International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12 – No. 3, June 2017 – www.ijais.org

Investigating Websites and Web Application Vulnerabilities: Webmaster's Perspective

Vincent Appiah
West African Center for Cell Biology of Infectious Pathogens
Department of Biochemistry, Cell and Molecular Biology
University of Ghana

Isaac Kofi Nti
Department of Computer Science
Sunyani Technical University
Sunyani, Ghana

Owusu Nyarko-Boateng
Innerjoy Digital Systems
Sunyani, Ghana

ABSTRACT
The Development in Information Technology (IT) have raised up a lot of fears about the risk to information concomitant with feeble IT security, including weakness to malware, attacks, virus and compromise of network systems and services. Anyone who goes on the net is vulnerable to security threats. Inadequate IT security may result in compromised integrity, confidentiality and the release of sensitive data to unauthorized persons. In most development communities and countries, IT vulnerability has become an important concept employed to guide the evaluation, design and targeting of programs. Remaining ahead of the ever-evolving threat of an information break on websites and web application necessitates conscientiousness on the part webmasters and heads of IT sections within an organization in understanding and anticipating the risks. This paper seek to examine the knowledge of webmasters and heads of IT sections on threats and vulnerabilities on the cyber world of selected institutions in Ghana through semi-structured questioners and one-on-one interview and proposed away forward in boosting the knowledge base of IT and Webmaster, hence contribute to the reduction of cyber-crime in the country and also outline some guidelines on how to surf the web safely to end-users. The survey showed that, on an average 47% of the respondent have little or no knowledge in at least one or more of the existing website vulnerabilities.

General Terms
Websites and web application vulnerabilities

Keywords
Website-Security, Web-application-Security, Security-risk, SQL-injection, Firewall, Intrusion-Detection-System, Web-security-vulnerability, Web-Vulnerabilities

1. INTRODUCTION
Most modern website and Web applications are employed to carry out most major tasks, which includes forms for collect personal, secret and private info such as health history, debit, credit and bank account info as well as user satisfaction criticism. The security of a computer system is important to offer protection to the systems and the data store in it, this has made computer security the most discuss topic in the IT world [1]. An essential fact in web applications and Internet security is that 100 % assurance that a computer system is reliable and confident is not possible [1]. Vulnerability on a website or in a web application on the internet may compromise all the sensitive data and continuously give report which consequences is damage of cost [2]. Website and web applications such as educational website, governments' website, healthcare application and financial applications interact with its backend (database) several times upon a client request and there is a compromised in the security of such website and web application it results in loss of information, financial loss, law suits and identity theft [3]. According to Web Application Security Consortium the security of website that are used to collect users data and web applications are of most important, a report from Web Application Security Consortium shows that 49 percent of web application has a high severity level vulnerabilities and 13 percent are exposed to security vulnerabilities automatically. This unsecure website and web application leads to the known security liabilities such as Cross-side scripting, sql Injection, security misconfiguration, cookie theft, self-propagating worm's attacks and session hijacking [3].

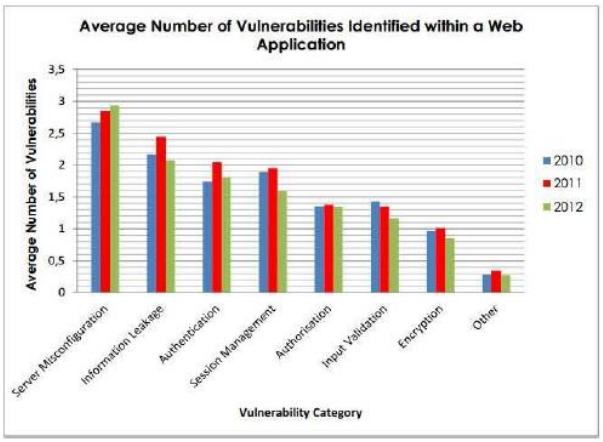

Figure 1 Average number of vulnerabilities within web application (Source: Chaudhari & Vaidya, 2014)

Figure 1 shows a graph of vulnerabilities within a web application from 2010 to 2012. From the graph in figure 1 it can be seen that this vulnerabilities in web applications is in a rise from year to year. Computer security is now employed in every field which deals with information processing and data storage. The use of debit, credit and ATM cards, and authentication mechanism and information access all encompasses computer security to safe guard the activities computer users and system [4].

