A Method for Vulnerability Database Quantitative Evaluation

Tiantian Tan[1, *], Baosheng Wang[1], Yong Tang[1], Xu Zhou[1] and Jingwen Han[2]

Abstract: During system development, implementation and operation, vulnerability database technique is necessary to system security; there are many vulnerability databases but a lack of quality standardization and general evaluation method are needed. this paper summarized current international popular vulnerability databases, systematically introduced the present situation of current vulnerability databases, and found the problems of vulnerability database technology, extracted common metrics by analyzing vulnerability data of current popular vulnerability databases, introduced 4 measure indexes: the number scale of vulnerabilities, the independence level, the standardization degree and the integrity of vulnerability description, proposed a method for vulnerability database quantitative evaluation using SCAP protocol and corresponding standard, analyzed a large number of vulnerabilities in current popular vulnerability database, quantitative evaluated vulnerability database by the law of normal distribution, the experimental results show this method has strong versatility and science, and it is beneficial to improve the quality and standardization construction for vulnerability database development.

Keywords: Vulnerability management, vulnerability database, quantitative evaluation.

1 Indroduction

Since data security and privacy protection become one of the most important reasons for users to choose edge systems, privacy security has become one of the most important technologies in edge computing. However, the current effective edge computing security mechanism is still a blank space, and some efficient network security mechanisms can be applied to edge computing platform, for some examples, in 2011, a more robust DDoS detection method on the basis of Conditional Random Fields model is proposed by Liu et al. [Liu, Cai and Zhong (2011)]; in 2013, a mechanism for multi-monitor joint detection with lower communication overhead is proposed by Cai et al. [Cai, Wang and Zheng (2013)]; in 2015, a distributed Ternary Content Addressable Memory (TCAM) coprocessor architecture proposed by Cai et al. [Cai, Chen, Chen et al. (2015)] for Longest Prefix Matching (LPM), Policy Filtering (PF), and Content Filtering (CF); in 2018, a MPTCP scheduler is proposed for Web Transfer by Yang et al. [Yang, Dong, Tang et al. (2018)]. Vulnerabilities exist in the implementation and operation of security

[1] National University of Defense Technology, Deya village, Changsha, China.

[2] University of British Columbia, Vancouver, Canada.

[*] Corresponding Author: Tiantian Tan. Email: happinesschild@126.com.

CMC. doi:10.32604/cmc.2019.06051

mechanisms, it is not realistic to completely eliminate vulnerability [Tan, Wang, Zhou et al. (2018); Tan, Wang, Zhou et al. (2018)], once exploited by an attacker, the damage and loss is difficult to repair, vulnerability database is a basic tool for vulnerability management [Ou, Hu, Zhang et al. (2007)], it can provide comprehensive functions, such as collection and release of vulnerabilities, vulnerability description, etc., it is the primary technology in the information security field. However, in development of current vulnerability database technology, there are some problems:

- There are a lot of popular vulnerability databases with different characters, such as data scale, data source, standardization and integrity degree, it is a lack of a survey of vulnerability databases research to systematically summarize and introduce the characters of current popular vulnerability databases.
- Due to various network equipment manufacturers, Internet companies and research institutions, in different vulnerability databases, the same vulnerability may have different release time and description data structure, heterogeneous data structures in different vulnerability databases prevent standardization construction and data sharing from each other.
- Different vulnerability databases have different quality; there is a lack of a common evaluation method to evaluate the quality of vulnerability database, a common method for vulnerability database quality quantitative evaluation need to be proposed.

To solve above problems, on the basis of summarizing a large number of vulnerability data of current popular vulnerability databases, this paper proposed a vulnerability database evaluation method to evaluate the quality of vulnerability database. The contributions of this paper are as follows:

- This paper systematically summarized all popular vulnerability databases at home and abroad, systematically introduced the details of current popular vulnerability databases.
- Based on SCAP protocol, this paper proposed vulnerability database evaluation method, analyzed a large number of vulnerability data in popular vulnerability databases, extracted the major features, such as data scale, the source independence level, integrity and standardization degree of vulnerability data as 4 measure indexes to quantify and grade the vulnerability database.
- The evaluation method using normal distribution quantitative evaluated current popular vulnerability databases, the result can show that it is beneficial to regulate the vulnerability database construction and operations, promotes the quality standard construction of vulnerability database and provides a reference for vulnerability database standardized construction. Compared with method which needs to set fixed value for measure index, this method has the advantage of keeping high accuracy with the development of the vulnerability technology.

