# Trend Analysis of the CVE Classes Across CVSS Metrics

Bindu Dodiya
Institute of computer Science
Vikram University Ujjain

Umesh Kumar Singh, PhD
Institute of computer science
Vikram University Ujjain

Vivaan Gupta
Suncity Institute
Gurgaon, Haryana

## ABSTRACT
Understanding vulnerability trends is important for risk management process.. Understanding trends helps in early detection of problems and also in planning defense mechanisms. In this paper analysis of the trends of Common Vulnerabilities and Exposures (CVE) from the National Vulnerability Database (NVD) for 2005 to 2020 has presented. 136566 CVEs has been extracted for sixteen years, also their Common Vulnerability Scoring System (CVSS) scores has been collected from the NVD, then analysis of severity, and CVSS base metrics trends ,and trends for classified vulnerability data has been done . Such analysis of vulnerability data according to their type, CIA impact, access vector and access complexity helpful in identifying most critical class of vulnerability relative to system environment and improve risk mitigation process.

## Keywords
Vulnerability, Trend analysis, CVSS metrics, CWE, NVD.

## 1. INTRODUCTION
Vulnerability is a flaw or weakness in system security procedures, design , implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. [1].The number of vulnerabilities identified has greatly increased in last few years. The number of vulnerabilities listed in national vulnerabilities database was 1677 in 2001,2156 in 2002,5733 in 2009,4639 in 2010,7946 in 2014,6484 in 2015,6447 in 2016,14714 in 2017 ,16555 in 2018, 17344 in 2019 and 18325 in 2020.Number of vulnerabilities increased drastically in 2017 there was 128% Increase in 2017 from 2016 and 112% increase in 2018 from 2017. In view of such a large growing population of vulnerabilities it is necessary to convert such large amount of data into actionable information. Understanding vulnerability evolution is important in order to improve system security. For this, it is necessary to analyze current state and trends. Knowledge of current security vulnerability trends can have significant benefits to a wide range of IT and security professionals in order for them to better understanding in preventing and mitigating the impact of the attacks.

This work focus on trend analysis of vulnerabilities on properly classified data. In this paper a fine grained trend analysis of vulnerabilities is presented with the objective to analyze how the number of vulnerabilities varies over time in different severity levels and in different severity measuring factor. Further, it analyzes similar trends for different vulnerability classes and investigates which classes follow general trends and which classes shift from

general trends and in which direction. It will be helpful in ranking vulnerability classes as per system security policies. For example some classes may affect confidentiality more as compared to availability. So system administrator can take decisions as per requirement of the system. This trend analysis will be helpful in understanding basic impact characteristics of vulnerability classes and thus in dealing with similar vulnerabilities tactfully. This trend analysis may assist security administrator in finding right combination of vulnerability prevention mechanism and designing proper security policies.

The paper is organized as follows. Section II gives the related work. Section III presents methodology and section IV Presents overall vulnerability trends and observations. Section IV presents vulnerability trends on classified data and comparison with overall trends. Finally section V is conclusion of the paper and some future works also shown.

## 2. RELATED WORK
R.Kunh et al [2] presented vulnerability severity trends based on NVD data in year range 2008-2016, They grouped the NVD CWE classes into primary types of Configuration, Design, and Implementation and presented three class's severity trends. In [1] vulnerability severity trends are presented based on NVD data in year range 2001 to 2008. Further, a view on vulnerability population distribution among categories based on CWE in year 2008 presented and related implications also given. [3] is a follow-up of [1] to measure progress in vulnerability trends. In [3] besides severity levels, trends related to access vector and access complexity are also presented for ten years. These two studies are very short and basic and don't provide detailed analysis. In [8] trend analysis of vulnerabilities in five software artifacts has been done by aggregating information from publicly available resources, such as ICAT, Bugtraq and CVE. This analysis suggests that discovery of a vulnerability may influence discovery of more vulnerabilities of same type. Further, it suggests developing a retrospective metric by measuring vulnerability occurrences and predictions based on it. Tim Shimeall et. al. [9] proposes a framework to conduct information security trend analysis using incident reports to CERT. Framework offers a common ground to resolve issues involved in performing the trend analysis and an example analysis process also presented. It is always appropriate to revisit trends as suggested in [3]. Keeping this objective in mind this work provides in depth vulnerability trend analysis on categorized vulnerability data of last sixteen years across CVSS base metric vectors in following sections.

This research references the paper" analyzing trends in vulnerability classes across CVSS metrics " by anshu et.al [10].The differences between both work are as following:

1) Their data collection is from 2000 to 2011 ,this paper analyzes trends for data from year 2005 to 2020.
2) They analysed distribution of vulnerabilities in three severity levels according to CVSS 2.0 ranges:0.0-3.9, 4.0-6.9 and 7.0-10.0 for low, medium and high respectively. In this Paper analysis in five severity levels according to CVSS 3.0 ranges: 0, 0.1-3.9, 4.0-6.9 ,7.0-8.9,9.0-10.0 for none,low, medium ,high and critical respectively has been done.

