International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

Underpinning the Impact of Web Application Security on Businesses and Organizations

Labaran Idris Jega[1] , Abdulaziz Salihu Aliero[2], Umar Bawa Abdulmajid[3]

[1,2,3]*Kebbi State University of Science and Technology, Aliero, Kebbi State, Nigeria*

Abstract - *This paper will present an approach towards discussing one of the world's major development in the IT sector in the name of Web Application. Today, web applications have made a massive impact on millions of businesses and organizations especially by drastically minimizing cost, labor, efficiency and many others. Web application has gone beyond just a common web page, rather, to a much bigger tool which enables numerous organizations to smoothen and enhancing their business capabilities in terms of interacting with thousands of business partners, customers and even retailers. Moreover, this paper's main objective is on discussing an in depth overview of Web Application and web application security, the common functions of web application, the most common vulnerabilities in web application and their solution solutions, the attributes, as well as the underlying structure of web application, so as to enable the reader to have a theoretical as well as technical overview of the discourse in questions.*

Key Words: **Web security, session hijacking, ecommerce, security, hacking, ecommerce security,**

1. INTRODUCTION

The influence of web based applications is disputably the single most significant event in antiquity of computing. As web app flourished in importance, a discipline Web engineering approach adapted from software engineering principles, concepts process and methods has begun to evolve. Hence, Web apps are different from other classifications of computer software. They are network intensive, content driven, and continuous evolving products [1].

In a nutshell, unlike a website that simply provides its users with the opportunity to read information through the WWW windows; "a *Web Application* can be considered as a software system that exploits the WWW infrastructure to offer its users the opportunity to modify the status of the system and of the business it supports". In contrast, *web applications* are programs that are deployed in a novel way, allowing them to be accessed remotely across the internet. The first programs deployed on the web were simple applications that accepted form data from HTML pages and processed or stored the data. Today, modern applications are sophisticated, interactive programs with complex GUIs and numerous back-end software components that are integrated in novel and interesting ways [2].

2. THE CONCEPT OF WEB APPLICATION

As the world embraces cloud computing, more and more people are transacting business, conducting research, storing information, collaborating with co-workers, publishing personal thoughts, and fostering relationships via web Applications. In order to understand Web Application, first of all, let's define web application properly: web Application is a client-server application program that is stored on a remote server and delivered over the internet through a browser interface. However, we can elaborate by saying that web application or web app is a software program that runs on a web server. Unlike traditional desktop applications, which are launched by our operating systems, web apps must be accessed through web browsers [3].

Web apps have several advantages over desktop applications. Since they run inside web browsers, developers do not need to develop web apps for multiple platforms. Thus, developers do not need to distribute software updates to users when the web app is updated. (See figure 1). By updating the application on the server, all users access to the updated version. From a user standpoint, a web app may provide a more consistent user interface across multiple platforms because the appearance is dependent on the browser rather than the operating system. Additionally, the data you enter into a web app is processed and saved remotely. This allows you to access the same data from multiple devices, rather than transferring files between computer systems [5] .

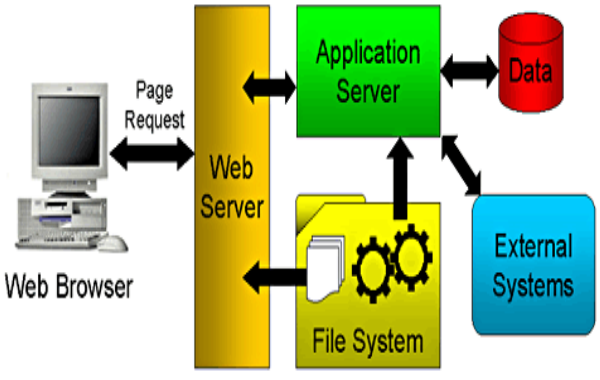

Fig1: Structure Of Web Application

While web applications offer several benefits, they do have some disadvantages compared to desktop applications. Since they do not run directly from the operating system, they have limited access to system resources, such as the CPU, memory, and the file system. Therefore, high-end programs, such as video production and other media apps generally perform better as desktop applications. Web apps are also entirely dependent on the web browser. If your browser crashes, for example, you may lose your unsaved progress. Also, browser updates may cause incompatibilities with web apps, creating unexpected issues [6] .

3. WEB APPLICATION FUNCTIONS

Web application have been created to perform practically every useful function you could possibly implement online. Below are some web applications functions that have risen to prominence in recent trends:

a. E-shopping and e-business such as Amazon and FlipKart
b. Banking and e-money
c. Social Network such as Facebook, LinkedIn
d. Web search like in Google search app for android
e. Auctions such as eBay
f. Web blogs and etc.

Applications that are accessed using a computer browser increasingly overlap with mobile applications that are accessed using a smartphone or tablet. Most mobile applications employ either a browser or a customized client that uses HTTP-based APIs to communicate with the server. Application functions and data typically are shared between the various interfaces that the application exposes to different user platforms [7].

