

Information Security Measures in PHP Website Design

Xu Zhiyong

Nanchang Institute of Science & Technology, Nanchang, China

Keywords: PHP, Website design, Information security, Defense measures

Abstract: As dynamic languages, PHP and ASP use wamp technology to integrate server, database and PHP, playing a significant role in optimizing website design. In website design, China is still in the preliminary stage. So improvement and reform are needed in website design and practical application. Despite advantages in practical application of PHP website design, there are still some problems, which has greatly affected the information security of PHP website design. The paper, starting from information security defense of PHP website design, analyzes existing problems and proposes targeted measures. It is aimed to strengthen information security defense of websites to achieve goals of PHP website design, providing reference for information security defense in PHP website design.

1. Introduction

In the Internet era, network has spread into all walks of life including both nation and individuals. The bold and resolute advent of network has brought radical changes in people's way of life as well as more convenient internet life, greatly improving people's life quality. Since personal information is exposed to network environment, how to ensure information safety in particularly important. Therefore, in the constant development of internet technology, PHP website design is born at the right moment, whose optimized website design manner has played a vital role in improving reliability and safety of websites. However, it cannot be denied that information security problems still exist in PHP website design. Specifically, in recent years, website establishment of China has become more and more common. The issue of the first national network security law has demonstrated the importance of internet information security as well as importance of national information security. Based on such reasons, how to effectively defend information security in PHP website design has become an issue to be settled urgently.

2. The importance of information security defense in PHP website design

As dynamic languages, PHP and ASP utilize wamp technology to integrate server and database, which plays an important role in website design optimization. The limited advantages of PHP website design in practical application have exerted positive impact on reliability and safety of websites. Specifically, the rise of network technology in recent years and the advent of network era have greatly transformed people's way of life. Since network spreads all walks of life, individuals and nations have relied heavily on network. The network overcame national boundaries and geographic restrictions, playing an irreplaceable part in promoting integration of world economy. Its wide application in life has hugely enhanced life quality. Under the network era, personal and national information has exposed to network. Once network collapses, information security is easily endangered and national information security even more. It can be seen from the first national network security law in China the importance of national information security as well as attention to website information security paid by the nation. Based on that, how to complete effective information security defense in PHP website design has become an issue demanding prompt solution. Strengthening information security defense in PHP website design from all aspects can effectively avoid impact of adverse factors on website information safety, promote safe and stable operation of websites, reaching important goals of PHP website design and promotion in the real sense.

3. Analysis of problems of information security defense in current PHP website design

Based on the nature of PHP website design, it has limited strengths in practical application. Utilizing wamp technology, it integrates server, database and PHP, playing a crucial part in website design optimization. Against network era, in order to actively promote optimization and reform of website design, China has to take existing problems of information security defense in current website design into account, know well about superiority of PHP website design, compare PHP website and other design methods to identify shortcomings and problems in PHP website design and practical application. According to PHP website design and its application in reality, the problems of information security defense in PHP website design can be stated as follow:

3.1 Invasion of structured language

Programmers often preset a piece of codes in website development program as a measurement of validity of data typed by other users, providing full guarantee for information security. However, in light of PHP website design and application, forgetting preset codes in design will lead some illegal users to inquire database by means of this loophole, control background according to codes responded by database and embezzle or temper user information, posing severe threats on information security in website design. Though setting of structured language exerts little effect on website running, its loophole will bring serious threats to websites, endangering information security defense of websites. When comes to common applied structured languages in present stage, SQL occupies a major part (figure 1). Proper application of SQL in PHP website design can offer security of information safety in some degree. But how to integrate these two objects and ensure structured language invasion codes to be given full play has become an issue demanding prompt solution in PHP website design at present.