# 3. METHODOLOGY

## 3.1 Data Collection

Data for the period of 2001 to 2020 has extracted from the National vulnerability database (NVD) [2] to analyze vulnerability trends over the years. NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). NVD provides fine-grained search capabilities for all known vulnerabilities and is continuously updated to provide data for automated vulnerability management, security measurement and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics. It records vulnerabilities since 1999, total 160480 vulnerabilities listed under CVE names [6] till August 2020. NVD is using CWE [7] as a classification mechanism; each individual CWE represents a single vulnerability type. Common Weakness Enumeration (CWE) defines a standardized description of software weaknesses designed to provide a common language for describing software security weaknesses. CWE provides developers and analysts a standard definition of terms for investigating security problems in architecture, design and code. CWE also helps system administrators compare tools that attempt to find security weaknesses. All individual CWEs are held within a hierarchical structure that allows for multiple levels of abstraction. NVD uses CWEs from different levels of the hierarchical structure, by providing a cross section of the overall CWE structure. This cross section of CWEs allows analysts to score CVEs at both a fine and coarse granularity, which is necessary due to the varying levels of specificity possessed by different CVEs. There are total 13 vulnerability types in NVD classification scheme, which are based on taxonomic features vulnerability cause and vulnerability impact. Vulnerability categories are: Denial of service,Code execution,Overflow,Memory Corruption,Sql Injection,Cross site scripting,Directory traversal, Http Response Splitting, Bypass something ,Gain Information, Gain Privileges, CSRF, File Inclusion. NVD supports extensive searching under various categories, published date range, last modified date range and under different CVSS base metric parameter values. Vulnerability severity scores provided by NVD are CVSS scores.

## 3.2 Measuring severity using CVSS:

The CVSS is an open framework to measure the relative severity of software vulnerabilities. It offers a structured approach by the standardized vulnerability scores and prioritized risk. There are three metric groups in CVSS: Base, Temporal, and Environmental. The metrics, which this paper uses, are the base score provided from NVD data feeds. The aim of the base group is to define the basic characteristics of vulnerability. The base metrics consist [8]: access complexity (AC), access vector (AV), authentication (AU), confidentiality impact (CI), integrity impact (II), availability impact (AI). The NVD provides severity rankings of “None” ,”Low”, “Medium” ,”High” and “Critical” in addition to the numeric CVSS scores [7] in CVSS3.0. These qualitative rankings are simply mapped from the numeric CVSS scores as table 1:

**Table 1.CVSS score districution in CVSS3.0**

| Severity | None | Low | Medium | High | Critical |
|---|---|---|---|---|---|
| Base score | 0 | 0.1-3.9 | 4.0-6.9 | 7.0-8.9 | 9.0-10.0 |

# 4. VULNERABILITY TRENDS

## 4.1 Appearance of Vulnerabilities

Figure 1 presents yearly trend in discovery of vulnerabilities. Number of new vulnerabilities reported is rising every year and highest in year 2020. After 2006 there is decline and number of new vulnerabilities reported in year 2010 is 29% less than in year 2006. It has increased drastically in year 2017..Number of vulnerabilities reported in year 2017 was 128% more than the number of vulnerabilities reported in year 2016.

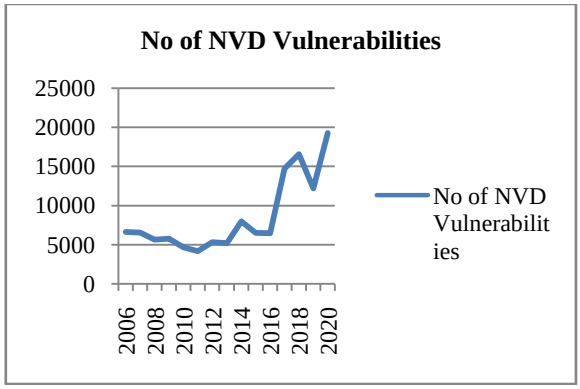


**Figure 1: Number of new vulnerabilities reported**

## 4.2 Severity Level

NVD ranks vulnerabilities by assigning one out of five severity levels none, low, medium, high and critical. These five severity levels have a mapping on the numeric CVSS scores in ranges:0, 0.1-3.9, 4.0-6.9 ,7.0-8.9,9.0-10.0 for none, low, medium ,high and critical respectively. Figure 2 presents trends in distribution of vulnerabilities among five severity levels. Number of low severity vulnerabilities is very less as compared to high and medium severity vulnerabilities. In aggregate analysis high severity vulnerabilities are 45.56%, medium severity vulnerabilities are 48.14% and low severity vulnerabilities are 6.28% of total population. Percentage of low severity vulnerabilities varies between 3.27% in year 2008 to 11.33% in year 2001. As compared to this medium severity vulnerability percentage range is 46..27% in year 2008 to 61.18% in year 2018. High severity vulnerability percentage varies between 13.93% in year 2014 to 35.32% in year 2006. These trends indicate that the proportion at each severity level has changed relatively little in last ten years with decrease in percentage of high severity vulnerabilities.

