Academia Journal of Scientific Research 8(5): 186-192, May 2020
DOI: 10.15413/ajsr.2020.0401
ISSN 2315-7712

Research Paper

Risk assessment model of cross site script vulnerability based on detection

Accepted 6th March, 2020

ABSTRACT

It has become necessary in recent years to study the security of different levels of interaction on network due to the increasing importance of network in all walks of life, in order to ensure the security of network applications and users. Cross site scripting vulnerabilities are common in web applications with frequent user interaction, which affect application security and user data security. In this study, the principle of cross site script vulnerability is evaluated, and the detection part of the model is designed based on the dynamic black box model. On the basis of the detection, the existing fuzzy comprehensive evaluation model is improved according to the dynamic detection results. The evaluation index system is established by selecting the evaluation index through AHP (Analytic hierarchy process), and the quantitative assessment model of cross-site scripting vulnerability risk for web applications is created. Through the experiment and comparison with the existing classical evaluation model and the evaluation results in related references, the effectiveness of the evaluation model is proved. The results show that the detection-based evaluation model designed in this study can measure the security of cross-site scripting vulnerabilities in Web applications.

Xiaolin Zhao, Yaoyuan Liang, Xinyu Hou, Jingfeng Xue*, Mingzhe Pei and Hui Peng

Beijing Institute of Technology, Beijing 100081, China.

*Corresponding author. E-mail: xuejf@bit.edu.cn or zhaoxl@bit.edu.cn.

Key words: Cross site script vulnerability, dynamic black box detection, fuzzy comprehensive evaluation, AHP.

Abbreviations: AHP, Analytic hierarchy process; **NVD,** National Vulnerability Database; **D-S,** Dempster/Shafer; **URL,** Uniform Resource Location; **CVSS,** Common Vulnerability Scoring System; **CVE,** Common Vulnerabilities and Exposures.

INTRODUCTION

Since the beginning of the 21st century, cross site scripting attacks are very common in all kinds of web applications (Germán et al., 2020). By injecting malicious code into the client, the attacker injects the attack load into the vulnerable web applications to achieve different kinds of cross site scripting attacks. Figure 1 shows the statistics of the number of vulnerabilities included in NVD from 1999 to the end of 2018. Cross site scripting vulnerabilities account for 12.3% of the total (Upasana et al., 2018).

Therefore, it is necessary to determine the cross site script vulnerabilities in time and prevent the cross site script attacks. According to the literatures on vulnerability assessment in recent years, there are three typical assessment methods: qualitative rating method, quantitative scoring method and the combination of the two methods (Liu et al., 2012). Through the design of detection and evaluation model, this study realizes the quantitative risk assessment of cross site script vulnerabilities in web applications. Comparison with the existing evaluation methods shows that the model is more real-time and can be evaluated in real time based on detection. Moreover, the combination of fuzzy evaluation method makes the scoring more objective (Zhonglin, 2019), and this provides a reference for improving the corresponding security protection.

RELATED RESEARCH

Vulnerability hazard assessment involves using relevant

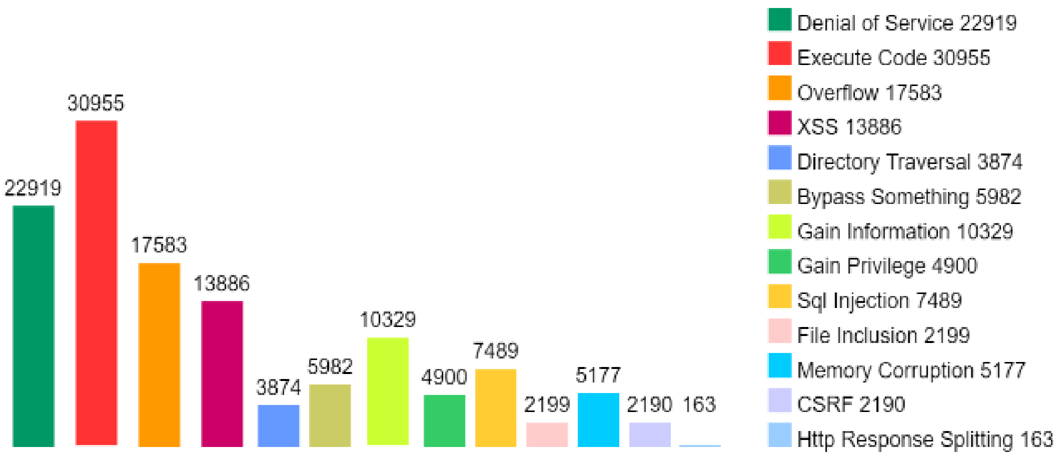

Figure 1: Statistics of NVD vulnerabilities.