In other to maintain a productive computing environment, computer security should be a priority. Cyber-crime is on the increase across the globe and as such organizations should

also protect their systems against such attacks [5]. In a report by [6] say that the government of Ghana official portal, which hosts fifty-Eight (58) websites of bureaus, departments and agencies was hacked by some unknown hacker and 11 website out of the 58 was under attached and substitute with a picture bearing a statement which reads "On us, the sword withdrawal of our homeland, unless entered, unless long suffering nation, unless anyone of us does damage to our homeland against our religion a bad idea to have all of the countries of virtual war will be opened in the Turks and tested my patience." The report attributed the hacked a software failure and vulnerability on the part of some webmaster and administrators to bring up to date their software. The Reports further indicated that the attacked was the 2nd time in 3 years that hackers have taken over the government website. This disastrous occurrences in Ghana has raised many queries with regards to the security of country's cyber space [6]. A Moroccan jihadist group hacked the websites of the KNUST, Ghana Post and some websites of the government were hacked, which included the website of the Registrar General's Department, The hacker introduced herself/ him as V3nom X, and marked the entire site of the registrar department with some symbol and words inscription "Security is just an illusion, wake up!!!' in print below the site [7]. In another report, shows that the website of the Electoral Commission (EC) of Ghana was under attacked by unknown hackers with the intention to change the electoral results with "fake results" of the just ended election conducted by the commission in December 2016, but the commission said the attacked did not materials even though the site went down for some period [8]. One way of ensuring protection is to identify such security flaws before the attackers does anything, but the increase in cyber-attacks raise a question whether the webmaster managing the various website of institutions in the country are abreast with the various cyber-attacks technologies. In view of this this research work seek to examine the knowledge of webmasters of twenty (20) randomly selected institutions in Ghana through semi-structured questioners and one-on-one interview and proposed away forward in reducing cyber-crime in the country.

2. STRUCTURE OF WEBSITE AND WEB APPLICATIONS

Figure 2, shows the basic business logic of a website and an internet application which has the client interface and the server end on a webserver and made known by a uniform resource locator (URL). The internet server is understood by its name. The browser (client) and server talk via a transport protocol TCP. Figure. 3 shows the fundamental architecture of data flow in website and a web application. The transport protocol is HTTP; the data format is Cascading style Sheets (CSS) and hypertext mark-up language (HTML). The user click or enters a URL to call the application or access the website [9]. A request via communication protocol is sent to the server from the clients. A script at the net server removes input from the consumer knowledge and creates a request to a backend application server, e.g. a mysql query to a database. The result is received from the backend by the webserver and returns a hypertext mark-up language (HTML) result page to the consumer. The result is displayed as a page by the client's browser. To show a page, the browser creates an interior picture for it. Captions should be Times New Roman 9-point bold. They should be numbered (e.g., "Table 1" or "Figure 2"), please note that the word for Table and Figure are spelled out. Figure's captions should be centered beneath the image or picture, and Table captions should be centered above the table body.