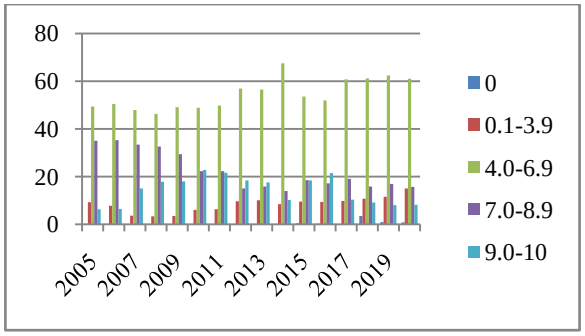


**Fig 2: Distribution of vulnerabilities by severity levels**

## 4.3 Access Vector

Access vector metric reflects how vulnerability can be exploited. Possible values for this metric can be Local System, Local Network and Remote. Local system describes vulnerabilities where the attack vector requires that the attacker is a local user on the system. From local network describes vulnerabilities where the attack vector requires that an attacker is situated on the same network as a vulnerable system (not necessarily a LAN).This category covers vulnerabilities in certain services for example, DHCP, RPC, administrative services, which should not be accessible from the Internet, but only from a local network and optionally a restricted set of external systems. From remote describes vulnerabilities where the attack vector does not require access to the system nor a local network. This category covers services, which are acceptable to expose to the Internet for example, HTTP, HTTPS, SMTP as well as client applications used on the Internet and certain vulnerabilities, where it is reasonable to assume that a security conscious user can be tricked into performing certain actions. Figure 3 presents trends in distribution of vulnerabilities with respect to CVSS base metric, attack Vector. In aggregate analysis 85.08% vulnerabilities are remotely exploitable, 12.02% requires local access and population belonging to local network metric is very low 2.35%. In year wise analysis remotely exploitable vulnerabilities range between 71% in year 2014 to 91.85% in year 2009, vulnerabilities that require local access range between 7.79% in year 2009 to 15.96% in year 2005. Vulnerabilities that require adjacent network access for exploitation are very low always range between 0.1% in year 2008 to 2.73% in year 2013.These trends clearly indicate that access vector metric value is high for majority of vulnerabilities and suggests to do network hardening to thwart attacks.

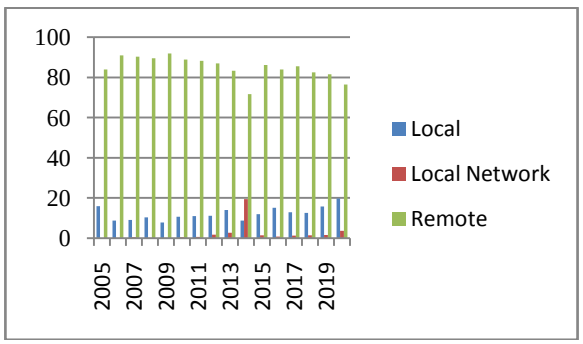


**Fig 3: Distribution of vulnerabilities by Attack Vector**

## 4.4 Access Complexity

Access complexity measures the complexity of the attack require to exploit the vulnerability after gaining access to system. Possible values for this metric can be low, medium and high. Low complexity means one that involves no specialized conditions, such as a default configuration, or an attack can be conducted manually and requires little skill. Medium complexity means that access conditions are somewhat specialized, such as involving no default configuration or requires specific system knowledge. High complexity involves specialized access conditions such as elevated privileges required, rarely seen configuration and chances of detection also high. Figure 4 presents trends in distribution of vulnerabilities with respect to CVSS base metric, Access Complexity. In aggregate analysis 55.79% vulnerabilities are easily exploitable, 60.16% are of medium access complexity and only 4.3% requires specialized conditions for exploitation. In year wise trends low access complexity vulnerabilities range between 41.45% in year 2014 to 78.21% in year 2005, vulnerabilities that require medium access complexity range between 16.43% in year 2005 to 55.86% in year 2014. Vulnerabilities that require high access complexity for exploitation are very low, range between 1.77% in year 2015 to 12.13% in year 2006 & 2007. In initial years most of the vulnerabilities were of low access complexity but now percentage of low access complexity is decreasing and percentage of medium access complexity is increasing proportionately. While percentage of high access complexity is low always below 6% with an exception of 12% in year 2006 and in 2007. These trends warn us that even not so skilled attackers have favourable chances to exploit the vulnerabilities.

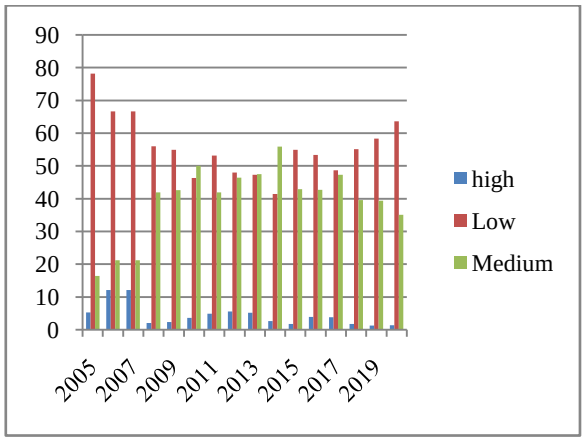


**Fig 4: Distribution of vulnerabilities by Access Complexity**

## 4.5 Authentication

Authentication measures number of times an attacker requires authenticating after gaining access on the target system in order to exploit the vulnerability. Possible values for this metric can be none, single and multiple. Multiple authentication means attacker authenticate two or more times. Figure 5 presents trends in distribution of vulnerabilities with respect to CVSS base metric, Authentication. In aggregate analysis 86.64% vulnerabilities require no authentication, 10.97% require single authentication and multiple authentication population is negligible 0.94%. Up to year 2005, around 99% of vulnerabilities can be exploited once attacker gains access to the system, no further authentication needed.