Table 1: Comparison of common vulnerability assessment models.

Vulnerability assessment method	Theoretical basis	Input	Output	Advantages	Disadvantages
Evaluation method based on AHP (Wang et al., 2018)	Based on mathematical model	Many factors affecting the harm of loopholes	Damage degree	Achieve comprehensive assessment of indicators	The model is not detailed enough and lacks pertinence
Evaluation method based on attack graph model (Cui et al., 2019)	Based on Knowledge reasoning	Vulnerability data and attack data	Vulnerability hazard score	Be able to describe the attack path	It is difficult to establish and calculate attack graph
Evaluation method based on D-S evidence theory (Yu et al., 2018)	Based on Knowledge reasoning	Network and host scan data	Safety score	Comprehensive time and other parameters	Small available range
Vulnerability assessment model based on risk matrix (Ren et al., 2018)	Based on mathematical model	Vulnerability data	Vulnerability utilization	Be able to consider the relationship between vulnerabilities	Data acquisition and calculation are difficult
Evaluation method based on fuzzy comprehensive evaluation (De Alvare, 2015)	Based on mathematical model	Fuzzy evaluation index	Vulnerability score	The difficulty of calculation is moderate, and comprehensive calculation can be realized	Based on expert experience

assessment technology to get the level and score of vulnerability threat (Song, 2018). According to different forms of evaluation results, it can be divided into qualitative evaluation and quantitative evaluation methods. According to the theoretical basis of evaluation, it can be divided into the evaluation method based on mathematical model and the evaluation method based on knowledge reasoning.

Table 1 shows the comparison of common vulnerability assessment models. Due to lack of pertinence and objectivity caused by the existing evaluation methods, the present study improves the above problem, establishes a detection-based evaluation model for cross-site scripting vulnerabilities, applies the fuzzy comprehensive evaluation method to the hierarchical model, refines and improves the detection object and evaluation method, and make evaluation methods more feasible and available.

DESIGN OF CROSS SITE SCRIPT RISK ASSESSMENT MODEL BASED ON VULNERABILITY DETECTION

Overview of cross site script risk assessment model based on vulnerability detection

To make the model more real-time, the overall design of cross site script evaluation model based on vulnerability detection is carried out. This model is divided into two parts: Web application vulnerability detection and cross site script vulnerability risk assessment.