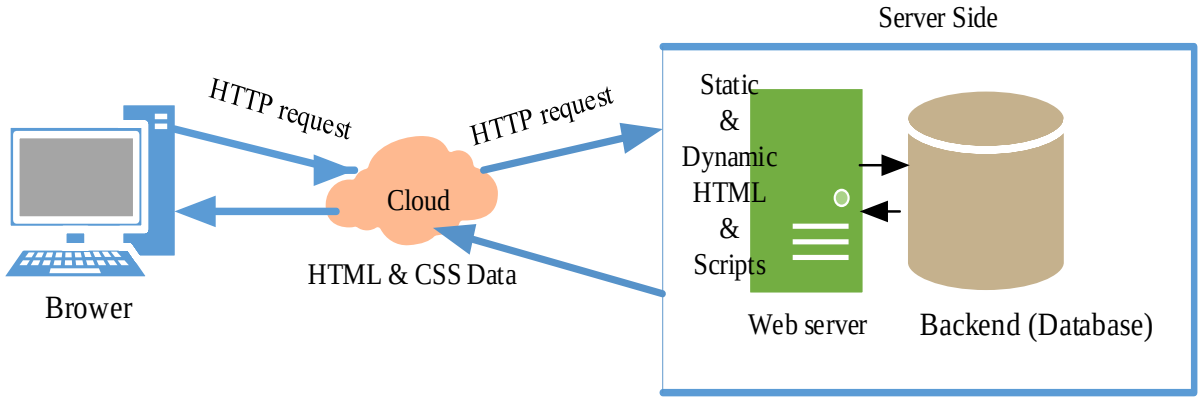

Figure 2 Architecture of Website/Web Application

2.1 Website Security Risks

The following section centers on areas that need to be observed from a technical perspectives by IT practitioners, in order to increase the reliability and security of all program and systems involved.

Websites now face a great deal of security risks. These risks can affect confidentiality, integrity or availability of data. Negative impact of some of these risks is very low while others can be very devastating. Some of the security risks are:

Buffer overflows

- ✓ Denial of service attacks (Dos)
- ✓ OWASP Top 10

2.1.1 Buffer Overflow

This is the situation where data being written by a program to a buffer is more than the capacity of the buffer. As a result the extra data flows to the adjacent memory locations. Buffer overflows occur due to deficiency in memory management implementations in a program such as bounds checking mechanisms. Programs that are written in C usually face this issue. For example if a program allocates 20 bytes to a memory buffer and attempts are made to store 25 bytes, the extra 5 bytes will flood to the adjacent buffer and this might cause the program to crash. If a data in that adjacent space it

might be overwritten. Buffer overflows can lead to the crashing of a program (denial of service) or insertion of a remote shell which can be used to execute arbitrary codes [10].

2.1.2 Denial of Service

This is an attack that renders an application or network unable to function properly. This is usually performed by sending several requests to the application. If the number of requests is more than it can handle, the application hangs and users will not be able to use the service. Buffer overflow attacks can also cause denial of service by flooding the memory with data.

A distributed denial of service is used to describe the situation where large numbers of computers are used to cause denial of service [11]. Denial of service attacks can take several forms which include:

- ✓ Buffer overflow
- ✓ Smurf attack
- ✓ Tear drop attack

Buffer overflow attacks are usually performed by sending data which is larger than the allocated memory buffer. As a result the extra bytes flood to adjacent buffers and the program crashes.

Smurf attack involves the attacker sending packets to a receiving machine. The request is then sent to all hosts on the network using the broadcast address. The packet then sent to the address indicated in the packet headers. This is usually the address of the target address (IP spoofing). Because this is a broadcast, all the hosts which received the request also send their response to the same address. If the packets are overwhelmingly large, then the target address is unable to receive all other incoming traffic.

The tear drop attack involves sending large packet data to the target machine. The Internet Protocol (IP) unable to handle reassembly of the packet fragments due to a confusing offset value eventually causes the system to crash.

2.1.3 Weakness of the Web Environment

Organizations have been solely dependent upon security measure at the perimeter of networks, such as firewalls and intrusion detection in order to protect IT infrastructures [12]. Nevertheless, now that numerous attacks are been geared towards security flaws in web design and web application, such as injection flaws, the traditional way of network security may not be adequate to safeguard web and web application and users [12]. Ten security risks has also been identified by Open Web Application Security Project (OWASP) as the most critical security risks associated with web applications. These risks are known to be common forms of attacks. Aside that they are known to be exploitable and can have a negative impact on websites when executed hence their rank as the top 10. The top 10 risks as published by OWASP are:

- Injection flaws
- Broken authentication and session management.
- Cross site scripting.
- Insecure direct object references.
- Security misconfiguration.
- Sensitive data exposure.
- Missing level access control.
- Cross site request forgery (CSRF).
- Using components with known vulnerabilities.
- Unvalidated redirects and forwards.

Injection Flaws: SANS institute explains that injection flaws occur when an unexpected data is sent by a malicious client. Injection flaws allow an attacker to inject code into the vulnerable computer system. If the injected code is executed, the effect can be disastrous. Aside from the stealing information, injection attacks can cause denial of service or multiplication of worms in a system. Injection attacks include SQL injection, OS injections and LDAP injections. Injection flaws occur when a user input is not properly filtered for string escape characters that are often embedded in SQL statements [13] [12].