After year 2005 also this percentage is above 91. So these trends clearly indicate that for a successful attack, an attacker just requires to gain access to the system that is also possible remotely and with not so specialized skill set.

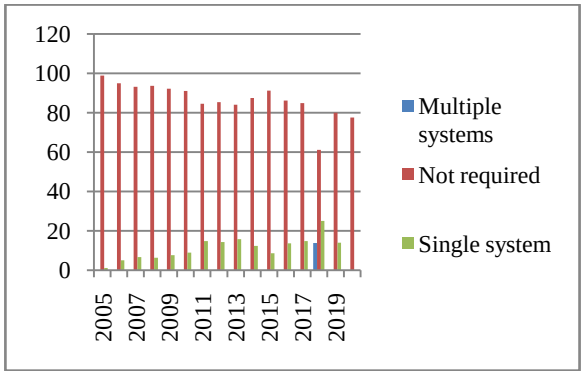


**Fig 5: Distribution of vulnerabilities by Authentication**

## 4.6 Confidentiality Impact

This metric measures the impact on confidentiality that is controlling access and disclosure of information to unauthorized persons. Possible values for this metric can be none, partial and complete. Complete refers to total information disclosure, partial refers to considerable information disclosure and none refers no impact on confidentiality of system. Figure 6 presents trends in distribution of vulnerabilities with respect to CVSS base metric, Confidentiality impact. In aggregate analysis 32.30% vulnerabilities result in no impact, 20.95% vulnerabilities impact completely and 46.32% vulnerabilities impact partially, confidentiality of system on exploitation. In year wise trends percentage population of vulnerabilities with partial impact is always higher ranging from 36% in year 2013 to 61% in year 2006. Then vulnerabilities with no impact in the range 28.48% in year 2007 to 37% in year 2005. Vulnerabilities that result in complete disclosure are in range 10% in year 2006 to 31% in year 2016. These trends reveal that vulnerabilities with complete impact were continuously rising from year 2005 to year 2016, year 2007 shown maximum increase more than double from 10% in year 2006 to 22% but from last two years it started decreasing and it is 17% and 14% respectively in year 2017 and 2018 after reaching it's highest value in 2016.

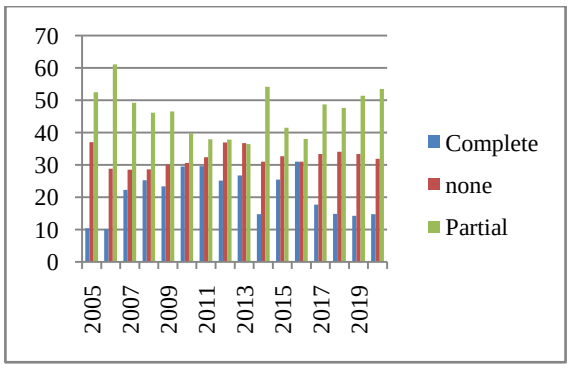


**Fig 6: Distribution of vulnerabilities by Confidentiality Impact**

## 4.7 Integrity Impact

This metric measures the impact on trustworthiness and veracity of information. Possible values for this metric can be none, partial and complete. Complete refers to compromise of entire system, partial refers to attacker can modify some information but scope of affect is limited and none refers no impact on integrity of system. Figure 7 presents trends in distribution of vulnerabilities with respect to CVSS base metric, Integrity impact. In aggregate analysis 27.37% vulnerabilities result in no impact, 20.21% vulnerabilities impact completely and 52.06% vulnerabilities impact partially, integrity of system on exploitation. In year wise trends percentage population of vulnerabilities with partial impact is always highest ranging from 36% in year 2016 to 70% in year 2006. Then vulnerabilities with no impact in the range 19% in year 2008 to 34% in year 2017. Vulnerabilities that result in complete compromise are in range 9% in year 2006 to 30% in year 2016. These trends reveal that vulnerabilities with complete impact are rising, year 2007 shown maximum increase more than double from 9% in year 2006 to 21%. but from 2017 it started decreasing and it is 17% and 14% respectively in year 2017 and 2018 after reaching it's highest value in 2016

