# Assignment 4: Learning to be a Security Admin (Have Fun!)

## Description

In this assignment, you will be given a scenario where a small tax-preparation company leverages computer and network systems to operate their business. You are required to identify security issues in the use of the computer and network systems, justify why those are security issues (by explaining ways to attack those security issues and the potential consequences/damages the attacks can lead to), and propose solutions to mitigate the security issues.

## Scenario

**EasyTax** (fake name) is a small company providing tax-preparation service. It has three members:

* Alice: founder
* Bob: CPA
* Charles: customer service

EasyTax offers online service using a network as follows:



The **Web Server** provides web-based services (i.e., a website) for clients to register accounts, request tax preparations, check status of the request, upload documents, and communicate with Alice/Bob/Charles. The Web Server uses HTTP protocols, meaning that all the communications between the clients and the Web Server are based on HTTP protocols. The Web Server also relies on Apache Log4j2 versions 2.0-beta7 to do logging. The Web Server uses a login web page which we publish at <https://drive.google.com/file/d/1QSd14zjOvUeTYsmguznwtcaVBQKTAZpV/view?usp=sharing>. When a user gives a wrong username, the web page will give an error message to notify the user with the username reflected (you can try to play with this by loading the HTML page to your web browser, giving it any username you would like, and clicking the “Log In Here” button).

The **Database Server** is used by the Web Server to keep data, including client data (e.g., client and password), business data (e.g., request information and request status), and tax data (e.g., tax returns and W2s). All the data saved to the Database Server is plain data (i.e., the data is not encrypted when stored to the database). When a user tries to log in, the Web Server will send the Database Server the following SQL query to check whether the user gives the right username and password:

SELECT \* FROM Users WHERE username = '$input1' and password = '$input2';

In the above SQL query, $input1 and $input2 are inputs from the user (anything else belongs to the SQL query). In addition, $input1 will be checked; Any single quotes and double quotes contained in $input1 will be removed before sent to the above SQL query.

The **Work Station** is a desktop, which runs Windows Operating System, the XP version, inside EaxyTax’s network. It is connected to both the Web Server and the Database Server. Bob uses this Work Stationto do tax preparations for the clients. Besides using the Work Station for work, Bob also uses it for personal purposes. He uses the Work Station to check personal emails and he likes to download and open any files sent to his personal email boxes. He also uses the Work Station to surf the internet, visiting all kinds of websites.

During the pandemic, Bob often needs to work from home. To make remote work easier, EasyTax configures a static IP for the Work Station and makes the Work Station directly accessible from the internet. Further, Bob enables Remote Desktop on the Work Station and uses “123456” as the password to log into the Remote Desktop. Further, Bob enables Microsoft Server Message Block (SMB) to allow remote file access. The SMB version the Work Station runs is 1.0, namely SMBv1.

The Work Station also offers a “secure” communication channel between Bob and the clients. All messages going through this channel are encrypted using the DES algorithm.

On April 1st 2022, Bob noticed that some files on the Work Station were messed up and a message on the desktop saying that data on the machine had been locked until some ransom money was paid. Fortunately, Bob found that the data can be recovered from the database. He did that and then continued using the Work Station to process requests from the clients.

## Submission and Grading

* You are required to pinpoint at least 10 security issues from the above scenario.
* Each correctly identified security issue will win you 10 points.
* You will need to use the same format as shown in the “Example Answer” below to describe each security issue you found.
* You will need to include the description of all the security issues you found in a PDF document and submit the PDF document to Gradescope: <https://www.gradescope.com/courses/347861/>

## Example Answer

**Security Issue:** the Web Server uses Apache Log4j2 versions 2.0-beta7 for logging. This version of Log4j2 is known to have a security vulnerability as explained at <https://logging.apache.org/log4j/2.x/security.html>.

**Potential consequences:** This vulnerability can lead to a remote code execution (RCE) attack where an attacker with permission to modify the logging configuration file can construct a malicious configuration using a JDBC Appender with a data source referencing a JNDI URI which can execute remote code (**in your answer, you do not have to be this formal and precise; You can use more general, high-level description**).

**Mitigation:** Upgrade to Log4j 2.3.2 (for Java 6), 2.12.4 (for Java 7), or 2.17.1 (for Java 8 and later).

## Notes

* Everything in the above scenario is made up; Nothing of it comes from any real organization.
* When talking about security issues, you can assume the attackers are powerful (e.g., they have the capability to monitor the communication on the Internet and they know the IP address of the Web Server and the Work Station). If you are not sure whether you are making proper assumptions about the attacker, ask JX first.
* Please do not give super vague answers. For instance, points won’t be given to an answer like “the software used by TaxEasy **MAY** contain buffer overflow vulnerabilities, which can lead to remote code execution”. In this case, if you want to point out a security issue related to vulnerabilities, you need to specify which software and what vulnerabilities (following what is presented in the example answer).
* In the cases of the login web page and the SQL statement, if you find security issues related to them, please make your answer specific by explaining how to exploit the security issues to launch attacks and what consequences the attacks may cause (following what you did for in-class Practice 2).
* When talking about consequences/damages, you can consider consequences/damages occurring to either EasyTax or the clients.
* **Topics related to all the security issues have been covered by the lectures.** The only exception is the log4j2 case (a logic vulnerability in Java code), which is, again, covered by the Example Answer.