Table 1: Vulnerability databases published by International government

Operating Agency	Vulnerability Database	Abbr.
The National Vulnerability Database	National Vulnerability Database [US-CERTSOC (2018)]	NVD
Carnegie Mellon University	CMU Cert Vulnerability Notes Database [CMU (2018)]	CVN
Australia Computer Emergency Readiness Team	Australian CERT [ACERT (2018)]	AusCERT
Japan Vulnerability Notes	Japan Vulnerability Notes [JVN (2018)]	JVN
China Information Technology Security Evaluation Center	China National Vulnerability Database of Information Security [CITSEC (2018)]	CNNVD
China Research Center for Information Technology Security, CNCERT/CC.	China National Vulnerability Database [CNCERT/CC (2018)]	CNVD
National Computer Virus Emergency Response Center (NCNERC), Anti-Virus Products Testing and Certification Center, Key Laboratory of Computer Network and Information Security Ministry of Education.	Security vulnerability database [NCNIPC (2018)]	NIPC
Tsinghua University	Security Content Automation Protocol Chinese Community [TU (2018)]	SCAP Chinese
Shanghai Jiao Tong University	Education Vulnerability Report Platform [ESVRP (2018)]	Edu-info

2 The research of vulnerability database technique

Nowadays, popular vulnerability databases were published by 2 agency, such as governmental vulnerability databases and enterprise vulnerability databases, each category has its major functional requirements, such as vulnerability management and security services [Wang, Guo, Wang et al. (2009)].

2.1 Vulnerability databases published by International government

For the development of vulnerability technology, international authorities have built a lot of influential governmental vulnerability databases, such as the national vulnerability database NVD, us-cert constructed by Computer Emergency Readiness Term, Australian CERT vulnerability database, etc. In 2009, China successfully established three vulnerability databases: CNNVD, CNVD, and NIPC. Subsequently, in 2012, Tsinghua University completed the construction of SCAP Chinese vulnerability database, the operating agency and abbreviation of the popular governmental vulnerability databases are shown in Tab. 1.

Table 2: Vulnerability databases published by International enterprise

Operating Agency	Vulnerability Database	Abbr.
IBM	IBM ISS X-Force [IBM (2018)]	IBM X-Force
Open Security Foundation	Open Source Vulnerability Database [Martin and Kouns (2018)]	OSVDB
Security Focus	Bugtraq Security Focus [SF (2018)]	Security Focus
Flexera Software	Secunia[FS (2018)]	Secunia
Offensive Security	Exploit Database [OS (2018)]	EDB
Security Focus	CXSecurity [SF (2018)]	CXSecurity
SecurityLab	SecurityLab [SL (2018)]	SecurityLab
Security Tracker	Security Tracker [ST (2018)]	Security Tracker
PacketStorm	PacketStorm Security Sevices [Packetstorm (2018)]	PacketStorm
ZeroDay	ZeroDay [ZeroDay (2018)]	ZeroDay
1337Day	1337Day [1337day (2018)]	1337Day
Cisco	Cisco Security Advisories and Alerts [Cisco (2018)]	Cisco Security Vulnerabilities
NSFOCUS	NSFOCUS Security Vulnerability Database (Chinese) [Nsfocus (2018)]	NSFocus
Venus Tech	Venus Tech Security Vulnerability Database (Chinese) [VT (2018)]	Venus
SCANV	Seebug[Seebug(2018)]	Seebug
Qihoo360	Butian Vulnerability Response Platform [Qihoo360 (2018)]	Butian
HUAWEI	HUAWEI Security Warning [HS (2018)]	HUIWEI Security Warning
FreeBuf	Vulnerability Box [FreeBuf (2018)]	Vulnerability Box
Wooyun	Wooyun [Wooyun (2018)]	Wooyun

2.1.1 NVD

U.S. National Vulnerability Database (NVD) is constructed by the U.S. National Institute of Standards and Technology (NIST) which was established in 2005, supported by the Department of Homeland Security (DHS), network security department and the United States Computer Emergency Readiness Team(us-cert). Due to the abundant data resources, detailed vulnerability information description, standardized vulnerability database structure, authoritative and reliable content, NVD is beneficial to many advanced technologies, such as vulnerability mining, and vulnerability exploit, vulnerability assessment, vulnerability management, etc. NVD vulnerability database has become the worldwide industry standard, about 50%~60% of the vulnerabilities in the other popular vulnerability database also use CVE id to identify vulnerabilities, that is beneficial to standardization. NVD uses CVSS standard to evaluate vulnerability risk level, uses CPE standard to describe relevant software versions and platforms, and classifies vulnerabilities according to CWE and SCAP.