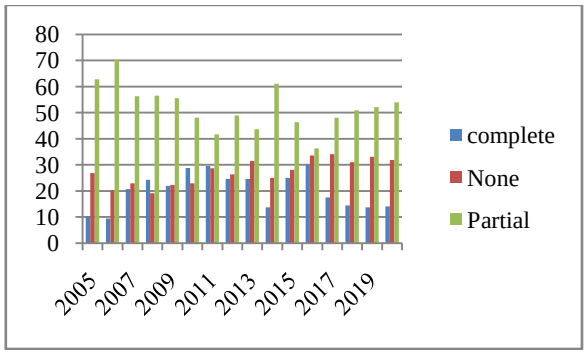


**Fig 7: Distribution of vulnerabilities by Integrity Impact**

## 4.8 Availability Impact

This metric measures the impact on accessibility of information resources. Possible values for this metric can be none, partial and complete. Complete refers to total shutdown of affected resource; partial refers to reduced performance or interruptions in availability of resource and none refers no impact on availability of resource. Figure 8 presents trends in distribution of vulnerabilities with respect to CVSS base metric, Availability impact. In aggregate analysis 34.26% vulnerabilities result in no impact, 24.46% vulnerabilities impact completely and 41.19% vulnerabilities impact partially, availability of system on exploitation. In year wise trends percentage population of vulnerabilities with partial impact is always highest ranging from 31% in year 2013 to 55% in year 2006.Then vulnerabilities with no impact in the range 25% in year 2007 to 39% in year 2018. Vulnerabilities that result in complete compromise are in range 12% in year 2006 to 35.71% in year 2016. These trends reveal that in last five years vulnerabilities with complete impact are rising, year 2007 shown maximum increase more than double from 12% in year 2006 to 27%. but from 2017 it started decreasing and it is 21% and 18% respectively in year 2017 and 2018 after reaching it's highest value in 2016.

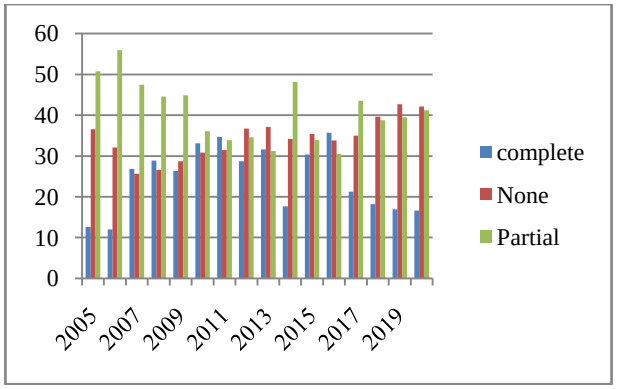


**Fig 8: Distribution of vulnerabilities by Availability Impact**

## 5. TRENDS IN VULNERABILITY CLASSES

With the aim of gaining insight into level of affect caused by different vulnerability classes on various security measuring factors, in this section trend analysis done on classified vulnerability data across six base metric vectors of CVSS framework. Classification scheme is same as adopted by NVD which classify vulnerability data in 13 classes based on CWE. Classes are Denial of service,execude code,overflow,XSS,Directory traversal,Bypass Something,Gain Information,Gain Privilege,sql injection,file inclusion,Memory Corrouption,CSRF,Http Response splitting.

### 5.1 Population Distribution in Classes

Figure 9 presents distribution of vulnerability population across 13 vulnerability classes. Five most populated vulnerability classes are Dos 16.6%,Code execution 24.8%,XSS 12.6%,Overflow 12.8 % and Gain Information 8%.In all these top five vulnerability categories contribute 74.8% of total vulnerability population..

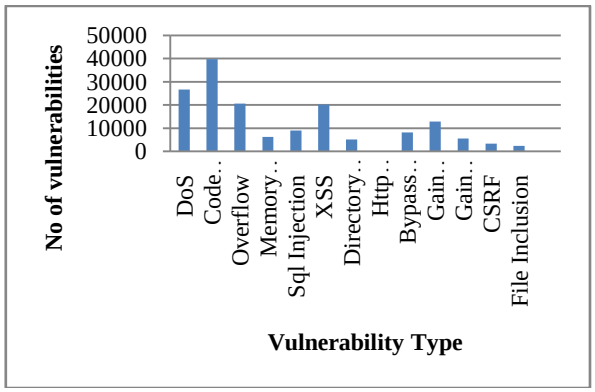


**Figure 9. Distribution of vulnerability population in Classes**

### 5.2 Severity Level

Figure 10 presents distribution of vulnerability population in vulnerability classes across five severity ranking levels: “None” ,”Low”, “Medium” ,”High” and “Critical”. Memory Corruption vulnerability class has 54.81 % of vulnerabilities of Critical severity.SQL injection vulnerability class has 77.83% of vulnerabilities of high severity. File Inclusion has 61.85% of vulnerabilities of high severity and Gain Privileges has 43.43% vulnerabilities of high severity. CSRF includes 93.20% of vulnerabilities of medium severity and just 2.63% of high severity.


