SURAJ ESWARAN
CS559 QUANTITATIVE SECURITY

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.

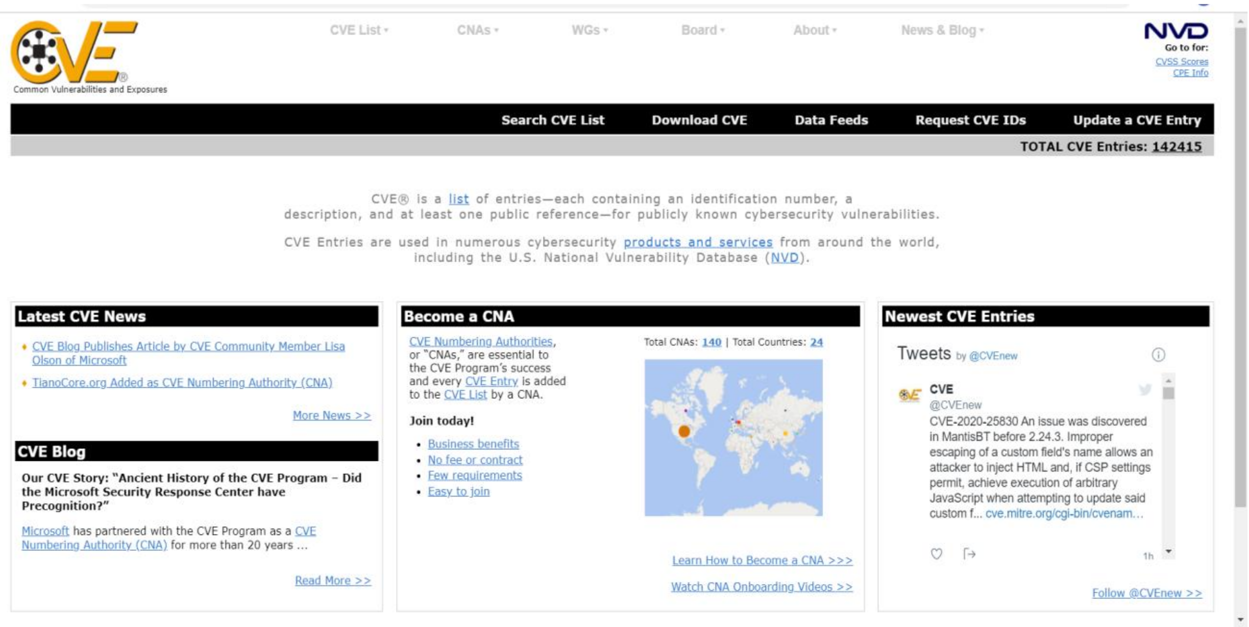
Web server is a program which process the network requests and serves them with files in order to create web pages with the help of Hyper Text Transfer Protocol(HTTP). Web servers are used to store HTTP files for creating websites. When the client requests the website, it will deliver the requested website 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*



TOTAL CVE Entries: 142415

CVE® is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.

CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD).

Latest CVE News

- CVE Blog Publishes Article by CVE Community Member Lisa Olson of Microsoft
- TianoCore.org Added as CVE Numbering Authority (CNA)

More News >>

CVE Blog

Our CVE Story: "Ancient History of the CVE Program – Did the Microsoft Security Response Center have Precognition?"

Microsoft has partnered with the CVE Program as a CVE Numbering Authority (CNA) for more than 20 years ...

Read More >>

Become a CNA

CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Entry is added to the CVE List by a CNA.

Total CNAs: 140 | Total Countries: 24

Join today!

