Turkish Journal of Computer and Mathematics Education Vol.12 No. 11 (2021), 6246 - 62450
Research Article

Review the Various Threats specific in Application Layer for speedup to Web Security Evaluation

Ritesh Rastogi [a], Sandeep Srivastava [b], Phaneendra Puppala [c], Varsha Sahni [d], Sandeep Mathur [e]

[a] Associate Professor of MCA Dept., Noida Institute of Engineering & Technology, Greater Noida, India.
[b] Assistant Professor of MCA Dept., GL Bajaj of Institute of Technology & Management, Greater Noida, Pin 201306, India.
c Lecturer of Faculty of Information Technology, Asia-Pacific International University, Muak Lek - 18180, Saraburi,Thailand.
[d] Department of Computer Science and Engineering, CT Group of Institute (CTIEMT), Shahpur, Jalandhar, Pin 144020, India, [d] I.K.Gujral Punjab Technical University, Jalandhar, Pin 144603, India.
[e] Assistant Professor of Amity Institute of Information technology, Amity University, Noida, Pin 201301, India.

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May2021

Abstract: The motive of the present study is to pay some light on the contribution of Security in the field of Web. The Web application has become an incredible field in the world of corporate .The SECURITY is defined as overall quality, authenticity, reliability, scalability, confidentiality and authorisation. This research work is about security principles in web applications. This paper is centralised to reach out the attack and threat on web application and resume the concern security principles or method to overcome. According to evidence, exploitable vulnerabilities present in the source code could enable up to 60% of attacks on enterprise web applications. In this article, we examine the different risks unique to the application layer, as well as the associated compensating controls. Threats unique to each tier of an enterprise web application are addressed, with an emphasis on threat modelling. Security is the necessary, significant and cardinal point in web application. The security is the key concept in the world of web. Web application security is an essential key point of concern because it has become a way to interact with the internet and computing system. The methodology to overcome vulnerability is penetration tools, backtracking. Input validation etc.

Keywords: Web Application, security, Protocol Stack, Online attack, vulnerability, back tracking, authenticate.

1. Introduction

Web security plays a vital role nowadays in web applications. The loopholes in security can create big trouble in the society. So it is tackling it very efficiently. We have two types of web security namely web browser security and web application Security. Web browser security is also the topic of concern but not as web application. Web application security has been designed to keep concern of all the vulnerabilities. Security is an important aspect because it deals with multiple enormous, valuable and sensitive data. Web application threat leads to the stolen debit card, defaced sites and also sql injection. The key security resources collectively known as CI4A are the security standards for evaluating web application security (Confidentiality, Integrity, Authentication, Authorization, Availability, and Accountability). Another intelligence service associated with transparency is non-repudiation. Confidentiality in the case of corporate web applications refers to the secrecy of data that flows through or is stored within the web application. Integrity means that the evidence used has not been tampered with, either intentionally or accidentally. Authentication is the process of verifying a person's identity. The concept of authentication can also be extended to source legitimacy (Taherdoost, H. 2017). Access privileges to different device subsystems, features, and data are the subject of authorization. Availability, an often overlooked feature of protection, is a critical metric for the web application's security posture. (Gayan Nayanajith, D. A., Damunupola, K. A., & Wanninayake, W. M. C. B. ,2019) defines many attacks that threaten service availability take advantage of coding errors that could have been easily avoided at the application root stage. Non-repudiation tackles the need to demonstrate that an identity has taken a certain step without being able to deny it. People may be held accountable for their decisions if they have accountability and non-repudiation.

The Security of the web application depends upon the levels of protection tools that have been used on it. There are some common and generally threats or vulnerabilities which are used to hack the web application. The most common threats are SQL injection, password breach, cross site scripting, remote file inclusion code, and code injection.

2. Mitigate security risks in web application

To prevent security breaches, web application creation, regardless of the platform used, necessitates proper Web application and server management. In fig.1, despite the fact that many businesses host their web apps in the cloud and use a private cloud for their web applications, hackers and web spiders are still on the lookout (Praseed, A., & Thilagam, P. S. (2018). What matters is that you pay special attention to Web application protection and upkeep. In reality, it all begins with a developer who can write stable code and keep the application up to date. (Chandramouli, R., Iorga, M., & Chokhani, S. 2014)

