***ASSIGNMENT 2: VULNERABILITY DATA EXTRACTION AND ANALYSIS***



***INTRODUCTION***

*Vulnerability Analysis involves identifying, analyzing, and prioritizing the vulnerability in a system. For this assignment ,we have to extract the data from the database, preprocess them and perform an analysis. The system that we are planning to analyze were Windows 10 and Apache HTTP Server.*

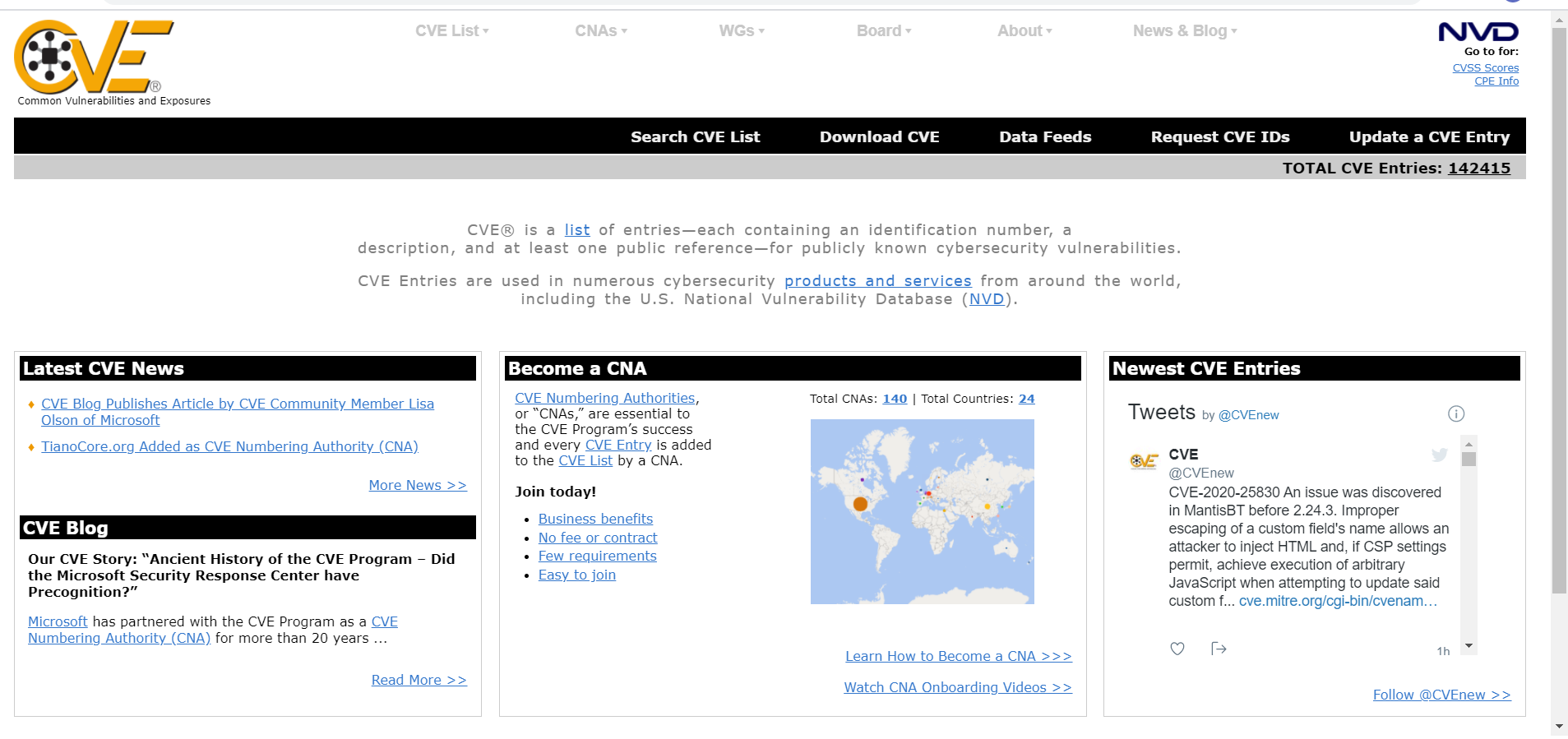
*Web server is a program which process the network requests and serves them with files in order to create web pages with the help of Hyper Text Transfer Protocol(HTTP). Web servers are used to store HTTP files for creating websites. When the client requests the website, it will deliver the requested website back to the client.  Let us consider this example of Facebook while entering the URL in the search bar, it will send an HTTP request to view the Facebook webpage to another system which is considered as the webserver. This webserver contains all the files which make up the website like text, images, gif files, etc. After processing the request, it will send the requested website-related files to your system and then you can reach the website. There are so many web servers available in the fields, one such is Apache HTTP Server.  It is the most popular web server and about 60 percent of the world’s web server machines run this web server. The Apache HTTP web server was developed by the Apache Software Foundation. It is an open-source software which means that we can access and make changes to its code and mold it according to our preference. The Apache Web Server can be installed and operated easily on almost all operating systems like Linux, MacOS, Windows, etc.*

