International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 12
August 2016

Analysis of Possible Security Threats to Web Servers on the Internet and Countermeasures.

[1]Amadi E. C., [2]Enyia E.C., [3]Nwamara O.E., [4]Mbara E.I.
[1-4] Department of Information Management Technology, Postgraduate School, Federal University of Technology Owerri.
brainnoble21@yahoo.com, emmanuel.amadi@futo.edu.ng

Abstract
While Web server security continues to increase in sophistication to protect against threats, web servers on the internet have been faced with series of renewed attacks with high level of sophistication, bringing down even the most secured servers. Generally, the web is an open environment and has been termed as unsecured making IT experts continuously worried about what thy place on web servers running on the internet. It is therefore imperative that web servers on the internet are secured o a very large extent to militate against attacks which are inevitable. In this paper, we consider possible security threats to web servers on the internet and counter measures to these attacks. These threats could be internal or external. An overview of major attacks that has occurred over the years on web servers was also reviewed.

Keywords: Internet, Web server, Security threats.

1- Introduction:

People use the internet for various reasons such as e-commerce and online communication. One of the major concerns when purchasing and communicating online is web server security (Dhillon and Backhouse, 2000). A web server is an information technology that processes requests via HTTP, the basic network protocol used to distribute information on the World Wide Web. The term can refer either to the entire computer system, an appliance, or specifically to the software that accepts and supervises the HTTP requests. The HTTP (or HTTPS) protocol is a protocol used mainly to access data on the World Wide Web (www.mhhe.com/forouzan). HTTP is the standard that makes it possible to transfer web pages via a request and response system .mainly used to transfer static web pages, that web has quickly become an interactive tool making it possible to provide on-line services.

Attacks with criminal motives of intentional harm to the victim system evolved from simple spoofing other's password to the complicated Web-based attacks. Because more and more systems are reliant upon the Web server to get and exchange information through the Internet, Web-based attacks have become an important subject in the security field. In addition, defending against Web-based attacks has become increasingly complex and hard, and intruders try to bypass the traditional attack path. Web-based attacks expose the vulnerability of the victim system and spread malwares to other hosts communicating with the victim system.

The current study discuss in details possible security threats, its types and Network/security issues related to it. A web server faces some attacks that are: distributed denial off service attack, cross site scripting , SQL injection, malicious file execution, insecure direct object reference, cross site request forgery, information leakage and improper error handling, broken authentication and session management, insecure cryptographic storage, and failure of restrict URL access.

2- Security Threats:

Information security is concerned with the protection of three characteristics of information: confidentiality, integrity, and availability through the use of technical solution and managerial actions (Gordon and Loeb, 2002).All internet enable computers have vulnerabilities; these vulnerabilities create opportunities for

possible threats to the web server. Web server security threats can be classified into several categories from internal to external, human or non-human, and intentional or non-international (Loch, et al, 1992; Whitman, 2003). When these threats happen it can lead to the possibilities of disclosure, modification, destruction, or denial of use of that information.

There are various threats to information security that protectors of web servers must be aware of and account for. The table1 list many threats to a web server but is not exhaustive of all possible threats that may exist

Table1: Web Server Security Threats

Attack source		Accidental	Intentional
Internal	Human	• Acts by employees. • Accidental entry bad data. • Accidental destruction of data by employees. • Administrative Procedures. • Weak/ineffective physical control.	• Acts by employees. • Intentionally destroy data by employee. • Intentional entry of bad data by employees. • Unauthorized access by employees.
Internal	Non- Human	• Mechanical and Electrical faults • Web Application Program problems	• Mechanical and Electrical Faults. • Web Application Program Problems
External	Human	• Competitors • Media	• Hackers. • DDOS Attacks • Social Engineering
External	Non- Human	• Fire. • Wind • Water and other Natural disaster	• Computer Virus • Worms • Trojan • Spyware

Research has shown that more than two thirds of all Americans view external threats such as hackers and cyber criminals, as a higher risk to security than internal threats (McCrohan, 2003). Furthermore, it was reported that between 50 and 75 percent of all security related incidents originated from within the organization (D' Arcy et al, 2009). Most organization often emphasize the need for security measures concerning external threat over internal threats which has resulted to accidental or intentional attack on the web server,

3- Internal threats

Internal threats can steam from three areas: the application development department, the infrastructure, and the data center (Hyle, 2006). Threats halting from the application department could result from logical error in the applications developed by the project programming team. An application that is not programmed correctly could potentially cause vulnerabilities in the security mechanisms of a web server allowing unauthorized individuals to access private information. An organization's infrastructure has a major security implication by determining access level and privileges granted to employees. When access is granted to information that is unrelated to an employee's job functions, it increases the probably of user compromising the data either intentionally or unintentionally. Data centers are the biggest internal threat of a web server attack, because users enter,

delete, and maintain important company data.

