ANALYSIS OF WEB SERVER SECURITY CHALLENGES

[1]AMADI E.C., [2]ONEBUNNE F. C., [3]IHEUKWUMERE O. C., [4]ONYEYIRI U. N.

[1.4]DEPARTMENT OF INFORMATION MANAGEMENT TECHNOLOGY,
FEDERAL UNIVERSITY OF TECHNOLOGY, OWERRI.

emmanuel.amadi@futo.edu.ng

ABSTRACT

As the web expands in size and adoption, so does the interest of attackers who seek to exploit web applications and infiltrate user data. While there is a steady stream of news regarding major breaches and millions of user credentials compromised. It is logical to assume that overtime, the applications of bigger players of the web are becoming more secure. However as these applications become resistant to most prevalent attacks, adversaries may be tempted to move easier, unprotected target would still hold sensitive user data. This article reviews some of the security challenges being faces by web server on the internet.

KEYWORDS: Web, servers, security, vulnerabilities**.**

1.0 INTRODUCTION

A web server is an information technology system that stores files (usually web pages), processes requests via HTTP (Hypertext Transfer protocol) from clients or end users and makes them accessible via the network or internet. A web server requires both hardware and software. Attackers usually target the exploits in the software to gain authorized entry to the server. (Guru99, 2015)

1.1 TYPES OF WEB SERVERS

We have different types of web servers. They are: Apache web server, Internet Information Services (IIS), Lighttpd web servers, Sun Java System web servers, Jigsaw Web servers and others like Novell's web server and IBM's Lotus Domino servers.

APACHE WEB SERVER- This is the most commonly used web server on the internet. It is cross platform but it is usually installed on Linux. Most PHP websites are hosted on apache servers. (Guru99, 2015)

INTERNET INFORMATION SERVICES (IIS) - It is developed by Microsoft. It runs on windows and it is the second most used web server on the internet. Most asp and aspx websites are hosted on IIS servers. (Guru99, 2015)

2.0 WEB SERVER SECURITY

Web server security is the protection of information assets that can be accessed from a web server. Web server security is important for any organization that has a physical or virtual web server connected to the internet. It requires a layered defence and is especially important for organizations with customer-facing websites. Separate servers should be used for internal and external-facing applications and servers for external-facing applications should be hosted on a DMZ or containerized service network to prevent an attacker from exploiting a vulnerability to gain access to sensitive internal information. (Rouse, 2015)

2.1 WEB SERVER SECURITY CHALLENGES

The web server security threats or issues or challenges are as follows:

- Directory traversal attacks
- Denial of service attacks(DOS)
- Domain name system hijacking
- Sniffing
- Phishing
- Pharming
- Defacement

- Profiling
- Unauthorized access
- Arbitrary code execution
- Elevation of privileges

2.1.1 DIRECTORY TRAVERSAL ATTACKS

This type of attack exploits bugs in the web server to gain unauthorized access to files and folders that are not in the public domain. Once the attacker has gained access, they can download sensitive information, execute commands on the server or install malicious software (Guru99, 2015). Directory Traversal attacks can be viewed in two basic groups: attacks that target directory traversal vulnerabilities in the web server and attacks that target vulnerabilities in application code. Attackers are able to exploit vulnerabilities in application code by sending URLs to the web server that instructs the server to return specific files to the application. Directory traversal vulnerabilities that exist on web servers are typically exploited to execute files.

2.1.2 DENIAL OF SERVICE ATTACKS (DOS)

This is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. This will typically happen through one of the following ways: crashing the target host system, disabling communication between systems, in intent to make the system or network down or have it operate at a lower speed to reduce its performance, lock the system so there is provision to automatic rebooting of the same so that the production is disrupted. This occurs when your server is overwhelmed by service requests. The threat is that your web server will be too overwhelmed to respond to legitimate client requests. The vulnerabilities are weak TCP/IP stack configuration, unpatched servers. The attacks are buffer overflows, flooding the web server with requests from distributed locations.