*Let us see how we have analyzed the vulnerability trend from the release of the version to the present situation.*

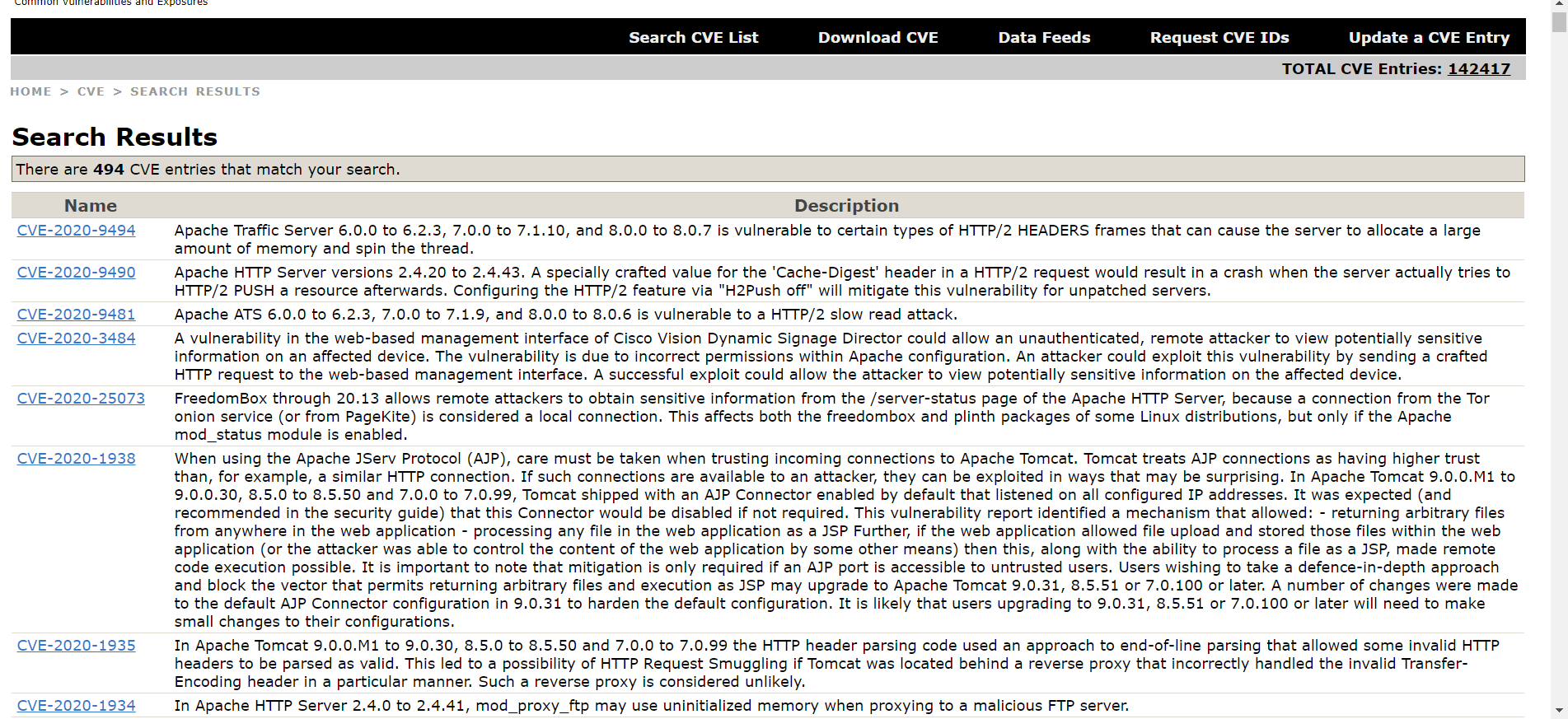
***DATABASE USED***

*The database that we used for analyzing the vulnerabilities are from the website named “CVE-Mitre” which has a list of all the cybersecurity vulnerabilities. We searched