4. WEB APPLICATION SECURITY

Web application security is a branch of information security that's deals specifically with security of websites, web applications and web services. At the high level, web application security draws on the principles of application security but applies them specifically to internet and web systems. As with any new class of technology, web applications have brought with them a new range of security vulnerabilities. The set of most commonly encountered defects has evolved somewhat over time. New attacks have been conceived that were not considered when existing applications were developed. Some problems have become less prevalent as awareness of them has increased. New technologies have been developed that have introduced new possibilities for exploitation. Some categories of flaws have largely gone away as the result of changes made to web browser software [7].

The most serious attacks against web applications are those that expose sensitive data or gain unrestricted access to the back-end systems on which the application is running. High-profile compromises of this kind continue to occur frequently[8] . For many organizations, however, any attack that causes system downtime is a critical event. Application-level denial-of-service attacks can be used to achieve the same results as traditional resource exhaustion attacks against infrastructure. However, they are often used with more subtle techniques and objectives. They may be used to disrupt a particular user or service to gain a competitive edge against peers in the realms of financial trading, gaming, online bidding, and ticket reservations.

5. KEY PROBLEM OF WEB APPLICATION

The majority of web applications are insecure, despite the widespread usage of SSL technology. However, professionals have pin pointed several instances of problems or attacks that are liable to invade any web application security [9]. Ten most critical web application security vulnerability were highlighted, although, only few shall be discussed in this paper:

5.1 SQL Injection

Most of web applications that use a database build an SQL statement based on user input. This means if the SQL statement-building process is not securely guarded, attacking and manipulating the database would become possible. This issue is called "SQL Injection vulnerability" and the attacking method exploiting this vulnerability is called "SQL Injection attack". (See figure 2)

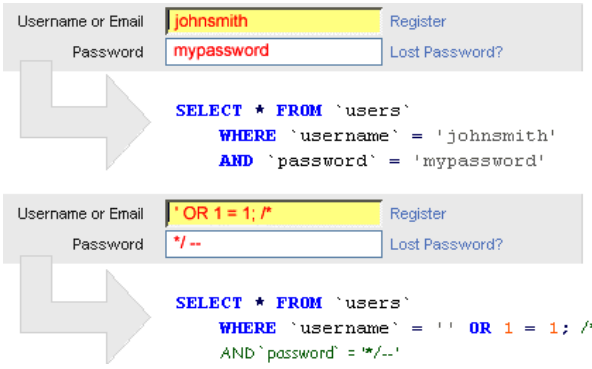

Fig 2: Sql Injection Attack

5.2.1 Solution for SQL Injection

Usually, the SQL has a mechanism to build an SQL statement using placeholders. It is a mechanism to put a symbol (placeholder) at the place of the variables in the template of an SQL statement and replacing it with an actual data value mechanically later.

5.3 Unchecked Path Parameter

Some web applications allow to specify the name of files stored on the web server directly using external parameters. If such web application is not carefully programmed, attackers may specify an arbitrary file and have the web application execute unintended operations. This issue is called "Directory Traversal vulnerability" and one of the attacking methods exploiting this vulnerability is called "Directory Traversal attack".

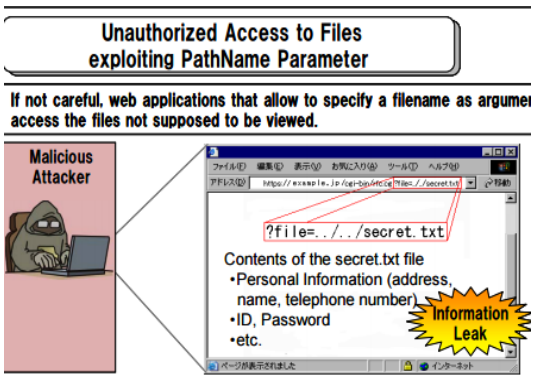

Fig3: Unchecked Path

5.3.1 Solution For Unchecked Path

When a web application allows a filename to be specified directly using an external parameter, an attacker could manipulate the parameter specifying arbitrary files and view the file contents that should not be disclosed. For example, in an implementation case where the name of a file stored in the web server is specified in the hidden parameter and that file is used in the web page template, an attacker can output arbitrary file as a web page by manipulating the parameter.

5.4 Improper Session Management

Some web applications issue session ID, which is the information to identify the user, to manage sessions. If session ID is not created and managed properly, an attacker could steal the session ID of a legitimate user and gain unauthorized access to the services pretending to be the legitimate user. The attacking method exploiting this vulnerability in session management is called "Session Hijacking".