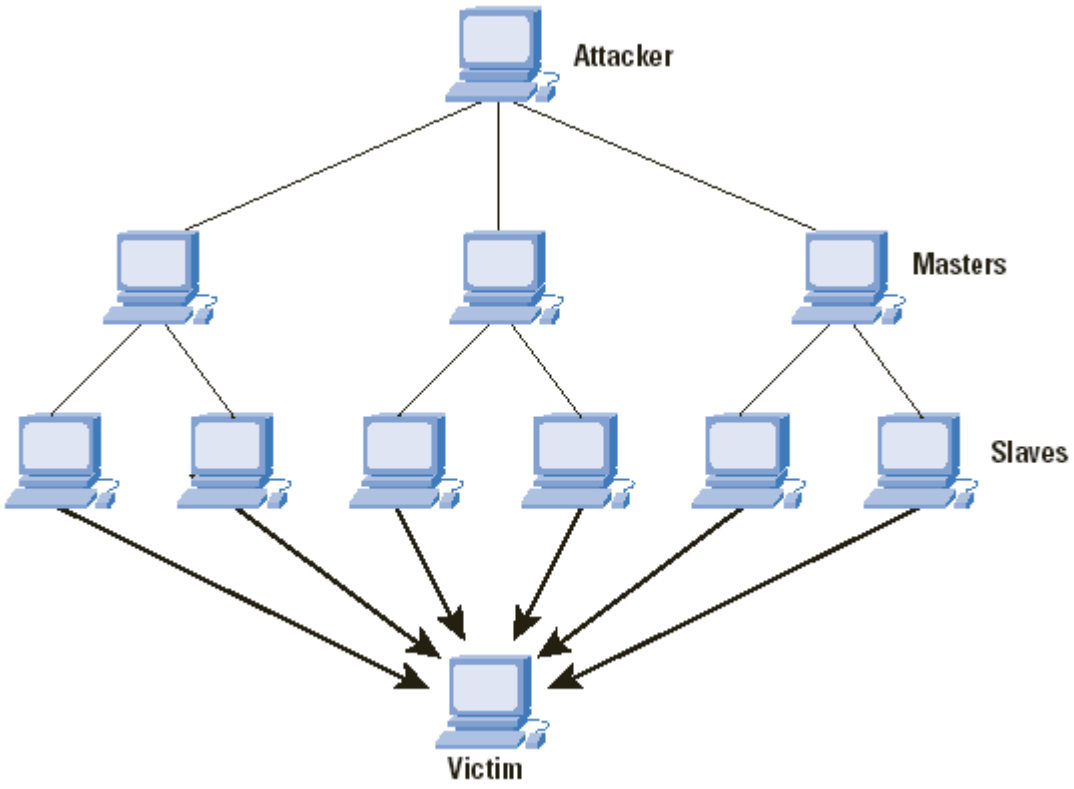

Fig 1: *a DDOS attack* (Patrikakis, Masiko, & Zouraraki, 2004)

2.1.3 DOMAIN NAME SYSTEM HIJACKING

This is a type of DDoS attack in which an attacker sends a DNS look up request to an open DNS resolver with the source address spoofed to be the victim's address. When the DNS server sends the DNS record response, it is sent to the victim (the source address that was used in the spoofed request). Because the size of the response is typically considerably to be larger than the request, the attacker can amplify the volume of traffic directed to the victim. By leveraging a botnet to perform additional spoofed DNS queries, an attacker can produce an overwhelming amount of traffic with very little effort.