for the product which would give the number of CVEs for that product. Then ,we have downloaded the entire list of vulnerabilities named “alliterms.csv” and delete those lines which does not match the product.*

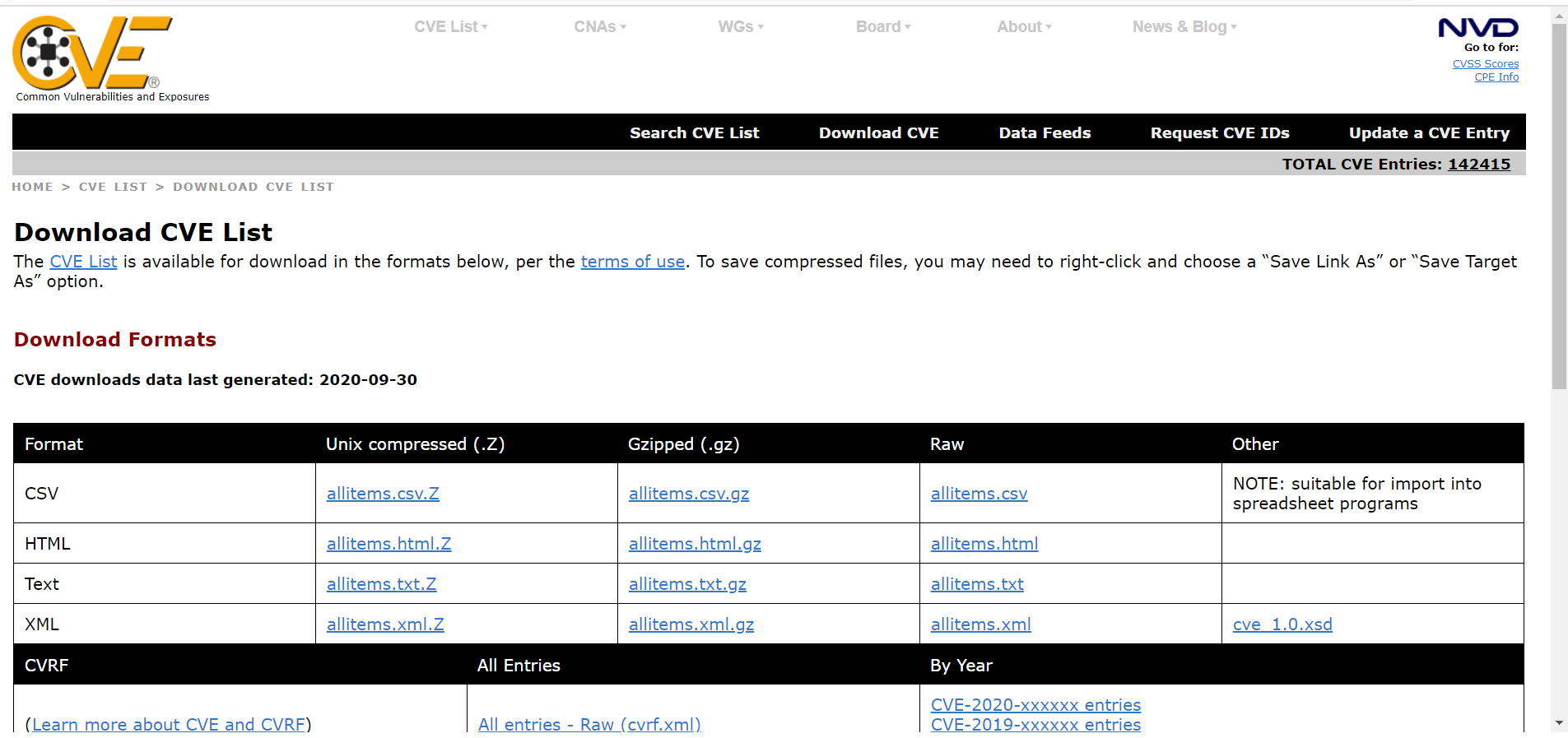
* *Go to the website:*[*https://cve.mitre.org/index.html*](https://cve.mitre.org/index.html)