The vulnerability entries of NVD vulnerability database are more than 80,000. NVD has its own us-cert vulnerability announcement, us-cert security warning, OVAL information and CPE information, NVD is one of the most complete vulnerability databases in the world. The NVD and CVE [NCVERC (2018)] vulnerability databases are compatible with each other and NVD contains all the vulnerability data of CVE database. In the NVD vulnerability database, the vulnerability information can be searched according to the CVE id. Therefore, the NVD vulnerability database has good universality.

NVD mainly focuses on the vulnerabilities in system and protocol layer rather than Web vulnerabilities are less. The NVD vulnerability database adopts SCAP standard protocol. Each vulnerability has 15 fields, includes the CVE id, vulnerability title, vulnerability description, CVSS score, risk level, release date, update date, exploit method, risk type, reference, affected version and platform. Because of long time for auditing vulnerabilities, the timeliness of NVD is obviously insufficient.

2.1.2 CVN

In 1998, the U.S Defense Advanced Research Projects Agency (DARPA) at Carnegie Mellon University's software engineering institute set up Computer Emergency Readiness team/coordination center (CERT/CC) to collect and publish the Internet security incidents and security vulnerabilities, provide safety techniques, security update advice and safety emergency response. CERT/CC established CERT Vulnerability Notes (CVN). CVN has an authoritative data source, and proposed the risk metric method of vulnerabilities. However, CVN has only one data source, the number of vulnerabilities is not large enough, and the vulnerability data is not comprehensive enough.

2.1.3 CNVD

China National Vulnerability Database(CNVD) is constructed by China Research Center for Information Technology Security and CNCERT/CC, CNVD has rich vulnerability resource, the number of vulnerability entries is over 90000, its vulnerability identification form is: CNVD-YYYY-NNNN, each vulnerability information record 14 properties, risk evaluation has 3 grades: high, medium and low, update delay is 1-2 days.

2.1.4 NIPC

Security vulnerability database (NIPC) is constructed by National Computer Virus Emergency Response Center (NCNERC), Anti-Virus Products Testing and Certification Center, and Key Laboratory of Computer Network and Information Security Ministry of Education. The NIPC vulnerability database contains nearly 90,000 vulnerability entries which are in form of nipc-yyyy-nnnnn, and each vulnerability entry has 19 attributes. The risk evaluation has 3 grades: high, medium and low, and the update delay are 1-2 days. By studying relevant standards of vulnerability database and fusion algorithm for heterogeneous vulnerabilities, the vulnerability information of NIPC has a high exploit rate.

2.1.5 SCAP

The SCAP vulnerability database integrates the vulnerability data from a large number of vulnerability databases and some corresponding standards of security vulnerabilities, including NVD, OSVDB, Securityfocus, Packet-Storm, CNNVD and SCAP standards, etc. Through in-depth analysis, the security vulnerability data sharing and security services are established. SCAP is a vulnerability information sharing platform which provides vulnerability information query services. Vulnerability information includes detailed information and partial proof of concept (POC). SCAP introduced the SCAP standard in detail, such as CCE, CWE [TU (2018)], OVAL, Android special vulnerability databases [Yang, Wen and Zhang (2015)], and reclassified the vulnerabilities according to the structure level of Android system.

2.2 Enterprise vulnerability databases

For the propose of collecting the vulnerability information of the corresponding business system and establishing an emergency response center to minimize the loss caused by the vulnerability exploit, improving their products, sharing and trading of vulnerabilities, etc.. As shown in Tab. 2, many enterprises have built vulnerability databases based on their own business and technical characteristics, such as the Common Vulnerabilities and Exposures(CVE) constructed by Mitre corporation, Open Source Vulnerability Database(OSVDB), SecurityFocus vulnerability Database, X_Force Vulnerability Database constructed by IBMISS, Secunia Vulnerability Database in Denmark, VUPEN [VVRT (2018)] Vulnerability Database in France, NSFocus Vulnerability Database constructed by NSFOCUS corporation, Wooyun vulnerability Database, SeeBug, Chinese Vulnerability Database constructed by Venus Tech corporation, IBM's x-force and Cisco’s vulnerability database (a vulnerability information sharing platform built to improve their products), ZeroDay, 1337Day (a vulnerability sharing and trading platform), etc.