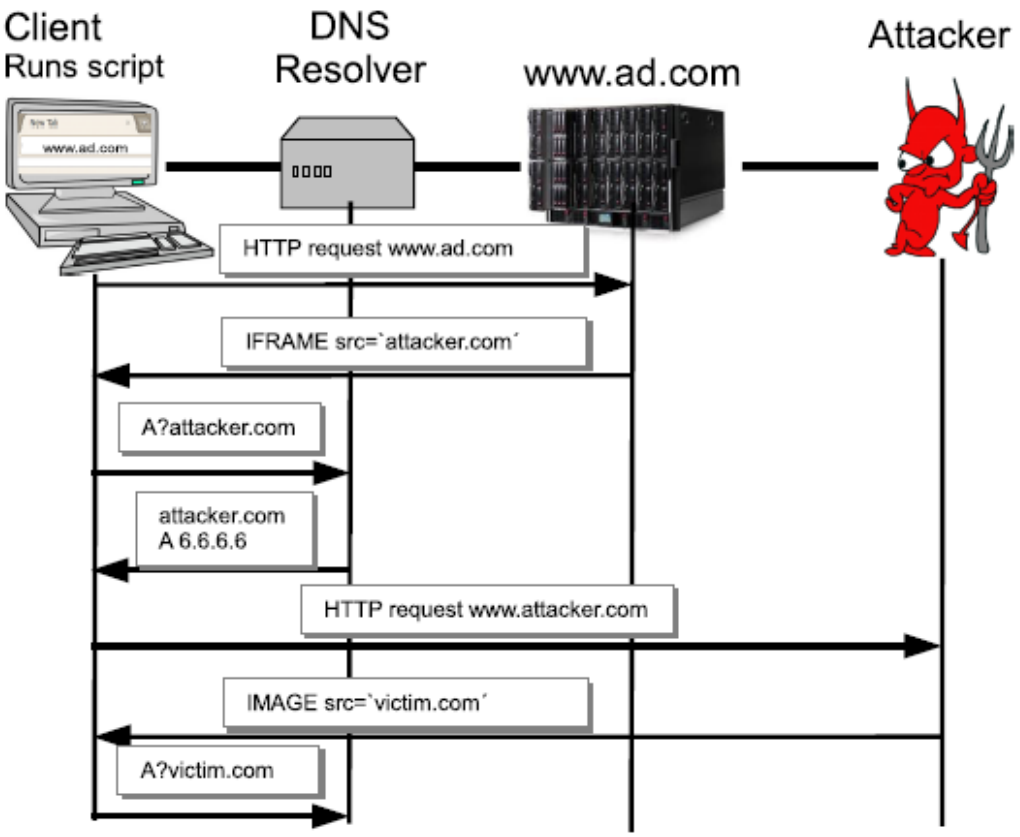

Fig 2: *a DNS hijacking attack* (Shulman & Waidner, 2014)

2.1.4 SNIFFING

Unencrypted data sent over the network may be intercepted and used to gain unauthorized access to web server. (Guru99, 2015)

2.1.5 PHISHING

In this type of attack, the victim is led to believe that he or she is on a website which is true or real when in fact it is just a copy of the real one but not true. It means it is the fake presence of showing the look as same as the trusted web domain. This type of attack mainly targets the official email and high profile identity.