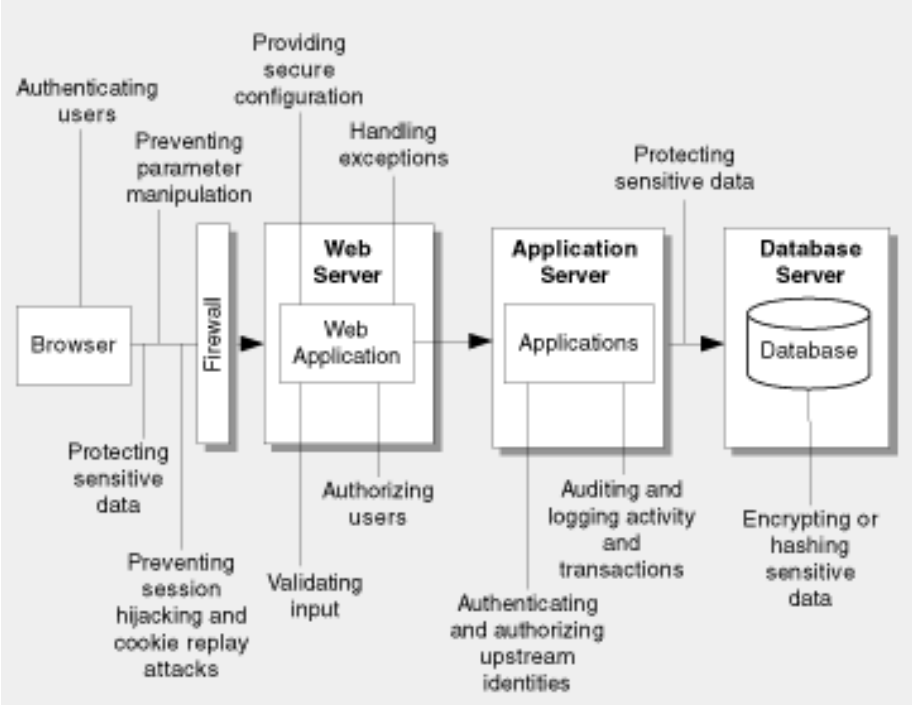

Figure 1. Reducing security vulnerabilities and ensuring Web site security

The web Security where some of the threats or attacks are analysed by using penetration tools. Vulnerability is a serious issue today. Generally vulnerabilities occur into two ways they are as given follow:

Protocol Stack

Online attack

2.1 Protocol Stack

Generally attacks in the protocol stack are not taken as a major task but are also an important point of concern. In fig.2, it can solve relevantly by using some relevant methods.it goes out in three layers such as network layer, transport layer and application layers. The methodology to overcome protocol stack is use of strong password and correct configuration of management protocol (Liu, J., Xiao, Y., Li, S., Liang, W., & Chen, C. P. , 2012). We can encrypt data packets in all network layers. We can set one security (example: we can apply this by using brute force. The concept is to model the 3*3 dots as a graph, then explore all the possible way that 4 or any number<=9 nodes be joined to each other. None of them be explored twice. Like this we can create a special pattern denoting the non-reachable nodes of each node and question in every data packet or network layer.

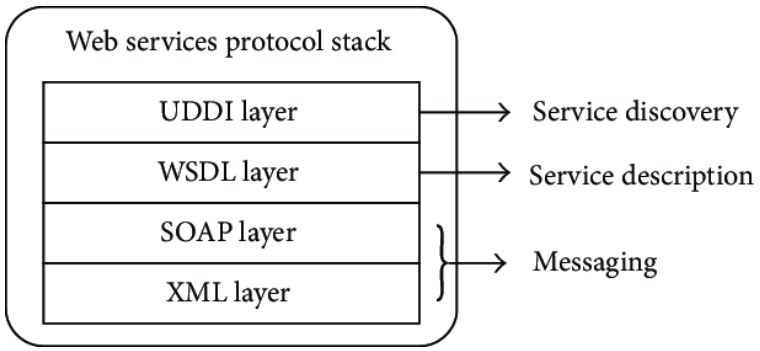

Figure 2. Protocol stack for web providers.

2.2. Online attack

There are several online attacks that create defects in web applications and affect web security attack taken for consideration are SQL injection and Cross Site scripting. A web service flaw is a device error or mistake in a

web-based network.(Deepa, G., & Thilagam, P. S., 2016).They've been around for a long time and can be used to compromise an application's protection due to a lack of form validation and sanitization, as well as misconfigured web servers and design flaws. Other kinds of vulnerabilities, such as network and asset vulnerabilities, are not the same as these. They exist because web apps must communicate with multiple users through multiple networks, and hackers can easily exploit this degree of usability (Fonseca, J., Seixas, N., Vieira, M., & Madeira, H. 2013).