2.2.1 SecurityFocus

The SecurityFocus vulnerability database established by Symantec Company contains over 90,000 vulnerability entries. Its major feature is that the vulnerability information not only includes a brief description, but also contains many details, such as the attack method, script instance and other contents provide convenience for analyzing the vulnerability. Compared with the government vulnerability database such as NVD, the vulnerability release approach of SecurityFocus is more convenient and timelier; it has a greater international influence. However, SecurityFocus has some deficiencies in the processing of vulnerability data. It lacks standardized systematic vulnerability classification and authoritative vulnerability risk assessment.

2.2.2 X-Force

X-force vulnerability database updates data timely, through the web site xforce.iss.net, the majority of users can query the vulnerability information. Relying on the product platform of IBM, the x-force vulnerability database has been transformed into security products such as security scanner, and it is one of a few vulnerability databases that can transform security vulnerability data into security services.

2.2.3 EDB

The EDB database is a security vulnerability database developed and maintained by OffensiveSecurity, which provides vulnerability query services for free. EDB uses CVE id to identify vulnerabilities and provides verification code for a large number of vulnerabilities, it has great influence in the security field. The deficiencies of EDB are mainly reflected in the lack of natural language description of vulnerabilities, the classification and risk assessment of vulnerabilities.

2.2.4 NSFocus

NSFocus contains 36,000 vulnerability entries, and provides users with security scanning and protection services based on a large amount of vulnerability data.

2.2.5 Seebug

Seebug vulnerability information is released through manual processing, and the vulnerability data is authoritative. In addition, over 80% vulnerability entries provide proof of concept (POC) which brings convenient to security researchers to study the vulnerabilities.

Table 3: The information of 15 international popular vulnerability databases

vulnerability database	Language	Vulnerability Number (104)	Field Number	CVE (%)	CVS (%)	CWE (%)	Has POC or not
NVD	English	8.4	13	100	100	100	No
SecurityFocus	English	9.1	13	38	46	46	Yes
OSVDB	English	11.4	16	75	66	66	No
X-Force	English	10.8	15	75	72	72	No
Secunia	English	7.2	14	80	43	43	No
EDB	English	3.7	8	58	62	62	Yes
CXSecurity	English	2.6	11	56	46	46	Yes
PacketStorm	English	4.1	8	9	8	8	Yes
CNVD	Chinese	9.1	15	52	46	46	No
CNNVD	Chinese	9.2	9	92	95	95	No
NIPC	Chinese	8.0	19	93	93	93	No
SCAP Chinese	Chinese	9.1	10	95	95	95	No
Seebug	Chinese	5.2	7	16	18	18	Yes
NSFocus	Chinese	3.6	12	52	48	48	No
Wooyun	Chinese	2.4	9	0	0	0	No

2.3 Summary

The information of 15 international popular vulnerability databases is shown in Tab. 3, the details includes country, language, the number of vulnerabilities, proportion of vulnerabilities with CVE id, CVSS and CWE, etc. The vulnerability database with largest vulnerability number is OSVDB. It is shown that the number of vulnerabilities and fields in each vulnerability databases are different, only a few vulnerability databases contain proof of concept (POC), many vulnerability databases use the CVE id.

3 Quantitative evaluation method based on SCAP protocol

The Security Content Automation Protocol (SCAP), designed by the United States National Institute of Standards and Technology (NIST) [Mell and Grance (2002)], is a complete and mature mechanism for standardized vulnerability assessment, and its major feature is the standardized and automated architecture. SCAP integrates six methods: CVE, CVSS [Grance, Kuhn and Landau (2007)], OVAL, CPE [NISTCPET (2014); Zhang, Wu, Liu et al. (2011)], CCE, XCCDF. Standardization is the major advantage of SCAP, SCAP provides the solution for the field of security standardization, including input and output data format, standard processing method, uniform field and risk level measurement, it can automatically audit complex system configuration, and improve the degree of versatility and automation.

To better grasp the latest progress in the field of vulnerability databases research and implementation, this article analyzed popular vulnerability database from the aspect of operating agency, data features, operation, etc., proposed a metric for vulnerability database evaluation, extracted the vulnerability data scale, the data independence level, data standardization level, and integrity level as four measure indexes, it can provide the theoretical basis for rapid, comprehensive and accurate evaluation of vulnerability databases, and help to improve vulnerability database system, promote the development of vulnerability database technology.

3.1 Vulnerability database scale (VD) and data source independency level (SIL)

To a large extent, the number of vulnerability entries can reflect the vulnerability database's scale and how many CWE types the vulnerability database has. The independence of vulnerability data source can represent the viability of a vulnerability database. Currently, referring to each other has become a common phenomenon for vulnerability databases, the more independency the vulnerability data source has, the less data refers from other vulnerability database and the more vulnerability entries are obtained through its own way.

