World Academics Journal of Engineering Sciences
Vol.6, Issue.1, pp.52-54, October (2019)

Review Paper

E-ISSN: 2348-635X

Web Security: An Overview and Current Trend

P. K. Paul[1*], P. S. Aithal[2]

[1]MCIS, Department of CIS, Raiganj University (RGU), West Bengal, India
[2]Vice Chancellor, Srinivas University, Karnataka, India

**Corresponding Author: pkpaul.infotech@gmail.com*

Available online at: www.isroset.org

Received: 05/Oct/2019, Accepted: 23/Oct/2019, Online: 31/Oct/2019

Abstract- Websites are the mirrors ofthe modern IT Age. It is very difficult to find out the areas and sectors where Websites are not using. Initially, only big organizations and multinational companies being uses websites but gradually small organizations and institutions and individuals are also having websites of different kinds and purposes. It is (Website) the collection of resources of different network web resources viz. multimedia, contents, etc and published in one or more servers. In websites domain names, IP addresses are a very important concern. There may be different kinds of websites viz. static, dynamic and in all these abilities to keep a large amount of data. In the recent past, websites increased radically. Due to the wide uses and number of websites, today a huge amount of data stored into the systems and thus their security also becomes an important concerned. Thus, the concept of Web Security or Web Application Security has emerged. Today it is an important concern of Information Technology Security. Web Security is the affairs of security related to the websites, web services and web based applications as a whole. This paper is a kind of review and trend analysis of website and web security. Paper described the basics of web security, the reasons/ threats including various defending mechanism as well. Paper highlighted the challenges and issues as well in a simple context.

Keywords- Web Security, IT Security, Web Portal, Information Security, Information Services, Emerging Services

I. INTRODUCTION

Web Security is an important concern of IT Security. Information Technology Security is the emerging concept of Security it includes the different security domains and sectors viz. Network Security, Database Security, Web Security and also emerging security concerns such as Cloud Security, Mobile Security, IoT Security, etc [1], [5]. As far as Web Security is concerned, it includes the applications of appropriate tools, techniques, and procedure to maintain the security of the websites, web applications, web services, etc. There are different reasons for the security threats and among these few important are include SQL Injection, Password breach, Remote file injection, code injection, etc [2], [3]. In an advanced level, Web Security is concern about the principles of application security with special reference to the websites and internet systems. Secure web application development needs healthy and planned security checkpoints as well as techniques at the early stages of development. Moreover, it is required throughout the software development lifecycle of the system or software development.

II. OBJECTIVE AND AGENDA

The present paper is conceptual and theoretical in nature and it is mainly conducted to deal with the following—

- To learn about the basics of the web including generations and types in a basic and simple manner.
- To learn about the basics of Websites as well as Web Security in a simple and general context.
- To know about the basic security related threats in connection to Web Security, Web Services and Applications.
- To learn about the trends in threats of Web Security and also various security technologies in the simple and basic sense.
- To learn about the currents challenges, issues in respect of Web Security as well.

Web Security: The Root

The Web Security mainly concern with the Websites. It should be very clear that Web Security is the part of IT Security. And there are different other security areas in the IT Security viz. Network Security, Database Security, Web Security and also sub fields like Cloud Security, Mobile Security, IoT Security [4], [7]. Initially, there was a very limited number of websites but a gradually various and large

number of websites have been developed internationally and this is increasing with other facets viz. web application security, web services, etc. Today most of the commercial organizations, institutions are doing well in saving their data and contents into the websites and thus it is very important that proper security should be provided into the systems. As we are aware that there are two major websites viz. Static and Dynamic and among these two Dynamic are much more active and multiple services based and thus their security is an important concern here as well. In common computer systems, Internet Security Pack or Web Security Pack is noticeable and its uses are increasing rapidly.

Web Security: Allied Concepts

There are different concepts related to the Web Security and among these important are Web Services Security, Web Applications Security, Web IT Security, etc. The Web Security should be very close with the Database and Network Security; as these are connected each other. There are different concepts in Web Security viz.—

- Vulnerabilities
- Malware
- Spyware
- Virus
- Worms
- Keyloggers
- Backdoors
- Web Shells
- Phishing etc

It is worthy to note that, the maximum number of Web Security requires in the places of cross site scripting, SQL Injections, etc (Refer Table: 1 for more details; source Cenzic// Wikipedia). There are different security backups protocols and guidelines etc [8], [10], [12].

Table: 1-The kind of web attacks with percentages

Percentage of Vulnerability	Kind of Attacks
37	Cross Side Scripting
16	SQL Injection
5	Path Discloser
5	Denial of Service Attack
4	Arbitrary Code Execution
4	Memory Corruption
4	Cross Site Request forgery
3	Data Breach
3	Arbitrary File Inclusion
2	Local File Inclusion
1	Remote File Inclusion
1	Buffer Overflow
15	Miscellaneous including Code injection etc

Web 2.0 and Attacks

The development of websites has been mapped with the generation the first of its kind treated as Web 1.0, Web 1.5, Web 2.0. The nature of Web 1.0 is basically having the nature of standalone but Web 2.0 is kind of active and dynamic in which people can be entered into the web systems. This is current age major websites; this is may also be called as *Participatory Web*, *Social Web* as well [7], [9], [11]. Today's most of the websites are interactive and data and information can be updated into the systems and thus Web 2.0 or current websites are coming with different challenges and risks viz. –

- SQL Injection
- Cross Site Scripting
- Denial of Service Attack
- Arbitrary Code Execution
- Data Breach
- Remote File Inclusion
- Insecure deserialization
- Using components with known vulnerabilities
- Insufficient logging and monitoring
- Buffer overflow
- Local file inclusion etc.