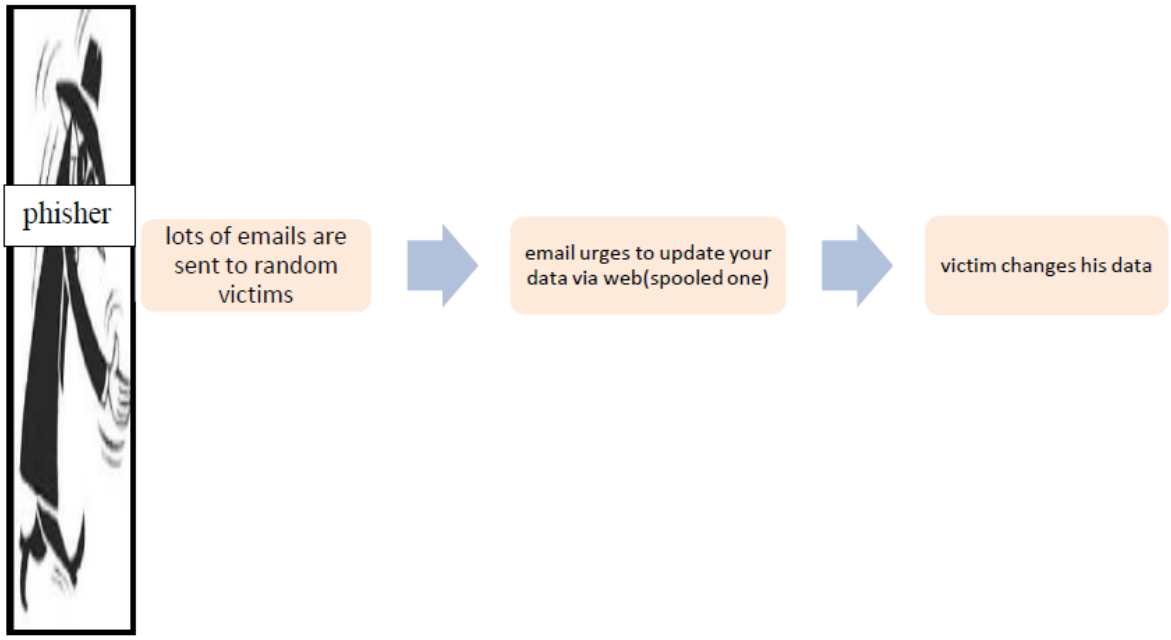

Fig 3: *Phishing process* (Chhikara, Dahiya, Garg, & Rani, 2013)

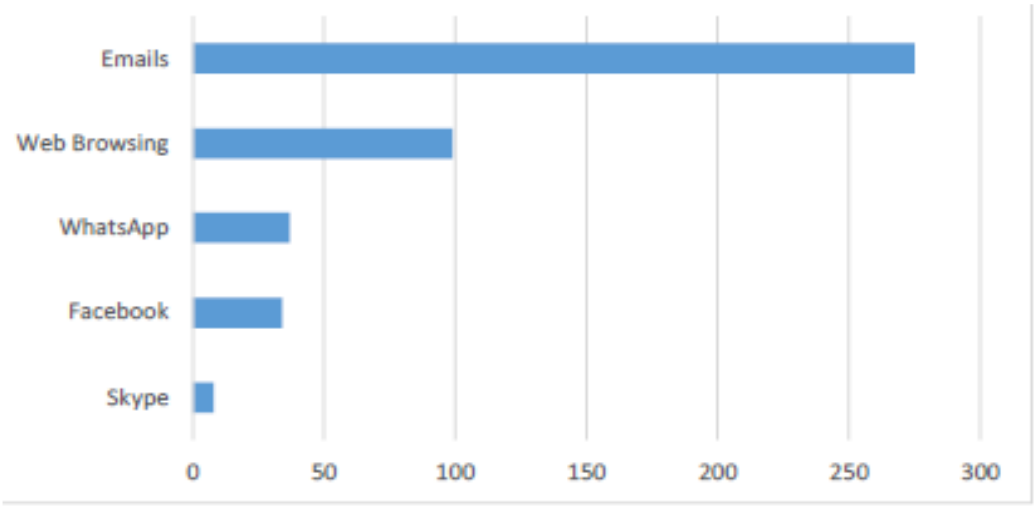

Fig 4: *phishing attack per service* (Yeboah-Boateng & Amano, 2014)

2.1.6 PHARMING

This is the exploitation of vulnerability in Domain Name Services (DNS) server software that allows a hacker to redirect a website's traffic to another website. This is an instant scamming practice in which malicious code is installed on a person's computer or server misdirecting users to fraudulent websites without knowledge or consent. For e.g imagine whenever a user wants to go to his bank, he picks up a phone directory and looks up for his bank's address, he goes directly to his bank account. In pharming, attackers replace the phone book with a fake one they created.

2.1.7 DEFACEMENT

With this type of attack, the attacker replaces the organization's website with a different page that contains the hacker's name, images and may include background music and messages. (Guru99, 2015)

2.1.8 PROFILING

Profiling or host enumeration is an exploratory process used to gather information about your website. An attacker uses this information to attack known weak points. (Meier, et al., 2006). The common vulnerabilities that make the server susceptible to profiling are: Unnecessary protocols, open ports, web servers providing configuration information in banners. The common attacks used for profiling are: port scans, ping sweeps.

2.1.9 UNAUTHORIZED ACCESS

Unauthorized access occurs when a user without correct permissions gains access to restricted information or performs a restricted operation. The vulnerabilities are weak IIS Web access controls including web permissions, weak NTFS permissions.

2.1.10 ARBITRARY CODE EXECUTION

Code execution attacks occur when an attacker runs malicious code on your server either to compromise server resources or to mount additional attacks against downstream systems. (Meier, et al., 2006). The vulnerabilities are weak IIS configuration, unpatched servers.