Based on the dynamic black box vulnerability detection

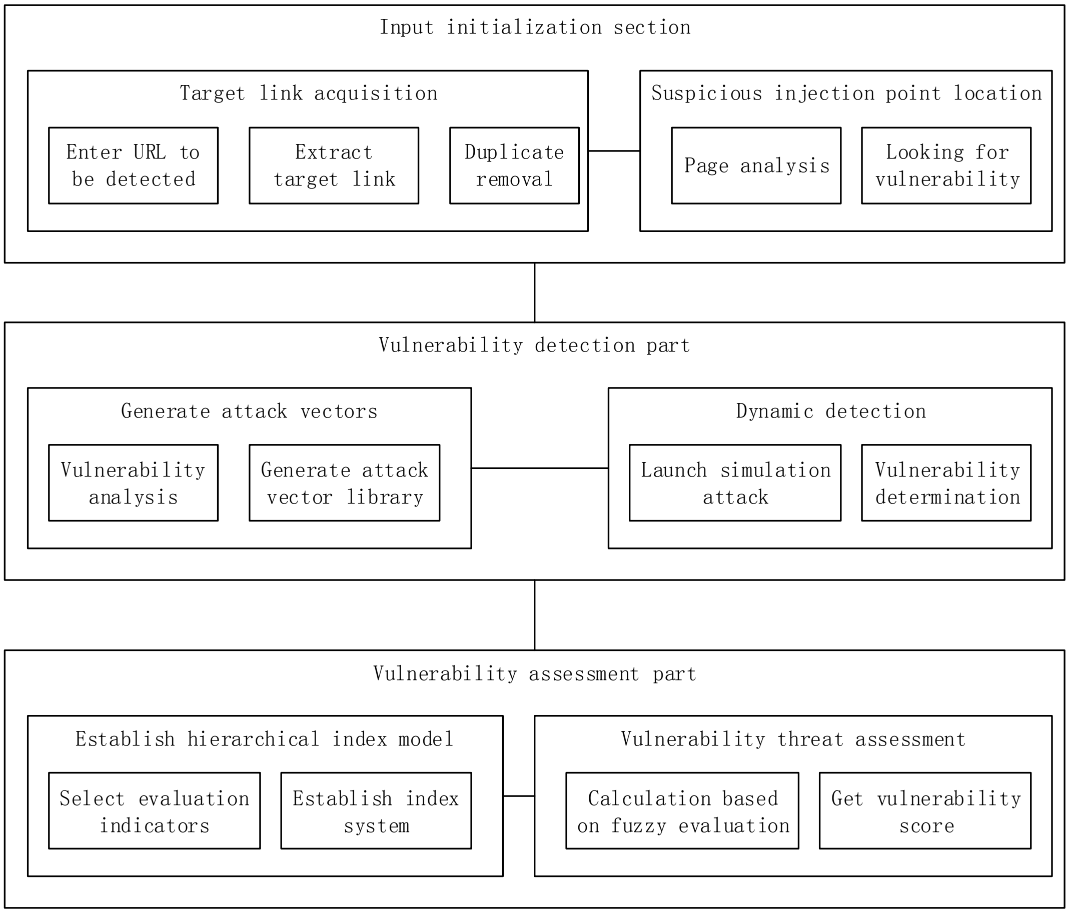
Input initialization section
Target link acquisition
Enter URL to be detected
Extract target link
Duplicate removal
Suspicious injection point location
Page analysis
Looking for vulnerability
Vulnerability detection part
Generate attack vectors
Vulnerability analysis
Generate attack vector library
Dynamic detection
Launch simulation attack
Vulnerability determination
Vulnerability assessment part
Establish hierarchical index model
Select evaluation indicators
Establish index system
Vulnerability threat assessment
Calculation based on fuzzy evaluation
Get vulnerability score

Figure 2: overall architecture of cross site script risk assessment model based on vulnerability detection.

method (Deepa et al., 2018), the present study refines the detection scheme, designs and realizes the cross site script vulnerability detection, and then improves the calculation method of the hierarchical evaluation model. On the basis of the original matrix calculation, the fuzzy comprehensive evaluation method is applied to the calculation of the weight vector to improve the calculation method of the vulnerability index system. The specific steps are: (1) detection target analysis, (2) Conduct a simulated attack, (3) Cross site script vulnerability determination, and (4) Vulnerability quantitative assessment.

Figure 2 shows the overall architecture of this model.

Design of cross site script vulnerability detection

The cross site script vulnerability detection in this study is based on the dynamic black box vulnerability detection method (Zhang et al., 2019). The detailed steps are as follows:

1). Detection target analysis: First of all, we need to obtain the basic URL of the target web program to provide the address for the subsequent simulation attacks. Then, the black box test case is designed as the attack vector through the attack principle and characteristics, and the vulnerability determination method is set.

2). Conduct a simulated attack: The set attack vector is selected, and the attack request is generate by combining with the basic URL obtained in the target analysis stage. The selection and deformation of attack vector is the key point of simulation attack.

3).Cross site script vulnerability determination: Regular matching method is used to analyze the response results. Through the analysis of the response page content returned by the server, we can verify whether or not there is characteristic value of the injected attack vector, and need to record the attack vector that successfully attacks, vulnerability type, attack times, target link URL and so on. To ensure the balance between the efficiency of the detection model and the accuracy of detection, it is necessary to set the maximum number of simulated attacks. If the threshold value is exceeded, it is determined that there is no cross site script vulnerability.