**Figure 10. Distribution of vulnerabilities by severity level across classes**

### 5.3 Distribution of vulnerabilities by Access Vector across classes

Figure 11 represents distribution of vulnerability population in vulnerability classes for access vector. Local, Local network and Remote. Most of the vulnerability classes follow trends similar to common trends that is remotely exploitable vulnerabilities includes maximum population above 70% and Local network includes negligible number of vulnerabilities. Vulnerability percentages with local access are also low below 20% in maximum classes. Gain Information and Gain Privileges are only two classes having high percentage of locally exploitable vulnerabilities

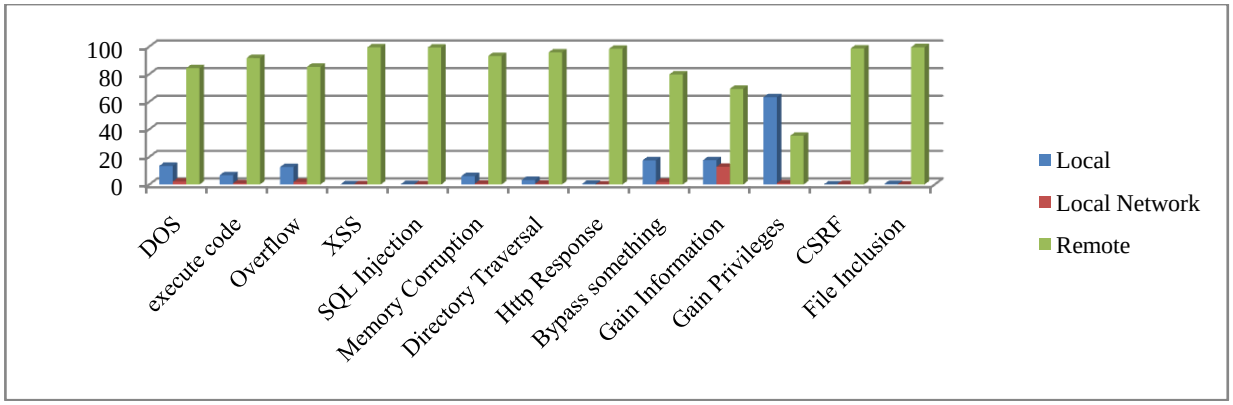


**Figure 11.Distribution of vulnerabilities by Access Vector across classes**

## 5.4 Access Complexity

Figure 12 presents distribution of vulnerability population in vulnerability classes with respect to access complexity metric values: low, medium and high. Access complexity is low for 50% of vulnerability population in most of the classes. Population percentage for medium access complexity is also around 50%. High access complexity is below 5% in majority of classes. These trends indicate that even not so skilled attackers can exploit the vulnerability belonging to any class. For 93 %Vulnerabilities in class XSS access complexity is medium.

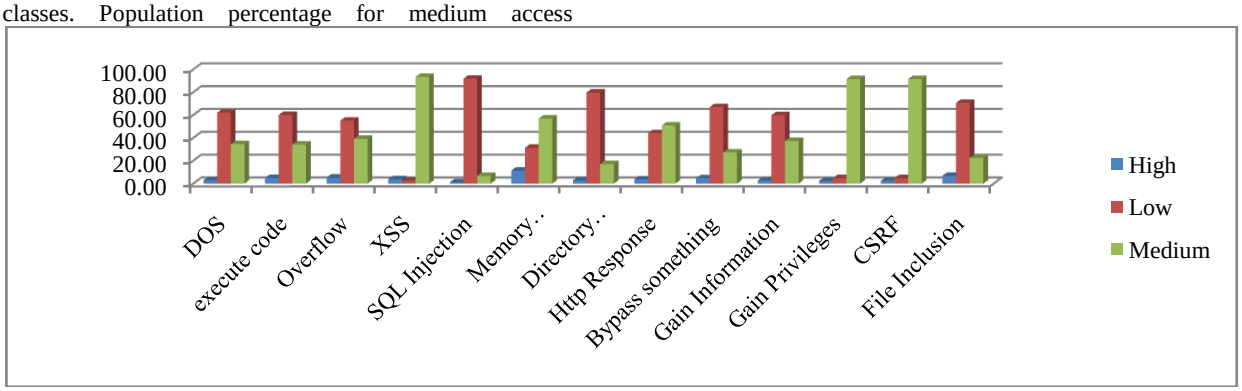


**Figure 12..Distribution of vulnerabilities by Access Complexity across classes**

## 5.5 Authentication

Figure.13 presents distribution of vulnerability population in vulnerability classes with respect to Authentication metric values: multiple system, single system and not required. More than 80% vulnerabilities in all classes require no authentication to be exploited.