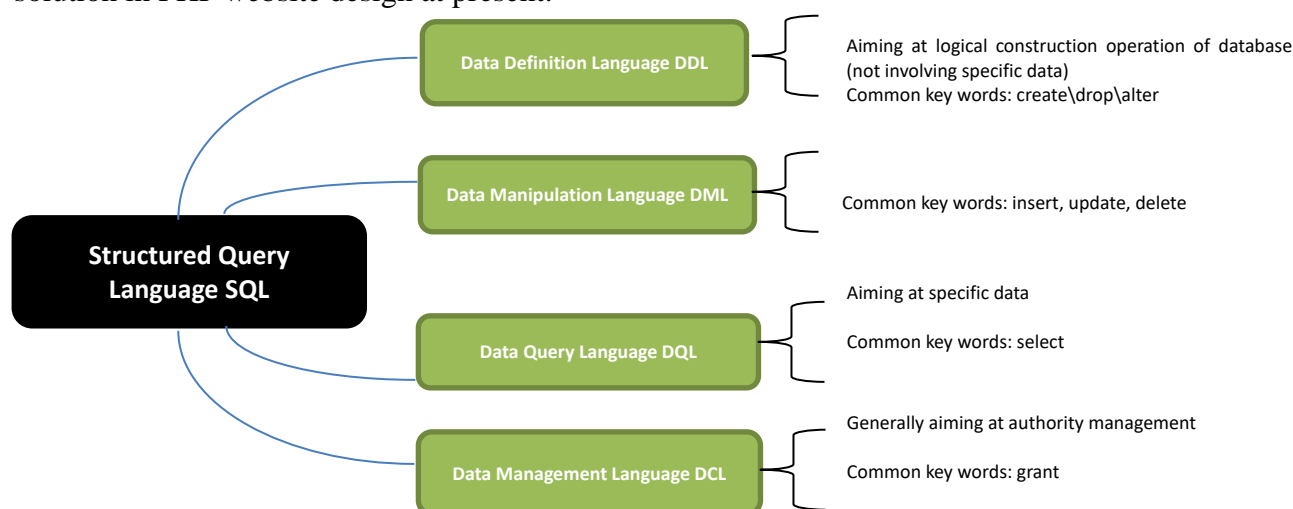


Figure 1 function diagram of structured query language

3.2 Use of program statement

Program statement has something in common with structured language, which pose huge threat on information security on websites. The specific form of program statement is “or1=1”, being widely applied in website information security attack. Its concrete statement structure is shown in figure 2. While application statement can make illegal attackers skip password authentication when logging website system. In most cases, relevant login password is set in supervising website information security. Only when administrators pass password authentication can information be accessed by users. However, in some cases, such program statement means direct skipping over password authentication to access information, posing serious threats on user information security. This situation is common in information security management, therefore, how to prevent damage of information security brought by program statement has become an issue worth consideration and study. The reason for program statement directly attacking information security defense lies in that,

it utilizes character strings without verification in computer program of website designers. Attackers take it as an attack point to easily break through the supervision of website information security and access information illegally.