Broken Authentication and Session Management: This is the second most common flaw in the OWASP top 10. This stems from the fact that flaws exist in session management implementations in web applications. Misconfigurations such as storage of passwords in plain texts or weak encryption of user credentials can lead to this form of attack. According to OWASP, flaws in the implementation of password management, logout mechanism, and timeout, remember me, forgot my password etc can also lead to broken authentication and session management attacks [11].

Cross-Site Scripting (XSS): This is a type of vulnerability in which malicious code injected by a client is executed by the web application. The execution is made possible because the web application is unable to properly filter input properly. This can lead to stealing of cookies, website defacement and session hijacking. XSS is amongst the most common vulnerabilities of web applications [3] [9] [12]. There are three main types of XSS and these are; Stored XSS, Reflected XX and DOM based XSS.

Insecure Direct Object References: This is where unauthenticated clients are given access to restricted resources such as directories and configuration files. An example is a situation where a directory or a password file that should be available to only administrators on network is exposed to other users on the network. The absence of access control check can often result in unauthorized access to such resources through manipulation of URL parameters [12] [13].

Security Misconfiguration: This flaw exists if web applications enable certain features by default. For example default passwords, default accounts, enabled directory listing, bugs in source codes and other misconfigured settings. Security misconfigurations can give way to external and internal attacks and according to OWASP can result in unauthorized access or complete system compromise. Secure configuration settings should be used to ensure use of web applications.

Sensitive data exposure: Sometimes sensitive data is left unprotected on web applications. These can be stolen or modified by attackers and used to gain access or perform unauthorized transactions. Using weak encryption schemes can also result in sensitive data exposure. Attackers can use brute-force to obtain the plain text. Also sensitive data can be

used to exploit the web application or find other exploitable vulnerabilities on the web application.

Missing Level Access Control: This occurs when users are not properly authenticated but given access to restricted resources. A web application must be able to limit and control the access to resources. If the application is unable to do this, then attackers can leverage this to gain access to restricted resources and even modify data on the server. This might affect the integrity of the data. There should be security checks to ensure that a user is properly authenticated and given the proper access rights especially if several users with different roles are exist on the web application [3] [1].

Cross-Site Request Forgery (CSRF): This is a type of attack where unauthorized HTTP requests are sent from a user's browser to a web application in which the user is currently logged on. In contrast to XSS, CSRF exploits the trust that a site has in a user's browser. Because there is trust, the web application is forced to execute these requests [3].

Using Components with Known Vulnerabilities: Applications with known vulnerabilities are likely to be compromised because exploits might be available. If such applications are compromised, an attacker might gain full access to the network and this will affect confidentiality.

Unvalidated redirects and forwards: This is due to improper validation / unvalidation of user data. Attackers can leverage this to redirect victims to malicious webpages as well. Also forwards can be used to access restricted pages. This can affect confidentiality of data.

Table 1 Examples of vulnerabilities

Hack attack	What hackers use it for
1. Cookie Poisoning	Session Take-over and personality theft
2. Hidden Field Manipulation	E-Shoplifting
3. Parameter Tampering	Scam
4. Buffer Overflow	Denial of Service/ Closure of Business
5. Cross-Site Scripting	Skyjacking/ Identity Theft
6. Backdoor and Debug Options	Intruding
7. Forceful Browsing	Entering and Transgression
8. HTTP Response Splitting	Personality Theft, Phishing and e-Graffiti
9. Stealth Commanding	Obscuring Weapons
10. 3rd Party Misconfiguration	Devastating a Site
11. Known Vulnerabilities	Taking control of the site
12. XML & Web Services Vulnerabilities	New layers of attack vectors & malicious use
13. SQL Injection	DB info Manipulation

Table 1 give a summary of some known hack attack executed by ill-intention personal on website and web application and what they seek to achieved.

3. TOOL AND METHODS

A non-probability random sample technique was adopted by this paper to provide a range of alternate techniques established on researchers' subjective judgment. Microsoft Excel and SPSS were used for analysis and interpretation of the collected data. Twenty (20) webmaster and IT personal from randomly selected schools, corporates and microfinance were defined as population of interest. The questions were characterized into two fragments. The demographic information (non-technical) of the webmaster's (respondents) is acquired in the first section whiles the second section (Technical) collects knowledge of webmaster's (respondents) on the above discussed website and web application vulnerabilities.