- Business benefits
- No fee or contract
- Few requirements
- Easy to join

Learn How to Become a CNA >>>

Watch CNA Onboarding Videos >>

Newest CVE Entries

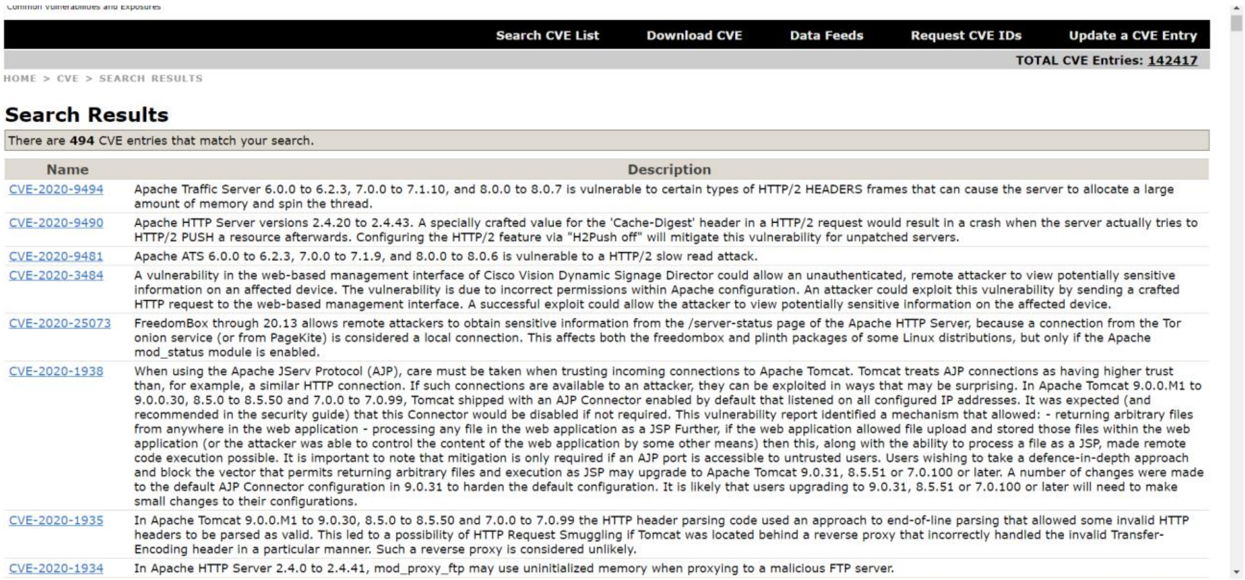
Tweets by @CVEnew

CVE
@CVEnew
CVE-2020-25830 An issue was discovered in MantisBT before 2.24.3. Improper escaping of a custom field's name allows an attacker to inject HTML and, if CSP settings permit, achieve execution of arbitrary JavaScript when attempting to update said custom f... cve.mitre.org/cgi-bin/cvenam...

1h

Follow @CVEnew >>

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



TOTAL CVE Entries: 142417

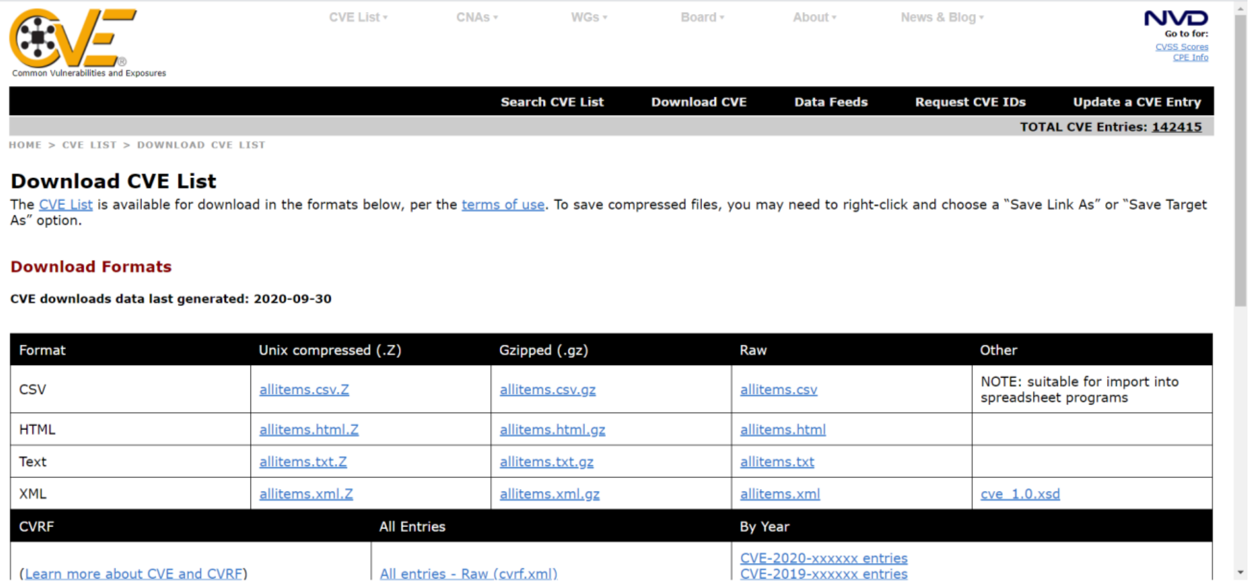
HOME > CVE > SEARCH RESULTS

Search Results

There are **494** CVE entries that match your search.