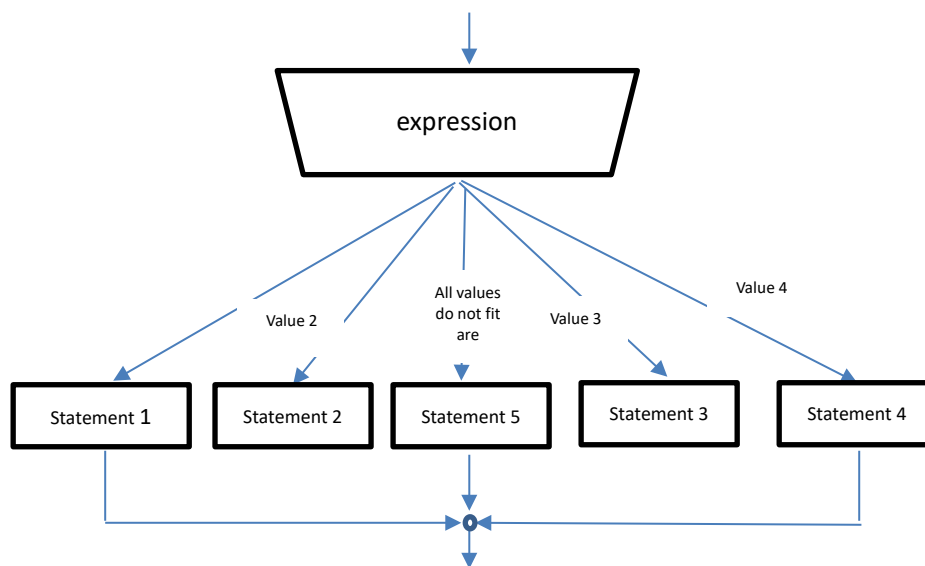


Figure 2 program flow chart

3.3 XSS (Cross-site Script Execution)

XSS is short of Cross Site Script Execution, whose fundamental principle is that attackers utilized designed website program to start from insufficient user filtering and break through the information security defense system, directly invading systems and information security of other users. Such behavior usually appears in maliciously embezzlement of user information and website attacking, whose wide coverage seriously effects the website information security. In website information browsing, small-page pop-up windows in web pages (figure 3) actually means that attackers make users be infected Trojan virus in looking through websites by use of cross-site script execution program, thus, causing paralysis of user information security supervision system eventually, exerting adverse impact on website information safety.

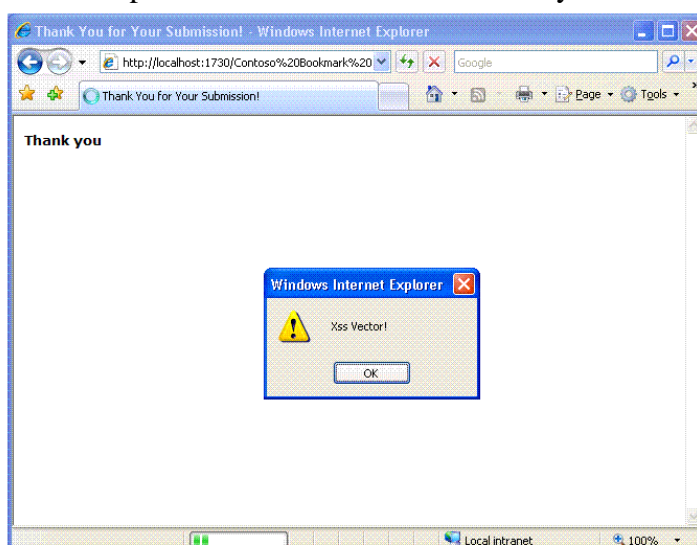


Figure 3

In a word, it is an urgent issue for strengthening information security defense in PHP website design. Whether invasion of structured languages or program statement and cross-site attacks, they will lead to adverse effect on website information security. On the current network context, personal

and national information is exposed to network systems. As long as system is attacked or invaded maliciously, information leakage will take place, having a negative impact. Thus, how to achieve efficient information security defense in PHP website design is associated with its key goals.

4. Effective measures in information security defense of PHP website design

Information security defense of PHP website design is linked with information safety of users as well as website normal operation and important goals of PHP websites. Nonetheless, given the current information security defense in PHP website design, there are many problems. Invasion of structured language, program statement and cross-site attack will pose threats on information security of websites. Based on superiority of PHP website design and promotion, wamp technology integrates server, database and PHP, playing a vital part in website design optimization. Therefore, strengthening information security defense in PHP website design is an urgent issue. In order to solve this problem, it is evitable to start from the root.

4.1 Inform users of information security defense measures

Information security measures should be informed to users when they use websites. The main reason is the vital role of user engagement in website information security supervision. If users guide their behaviors in accordance with relevant requirements, they can avoid malicious invasion in some extent. For instance, the pop-up windows in browsing websites is actually a cross-site script execution program. If users click on the pop-up windows, their information will be spied maliciously. The basic principle of cross-site script execution is that attackers utilize insufficient user filtering in the designed website program as an entry point, breaking through information safety defense system of websites and directly invading systems and threatening information security of other users. Based on such phenomenon, in the management of PHP website information, it is necessary to inform users of information security defense methods and follow users' data in a legal manner at the same time. The main reason is that network technology has exerted huge impact on people's lifestyle, and the rapid development of network technology has accelerated the progress of human society.