3. SQL Injection

SQL is one of mainly used vulnerabilities. In sql injection makes use of code to exploit database. It inserts new data or removes the data or edit the data accordingly but do not hemp the resource fetching data by using sql code. The reason of this sql injection is wrong validation of input or weak and improper filtration of the input data (Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., & Shakarian, P., 2017).The methodology we can use is using Blind sql is a type of sql targeted for security where an attacker can not reach the result or data. This one way to keep our result safe. By proper input validation Through Sql query command The preventing measure can be taken. The other way is to put wrong input in first chance and put right input in second or third attempt (Ahmad, H., Dharmadasa, I., Ullah, F., & Babar, A., 2021).

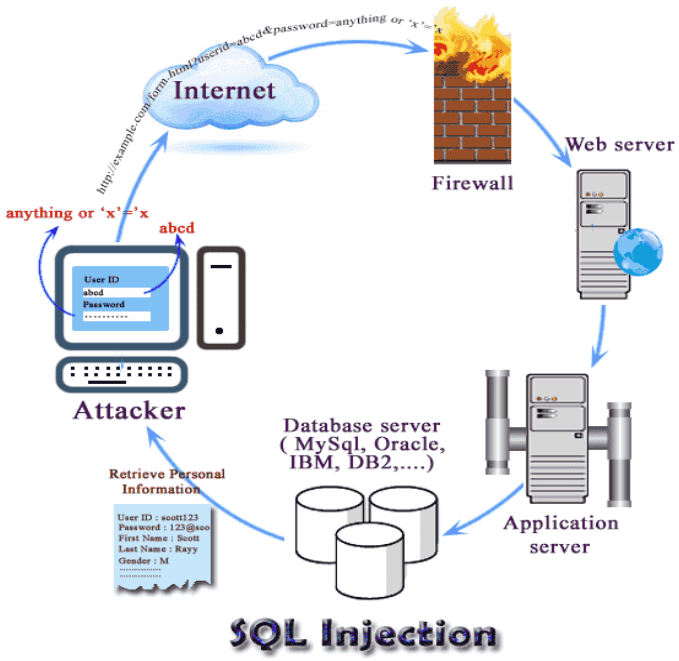

Figure 3. SQL injection is a method of attacking data-driven programmes

4. Cross Site Scripting

Cross site script names were given by CERT 2000 and In February 2000 it was published .This attack is very much similar to the sql injection, we can say that both are siblings in common language but there is quite a difference in it like brother and sister of same parent, it runs on java script.The client side web is hacked by the hacker through the malicious JavaScript (Alwaghid, A., 2019). The scripting runs the certain commands on the html pages. The consequence of this attack is modification of data, steal access credential, and insert wrong data.

The Strategies of attacker to perform attack are as below (Hamam, H., & Derhab, A. 2021).

- Create a malicious code.
- Send the malicious code message.
- The message code was stored by the server.
- The request for the server site for the data is done by the user to the server.
- The user gets a response from the server.
- Then finally the script was executed by the user.

- This malicious code attacks the client.
- Consequences of the above step are that Client access is denied.

The two popular methods of revealing passwords are dictionary and brute-force attacks. (Mereani, F. A. 2021). These methods involve a file containing words, sentences, standard passwords, and other strings that are likely to be used as a password.

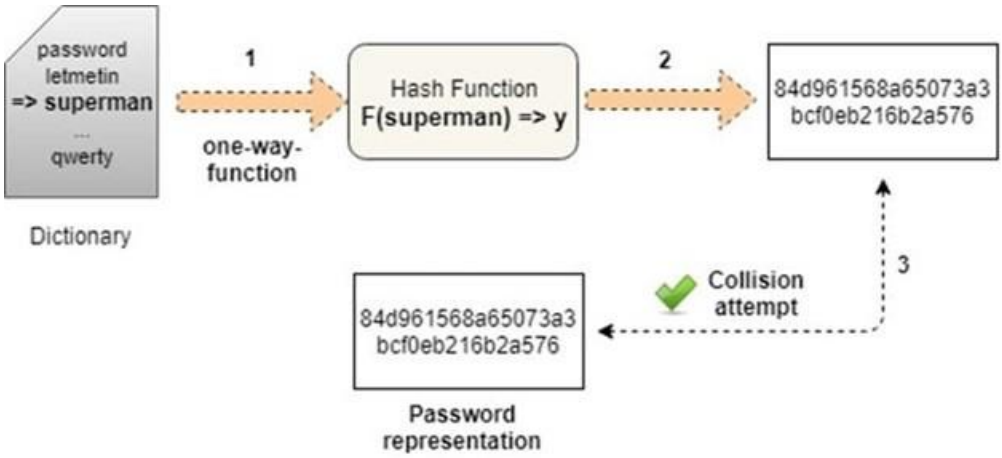

Figure. 4 Methods of guessing passwords are dictionary and brute-force attacks.