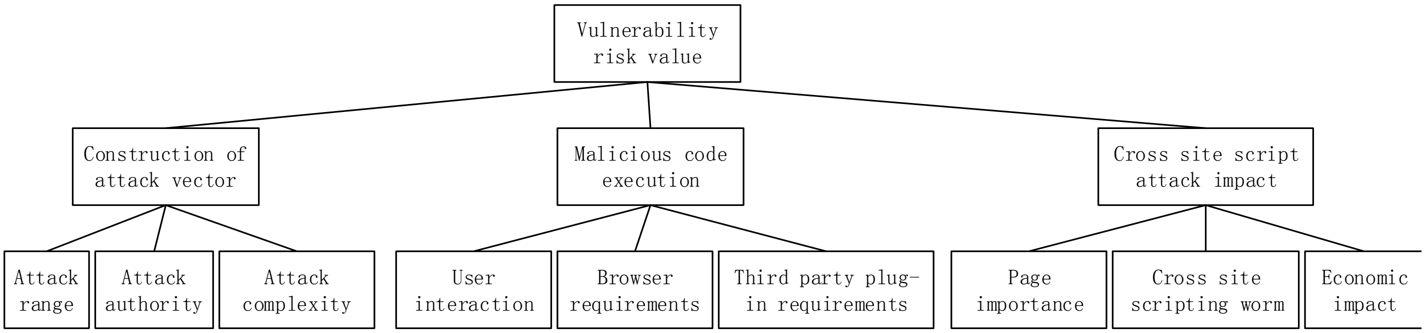

Figure 3: Hierarchical cross site script vulnerability quantitative index system.

Establishing the hierarchical index system of vulnerability assessment

The model in this study refers to the existing rules of vulnerability evaluation index selection, and redesigns the evaluation index system (Ju et al., 2019). The hierarchical model as shown in Figure 3 is established.

After that, by reading the official CVSS3.0 document (2001) and referring to the index scoring method, this study designs the scoring method for the above index system as shown in Table 2.

Design of vulnerability evaluation rules based on fuzzy evaluation

The evaluation model designed in this study improves the traditional evaluation model based on fuzzy information fusion, and designs a new quantitative evaluation model combined with the vulnerability detection results in the previous chapter.

First, you need to make sure that the elements of the target set are U={u_1,u_2,...u_n},u_i is the i-th non lowest index in the quantitative evaluation index system, then its value is determined by the corresponding index of the next layer .

Then the elements of the evaluation set are confirmed. Evaluation set can be expressed as V={v_1,v_2,...v_m}, representing m possible results. To facilitate comparison, this study follows the commonly used vulnerability classification method, and divides the evaluation set into V = { v_1, v_2, v_3, v_4} = {critical, high risk, medium risk, low risk} (Li, 2016). The corresponding numerical vector V = { 0,4.5,7.5,10}.

In the process of quantitative evaluation, a discriminant matrix C is constructed by comparing n indexes of the layer in pairs. The value here depends on the expert experience to give the estimated value. To ensure the consistency as much as possible and make the calculation based on a more objective basis, a rule of value based on relative importance is generally stipulated, and the qualitative index description is quantified. The quantized index matrix is shown in Formula 1:

$$C = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1m} \\ c_{21} & c_{22} & \cdots & c_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ c_{n1} & c_{n2} & \cdots & c_{nm} \end{bmatrix} \qquad (1)$$

Each element in matrix C is determined by comparison between two; so, the values of c_{ij} and c_{ji} in the matrix are mutually inverse, they are used to express the relative importance between indicator element i and indicator element j. The quantitative methods of qualitative indicators are shown in Table 3.

The weight matrix of the three dimension layers of the attack process relative to the vulnerability risk assessment layer is shown in matrix A:

$$A{=}\begin{bmatrix} 1 & 1/1.618 & 1/2.618 \\ 1.618 & 1 & 1/1.618 \\ 2.618 & 1.618 & 1 \end{bmatrix} \qquad (2)$$

The weight matrix of index layer relative to three dimension layers of attack process is B1, B2 and B3 respectively.

$$B1 = \begin{bmatrix} 1 & 1/2.618 & 1/4.618 \\ 2.618 & 1 & 1/1.618 \\ 4.618 & 1.618 & 1 \end{bmatrix} \qquad (3)$$

$$B2 = \begin{bmatrix} 1 & 1.618 & 2.618 \\ 1/1.618 & 1 & 1.618 \\ 1/2.618 & 1/1.618 & 1 \end{bmatrix} \qquad (4)$$

$$B3 = \begin{bmatrix} 1 & 2.618 & 1/1.618 \\ 1/2.618 & 1 & 1/4.618 \\ 1.618 & 4.618 & 1 \end{bmatrix} \qquad (5)$$

All the above matrices have passed the consistency test.