More and more user information is exposed to the network as more and more people have become members of network family. To prevent damages of information, user data should be timely followed legally in the using process. However, designers and developers without rich experience are difficult to follow dynamic data effectively given the present website design. Thus, operating principle of WEB is needed and data following capacity is to be strengthened so as to strengthen information security management in PHP website design. What's more, filtering of user input information should be enhanced for attackers can user any user name to invade website data system in the real life. In conclusion, normalizing user information security should be solved from the root.

4.2 Strengthening information security defense in website design

In terms of information security defense in PHP website design, there are numerous problems in this respect. Structured language, program statement or cross-site script execution will have negative effect on information safety of websites. Therefore, adverse factors should be dealt with respectively to strengthen information security defense in website design. For example, major designers must reserve structured language codes in website design to prevent attackers from utilizing invasion of structured language to invade websites. As for defense in cross-site script execution, it is necessary to begin with arousing the enthusiasm of user information management, informing users of relevant measures. In the practical defense and supervision, information security behavior should be normalized to strengthen information security defense in PHP website design in the real life.

5. Conclusion

Above all, the rapid development of network technique has brought drastic changes for people's

way of life. More convenient network life has greatly enhanced living standards. However, due to the exposure of personal information in network environment, how to guarantee information safety has become more and more important. Therefore, PHP website design emerges as the times require, whose optimized website design method plays a crucial role in reliability and safety enhancement. It is undeniable that information safety problems still exist in PHP website design. And the effective defense of information safety in PHP website design concerns the normal operation of PHP websites.

References

- [1] Ma Shuang. A brief analysis of information safety defense strategy in PHP website design [J]. Heilongjiang Science, 2015, (16):29-29, 43.
- [2] Li Caiyun. Discussion on messy codes in photos in uploading Chinses filename in PHP+MySQL website. [J]. Fujian quality management, 2017, (13):235.
- [3] Wang Fang. User management system development based on PHP & Apache & MySQL [J]. Digital technology and application, 2014, (3):162-162.
- [4] Li Changqi, Wang Han, Wang Zonglian, et al. Research on development of musical websites in universities based on PHP—taking website of conservatory of music of Baoshan University as an example.[J]. Shangqing, 2017, (29):273-276.
- [5] Yao Shengyuan. Young volunteer website construction based on PHP+Mysql—taking young volunteer website of school of computing in Sichuan University as an example [J]. Computer CD Software and Applications, 2014, (11):104-104,106.
- [6] Zhai Wenjia. Website construction of party school based on PHP technique—taking municipal party school of Chaoyang city as an example [J]. Computer CD Software and Applications, 2013, (17):302-303.
- [7] Rao Ruyan. School website construction based on PHP technique—taking a department website of Xiamen Ocean Vocational College as an example [J]. Journal of Zhangzhou Institute of Technology, 2010, 12 (4):10-14.
- [8] Li Ying, Ganlin. Discussion on risk aversion like information leakage and tampering of campus website [J]. Computer Knowledge and Technology, 2015, (13):45-46.
- [9] Finland—A high-end natural science seek & Chinese website/organization dynamic simulation application in engineering design/Czech information security and secrecy system project looking for Chinese partners [J]. Computer and telecommunication, 2010, (4): 23.
- [10] Li Jun. High attention payed to file and electronic file registration as the public key to government information security given Frequent hacker attacks on government websites [J]. Zhejiang archives,2011, (5):11-12.
- [11] Zhang Lixin, Zhou Xiuxia, Xu Liang, et al. Construction of university information security policy system based on risk control -- based on the practical analysis of 8 universities in the United States [J]. Modern intelligence,2016, 36(10):102-106.
- [12] Chen Yu, Wang Zhiqi, Wang Lei et al. Design and application of website security risk monitoring system based on "network defense G01" and big data technology [J]. Police technology, 2017, (2):20-23.