2.1.11 ELEVATION OF PRIVILEGES

Escalation of privileges requires a malicious user to either already possess or gain through unlawful methods authorization privileges of a regular user. This occurs when an attacker runs code by using a privileged process account. The vulnerabilities are over-privileged process account, over-privileged service account.

Table 1. Types of Security breaches

CATEGORY	DESCRIPTION
Denial of Service (DoS)	In DoS attacks, the attacker sends large number of information requests to the web servers of target company. The purpose of this attack is to overload the web servers and make the websites unavailable for legitimate use. This type of security breach is important especially for companies that depend highly on their web presence for revenue generation (e.g pure e-commerce firms). However, the consequences of this attack rarely results in loss of confidential data.
Unauthorized access to customer data	In this attacks, unauthorized individuals gain access to customer data. This can be accomplished physically through theft of a laptop, hard disk drive, back up types, or electronically through accessing the target company's network. Depending on the target company, the customer data can be names, addresses, birthdates, credit card details, social security numbers, medical records, online purchasing behaviour etc. These types of attacks are mostly considered as breach of confidentiality and can have negative effect on customer loyalty regardless of business type or business type or industry membership.
Unauthorized access to employee data	This type of security breach is similar to unauthorized access to customer data. Using similar strategies, the attacker can gain access to confidential employee data including names, social security numbers, salary information etc. However, the scale of these attacks is smaller. That is, the number of employees affected from such a breach is considerably smaller than the thousands (and sometimes millions) of customers getting affected from an unauthorized access.
Unauthorized access to company data	Company data can be a design of a new aircraft, source code of an operating system, portion of an upcoming movie or computer game, documents of a company acquisition report etc. Depending on the sensitivity of the data, these security breaches can significantly hurt a company's competitive advantage and consequently its existence.
Website alteration/defacement	In these attacks, the attacker gains access to the web servers of a target company. Afterwards, the attacker can alter the website with a message, logo or inappropriate material, or delete all the files and completely shut down the website. Similar to DoS attack, website alterations are important especially for companies that depend on their web presence for revenue generation.

The Target	**Date of Attack**	**Details**
Tunisian Government Websites	3 January 2011	Web site outage that included the president, prime minister, ministry of industry, ministry of foreign affairs, and stock exchange
FINE GAEL's News Website www.finegael2011.com	9 January 2011	One-night content outage by an anonymous attacker using the LOIC tool
Egyptian government Websites	25 January 2011	Site went offline from the beginning of the revolution until the president stepped down
HB Gary Federal	5-6 January 2011	Hacked by dumping 68,000 e-mails from the system
Operation Ouraborus	16 February 2011	Threats from an anonymous attacker who hacked the site and caused irreversible damage
NEW YORK (CNN Money)	3 March 2011	The huge attack hit the company's data centres with tens of millions of packets per second
Operation Empire State Rebellion	14 March 2011	Threat from anonymous attacker affecting the Bank of America
Operation Sony	April 2011	Outage of the play Station Network

Spanish Police	12 June 2011	DDoS attack lasted for approximately one hour
Operation Malaysia Malaysia.gov.my	15 June 2011	Outage of 91 websites of the Malaysian Government that started
Operation Orlando	16 June 2011	Orlando government Web sites went offline daily because of LOIC tool
Visa Card, Master Card, Wikileaks and www.paypal.com	27 July 2011	Payment processing fromWikileaks through Paypal were continuously denied
Hong Kong stock exchange	15 August 2011	Hundreds of companies were affected with a single target
Justice gov,MPAA.org, White House, the FBI, BMI.com, Copyright.com,Viacom,Anti-piracy.be/nl,Vivendi.fr, Hadopi.fr, and ChrisDodd.com	19 January 2012	The largest attack for 2012 from an anonymous attacker who shut down all the affected sits for 10 minutes

Source: Esraa Alomari, Selvakumar Manickam, B. B. Gupta, Shankar Karuppayah, Rafeef Alfaris **Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art** *International Journal of Computer Applications (0975 – 8887) Volume 49– No.7, July 2012*

2.2 WEB SERVER VULNERABILITIES

Web server vulnerabilities are those weak points of a web server that makes the web server easily attacked. These vulnerabilities are: Default settings, Misconfiguration of operating systems and networks, Bugs in the operating system and web servers, Lack of security policy and procedures. (Rouse, 2015)