For each decision matrix in the hierarchical model, since the matrix is a positive matrix, the eigenvalues and eigenvectors are calculated as weights. According to this method, the weight vector of each layer relative to the target layer is calculated. The specific method is: it is known that the weight vector of the K-1st layer relative to the target layer is W^{k-1}=$(w_1^{k-1}, w_2^{k-1}, \ldots, w_x^{k-1})^T$, the weight vector of the k-th layer with respect to an element i in the k-1 layer is Z_i= $(w_{1i}^k, w_{2i}^k, \ldots, w_{yi}^k)^T$, according to the above

Table 2: Scoring method of index system.

Index elements	Measure value	Score value
Attack range	Remote / adjacent network / local / physical	0.85/0.62/0.55/0.2
Attack authority	No requirement / low right / high right	0.85/0.62/0.27
Attack complexity	Low / high	0.77/0.44
User interaction	No interaction / interaction	0.85/0.62
Browser requirements	No requirement / requirement	0.85/0.62
Third party plug-in requirements	No requirement / requirement	0.85/0.62
Page importance	High / low / no	0.85/0.62/0
Cross site scripting worm	Yes / no	0.85/0
Economic impact	High / low / no	0.85/0.62/0

Table 3: Quantitative results of vulnerability assessment indicators.

Scale of indicators	Meaning of quantitative results
1	Two indicators have the same importance
1.618	The weight of the previous index is slightly larger
2.618	The weight of the former index is significantly greater than that of the latter
4.618	There is a big gap between the weight of the former index and the latter one
Reciprocal	Describe the weight of the latter indicator relative to the former

weight vector, the weight of the k-th layer relative to the target layer can be calculated using Formula 6:

$$W^{k^T}=(Z_1,\ Z_2,Z_3,\dots,\ Z_{nk})*W^{k-1} \quad (6)$$

According to the weight matrix A, B1, B2 and B3, the total weight vector can be calculated comprehensively as W=(0.023,0.063,0,105,0.155,0.096,0.059,0.164,0.061,0.27).

Then, the quantitative mapping between objective set and evaluation set is established by fuzzy membership function. This function can be graphically shown in Figure 4.

Given the combination of evaluation sets, the final evaluation grade vector can be calculated by quantifying the hazard grade index into the (0, 10) quantification domain and inputting the membership function.

To facilitate the calculation, it is necessary to establish a fuzzy evaluation matrix. The basic score vector of each attribute of the indicator layer r_i(i =1, 2,..., n) bring in the hierarchical membership function f_j(j =1,2,..., n). The combination of all fuzzy membership degrees, such as matrix R, is the fuzzy evaluation matrix:

$$R=\begin{bmatrix} f_1(r_1) & f_2(r_1) & \cdots & f_n(r_1) \\ \vdots & & \ddots & \vdots \\ f_1(r_m) & f_2(r_m) & \cdots & f_n(r_m) \end{bmatrix} \quad (7)$$

Finally, the score of vulnerability hazard level can be obtained using Formula 8. Where vector V1 is the transpose of evaluation vector V. In this way, the calculated score s will be used as the corresponding cross site script vulnerability security risk reference value:

$$S = W * R * V1 \quad (8)$$

EXPERIMENTAL DESIGN AND RESULT ANALYSIS

Cross site script vulnerability detection experiment

In this experiment, different types of cross site scripting vulnerabilities are selected for experiments. Here, only the reflection cross site scripting vulnerabilities are described in detail. In this study, attack vectors are selected to verify the detected vulnerabilities. By analyzing the detection results and collecting the information of the detected vulnerabilities, the basic information of the vulnerabilities is summarized as shown in Table 4.