Name	Description
CVE-2020-9494	Apache Traffic Server 6.0.0 to 6.2.3, 7.0.0 to 7.1.10, and 8.0.0 to 8.0.7 is vulnerable to certain types of HTTP/2 HEADERS frames that can cause the server to allocate a large amount of memory and spin the thread.
CVE-2020-9490	Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.
CVE-2020-9481	Apache ATS 6.0.0 to 6.2.3, 7.0.0 to 7.1.9, and 8.0.0 to 8.0.6 is vulnerable to a HTTP/2 slow read attack.
CVE-2020-3484	A vulnerability in the web-based management interface of Cisco Vision Dynamic Signage Director could allow an unauthenticated, remote attacker to view potentially sensitive information on an affected device. The vulnerability is due to incorrect permissions within Apache configuration. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface. A successful exploit could allow the attacker to view potentially sensitive information on the affected device.
CVE-2020-25073	FreedomBox through 20.13 allows remote attackers to obtain sensitive information from the /server-status page of the Apache HTTP Server, because a connection from the Tor onion service (or from PageKite) is considered a local connection. This affects both the freedombox and plinth packages of some Linux distributions, but only if the Apache mod_status module is enabled.
CVE-2020-1938	When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.
CVE-2020-1935	In Apache Tomcat 9.0.0.M1 to 9.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99 the HTTP header parsing code used an approach to end-of-line parsing that allowed some invalid HTTP headers to be parsed as valid. This led to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely.
CVE-2020-1934	In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

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



Download CVE List

The CVE List is available for download in the formats below, per the terms of use. To save compressed files, you may need to right-click and choose a "Save Link As" or "Save Target As" option.