2.2.1 DEFAULT SETTINGS

The settings such as default user id and passwords can be easily guessed by the attackers. Default settings might also allow the performance of certain tasks such as running commands on the server which can be exploited. (Guru99, 2015)

2.2.2 MISCONFIGURATION OF OPERATING SYSTEMS AND NETWORKS

Certain configurations such as allowing users to execute commands on the server can be dangerous if the user does not have good password. (Guru99, 2015)

2.2.3 BUGS IN THE OPERATING SYSTEM ND WEB SERVERS

Discovered bugs in the operating system or web server software can also be exploited to gain unauthorized access to the system. (Guru99, 2015)

2.2.4 LACK OF SECURITY POLICY AND PROCEDURES

Lack of security policy and procedures such as updating antivirus software, patching the operating system and web server software can create security loop holes for attackers. (Guru99, 2015)

Aside the web server vulnerabilities, we also have the web application vulnerabilities which are Remote code execution, SQL injection, Format string vulnerabilities, Cross Site Scripting (XSS), Username enumeration. But in this work, we are concerned with web server.

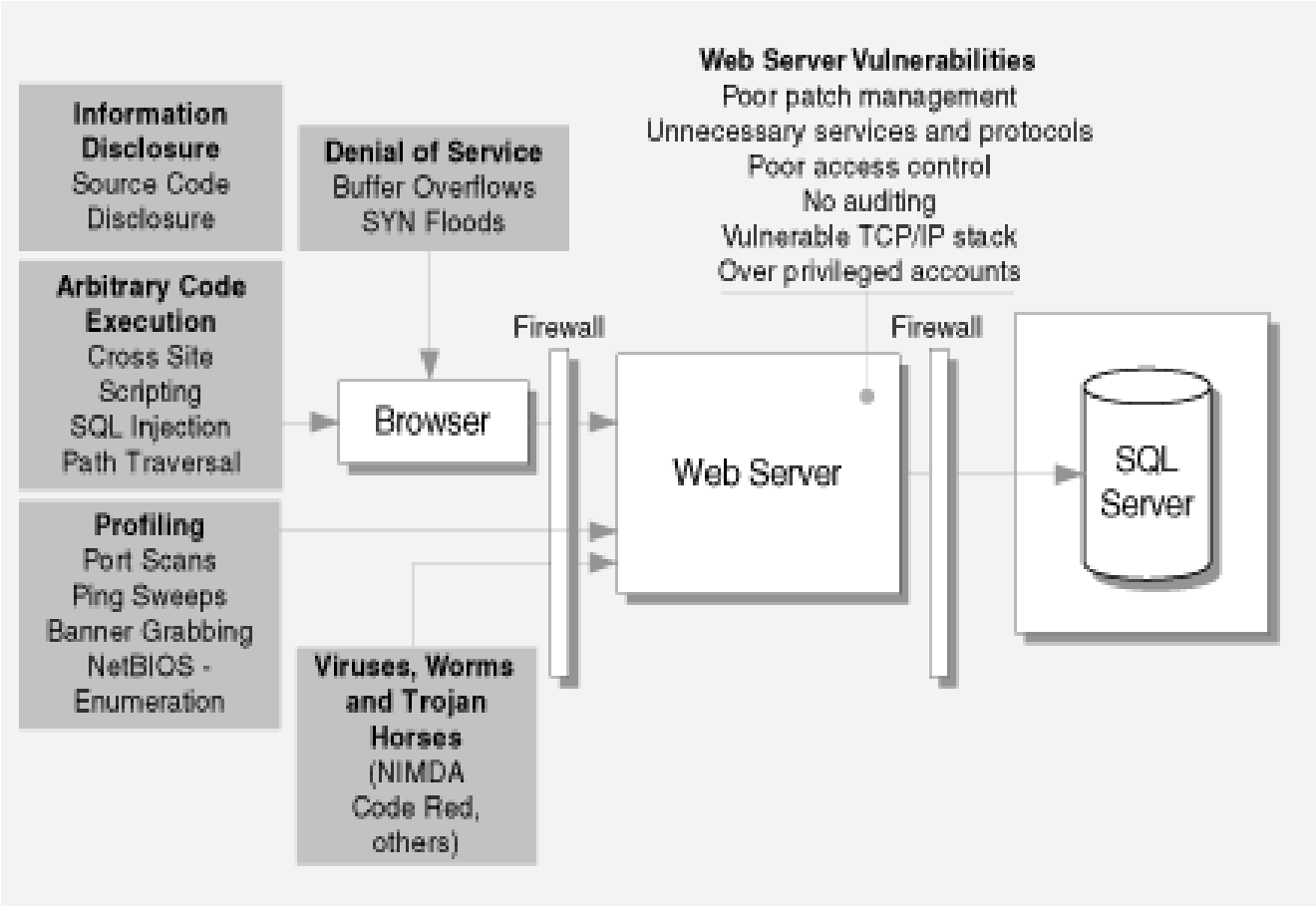

Fig 5: ***a diagram showing the web server security challenges, vulnerabilities and a configured firewall for protecting against illegal entry.*** *(Meier, et al., 2006)*

2.3 DIFFERENT WEB SERVER ATTACKS OVER THE YEARS.

In June 2014, the web servers of J.P. Morgan at chase.com and jpmorgan.com was compromised in a cyber security attack. This resulted in the loss of contact information of 76m household and 7m business former and current customers who had accessed the website either through the mobile or web platforms. Data lost to the thieves include names, email addresses, phone numbers and postal addresses. Financial information such as date of birth, social security number or bank account numbers however were compromised. This is said to be a profiling attack.

In August 2013, part of a Chinese internet went down early Sunday morning. The attack began at 2a.m and was followed by a more intense attack at 4a.m. This attack was aimed at the registry that allows users to access the site with the extension ".cn," and resulted in the shutting down of the registry for about two to four hours. This is said to be a Denial of Service (DoS) attack.

In August 1999, a DDoS attack occurred against a University and shut down the network for over two days.