Website security is a kind of techniques and critical component that protectswebsites as wellas servers. Website vulnerabilities can be checked using website security software for scanning backdoor hacks, redirect hacks, worms, viruses, Trojans, etc. Such security software notifies regarding the issuesas well as the solutions [14], [16], [17].

III. SECURITY MANAGEMENT &WEBSITES: THE TRENDS

Website securityis possible to bring by the different strategies and techniques and among them, few important are include—

- Black Box testing tools
- White Box testing tools
- Fuzzing tools
- Web Application Scanner (i.e. Vulnerability Scanner)
- WAF—Web Application Firewall
- Password Cracking

It is worthy to note that, Website security can be a threat by the broken authentication, insecure direct object references, security misconfiguration, missing function level access control, un-validated redirects and forwards, etc. It is important to note that there are various security standards in this regard and major of them are— Open Web Application Security Project, IEEE Guidelines, etc. Even Developer can use the following two important strategies for this viz.—

- Resources Assignment (It is the alarming or informing way to the developer by which secure web systems can be prepared)
- Web Scanning (Frequent uses of web scanning etc)

Moreover, it is worthy to note that website and complete web security is needed for various reasons viz. Web Sites Security Issues as it holds huge sensitive data. Insecure coding and multiple dynamic attributes without proper planning lead the security issue. So, it is important to design the websites such as a way in which security is highly paid. Many websites are these days offer visitor involvement by chatting, online communication and feedback, etc and it is important that an appropriate policy should be undertaken into this [13], [15].

IV. CONCLUSION

Today most of the organizations and institutions are using Enterprise Networks and their huge vulnerability can be an important issue for the websites and similar objects. The network, the server and the website when get connected together then the chances for vulnerabilities also become high and thus there is a requirement in the malware scanning and removal, spam monitoring, security monitoring, content delivery network, advanced DDoS mitigation, hack removal, etcfor better services. The organizations and institutions of a different kinds thus should proper step for the promotion of security related awareness, technicalities for the secure and sophisticated web services.

REFERENCES

[1] Borgesius, F. Z., Gray, J., & Van Eechoud, M. (2015). Open data, privacy, and fair information principles: Towards a balancing framework. *Berkeley Technology Law Journal*, *30*(3), 2073-2131.

[2] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

[3] George, B., & Valeva, A. (2006, March). A database security course on a shoestring. In *ACM SIGCSE Bulletin* (Vol. 38, No. 1, pp. 7-11). ACM.

[4] Holla, S., & Katti, M. M. (2012). Android based mobile application development and its security. *International Journal of Computer Trends and Technology*, *3*(3), 486-490.

[5] Krishnan, V., McCalley, J. D., Henry, S., & Issad, S. (2011). Efficient database generation for decision tree based power system security assessment. *IEEE Transactions on Power systems*, *26*(4), 2319-2327.

[6] Li, Y., Stweart, W., Zhu, J., & Ni, A. (2012). Online privacy policy of the thirty Dow Jones corporations: Compliance with FTC Fair Information Practice Principles and readability assessment. *Communications of the IIMA*, *12*(3), 5.

[7] Mathieu, R. G., & Khalil, O. (1998). Data quality in the database systems course. *Data Quality Journal*, *4*(1), 1-12.

[8] Murray, M., & Guimaraes, M. (2008). Expanding the database curriculum. *Journal of Computing Sciences in Colleges*, *23*(3), 69-75.

[9] Murray, M. C. (2010). Database security: What students need to know. *Journal of information technology education: Innovations in practice*, *9*, IIP-61.

[10] Neto, A. A., Vieira, M., & Madeira, H. (2009, June). An appraisal to assess the security of database configurations. In *2009 Second International Conference on Dependability* (pp. 73-80). IEEE.

[11] Ritchie, P. (2007). The security risks of AJAX/web 2.0 applications. *Network Security*, *2007*(3), 4-8.

[12] Rubin, A. D., & Geer, D. E. (1998). A survey of Web security. *Computer*, *31*(9), 34-41.

[13] Said, H. E., Guimaraes, M. A., Maamar, Z., & Jololian, L. (2009). Database and database application security. *ACM SIGCSE Bulletin*, *41*(3), 90-93.

[14] Sandhu, R. S., & Jajodia, S. (1993). Data and database security and controls. *Handbook of information security management, Auerbach Publishers*, 1-37.

[15] Smith, G. W. (1991). Modeling security-relevant data semantics. *IEEE Transactions on Software Engineering*, (11), 1195-1203.

[16] Srinivasan, S., and Anup Kumar. "Database security curriculum in InfoSec program." In *Proceedings of the 2nd annual conference on Information security curriculum development*, pp. 79-83. ACM, 2005.

[17] Stein, Lincoln D. "Web security." *Addison-Wesley, Massachusetts* 26 (1998): 1-4.