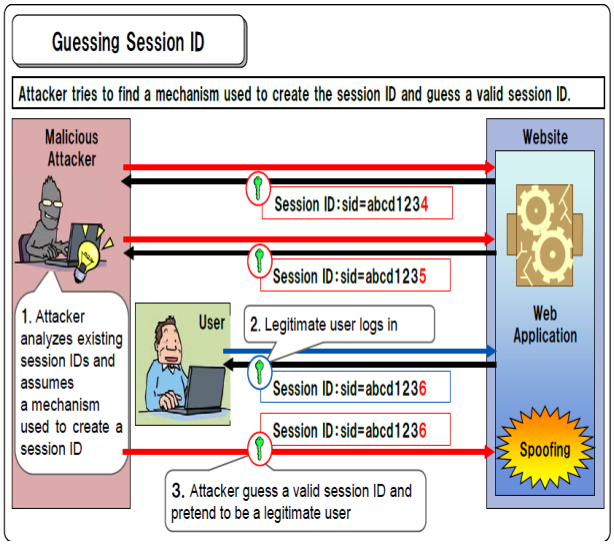

Fig4: Session Hijacking

5.4.1 Solution For Session Hijacking

If the session ID is fixed for each user, an attacker can perform session hijacking attacks anytime without time limitation once the attacker obtains the session ID. Do not use a fixed session ID and create a new session ID each time the user logs in.

5.5 Inefficient Authentication And Authorization Technique

It is absolutely true that some web applications are not properly and adequately secured. One could understand that from the way they fail authentication and authorization tests. Password has been the line if defense for many web applications. However, password has proven to be weak when it comes to authentication. With a simple brute force tool, intruder can be able to crack the passwords within no time. More so, not all application users should be given elevated authorizations. Some disgruntled employees could use their authorization level to harm the web application.

5.5.1 Solution To Inefficient Authentication And Authorization

To tackle authentication issues, implement a two tier or three tier authentication method which may comprise of password, token codes, and a security question or security question can be substituted with thump scanner for retina recognition depending on the budget of the company. Furthermore, least privileges should be given to low level users, this could protect application from intentional harm or unintentional harm. Also, admin login should only be used only when necessary.

6. OTHER SECURITY MEASURES FOR SECURING WEB APPLICATION

To safely operate a website, the administrator should not only secure web applications but also securely guard the web server. Thus the following recommendations help in hardening the chances of invading the system [4] .

a. Check OS and software vulnerability information constantly and take necessary actions accordingly.
b. Implement an authentication mechanism other than using password for remote server access.
c. When using password authentication, make sure to use a sufficiently complex string
d. Disable unused services and delete unnecessary accounts
e. Do not place a file you do not intent to make public under the public directory on the web server

7. CONCLUSIONS

To end this discussion, it is important for me to give a brief overview or an executive summary of what this paper contains. This paper starts with an introductory part where we have enumerated some various definitions web application and web application security. Both of them are subsidiaries of information security and they deal strictly with how user or organization tackles any form of security breach that could cause any violation of privacy or exposure of internal security in an organization. Subsequently, this paper discussed in depth the common example or instances of web application security problems, where we mentioned certain points that we think are responsible for the breach of security. Although, other types of web application problems were not mentioned due to limited time and resources. But the few others that we have left include Cross-site scripting, OS command injection, Cross-site request forgery and so on (Durkee, 2010).

Finally it is important to note that, in spite of all the efforts to eliminate these threats, yet, there are millions of people out there who spend sleepless nights trying to identifying new exploits that could be used to compromise various security infrastructures.

BIBLIOGRAPHY

1. IBM. (2008). Understanding Web application security challenges ., (January)
2. Wiesmann, A., Stock, a Van Der, Curphey, M., & Stirbei, R. (2005). A guide to building secure web applications and web services. *The Open Web Application Security Project*, 101–137, 147–160. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:A+Guide+to+Building+Secure+Web+Applications+and+Web+Services#2
3. Li, X., & Xue, Y. (2011). A survey on web application security. *Nashville, TN USA*, *25*(5), 1–14. Retrieved from http://isis.vanderbilt.edu/sites/default/files/main_0.pdf
4. Zinger, P. (n.d.). Six Essential Elements of Web Application Security Cost Effective Strategies for Defending Your Business. Retrieved from https://www.whitepapers.em360tech.com/wp-content/uploads/The-Six-Essential-Elements-of-Cost-Effective-Web-Application-Security.pdf
5. Belfort, M. A., & Saade, G. R. (n.d.). Web Application Security. *World Wide Web Internet And Web Information Systems*, *210*(10), 1–37. https://doi.org/10.1385/1592592910
6. Hoff, J. (n.d.). A Strategic Approach to Web Application Security. *WhiteHat Security*.
7. Government, T. H. K. A. (2008). Web Application Security, (February), 26. https://doi.org/10.1007/978-3-642-16120-9
8. Web Application Security Standards and Practices. (2011), *1*(January), 1–13.
9. Stuttard, D., & Pinto, M. (2011). *The Web Application Hacker's Handbook*. Indianapolis: John Wiley & Sons, Inc.