# Activity: Security Risk Analysis

## Objective

To practice the security risk analysis process, and to consider possible mitigations.

## Security Risk Analysis process

1. Describe *threats* to the system, e.g., starting with a STRIDE threat model
2. Identify the *assets* in the system, i.e., what is of value that we need to protect?
3. Identify potential *vulnerabilities* in the architecture and the data flow. Consider attack patterns. How might a threat be realized in the system?
4. Write down a set of *risks* (which asset is at risk and how it may be compromised) related to each threat.
5. Calculate the value for each security risk = $p(exploit) \bullet impact(asset)$
    1. Categorize the probability of an exploit in the presence of protection measures
    2. Categorize the business impact of an asset being compromised

Now, we can prioritize, discuss, and plan mitigations for the threats and risks.

## Part 1: Entire class activity

- Download:
    - **Dropbox.tm7** (https://uncw.instructure.com/courses/16302/files/483061/download?wrap=1) - a threat model of Dropbox created using the **Microsoft Threat Modeling Tool** (https://www.microsoft.com/en-us/download/details.aspx?id=49168)
    - **dropbox.htm** (https://uncw.instructure.com/courses/16302/files/483060/download?wrap=1) - a threat report generated by the tool. Open this in a web browser.
- From the report, we are going to discuss threat number 125: "An adversary can gain access to sensitive data by performing SQL injection through Web App"
- What are the assets in the system?
- What are *potential vulnerabilities* in the architecture and data flow?
    - Visit **dropbox.com** (dropbox.com) . Where (which pages) are the possible locations for SQL Injection?
- What are some of the *risks*, i.e., how an asset *might be* compromised? Think of how a *successful* SQL injection might damage an asset?
- Calculate the risk value $p(exploit) \bullet impact(asset)$
    - What is the probability an exploit will succeed despite protection measures?
    - What is the business impact of an asset being compromised?

# Part 2: Small groups

- Form groups of 3.
- The instructor will assign a threat to your group.
- Walk through the Security Risk Analysis steps 3-5.
- Read about the mitigations suggested by the threat modeling report and identified by the instructor.
- Be prepared to describe:
  - an overview of the threat
  - a sample risk you came up with
  - What the recommended mitigations are
  - Are there any downsides, tradeoffs, or problems with the mitigations that you can think of?

## Threat 106: An adversary can perform action on behalf of other user due to lack of controls against cross domain requests

- The attack pattern here are XSS or CSRF primarily.
- Focus on the "ui-defenses" and "cors-aspnet" links
- What is CORS?
- What is the downside to CORS? How might you be vulnerable even with it enabled?
- What do the X-Frame-Options do? What is their downside? See the "Best Practices" section of **this webpage (https://blogs.msdn.microsoft.com/ieinternals/2010/03/30/combating-clickjacking-with-x-frame-options/)**

## Threat 114: An adversary may gain access to sensitive data from uncleared browser cache

- The attack here isn't necessary directed at Dropbox, but at the user's computer. For example, you stay logged into a lab computer after class is over.
- What "sensitive data" might Dropbox cache in the user's browser?
- Read the mitigation. What is the downside of the recommended mitigation?
- There is another problem with the mitigation. This guy evaluated how all the major browsers (Chrome, Firefox, Safari, Edge) handle caching - the section on "Request Cache Control" describes some undesirable behavior for the recommended mitigation.

## Threat 116: An adversary can get access to a user's session due to improper logout and timeout

- The attack here isn't necessary directed at Dropbox, but at the user's computer. For example, you stay logged into a lab computer after class is over.
- Read both mitigation links.
- What is one downside of the "inactivity-lifetime" mitigation from a usability perspective?

## Threat 119: An adversary can get access to a user's session due to improper logout and timeout

- Focus on the "autocomplete-input" mitigation. The attack involves the attacker having local access to the user's computer. What's the downside of the mitigation?
- Focus on the "forgot-pword-fxn" mitigation. The attack may by via CSRF or XSS. But what is the downside of the proposed mitigation?