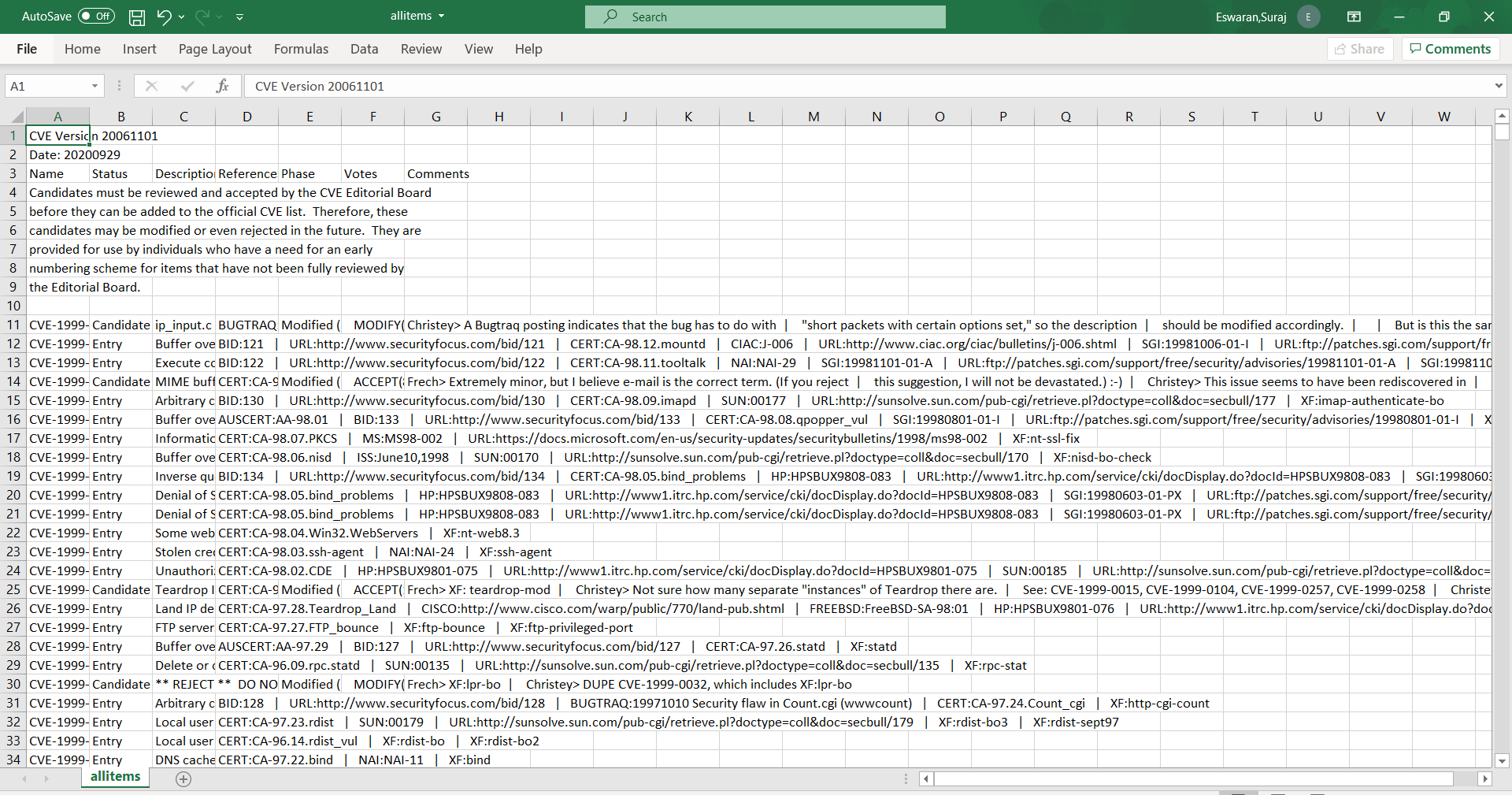
* *Search for the Product which will give you the number of CVEs for that product.*