4. RESULTS AND DISCUSSION

The percentile age distributions of the twenty (20) webmasters and IT sectional heads is as shown in figure 3.

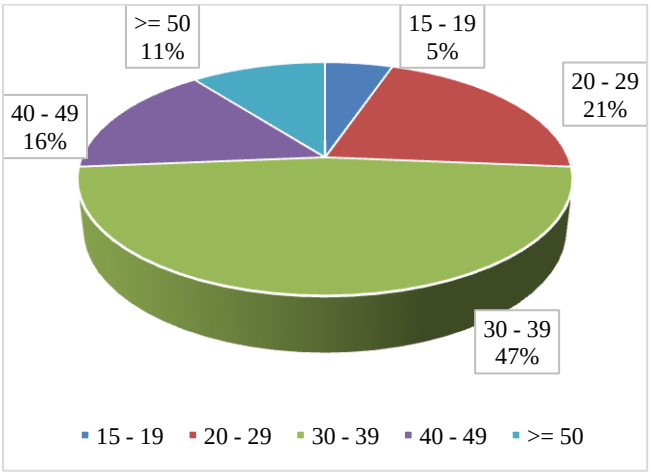

Figure 3. Age distributions of surveyed subjects

To give a good judgment in relation to the respondent years of practice and knowledge in current and existing website and web application vulnerabilities, respondents' years of practice in the field of IT were as shown in figure 4.

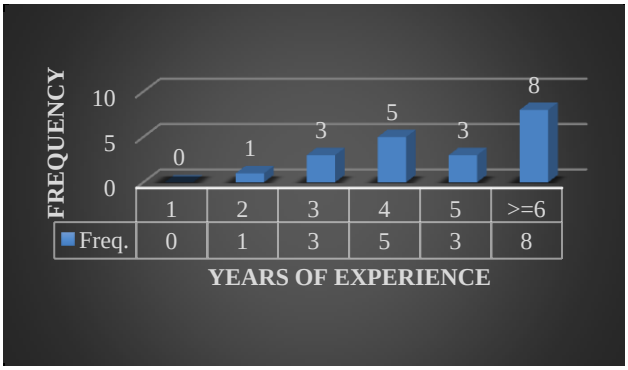

Figure 4 Bar chart of respondents' year of practice

From figure 4, Eight (8) respondent have been in practice for six year and above, three respondent in practice for five (5) year, five respondent in the service for 4 year, three for 3 year,

and one for 2 year respectively. Website and web application vulnerability knowledge by respondents. The knowledge of the respondent were tested against all the discussed cyber vulnerabilities.

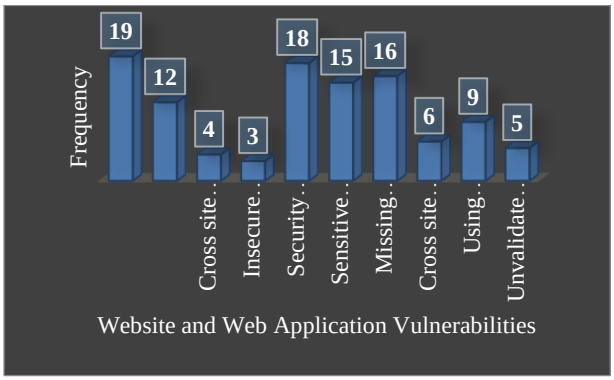

Figure 5 Website and web application vulnerability knowledge by respondents

It was overserved 95% representing 19 out of the 20 respondent interviewed had average knowledge on Injection flaws, with 60% representing 12 respondent hard knowledge Broken authentication and session management. Security misconfiguration scored 90%, that is 18 out of 20 respondents and it came to light that almost 95 % of this 18 people have in one way or the other encounter a problem with this vulnerability. Fifteen (15) out of the 20 respondent representing 75% are aware of Sensitive data exposure, on the other hand 16 out of 20 are aware of Missing level access control. Vulnerabilities such as Cross site request forgery (CSRF), using components with known vulnerabilities, Invalidated redirects and forwards, Cross site scripting and Insecure direct object references had 6,9,5,4,3 respectively out of the 20 respondents. Insecure direct object references recorded the lowest awareness of 15% implying that 85 % of webmasters and IT practitioners (respondents) have no knowledge about what insecure direct object references is.