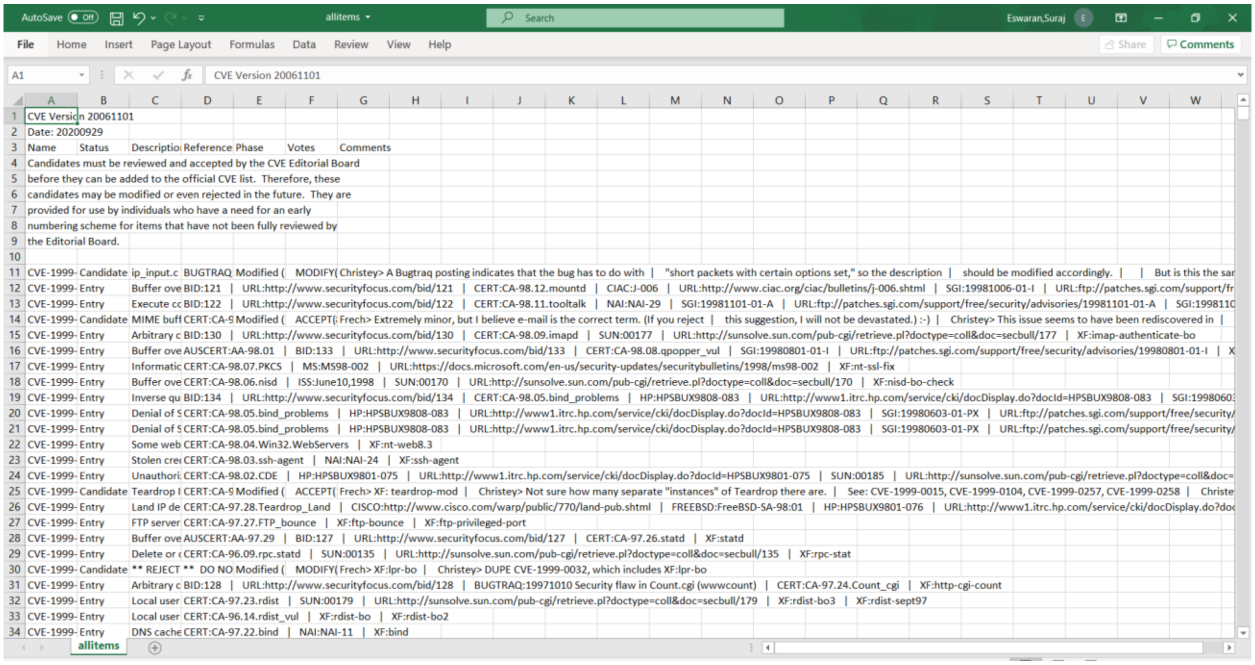
Download Formats

CVE downloads data last generated: 2020-09-30

Format	Unix compressed (.Z)	Gzipped (.gz)	Raw	Other
CSV	allitems.csv.Z	allitems.csv.gz	allitems.csv	NOTE: suitable for import into spreadsheet programs
HTML	allitems.html.Z	allitems.html.gz	allitems.html	
Text	allitems.txt.Z	allitems.txt.gz	allitems.txt	
XML	allitems.xml.Z	allitems.xml.gz	allitems.xml	cve_1.0.xsd

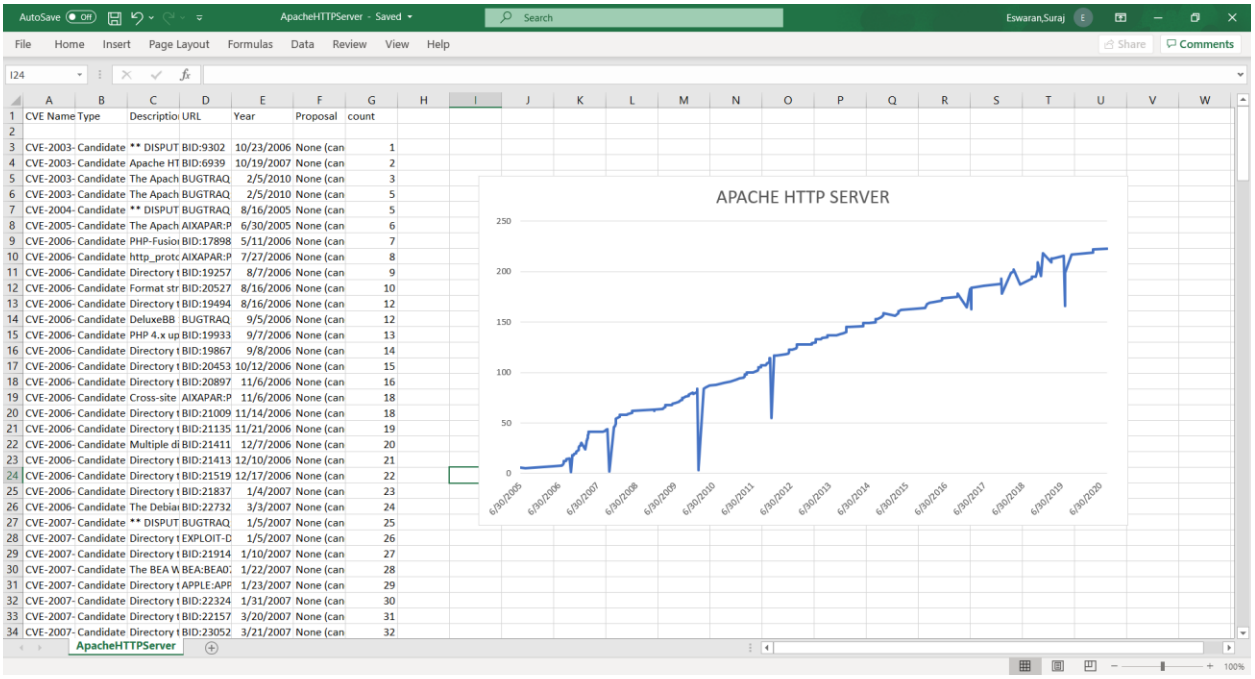
CVRF	All Entries	By Year
(Learn more about CVE and CVRF)	All entries - Raw (cvrf.xml)	CVE-2020-xxxxxx entries CVE-2019-xxxxxx entries