3.2 Vulnerability data integrity level (DI)

The more effective descriptive fields reflect more comprehensive vulnerability information, so number of effective descriptive fields can be used as an index to measure data integrity. Common fields include CVE id, vulnerabilities name, release and update time, risk level, classification, the affected version and platform, reference links, proof of concept (POC).

POC can greatly enhance the description ability, improve the efficiency of vulnerability analysis, it can attract more accession and more POC submission to form a benign circulation, improve the viability of the vulnerability database, therefore, having POC fields or not is an important standard of influence, and should be used as an index of integrity measure index.

In addition, cross-referencing data among international popular vulnerability databases has become a common phenomenon. Data source statement can improve the data integrity of vulnerability databases; therefore, data source statement should also be used as an index to measure data integrity.

3.3 Vulnerability data standardization Level (DSL)

The standardization degree of vulnerability data represents the scientific and rationality of the design of vulnerability database data structure. A more standardized vulnerability database is usually designed according to the corresponding international standard database, standardized data structures can facilitate data fusion and sharing among different vulnerability databases.

3.4 SCAP-based quantitative evaluation grading method

The vulnerability database scale (VD), data source independency level (SIL), data standardization level (DSL) and data integrity (DI) can be taken as four measure indexes of vulnerability database metric, the data of 4 indexes satisfied the normal distribution rules after statistical analysis, therefore, it can be quantified according to the normal distribution equation:

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{(x-\mu)^2}{2\sigma^2}} \tag{1}$$

where μ is the expectation, and σ is the variance, x is the specific value of measure index.

The quantitative rules of each measure index are as follows:

- **High(H).** $x \in [\mu + 2\sigma, \mu + data_{max}]$, Grade is 3, score is 3.
- **Middle(M).** $x \in [\mu - 2\sigma, \mu + 2\sigma)$, Grade is 2, score is 2.
- **Low(L).** $x \in [data_{min}, \mu - 2\sigma)$, Grade is 1, score is 1.

The overall evaluation score of the vulnerability database is calculated on the basis of the obtaining of four scores. The equation for calculating overall evaluation score is as the following equation:

$$Score_{VulnerabilityDatabase} = VDS + SIL + DSL + DI \tag{2}$$

The grading rules are as follows:

- **High(H).** Grade is 3, $Score_{VulnerabilityDatabase} \in (9, 12]$.
- **Middle(M).** Grade is 2, $Score_{VulnerabilityDatabase} \in (5, 9]$.
- **Low(L).** Grade is 1, $Score_{VulnerabilityDatabase} \in [0, 5]$.

Compared with the method of setting fixed reference value, the main advantage of this method using normal distribution rules can avoid the loss of accuracy with the development of vulnerability database technology.

4 Experiment and evaluation

This paper selected 15 international popular vulnerability databases for experiments, and obtained statistic results of vulnerability database scale, data source independence level, data standardization level, data integrity evaluation score to calculate the vulnerability database evaluation score.

4.1 The vulnerability database scale measurement results

The statistical results of the number of vulnerability entries are shown in Fig.1. Among them, OSVDB has the largest number of vulnerabilities, the databases with over 50,000 vulnerability entries includes OSVDB, x-force, CNNVD, CNVD, SecurityFocus, SCAP Chinese, NVD, NIPC, Secunia and Seebug. According to the normal distribution rules, the vulnerability database scale evaluation result is as Tab. 4.

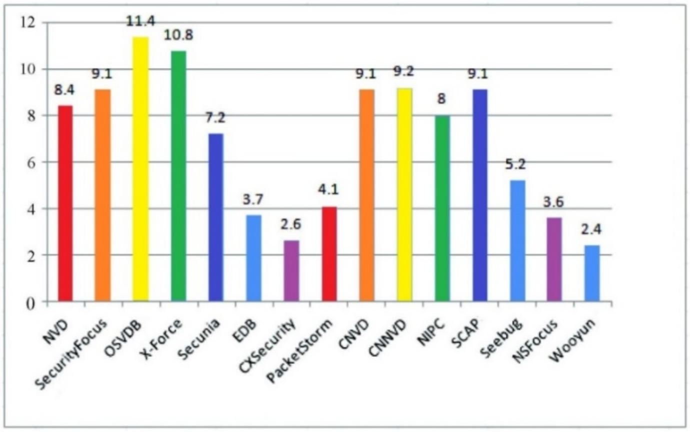

Figure 1: The number of vulnerability entries of popular vulnerability databases

Table 4: The vulnerability database scale evaluation results

Vulnerability Database	Score	Grade
OSVDB, X-Force, CNNVD	3	3
PacketStorm, CNVD, SecurityFocus, SCAP Chinese, NVD, NIPC, Secunia, Seebug, EDB	2	2
CXSecurity, NSFocus, Wooyun	1	1