In February 2000, a number of websites went offline for several hours after a DDoS attack.

In May 2001, the coordination center of the Computer Emergency Response Team was attacked making the availability of their website intermittent for more than two days after a DDoS attack.

In October 2002, all root name servers underwent an exceptionally intensive DoS attack with non-received DNS requests to an outsourced DNS service in Akamai, which were meant to enhance service performance.

In 2004, UK online bookmaking, betting and gambling sites were overwhelmed by DoS attacks launched by unidentified attacks.

In March 2006, a text-to-speech translation application in the Sun Microsystem's Grid computing system was disabled during its opening day by a DoS attack.

Table 2. a table showing the different documented web server attacks, date of occurrence, description of attack and its effects.

TYPE OF ATTACK	DATE OF ATTACK	DESCRIPTION OF ATTACK	EFFECT OF ATTACK
Profiling	June 2014	The web servers of J.P. Morgan at chase.com and jpmorgan.com was compromised in a cyber security attack	This resulted in the loss of contact information of 76m household and 7m business former and current customers who had accessed the website either through the mobile or web platforms. Data lost to the thieves include names, email addresses, phone numbers and postal addresses. Financial information such as date of birth, social security number or bank account numbers however were compromised
Denial of Service (DoS)	August 2013	Part of a Chinese internet went down early Sunday morning. The attack began at 2a.m and was followed by a more intense attack at 4a.m. This attack was aimed at the registry that allows users to access the site with the extension ".cn,"	Resulted in the shutting down of the registry for about two to four hours.
Distributed Denial of Service (DDoS)	August 1999	Attack occurred against a University	Shut down the network for over two days.
Distributed Denial of Service (DDoS)	May 2001	The coordination center of the Computer Emergency Response Team was attacked.	Made the availability of their website intermittent for more than two days after a DDoS attack.
Denial of Service (DoS)	October 2002	Attack aimed at the root servers	Root name servers with non-received DNS requests to an outsourced DNS service in Akamai, which were meant to enhance service performance
Denial of Service (DoS)	March 2006		A text-to-speech translation application in the Sun Microsystem's Grid computing system was disabled during its opening day.