Quantitative risk assessment

On the basis of vulnerability detection, according to the risk assessment model designed above, the following assessment experiments are carried out for the detected cross site script vulnerabilities.

It is known that four security levels can be quantified as evaluation set vector V=(0.0, 4.5, 7.5, 10.0, the vulnerability index quantitative score R = (8.5, 8.5, 7.7, 8.5, 6.2, 6.2, 8.5, 0, 8.5) is brought into the fuzzy membership function, according to this function, fuzzy membership

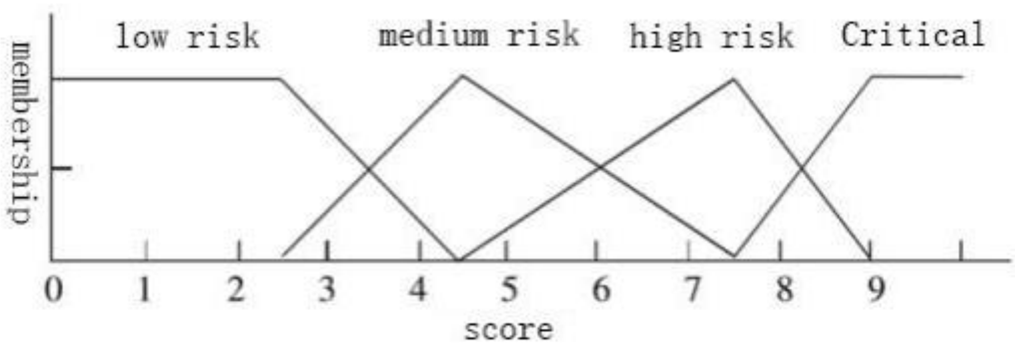

Figure 4: Hazard level membership function diagram.

Table 4: Summary of basic information of reflection cross site scripting vulnerability assessment.

Vulnerability information type	Detection result
Vulnerability type	Reflection cross site scripting vulnerability
Vulnerabilitydescription	Due to the lack of input validation for the name variable
Vulnerability page link	http://192.168.112.130/xss/example1.php?name=hacker
Number of simulated attacks	2
Is it a cross site scripting worm	no
Attack vectors used	http://192.168.112.130/xss/example1.php?name=%3Cscript%3Ealert(%27xss%27)%3C/script%3E

Table 5: Comparison between experimental results and CVSS evaluation model.

Vulnerability description	CVE number	Rating in NVD database	Evaluation results of this model
Code execution bypass	CVE-2017-15714	7.5	7.892
Reflection cross site scripting Vulnerability	CVE-2012-1886	8.3	8.014
CSRF cross site scripting Vulnerability	CVE-2017-17550	6.8	7.233
Injection of triggered cross site Script vulnerability	CVE-2010-1246	3.9	3.5

matrix A can be obtained. Each row of the matrix represents a vulnerability index attribute, and each column of the matrix represents the membership degree of the attribute to the corresponding evaluation level. So the sum of the elements in each row is 1:

$$A=\begin{bmatrix} 0 & 0 & 0.33 & 0.67 \\ 0 & 0 & 0.33 & 0.67 \\ 0 & 0 & 0.87 & 0.13 \\ 0 & 0 & 0.33 & 0.67 \\ 0 & 0.43 & 0.57 & 0 \\ 0 & 0.43 & 0.57 & 0 \\ 0 & 0 & 0.33 & 0.67 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0.33 & 0.67 \end{bmatrix}$$

Finally, the product of index weight vector and fuzzy membership matrix is calculated:

Rank=(0.061,0.06665,0.40377,0.46858).

So the measurement score of vulnerability $S=Rank*V^T=8.014$.

According to the above calculation, the comprehensive score for the detected vulnerability in Table 4 is 8.014, and the vulnerability rating is high risk.

Analysis of experimental results

Through the evaluation of multiple cross site script vulnerabilities, and comparison with the evaluation results of the existing classic evaluation model, the effectiveness of the evaluation model is proved. The comparison with the evaluation results of CVSS evaluation model is shown in Table 5.

As can be seen from the table, the assessment model in this study is in line with the vulnerability rating of the classic CVSS assessment, indicating the effectiveness of the vulnerability assessment model in this study, and as compared with other assessment models, it is more real-time and objective, greatly reducing human intervention.