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



	A	B	C	D	E	F	G
1	CVE Version 20061101						
2	Date: 20200929						
3	Name	Status	Descriptio	Reference	Phase	Votes	Comments
4	Candidates must be reviewed and accepted by the CVE Editorial Board						
5	before they can be added to the official CVE list. Therefore, these						
6	candidates may be modified or even rejected in the future. They are						
7	provided for use by individuals who have a need for an early						
8	numbering scheme for items that have not been fully reviewed by						
9	the Editorial Board.						
10							
11	CVE-1999-	Candidate	ip_input.c	BUGTRAQ	Modified (	MODIFY(	Christey> A Bugtraq posting indicates that the bug has to do with | "short packets with certain options set," so the description | should be modified accordingly. | | But is this the sar
12	CVE-1999-	Entry	Buffer ove	BID:121 | URL:http://www.securityfocus.com/bid/121 | CERT:CA-98.12.mountd | CIAC:J-006 | URL:http://www.ciac.org/ciac/bulletins/j-006.shtml | SGI:19981006-01-I | URL:ftp://patches.sgi.com/support/fr			
13	CVE-1999-	Entry	Execute cc	BID:122 | URL:http://www.securityfocus.com/bid/122 | CERT:CA-98.11.tooltalk | NAI:NAI-29 | SGI:19981101-01-A | URL:ftp://patches.sgi.com/support/free/security/advisories/19981101-01-A | SGI:1998110			
14	CVE-1999-	Candidate	MIME buff	CERT:CA-9	Modified (	ACCEPT(:	Frech> Extremely minor, but I believe e-mail is the correct term. (If you reject | this suggestion, I will not be devastated.) :-) | Christey> This issue seems to have been rediscovered in |
15	CVE-1999-	Entry	Arbitrary c	BID:130 | URL:http://www.securityfocus.com/bid/130 | CERT:CA-98.09.imapd | SUN:00177 | URL:http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/177 | XF:imap-authenticate-bo			
16	CVE-1999-	Entry	Buffer ove	AUSCERT:AA-98.01 | BID:133 | URL:http://www.securityfocus.com/bid/133 | CERT:CA-98.08.qpopper_vul | SGI:19980801-01-I | URL:ftp://patches.sgi.com/support/free/security/advisories/19980801-01-I | X			
17	CVE-1999-	Entry	Informatic	CERT:CA-98.07.PKCS | MS:MS98-002 | URL:https://docs.microsoft.com/en-us/security-updates/securitybulletins/1998/ms98-002 | XF:nt-ssl-fix			
18	CVE-1999-	Entry	Buffer ove	CERT:CA-98.06.nisd | ISS:June10,1998 | SUN:00170 | URL:http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/170 | XF:nisd-bo-check			
19	CVE-1999-	Entry	Inverse qu	BID:134 | URL:http://www.securityfocus.com/bid/134 | CERT:CA-98.05.bind_problems | HP:HPSBUX9808-083 | URL:http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX9808-083 | SGI:1998060			
20	CVE-1999-	Entry	Denial of S	CERT:CA-98.05.bind_problems | HP:HPSBUX9808-083 | URL:http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX9808-083 | SGI:19980603-01-PX | URL:ftp://patches.sgi.com/support/free/security/			
21	CVE-1999-	Entry	Denial of S	CERT:CA-98.05.bind_problems | HP:HPSBUX9808-083 | URL:http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX9808-083 | SGI:19980603-01-PX | URL:ftp://patches.sgi.com/support/free/security/			
22	CVE-1999-	Entry	Some web	CERT:CA-98.04.Win32.WebServers | XF:nt-web8.3			
23	CVE-1999-	Entry	Stolen cre	CERT:CA-98.03.ssh-agent | NAI:NAI-24 | XF:ssh-agent			
24	CVE-1999-	Entry	Unauthori:	CERT:CA-98.02.CDE | HP:HPSBUX9801-075 | URL:http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX9801-075 | SUN:00185 | URL:http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=			
25	CVE-1999-	Candidate	Teardrop I	CERT:CA-9	Modified (	ACCEPT(	Frech> XF: teardrop-mod | Christey> Not sure how many separate "instances" of Teardrop there are. | See: CVE-1999-0015, CVE-1999-0104, CVE-1999-0257, CVE-1999-0258 | Christe
26	CVE-1999-	Entry	Land IP de	CERT:CA-97.28.Teardrop_Land | CISCO:http://www.cisco.com/warp/public/770/land-pub.shtml | FREEBSD:FreeBSD-SA-98:01 | HP:HPSBUX9801-076 | URL:http://www1.itrc.hp.com/service/cki/docDisplay.do?doc			
27	CVE-1999-	Entry	FTP server	CERT:CA-97.27.FTP_bounce | XF:ftp-bounce | XF:ftp-privileged-port			
28	CVE-1999-	Entry	Buffer ove	AUSCERT:AA-97.29 | BID:127 | URL:http://www.securityfocus.com/bid/127 | CERT:CA-97.26.statd | XF:statd			
29	CVE-1999-	Entry	Delete or c	CERT:CA-96.09.rpc.statd | SUN:00135 | URL:http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/135 | XF:rpc-stat			
30	CVE-1999-	Candidate	** REJECT	** DO NO	Modified (	MODIFY(	Frech> XF:lpr-bo | Christey> DUPE CVE-1999-0032, which includes XF:lpr-bo
31	CVE-1999-	Entry	Arbitrary c	BID:128 | URL:http://www.securityfocus.com/bid/128 | BUGTRAQ:19971010 Security flaw in Count.cgi (wwwcount) | CERT:CA-97.24.Count_cgi | XF:http-cgi-count			
32	CVE-1999-	Entry	Local user	CERT:CA-97.23.rdist | SUN:00179 | URL:http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/179 | XF:rdist-bo3 | XF:rdist-sept97			
33	CVE-1999-	Entry	Local user	CERT:CA-96.14.rdist_vul | XF:rdist-bo | XF:rdist-bo2			
34	CVE-1999-	Entry	DNS cache	CERT:CA-97.22.bind | NAI:NAI-11 | XF:bind			