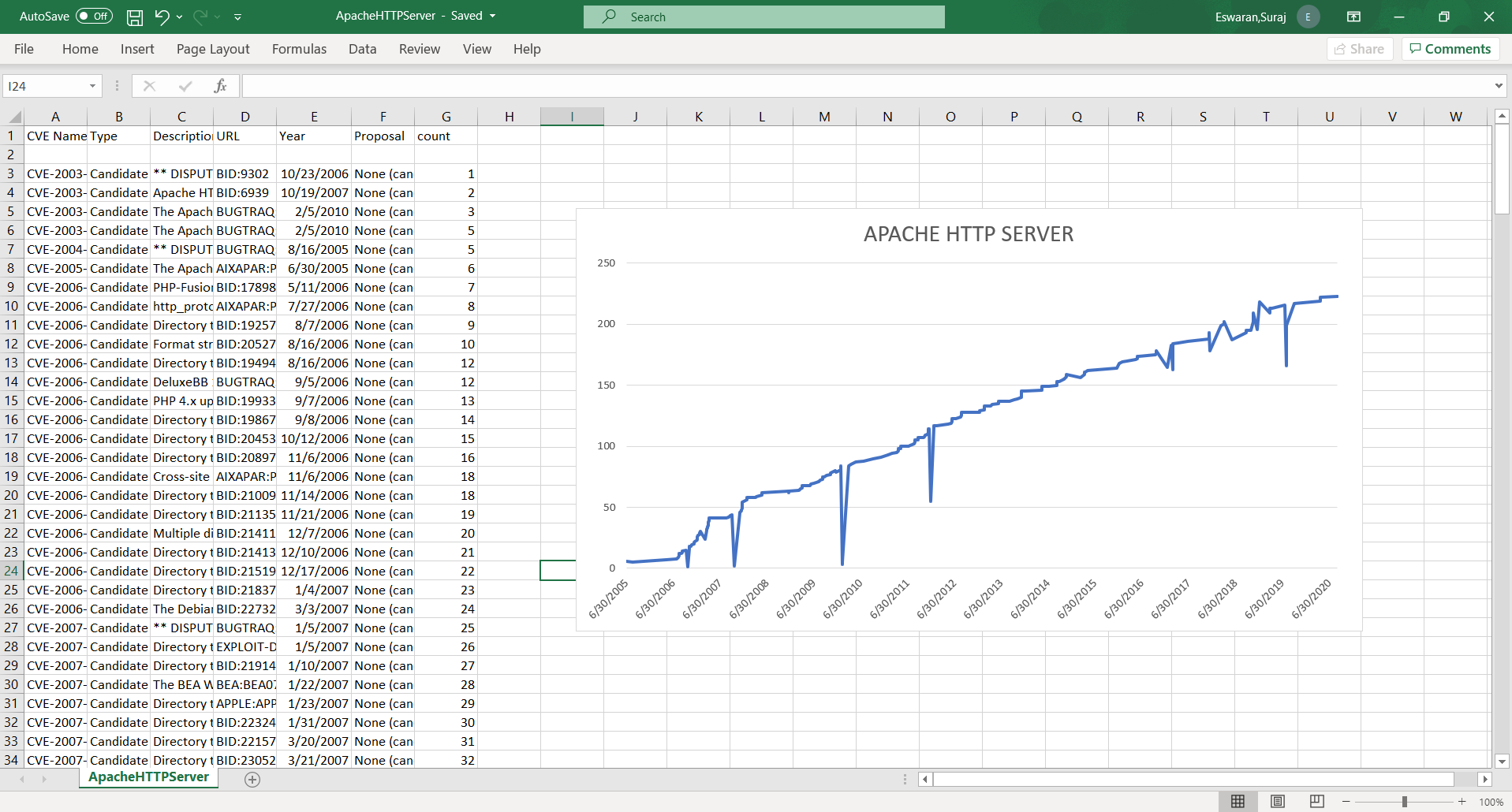
* *Download the 120MB file: allitems.csv.gz.  Open and export to CSV file.*