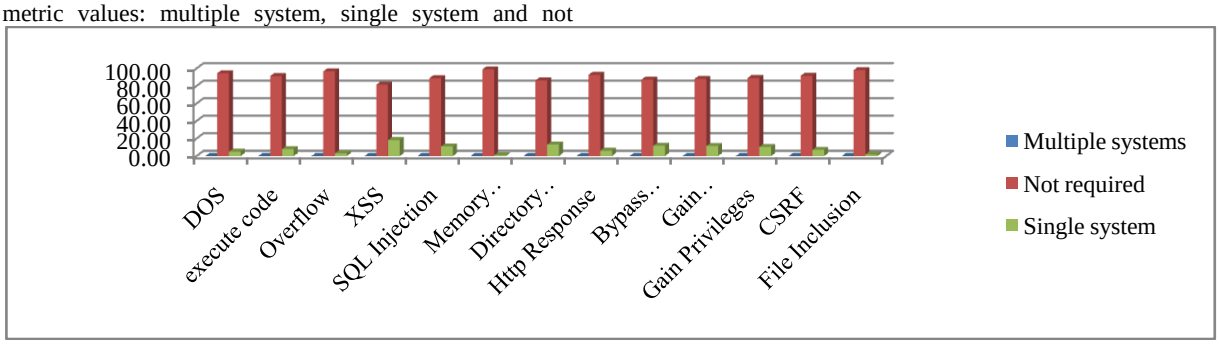


**Figure 13 Distribution of vulnerabilities by Authentication across classes**

## 5.6 Confidentiality Impact

Figure 14 presents distribution of vulnerability population in vulnerability classes with respect to Confidentiality Impact metric values: none, partial and complete. Overflow, execute code, Memory Corruption, Gain privileges are the classes that includes around 50% of vulnerabilities that have complete impact on confidentiality of system. In rest of the classes around 60% vulnerabilities have partial impact on confidentiality of system. Only XSS and Http response are exception in which more than 90% vulnerabilities have no impact on confidentiality.

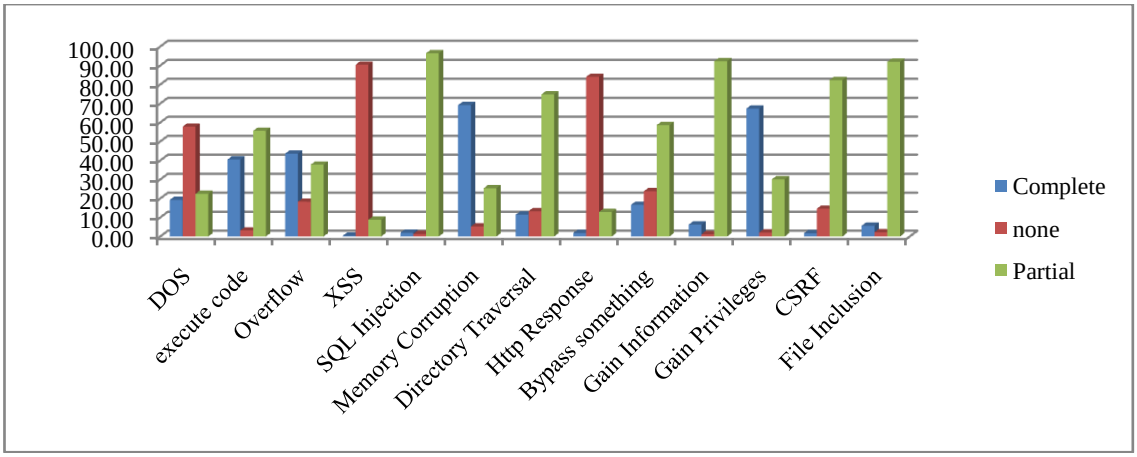


**Figure 14.Distribution of vulnerabilities by Confidentiality Impact across classes**

## 5.7 Integrity Impact

Figure 15 presents distribution of vulnerability population in vulnerability classes with respect to Integrity Impact metric values: none, partial and complete. Similar to confidentiality impact, Overflow, execute code, Memory Corruption, Gain privileges are the classes that includes around 50% of vulnerabilities that have complete impact on integrity of system. In CSRF, XSS ,http response and SQL injection classes more than 95% of vulnerabilities

have partial impact on integrity of system. In Authentication issues, Code injection and Path traversal classes around 60% of vulnerabilities have partial impact on integrity of system.

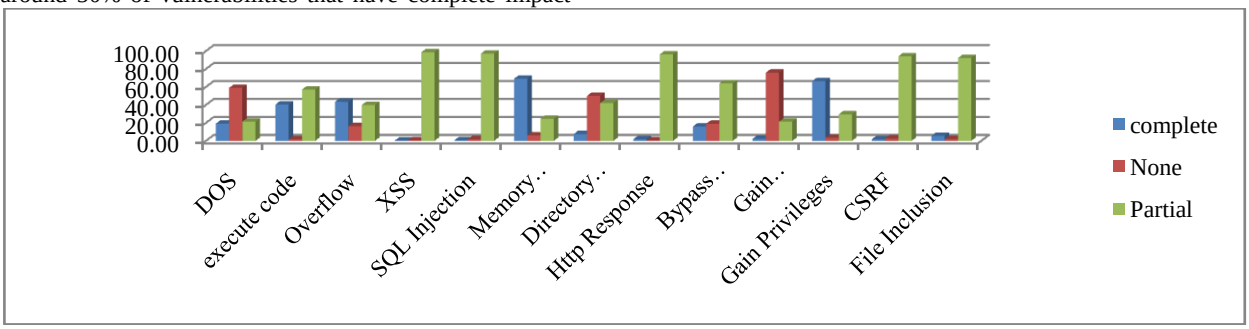


**Figure 15.Distribution of vulnerabilities by Integrity Impact across classes**

## 5.8 Availability Impact

Figure 16 presents distribution of vulnerability population in vulnerability classes with respect to Availability Impact metric values: none, partial and complete. Vulnerability classes' show diverse trends in case of availability impact. In XSS and Information leak/disclosure classes more than 90% of vulnerabilities have no impact on availability of system resources. In SQL injection class more than 99% of vulnerabilities have partial impact on availability of system resources. More importantly in classes Buffer errors, Insufficient information, Link following, Numeric errors, OS command injection, Race condition, Resource management more than 50% of vulnerability population affect availability of system resources completely.