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



	A	B	C	D	E	F	G
1	CVE Name	Type	Descriptio	URL	Year	Proposal	count
2							
3	CVE-2003-	Candidate	** DISPUT	BID:9302	10/23/2006	None (can	1
4	CVE-2003-	Candidate	Apache HT	BID:6939	10/19/2007	None (can	2
5	CVE-2003-	Candidate	The Apach	BUGTRAQ	2/5/2010	None (can	3
6	CVE-2003-	Candidate	The Apach	BUGTRAQ	2/5/2010	None (can	5
7	CVE-2004-	Candidate	** DISPUT	BUGTRAQ	8/16/2005	None (can	5
8	CVE-2005-	Candidate	The Apach	AIXAPAR:P	6/30/2005	None (can	6
9	CVE-2006-	Candidate	PHP-Fusio	BID:17898	5/11/2006	None (can	7
10	CVE-2006-	Candidate	http_protc	AIXAPAR:P	7/27/2006	None (can	8
11	CVE-2006-	Candidate	Directory t	BID:19257	8/7/2006	None (can	9
12	CVE-2006-	Candidate	Format str	BID:20527	8/16/2006	None (can	10
13	CVE-2006-	Candidate	Directory t	BID:19494	8/16/2006	None (can	12
14	CVE-2006-	Candidate	DeluxeBB	BUGTRAQ	9/5/2006	None (can	12
15	CVE-2006-	Candidate	PHP 4.x up	BID:19933	9/7/2006	None (can	13
16	CVE-2006-	Candidate	Directory t	BID:19867	9/8/2006	None (can	14
17	CVE-2006-	Candidate	Directory t	BID:20453	10/12/2006	None (can	15
18	CVE-2006-	Candidate	Directory t	BID:20897	11/6/2006	None (can	16
19	CVE-2006-	Candidate	Cross-site	AIXAPAR:P	11/6/2006	None (can	18
20	CVE-2006-	Candidate	Directory t	BID:21009	11/14/2006	None (can	18
21	CVE-2006-	Candidate	Directory t	BID:21135	11/21/2006	None (can	19
22	CVE-2006-	Candidate	Multiple di	BID:21411	12/7/2006	None (can	20
23	CVE-2006-	Candidate	Directory t	BID:21413	12/10/2006	None (can	21
24	CVE-2006-	Candidate	Directory t	BID:21519	12/17/2006	None (can	22
25	CVE-2006-	Candidate	Directory t	BID:21837	1/4/2007	None (can	23
26	CVE-2006-	Candidate	The Debiai	BID:22732	3/3/2007	None (can	24
27	CVE-2007-	Candidate	** DISPUT	BUGTRAQ	1/5/2007	None (can	25
28	CVE-2007-	Candidate	Directory t	EXPLOIT-D	1/5/2007	None (can	26
29	CVE-2007-	Candidate	Directory t	BID:21914	1/10/2007	None (can	27
30	CVE-2007-	Candidate	The BEA W	BEA:BEA0	1/22/2007	None (can	28
31	CVE-2007-	Candidate	Directory t	APPLE:APF	1/23/2007	None (can	29
32	CVE-2007-	Candidate	Directory t	BID:22324	1/31/2007	None (can	30
33	CVE-2007-	Candidate	Directory t	BID:22157	3/20/2007	None (can	31
34	CVE-2007-	Candidate	Directory t	BID:23052	3/21/2007	None (can	32