CONCLUSION

To solve the problem that the common cross site script vulnerability evaluation model is not real-time and needs to be scored manually, the present study designs a quantitative evaluation model based on detection. In the detection part of the model, the existing vulnerability detection model based on dynamic black box is improved, and the potential cross site script vulnerabilities are detected by means of simulation attack and analysis of feedback. In the evaluation part of the model, the fuzzy comprehensive evaluation theory is applied to the mathematical mapping between the evaluation index and the security evaluation which have no obvious logical relationship. The fuzzy evaluation matrix is generated by the fuzzy membership function to realize the quantitative evaluation of the loopholes.

The evaluation model in this study can evaluate the detected vulnerabilities in real time. As compared with traditional evaluation models such as CVSS, it has strong objectivity and timeliness, greatly reducing human intervention, and can be evaluated based on detection in real time without sufficient vulnerability library support. In the future, more vulnerability types can be studied to improve the evaluation model.

ACKNOWLEDGEMENTS

This work was supported by the National Key Research and Development Program of China under Grant 2016QY06X1205. The authors are grateful to the CVE's open vulnerability information and CVSS's open vulnerability assessment methods.

REFERENCES

Common Vulnerability Scoring System v3.0: Specification Document[EB/OL].https://www.first.org/cvss/v3.0/specification-document,2001.02.19.

Cui Y, Li J, Zhao W, Luan C (2019). Research on Network Security Quantitative Model Based on Probabilistic Attack Graph[J]. ITM Web of Conferences, 2019, 24.

De Alvare AM (2015). Fuzzy logic as an instrument to perform security analysis[D]. ProQuest Dissertations & Theses Colorado Technical University, USA, 129, 2015.

Deepa G, Thilagam PS, Khan FA, Praseed A, Pais AR, Palsetia N (2018). Black-box detection of XQuery injection and parameter tampering vulnerabilities in web applications.[j].Int. J. Information Secur. 17(2): 105-120.

Germán ER, Jenny GT, Pamela F, Diego EB (2020). Cross-site scripting (XSS) attacks and mitigation: A survey[J]. Computer Networks, p. 166.

Ju T, Tian G, Yang J (2019). Analysis of cross-site scripting attack vulnerability based on Web system [J]. Netw. Secur. Technol. Appl. 11: 27-28.

Li LH (2016). Introduction to related standards of information security vulnerabilities [J]. China Inf. Secur. 7: 68-72.

Liu Q-X, Zhang C-B, Zhang Y-Q, Zhang B-F (2019). Research on key technology of security vulnerability classification [J]. J. Commun. S1: 79-87.

Ren X, Chen J, Li C, Yang Y (2018). Vulnerability correlation hazard assessment of Internet of things system based on risk matrix [J]. Inf. Netw. Security, 11: 81-88.

Song J (2018). Research on Classification and Evaluation Technology of Information Security Vulnerability [D] .Strategy Support Army Information Engineering University, 2018.

Upasana S, Bhattacharyya DK, Kalita JK (2018). A survey of detection methods for XSS attacks[J]. J. Netw. Comput. Appl. 118: 113-143.

Wang H, Chen Z, Feng X, Di X (2018). Research on Network Security Situation Assessment and Quantification Method Based on Analytic Hierarchy Process[J]. Wireless Personal Communications, 2018.

Yu J, Hu M, Wang P (2018). Evaluation and reliability analysis of network security risk factors based on D- S evidence theory[J]. J. Intelligent Fuzzy Syst. 34(2): 861- 869.

Zhang H, Xiang C, Chen Haitao, Li Li, Wang N (2019). Application of computer network security and vulnerability scanning technology [J]. Electron. Compon. Inf. Technol. 3(09): 35-37.

Zhonglin C (2019). An indirect variable weights method to compute fuzzy comprehensive evaluation values[J]. Soft Comput. 23(23).

Cite this article as:

Zhao X, Liang Y, Hou X, Xue X, Pei M, Peng H (2020). Risk assessment model of cross site script vulnerability based on detection. Acad. J. Sci. Res. 8(5): 186-192.

Submit your manuscript at
http://www.academiapublishing.org/ajsr