is no attack flow in the attack pattern, you can make a note “missing attack flow from attack pattern” in the “Flow of Events” field of the abuse case.

To determine if an attack pattern is relevant to the use case, you could follow the guidelines below.

1. Read the summary of the attack pattern.
2. Read the attack flow of the attack pattern. The attack flow should be applicable to the use case. Some attack patterns may not have an attack flow. In this case, you can write the flow of events based on the description/summary of the attack pattern.

For each use case, provide at least 10 abuse cases.

## What to submit

Put all abuse case descriptions in one document.

**Project will be graded based on the following:**

1. Relevancy of the abuse case/attack pattern
2. The Quantity of the abuse cases per use case
3. The Quality of the abuse cases

Reference:

[1] <https://capec.mitre.org/index.html>