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.

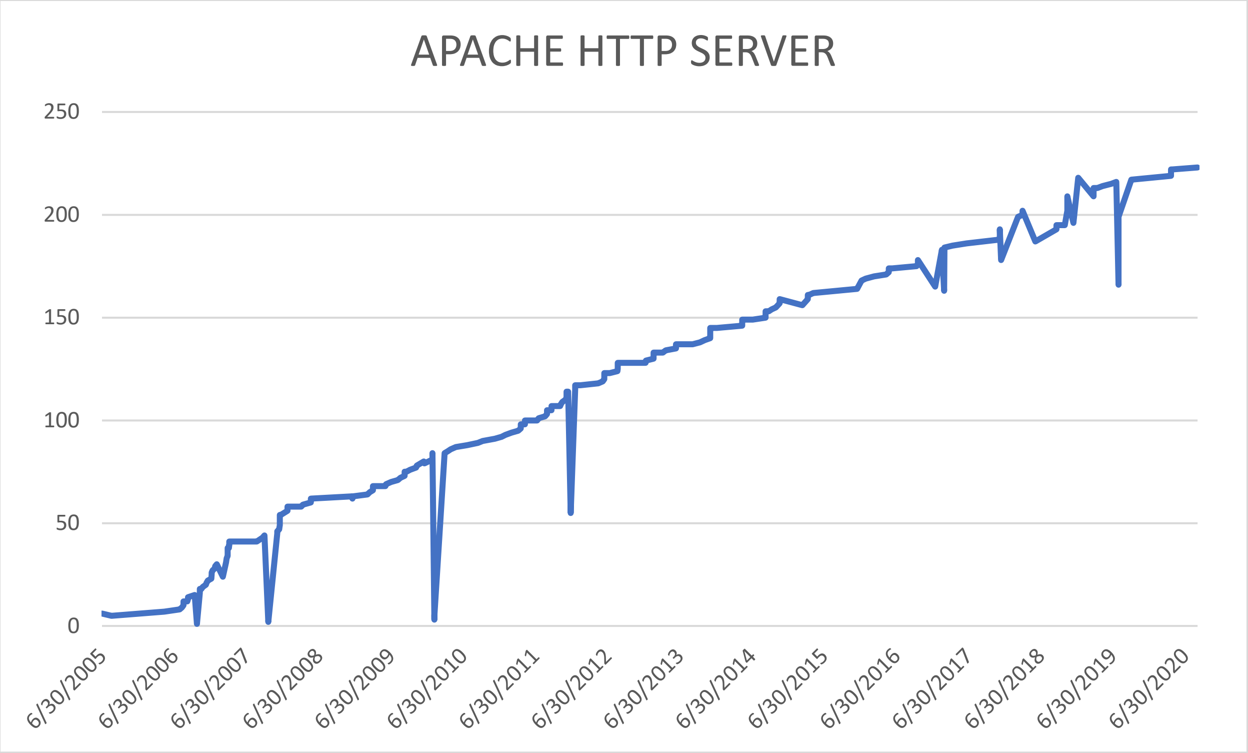
SCRIPTS USED

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*
- *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*
2. *https://school.stockcharts.com/doku.php?id=chart_analysis:trend_lines*
3. *https://httpd.apache.org/*