* *Downloading the allitems.csv and filtering the search.*



* *Open the csv file with ALL the CVEs for your product and plot the graph with number of vulnerabilities.*



***TOOLS USED***

*As far as this analysis concerned, it was done manually with the help of “CVE-Mitre” website. Thus, implementation of tools was not needed for this analysis.*

***SCRIPTS USED***

*Since we have done manually, so for this analogy we have not used any script programming language.*

***GRAPH***

*We have taken a graph of the amount of CVE reports concerning the Apache from 9th September 2006 to 2nd September 2020. From the graph, we can infer that there is a steady increase in the vulnerability trend. The slope shows the uptrend from 2001 to 2020 with lots of breaks and can be thought of as support when entering a position. Since the introduction of the platform started, discovery of the vulnerabilities were less. As years went on, the number of vulnerabilities tend to increase as new updates begun to function. On 2nd September 2020, it tend to have a total vulnerability of 223 in total. High trends indicates that net-demand is increasing even as the* *vulnerabilities rises. As long as vulnerability remain above the trend line, the uptrend is considered solid and intact.*

***GRAPH 1: DATE VS NUMBER OF VULNERABILITIES***

*We took over the date of published and counted the number of vulnerabilities per date. From the number of vulnerabilities vs date, we can infer that updates is not dependent on the product. There has been few trends where there is a down fall, which shows us that there is not any dependency on the update of the product. Few successes with lots of failures while updating the product for removing the vulnerabilities is what witness the apache HTTP Server.*

***PROCEDURE***

* *Go to this website:*[*https://cve.mitre.org/index.html*](https://cve.mitre.org/index.html)
* *Search for the Product which will give you the number of CVEs for that product.*
* *Download the 120MB file named allitems.csv.gz.  Open that RAR file and export to CSV file.*
* *Delete any line that does not match your product.  .*
* *Now we have the csv file for your product , so we just have to plot the graph and do an analysis.*

***REFERENCES***

1. [*https://cve.mitre.org/index.html*](https://cve.mitre.org/index.html )
2. [*https://school.stockcharts.com/doku.php?id=chart\_analysis:trend\_lines*](https://school.stockcharts.com/doku.php?id=chart_analysis:trend_lines)
3. [*https://httpd.apache.org/*](https://httpd.apache.org/)