4.2 The vulnerability data source independence measurement results

Statistic results of the number of popular vulnerability databases with CVE id is as shown in Fig. 2, The vulnerability data source of Wooyun, PacketStorm and Seebug have high independence level, while vulnerability entries of SCAP Chinese are referenced from other vulnerability databases. According to the normal distribution rules, the evaluation results of data source independence is shown as Tab. 5.

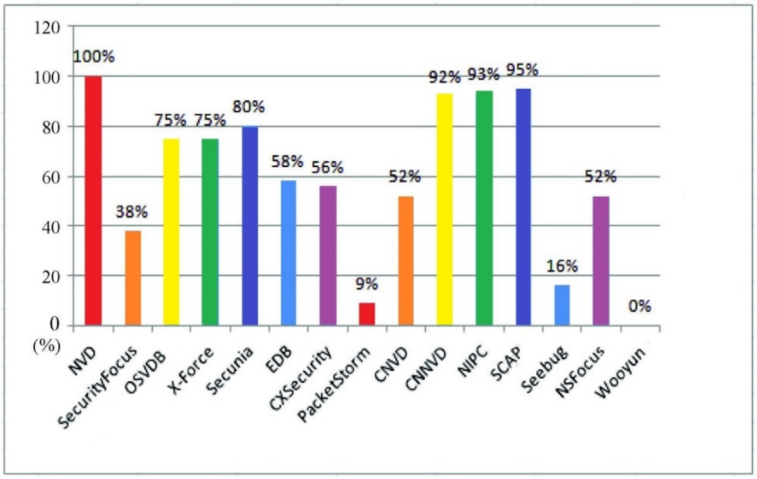

Figure 2: The number of popular vulnerability databases with CVE id

Table 5: The evaluation results of data source independence

Vulnerability Database	Score	Grade
PacketStorm, Seebug, Wooyun	1	1
CNVD, SecurityFocus, Secunia, EDB, OSVDB, X-Force, CNNVD, CXSecurity	2	2
SCAP Chinese, NIPC, NVD	3	3

4.3 Vulnerability data integrity measurement results

The statistic results of the number of fields in the popular vulnerability database are shown in Fig. 3. Most of popular vulnerability databases are more than 10 vulnerability description fields, such as NIPC, OSVDB, x-force, CNVD, Secunia, NVD, SecurityFocus, CXSecurity, NSFocus and SCAP Chinese. Only SecurityFocus, EDB, CXSecurity, PacketStorm and Seebug have POC field. At present, most of the vulnerability databases are short of copyright statement to descript the vulnerability data source. The popular vulnerability databases with copyright statement are shown in Tab. 6. The vulnerability data integrity measurement results are shown in Tab. 7.

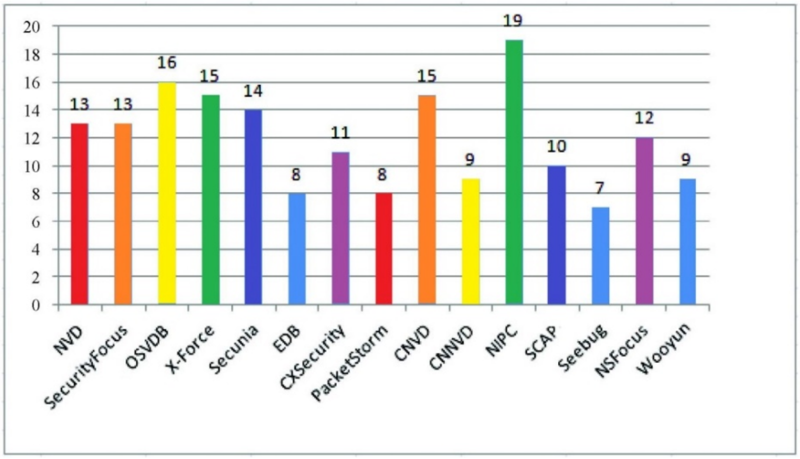

Figure 3: The number of fields of popular vulnerability databases

Table 6: Copyright statement of popular vulnerability databases

Vulnerability Database	Data Source
CNVD	Has source Url, no source vulnerability database
CNNVD	Has source Url, no source vulnerability database
SCAP Chinese	Has source Url and source vulnerability database
NSFocus	Has source Url, no source vulnerability database
Seebug	Has source Url, no source vulnerability database
Wooyun	Submit vulnerability data by Individuals

4.4 Data standardization level measurement results

The statistic results of data standardization degree of vulnerability databases are shown in Tab.7. NVD, SCAP Chinese, CNNVD and NIPC have over 90 percent in the average coverage rate of SCAP protocols, and relatively high data standardization degree. According to normal distribution rules, the data standardization degree measurement results are shown as Tab. 8.