Most internal threats occur because of the following reasons:

a. A lack of security common sense.
b. Staff not applying security procedures
c. Taking inappropriate risks
d. Deliberate acts of negligence
e. Deliberate attacks

Most organization often address these internal security issues through security awareness and training, also organization should conduct security audits to ensure employees are following proper procedures.

4- External threats:

These can cause serious setback to any organization. External threats may include hacker, viruses, denial of services attacks and even natural disasters. In February 2015, 78 million records were exposed in a major data breach at Anthem, the second largest healthcare providers in the US (www.symantec.com/2016 internet security threat report). Symantec organization was able to trace the attack to a well-funded attack group, named Black vine, that has associations with a China-based IT security organization, called Topsec. Black Vine is responsible for carrying out cyberspionage campaigns against multiple industries, including energy and aerospace, using advanced, custom- developed malware.

Other high-profile targets of cyberespionage in 2015 included the White House, the Pentagon, the German Bundestage, and the US Government's office of personal management, which lost 21.5 million personal files, including sensitive information such as health and financial history, arrest records, and even fingerprint data. Accidental leaks of corporate information are another risk that could result in bad publicity through the news media or other outlets damaging the reputation of the organization. Intentional web server attack has been a major concern to most organization; Table 2 shows Botnet-Based DDoS attack incidents 2011-2012

Table 2: shows Botnet-Based DDos attack incidents 20011- 2012

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 web site www.finegael 2011.com	9 January 2011	One-night content outage by an anonymous attacker using the LOIC tool
Egyptian government Web sites	25 January 2011	Site went offline from the beginning of the revolution until the president stepped down,
HB Gary Federal	5-6 February 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 center with tens of millions of packets per second.
Operation Empire State Rebellon	14 March 2011	Threat from an anonymous attacker affecting the Bank of American.

Operation Sony	April 2011	Outage of the Play Station Network
Spanish Police	12 Jun 2011	DDoS attack lasted for approximately one hour.
Operation Malaysia Malaysis.gov.my	15 Jun 2011	Outage of 91 websites of the Malaysian Government that started 7:30pm GMT
Operation Orlando	16 Jun 2011	Orlando government web sites went offline daily because of the LOIC tool.
Visa Card, Master Card, Wikileaks and www.paypal.com	27 July 2011	Payment processing from wikileaks 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 ChristDodd.com	19 Jan 2012	The largest attack for 2012 from an anonymous attacks who shut down all the affected sites for 10 minutes.

Source:(International Journal of computer Application (0975- 8887) volume 49-no7,July 2012)

From the chart below, when we compared 2015 year's data to 2013, 2014 year's data, we saw that the total number of attacks in 2015 was significantly higher than the previous year (see below). Conventional web attacks from XSS and SQLi rose by 200% and 150% respectively continuing the trend from 2013 and 2014, with larger numbers and larger volumes of scanning campaigns across the Internet.

Half of the applications analyzed were the target of more than 20 SQLi attacks within a six-month period. In terms of attack magnitude, the typical SQLi attack included 72 malicious requests, with the most intensive SQLi attack detected by our sensors amounting to 400,000 malicious requests. Additionally we found that Remote Code Execution attacks, in particular Shellshock, were launched against all of the applications in the research, with the typical application getting RCE-attacked 112 days over the report period, averaging more than four days per week. The volume and persistency of attacks indicate industrialization of and automation behind organized efforts.

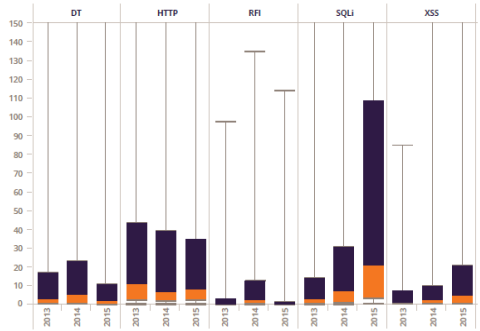

Figure1: comparison of number of incidents between years.

Source: (2015 Web Application Attack Report (WAAR) Imperva)

The attraction of attackers to CMS applications (which are attacked 3 times more often than non-CMS applications) and in particular to WordPress is not new. CMS frameworks are mostly open source, with communities of developers continuously generating sequences of plugins and add-ons, without concerted focus towards security. This developer model constantly increases the vulnerabilities in CMS applications, especially for WordPress which is also PHP based. We found that WordPress was attacked 3.5 times more often than non-CMS applications. Typically, WordPress and other CMS applications are derived from a common template, enabling automated scanning attacks that work effectively on multiple sites.