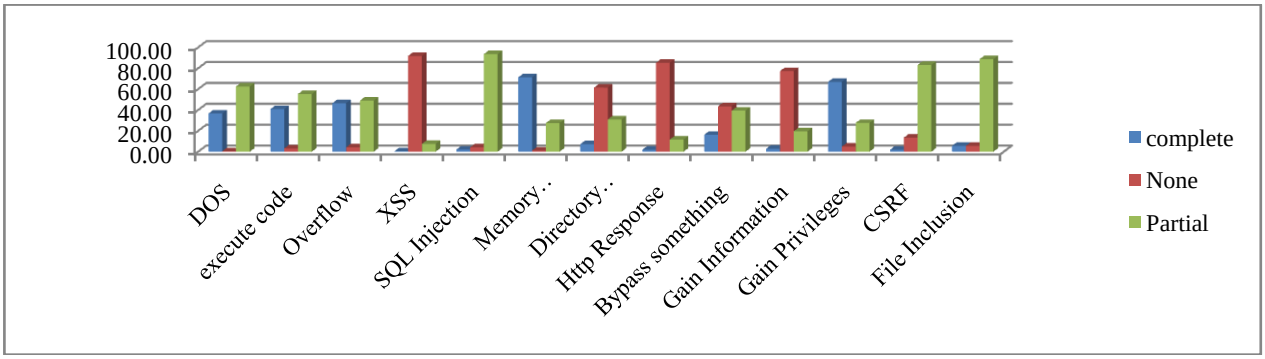


**Figure 16.Distribution of vulnerabilities by Availability Impact across classes**

## 6. CONCLUSION

In this paper 136566 CVEs from the NVD for the period 2005 to 2020 has been analysed. All of the CVE data were analysed by frequency, scores, and CVSS base metrics value. There are some significant findings as follows:

1. Medium severity vulnerabilities are always high, More than 50% for 2005 to 2016 and were more than 60% from 2017.and was highest 67% in 2016.

2. The proportion of attack Vectors has largely stayed the same since 2006, apart from Local network exploits which have grown .There is an outlier in 2014 4 which can be attributed to a
3. large number of a specific exploit in mobile applications with improper cryptography (CWE-
4. 310). Vulnerabilities with attack vector Local Network was highest 19 % in 2014.
5. The number of low complexities exploits consistently decreased until 2014 and started increasing from 2015 and is consistently increasing.
6. There has been a growth in single authentication attacks. Vulnerabilities with Single system authentication are always high more than 80% except 2018.

This paper is a contribution to ongoing research in vulnerability trend analysis, which helps the IT professionals to predict threats and protect organizations. Bringing focus on the vulnerability trends.Relative priority of different vulnerability classes can be decided depending on trend analysis presented in this work. Few Points are mentioned above. By analyzing vulnerability trends, Security professionals will be better informed in developing policies that more closely reflect the vulnerability threat landscape. Further research could examine more CWE's. There is also potential to investigate specific vendors and trends within CVE's specific to that vendor.

## 7. REFERENCES

[1] G Stoneburner, A Goguen, and A Feringa, "Risk Management Guide for Information Technology Systems", NIST Special Publication 800- 30, July 2002, Available: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[2] Richard Kuhn, M S Raunak and Raghu Kacker" An Analysis of Vulnerability Trends, 2008 – 2016", Proceedings, Software Quality, Reliability and Security (QRS-C), 2017 IEEE International Conference on (pp. 587-588).

[3] R. Kuhn and Chris Johnson, "Vulnerability Trends: Measuring Progress", IT Professional, 2010, pp. 51-53.

[4] National Vulnerability Database, http://nvd.nist.gov.

[5] Common Vulnerabilities and Exposures. [Online]. Available:http://cve.mitre.org

[6] Common Weakness Enumeration. [Online]. Available: http://cwe.mitre.org

[7] "NVD Common Vulnerability Scoring System Support v2", National Vulnerability Database, Available:https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?version=3

[8] R. Gopalakrishna, E. Spafford and J. Vitek, "A Trend Analysis of Vulnerabilities", CERIAS TR 2005-06, 2005.

[9] Tim Shimeall and Phil Williams, "Models of Information Security Trend Analysis", Available at http://www.cert.org/archive/pdf/info-security.pdf.

[10] Tripathi, A. Singh, U.K., " Analyzing Trends in Vulnerability Classes across CVSS Metrics", International Journal of Computer Applications (0975 – 8887) Volume 36– No.3, December 2011.