Table 7: The evaluation results of data integrity

Vulnerability Database	Score	Grade
X-Force, CNNVD	1	1
NVD, SecurityFocus, OSVDB, x-force, CXSecurity, Secunia, CNVD, NIPC, SCAP Chinese, NSFocus	2	2
EDB, PacketStorm, Seebug	3	3

Table 8: The data standardization degree measurement results

Vulnerability Database	Score	Grade
NVD, CNNVD, SCAP Chinese	3	3
X-Force, CNVD, NIPC, SecurityFocus, OSVDB, Secunia, NIPC, NSFocus, CXSecurity	2	2
PacketStorm, Seebug, Wooyun	1	1

Table 9: Evaluation results of popular vulnerability databases

Vulnerability Database	Scale	Source independence	Integrity	Standard level	Score	Grade
OSVDB	3	2	2	2	9	2
X-Force	3	2	1	2	8	2
CNNVD	3	2	1	3	9	2
PacketStorm	2	1	3	1	7	2
CNVD	2	2	2	2	8	2
SecurityFocus	2	2	2	2	8	2
SCAP Chinese	2	3	2	3	10	3
NVD	2	3	2	3	10	3
NIPC	2	3	2	2	9	2
Secunia	2	2	2	2	8	2
Seebug	2	1	3	1	7	2
EDB	2	2	3	2	9	2
CXSecurity	1	2	2	2	7	2
NSFocus	1	2	2	2	7	2
Wooyun	1	1	2	1	5	1

The result is shown as Tab. 9, although NVD and SCAP Chinese are the vulnerability databases with highest quality, both of them need to improve scale and integrity level. Every vulnerability database has its advantages which are found in its higher scores, and the advantages can provide guidance to other vulnerability databases for improvement. Every vulnerability database has its weakness which is found in its lower score, it needs to be improved for quality elevation.

5 Conclusion

With the rapid development of information technology, network security has become a hotspot of information technology. Vulnerability technology is the foundation of network security and occupies the primary position of network security research. Vulnerability database provides a feasible mechanism for vulnerability management and is one of the most important technologies in network security research. This paper systematically summarized current popular vulnerability databases, analyzed the characteristics of the current popular vulnerability databases, systematically introduced the scale, data source independence level, standardization level and data integrity of the vulnerability database, and proposed a method for vulnerability database quantitative evaluation based on the SCAP protocol, analyzed a large number of data in current popular vulnerability databases, extracted the scale, data source independence level, standardization and integrity level of the vulnerability database as four measure indexes to quantitative evaluate vulnerability database, the experiments proved that this method can quantitative evaluate vulnerability database scientifically and comprehensively, it is helpful to improve the quality of the vulnerability database, and promote vulnerability database standardization construction.

Acknowledgement: This work is supported by the National Key R&D Program of China under Grants 2017YFB 0802300 and The National Natural Science Fund (No. 0901065614001). The authors would like to thank for Prof. Xingmin Sun, Zhaoqing Pan in Nanjing University of Information Science & Technology for recommendation, Prof. Xuejun Yang, Yuhua Tang, Huaimin Wang, Zhiping Cai in National University of Defense and Technology for tutoring.

References

1337Day (2018): 1337day. http://www.1337day.com/.

ACERT (2018): AusCert. http://www.auscert.org.au/.

Cai, Z. P.; Chen, M.; Chen, S. G.; Qiao, Y. (2015): Searching for widespread events in large networked systems by cooperative monitoring. *Proceeding of International Conference on Network Protocols*, pp. 123-133.

Cai, Z. P.; Wang, Z. J.; Zheng, K. (2018)**:** A distributed TCAM coprocessor architecture for integrated longest prefix matching, policy filtering, and content filtering. *IEEE Transactions on Computers*, vol. 62, no. 3, pp. 417-427.

CMU (2018): Software engineering institute. http://www.kb.cert.org/vuls/.

CITSEC (2018): China national vulnerability database of information security.

http://www.cnnvd.org.cn/.

Cisco (2018): Cisco security-security advisories and alerts.

https://tools.cisco.com/ security/center/publicationListing.x.