3.0 CONCLUSION

The web has become the main target for numerous attacks originating from adversaries who attempt to monetize a user's sensitive data and resources. This paper laid emphasis on the different web server security challenges and vulnerabilities. Also, a detailed list of web application vulnerabilities were stated. In spite the fact that web servers

are likely to prevent attacks by implementing security features, the presence of vulnerabilities still make such slightly impossible as it makes the web server susceptible to attacks.

4.0 References

Ali Alper Yayla, Q. H. (2016). *The impact of Information security events on the stock value of firms: the effect of contigency factors*. Retrieved from Palgrave macmillian: http://www.palgrave-journals.com/jit/journal/v26/n1/fig_tab/jit201043.html

Bhupendra Singh Thakur, S. C. (June 2013). Content Sniffing Attack Detection in Client and Server side: A Survey. *International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)Volume-3 Number-2 Issue-10* , 4.

BISSON, D. (2016, January 14). *THE STATE OF SECURITY*. Retrieved from tripwire: http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/ddos-attacks-increased-by-180-compared-to-2014-reveals-akamai-report

Cox, R. (2013, August 26). *5 Notorious DDoS Attacks in 2013: Big Problem for the Internet of Things*. Retrieved from siliconANGLE: http://siliconangle.com/blog/2013/08/26/5-notorious-ddos-attacks-in-2013-big-problem-for-the-internet-of-things

Esraa Alomari, S. M. (2012). Botnet-based Distributed Denial of Service(DDoS) Attacks on Web Servers: Classification and Art. *International journal of Computer Application (0975-8887)*, 9.

Ezer Osei Yeboah-Boateng, P. M. (2014). Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices. *Journal of Emerging Trends in Computing and Information Sciences*, 11.

GLAZER, E. (2014, October 3). *J.P. Morgan's Cyber Attack: How The Bank Responded*. Retrieved from THE WALL STREET JOURNAL: http://blogs.wsj.com/moneybeat/2014/10/03/j-p-morgans-cyber-attack-how-the-bank-responded

Guru99. (2015, September). *How to hack a Web Server*. Retrieved from Guru99 Website: http://www.guru99.com/how-to-hack-web-server.html

Haya Shulman, M. W. (2014). DNSSEC for cyber forensics. *Shulman and Waidner EURASIP Journal on Information Security* , 14.

Ibrahim S. Alfayoumi, T. S. (2015). Client- Side Pharming Attacks Detection using Authoritative Domain Name Servers. *International Journal of Computer Applications (0975-8887) Volume113*, 6.

Jyoti Chhikara, R. D. (2013). Phishing & Anti-Phishing Techniques: Case Study. *International Journal of Advanced Research in Computer Science and Software Engineering*, 8.

Meier, J., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R., & Murukan, A. (2006). Improving Web Application Security: Threats and Countermeasures. In J. Meier, A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla, & A. Murukan, *Improving Web Application Security: Threats and Countermeasures* (p. Chapter 16). Microsoft Corporation.

Ms. Ritu Royal, D. P. (January 2012). DETECTING AND PREVENTING WEB ATTACKS BY FILTERS. *International Journal of Enterprise Computing and Business Systems*, 16.

Patrikakis, C., Masiko, M., & Zouraraki, O. (2004). Distributed Denial of Service Attacks. *The Internet Protocol Journal*.

Rouse, M. (2015, September). *What is web server security?* Retrieved from TechTarget: http://searchsecurity.techtarget.com/definition/web-server-security

Shulman, H., & Waidner, M. (2014). DNSSEC for cyber forensics. *EURASIP Journal on Information Security*.

Sumit Siddharth, P. D. (2006, April 27). *Five common Web application vulnerabilities*. Retrieved from Symantec: http://www.symantec.com/connect/articles/five-common-web-application-vulnerabilities

Tan, F. W. (May 2014). A SRVEY OF TRENDS IN MASSIVE DDOS ATTACKS AND CLOUD-BASED MITIGATIONS. *International Journal of Network Security & Its Applications (IJNSA), Vol 6.No 3*, 15.

Vina M. Lomte, P. D. (October 2012). A Secure Web Application: E-Tracking system. *International Journal of UbiComp(IJU), Vol. 3, No. 4*, 18.

Yeboah-Boateng, E. O., & Amano, P. M. (2014). Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices. *Journal of Emerging Trends in Computing and Information Sciences*.