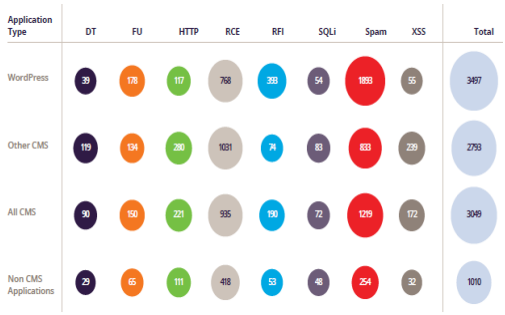

Figure 2 Attacks incidents Average per Application for CMS Slices

Unsurprisingly, the number of RFI attacks in WordPress (on average 393 per application during the report period) is significantly higher than the non-CMS applications, most probably due to WordPress being PHP based. This trend was first observed in our 2013 "CMS Hacking" research and was also confirmed by the Verizon DBIR 2014 report.
Healthcare web applications suffer substantially more XSS attacks than other sectors. When excluding SPAM and RCE, 57% of the attacks are XSS, significantly more than other sectors (with only 1%–16%). The average number of XSS attacks in the healthcare sector is almost 10 times higher than the other industries. Healthcare is possibly attractive for hijacking sessions through XSS, for the sake of stealing Personal Identifiable Information (PII).

5- Web server Attacks:
Vulnerabilities in a web server can cause the following attacks:

a. **Cross Site Scripting (XSS) :** XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that XSS allows attacks to execute script in the victim's browser which can hijack user sessions, deface web sites, possible introduce worms, etc.

b. **Injection Flaws:** injection flaws, particularly SQL injection, are common web applications. Injection occurs when users-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

c. **Malicious File Execution:** Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML any framework which accepts filenames or files from users.

d. **Insecure Direct Object Reference:** A direct object reference occurs when a developer exposes a reference to Attackers can manipulate those references to access other objects without authorization.

e. **Cross Site Request Forgery (CSRF):** A CSRF attacks forces a logged-on victim's browser to send a pre- authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker, CSRF can be powerful as web application that it attacks.

f. **Information Leakage and Improper Error Handling**: applications can unintentionally leak information about their configuration, internal workings or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks.

g. **Broken Authentication and session Management:** Account

credentials and session tokens are often not properly protected, Attackers compromise passwords, keys or authentication tokens to assume other users' identities.

h. Insecure Cryptographic Storage: Web applications rarely use cryptographic functions properly to protect date and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.

i. Insecure Communications: Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communication.

j. Failure to Restrict URL Access: Frequently, an application only protects sensitive functionality by preventing the display of links or URLS to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly. The following tables below shows analysis of eight (8) web attacks.

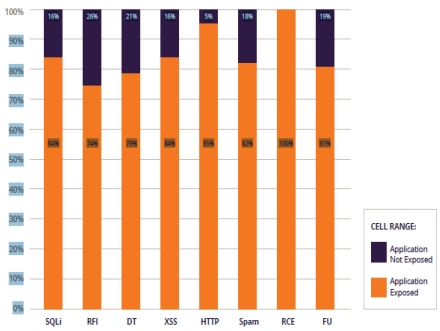

Figure 3 web Application Malicious Traffic Exposure Ration

Each of the attack types has at least 74% popularity, i.e., essentially at least three out of four applications were exposed to attack attempts of this type during the report period.

The most popular attack was Remote Code Execution, with attack attempts on every single application we examined. In Figure 4 above, we present a comparison of the different kinds of attack. The diagram shows the likelihood of an application to get malicious traffic of a certain type along a period of six months. On the other hand, RFI, Spam, and Directory Traversal attacks were seen in fewer applications than the previous year. Spam attacks are still widely used, but they are not spread among all applications. Instead, they focus on specific segments.

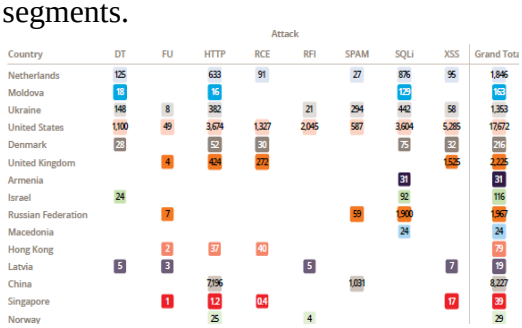

Figure 4: Number of Request per country for each attack type

Source: (Retrievedfromhttp://data.worldbank.org/indicator/IT.NET.USER.P2)

Figure 5 Shows Number of Host Per country for each attack

Source: (Retrieved fromhttp://data.worldbank.org/indicator/IT.NET.USER.P2)

6- Security Measures:

A variety of security threats were discussed, many threats can be minimized or prevented through various procedures. For instance, the threats of user errors could

be minimized with validation procedures upon data entry and increased training for information users.