The Methodology against the Cross Site Scripting is input validation or putting the wrong password in the first attempt to secure it from the hacker. The most provident way to secure this attack is back track. Backtrack is known as the penetration tool which is best known for the functionality of exploiting the vulnerability of online attacks (Μπαξεβάνος, I. 2014). It performs the task by assessment tools and vulnerability tests to make web applications safe and secure. IT detects the attack by 12 different categories of the tools (Nagpure, S., & Kurkure, S. , 2017) . The back track is one of the most popular and convenient methods of preventing online attacks. The method of performing test is as (Chaabouni, N., Mosbah, M., 2019):

- Gathering information.
- Assessment of vulnerability
- Target the assessing and maintenance point.
- Lastly track clearance.

5. CONCLUSION

In this research work we learn the security measures of web applications against the protocol stack vulnerabilities and online attack vulnerabilities as we analyse that security measures of web application is diverse and extreme, the topic covers many aspects of the society. The security of web application is an important area of knowledge which emphasises an intersectional method of exploring the security principles or measures and mechanisms that can be found in the web application. In this whole research paper we showed the viability and the preventive measures taken against it.The research work concluded that security is the most important and crucial point of the web application (our society). Later on we split the light on preventing measures of attacks or vulnerabilities. The Different methodology like input validation, strong password, security question, pattern and put wrong password first time and most cardinal method backtracking method.

References

1. Taherdoost, H. (2017). Understanding of e-service security dimensions and its effect on quality and intention to use. Information & Computer Security.

2. Gayan Nayanajith, D. A., Damunupola, K. A., & Wanninayake, W. M. C. B. (2019). EFFECT OF SUBJECTIVE NORMS AND SECURITY OF E-SERVICES ON MOBILE BANKING ADOPTION: A HIERARCHICAL LINEAR MODEL ANALYSIS. Manuscript submitted for publication. DOI, 10.
3. Chandramouli, R., Iorga, M., & Chokhani, S. (2014). Cryptographic key management issues and challenges in cloud services. In Secure Cloud Computing (pp. 1-30). Springer, New York, NY.
4. Praseed, A., & Thilagam, P. S. (2018). DDoS attacks at the application layer: Challenges and research perspectives for safeguarding Web applications. IEEE Communications Surveys & Tutorials, 21(1), 661-685.
5. Liu, J., Xiao, Y., Li, S., Liang, W., & Chen, C. P. (2012). Cyber security and privacy issues in smart grids. IEEE Communications Surveys & Tutorials, 14(4), 981-997.
6. Deepa, G., & Thilagam, P. S. (2016). Securing web applications from injection and logic vulnerabilities: Approaches and challenges. Information and Software Technology, 74, 160-180.
7. Fonseca, J., Seixas, N., Vieira, M., & Madeira, H. (2013). Analysis of field data on web security vulnerabilities. IEEE transactions on dependable and secure computing, 11(2), 89-100.
8. Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., & Shakarian, P. (2017). Darkweb cyber threat intelligence mining. Cambridge University Press.
9. Hamam, H., & Derhab, A. (2021). An owasp top ten driven survey on web application protection methods. In Risks and Security of Internet and Systems: 15th International Conference, CRiSIS 2020, Paris, France, November 4-6, 2020, Revised Selected Papers (Vol. 12528, p. 235). Springer Nature.
10. Mereani, F. A. (2021). Investigating the detection of stored scripting attacks using machine learning (Doctoral dissertation, City, University of London).
11. Μπαξεβάνος, Ι. (2014). Protecting with network security strategies a medium size enterprise and implementing scenarios attacks and countermeasures on cisco equipment (Master's thesis, Πανεπιστήμιο Πειραιώς).
12. Nagpure, S., & Kurkure, S. (2017, August). Vulnerability assessment and penetration testing of Web application. In 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA) (pp. 1-6). IEEE.
13. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials, 21(3), 2671-2701.
14. Qasem, A., Shirani, P., Debbabi, M., Wang, L., Lebel, B., & Agba, B. L. (2021). Automatic Vulnerability Detection in Embedded Devices and Firmware: Survey and Layered Taxonomies. ACM Computing Surveys (CSUR), 54(2), 1-42.
15. Pham, M., & Xiong, K. (2020). A survey on security attacks and defense techniques for connected and autonomous vehicles. arXiv preprint arXiv:2007.08041.
16. Alwaghid, A. (2019). A Study of Malware Behaviour of Webpages (Doctoral dissertation, Auckland University of Technology).
17. Mahbub, M. (2020). Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. Journal of Network and Computer Applications, 102761.
18. Snehi, M., & Bhandari, A. (2021). Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks. Computer Science Review, 40, 100371.