# Coding Challenge - Splunk

You will implement a tool that queries the Splunk API in order to identify certain behaviors.

## Prerequisites

Install a free evaluation version of Splunk:
*https://www.splunk.com/en_us/download/get-started-with-your-free-trial.html*

Upload the tutorial dataset to your Splunk installation:

*http://docs.splunk.com/Documentation/Splunk/7.0.2/SearchTutorial/Systemrequirements#Download_the_tutorial_data_files*

*http://docs.splunk.com/Documentation/Splunk/latest/SearchTutorial/GetthetutorialdataintoSplunk*

## Tool Generation

Using Python, Golang, or Node.JS, write a command line tool that interfaces with the Splunk REST API. The tool should have the following command line arguments:

- Splunk REST Server URL
- Splunk Username
- Splunk Password
- Splunk Query

The tool should execute the query against the spunk server and print the Splunk resultset to STDOUT formatted as CSV. You may want to include a ‘debugging’ flag to aid your development, but any debugging information should not be included in the STDOUT as to avoid tainting the CSV data.

The tool should be ‘production ready’, meaning it should be well documented and include all necessary information and instructions to deploy and execute the tool.

## Queries

Using the tutorial dataset, write queries that:

- Generate a list of usernames that were used in failed SSH login attempts from 27.0.0.0/8

- Generate a list of web pages that have been indexed by Google (“Googlebot”)
- Generate a table consisting of [Timestamp, Client IP, URL] where the HTTP Server’s response was a 50X error code.