Organization must take preventative measures to protect their sensitive corporate information. This includes information about the organization strategy, client information, financial information or any important information that could be damaging to the organization and its reputation. Oppliger (2003) operationalized security into five aspects

- Security Policy
- Host Security
- Network Security
- Organizational Security
- Legal Security

Addressing each aspect of security individually, organization must collectively work together to provide security and manage vulnerabilities to corporate information.Each of these operationalization of security will be defined next

a. Security Policy: Policies govern behaviors serving as a guide in the decision-making process when using a system (Sloman, 1994). Is important that organizations inform their staff of these systems what activities are acceptable and what activities are not. When evaluating security policies and procedures, there are two aspects that organization typically follows: descriptive and prescriptive. The descriptive aspect involves making employees aware of the policies and procedures while the prescriptive aspects requires employees to internalize and follow the security guidelines (Siponen and Kajava, 1998).
b. Host Security: includes the authentication of users, effective control and access to system resources, securely storing data, and audit trial of the information being access (Oppliger 2003).
c. Network Security: Network security may include passwords, authentication, firewalls and proxy servers among other things
    a. Newhouse (2007) discusses six resolutions to creating a secured network
        - Change password Quarterly
        - Download Patches and updates
        - Hire a hacker
        - Monthly Risk Assessments
        - Communicate and Review data Security Policy
        - Keep Network Virus Free

In all, organization must continuously review the security policy and make sure the employees are aware of what these procedures are.

d. Organizational Security: Most threats attack to a web server comes from the user. Hackers often try to exploit users through tactics known as social engineering (Winker and Dealy, 1995). Organization should train users and make them aware of policies, procedures, and vulnerabilities to information and security.
e. Legal Security: consist of legal actions to be taken against an attacker with the possibility of prosecution (Oppliger, 2003). Organization should have consequences in place to deter potential threat agents from compromising the organization's information. These consequences act as inhibitors decreasing the motivation of threat agents to violate security procedures. Legal security should be embedded within the organization security procedures and should be made aware to the Staff and all agents associated with the organization.

7- Conclusion:

Various possible web server attacks and countermeasures for protecting webserver against those threats were evaluated; As attackers become more efficient at launching targeted high volume attacks across a wide range of application it has become imperative for organization to educate themselves on the threats at hand and take steps to prevent and mitigate them. For it has been shown that attacks on web servers are harmful since the give the organization a bad image. A successful attack can have any of the following consequences; website defacement, stolen information, modification of data, and particularly modification of users' personal data, web server intrusion. Organization running a web server on the internet should apply more security measures to curtail both the internal and external web server attack on the internet.

Reference

Brhrouz, A. Fourth Edition Data Communication and Networking

www.mhhe.com/forouzan/dcnsm

D' Arcy, J., and Hovan, A. and Galleta, D. (2009). User Awareness of Security

Countemeasures and Its Impact on Information System Misuse: A Deterrence

Apporach. Information Systems Research, 20 (1), 79-98.

Dhillon, G. and Backhouse, J. (2000). Information System Security Management in the

New Millennium, Communications of the ACM, 43(7), 125-128.

Gordon, L. and Loeb, M. (2002). The Economics of Information Security Investments.

ACM Transaction on Information and System Security, 5 (4), 438-457.

Hyle, R. (2006). The Oops Factor. TechDecisions, 8 (4), 20-24.

McCrohan, K. (2003). Facing the Threats to Electronic Commerce, Journal of Business

And Industrial Marketing, 18 (2), 133-145.

Oppliger, R. (2003). Security Technologies for the World Wide Web. 2nd ed. Boston:

Artech House.

Sloman, M. (1994). Policy Driven Management for Distributed Systems. Journal of

Network and Systems Management, 2 (4), 333-360.

Winkler, I. and Dealy, B.(1995). Information Security Technology?.... Don't Rely on it.

A Case Study in Social Engineering. Proceedings of the Fifth USENIX UNIX

Security Symposium, Salt Lake City, Utah, 1-6.

Inforgraphic. What Happen in an Internet Minute in 2016?

Https://t.Coli82WOZGOOR https://t.co/YQPBBUOCR

International Journal of Computer Application (00975-8887),

Volume 49-no7, July 2012.

www.Symaantech.com/2016 internet Security Threat report.

www.imperva.com/docs/HII_web_Application_ Attack_Report_Eds.pdf