CNCERT/CC (2018): China national vulnerability database. http://www.cnvd.org.cn/.

ESVRP (2018): Education vulnerability report platform. https://src.edu-info.edu.cn/.

Flexera, S. (2018): Secunia. http://www.secunia.com/.

FreeBuf (2018): Vulnerability box. https://www.vulbox.com/.

Grance, T.; Kuhn, R.; Landau, S. (2007): Common vulnerability scoring system. *IEEE Security & Privacy*, vol. 4, no. 6, pp. 85-89.

HS (2018): Huawei security. https://www.huawei.com/cn/psirt/all-bulletins.

IBM (2018): IBM ISS X-Force. http://www-07.ibm.com/hk/gts/mss/xforce.html.

JVN (2018): JVN japan vulnerability notes. http://jvn.jp/.

Liu, Y.; Cai, Z. P.; Zhong, P. (2011): Detection approach of DDoS attacks based on conditional random fields. *Journal of Software*, vol. 22, no. 8, pp. 1897-1910.

Martin, B.; Kouns, J. (2018): Open source vulnerability database.

http://opensecurity- foundation. org/.

Mell, P.; Grance, T. (2002): Use of the common vulnerabilities and exposures (CVE) vulnerability naming scheme.

http://csrc.nist.gov/publications/nistpubs/800-51/sp800- 51.pdf.

NCNIPC (2018): National computer network intrusion protection center.

http://www. ni- pc.org.cn/.

NCVERC (2018): Common vulnerability and exposures. http://www.cve.mitre.org/.

NISTCPET (2014): Common platform enumeration. http://cpe.mitre.org/.

Nsfocus (2018): Nsfocus. http://www.nsfocus.net/index.php?act=sec_bug.

OS (2018): Offensive security's exploit database. https://www.Exploit-db .com/.

Ou, X. F.; Hu, M. Z.; Zhang, T.; Zhang, Y. Z. (2007): Study on construction and application of vulnerability database. *Application Research of Computers*, vol. 24, no. 3, pp. 213-217.

PS (2018): Packetstorm. https://packetstormsecurity.com/.

Qihoo360 (2018): Butian vulnerability response platform. https://butian.360.net/.

SCANV (2018): Wooyun. http://wooyun.jozxing.cc/.

SF (2018): SecurityFocus vulnerability database.

http://www.securityfocus.com/vulnera- bilities.

SF (2018): CXSecurity. http://cxsecurity.com/.

SL (2018): SecurityLab. http://www.securitylabs.com/.

ST (2018): Security-tracker. https://security-tracker.debian.org/.

Seebug (2018): Seebug. https://www.seebug.org/.

Tan, T. T.; Wang, B. S.; Zhou, X.; Tang, Y. (2018): The new progress in the research of binary vulnerability exploits. *Springer: Lecture Note in Computer Science*, vol. 11064, pp. 277-286.

Tan, T. T.; Wang, B. S.; Zhou, X.; Tang, Y. (2018): The new progress in the research of binary vulnerability analysis. *Springer: Lecture Note in Computer Science*, vol. 11064, pp. 265-276.

TU (2018): Common weakness enumeration. http://cwe.mitre.org/.

TU (2018): Scap Chinese. http://cve.scap.org.cn/.

US-CERTSOC (2018): National vulnerability database. http:// nvd.nist.gov/.

VVRT (2018): VUPEN. http://www.vupen.com/english/.

VT (2018): Venustech. https://www.venustech.com.cn.

Wooyun (2018): Wooyun. http://www.wooyun.org/.

Wang, A. J.; Guo, M. Z.; Wang, H.; Xia, M. (2009): Ontology-based security assessment for software products. *Proceeding of 5th Annual Workshop on Cyber Security and Information*, pp. 1-4.

Yang, G.; Wen, T.; Zhang, Y. Q. (2015): Design and implementation of android vulnerability database. *Netinfo Security*, vol. 9, pp. 240-244.

Yang, W. J.; Dong, P. P.; Tang, W. S.; Lou, X. P.; Zhou, H. J. et al. (2018): A MPTCP scheduler for web transfer. *Computers, Materials & Continua*, vol. 57, no. 2, pp. 205-222.

ZeroDay (2018): ZeroDay. https://www.zerodayinitiative.com/.

Zhang, Y. Q.; Wu, S. P.; Liu, Q. X.; Liang, F. F. (2011): Design and implementation of national security vulnerability database. *Journal of Communications*, vol. 32, no. 6, pp. 93-100.