How to protect yourself while surfing the web.
While end-users enjoys modern website and web application services, users should take adequate measures to protect themselves.

Common safety measures for end-users

- ✓ Don't use public computer, such café computer to login to critical or sensitive websites and web applications.
- ✓ Never cache your password and username on a computer
- ✓ Always do logoff at end of a session
- ✓ Don not use the same password for different websites and web application login details.
- ✓ Do regularly change your password for sensitive web application and websites.
- ✓ Immediate report and abnormalities in a website or web application service to the provider.
- ✓ Ensures that you have personal firewalls and anti-virus installed on your computer and they are up to date.

5. CONCLUSION AND RECOMMENDATION

The vulnerability assessment was helpful as it provided information about the level of understanding of webmasters and IT practitioners on the existing and current security issues associated with website and web application. It is therefore important to be abreast with these security issues, so that respondents will learn and know the techniques to combat these security threats. The survey showed that on an average 47% of the respondent have little or no knowledge on at least one or more or the existing website vulnerabilities.

In addition we notice that managerial issues or administration errors, such as the following contribute immensely to security threats.

- ✓ Mangers and webmaster of the institutions do not recognise that numerous security threats causes reduction of organization's reputation.
- ✓ Mangers of website don't consider the fact that the data on their websites is cost money, in addition to losing the ability of estimate the information cost.
- ✓ Most Mangers and webmaster depends on off the shell protection tool and software such as intrusion discovery system or firewall without doing regular monitoring them regularly and their websites.
- ✓ Because most institutions want to launch or re-launch their website as quickly as possible, well trained technical men are not given the website development contract due to cost (cheap labour) forgotten that there is a saying that says "if you think education is expensive try ignorance".

To have an effective and reliable secured website or web application, an implementation has to be done and it has to be done with attention, care and monitored and maintained. Based on the findings, it is recommended that:

- ✓ Management should organized refresher programs for their respective webmasters and IT personal to update their knowledge acquisition on current treats facing the cyberspace.
- ✓ Proper and adequate security measures should be in-place to protect organizational website, data and clients information from hackers.
- ✓ Websites owners must get in-line with industry standards, such as SSL/TLS implementation, and SHA-2 migration.

6. FEATURE WORK

The survey reveals that, the general knowledge of respondents (Webmaster and IT heads) on the various vulnerability is low, hence one can foresees that the websites and web application managed by these personnel's are exposed to this numerous vulnerabilities. In light of this our feature research will focus on vulnerability assessment for few selected sites to identify the vulnerability infections and proposed measure to alleviate these weakness to improve security.

7. ACKNOWLEGEMENTS

We would like to thank the Almighty God for His Grace and Protection.

8. REFERENCES

[1] A. Hesham and S. Mohammad, "Survey of Web Application and Internet Security Threats," International Journal of Computer Science and Network Security, vol. 12, no. 12, pp. 67-76, 2012.

[2] K. Durai and k. Priyadharsini, "A Survey on Security Properties and Web Application Scanner," International Journal of Computer Science and Mobile Computing, vol. 3, no. 10, pp. 517-527, 2014.

[3] X. Chaudhari and M. Vaidya, "A Survey on Security and Vulnerabilities of Web Application," International Journal of Computer Science and Information Technologies, vol. 5, no. 2, pp. 1856-1860, 2014.

[4] I. K. Nti, J. A. Ansere and A. Appiah, "Investigating ATM Frauds In Sunyani Municipality: Customer's Perspective," International Journal of Science and Engineering Applications, vol. 6, no. 02, pp. 59-65, 2017.

[5] F. Twum, K. Nti and M. Asante, "Improving Security Levels in Automatic Teller Machines (ATM) Using Multifactor Authentication," International Journal of Science and Engineering Applications, vol. V, no. 3, pp. 126-134, 2016.

[6] N. A. Acquaye, "Software vulnerability led to Ghana govt site hack," 2015. [Online]. Available: http://www.biztechafrica.com/article/software-vulnerability-led-ghana-govt-site-hack/9583/. [Accessed 1 November 2016].

[7] Ghanacelebrities.com, "Website of Registrar General's Department Hacked," 2014. [Online]. Available: http://www.ghanacelebrities.com/2015/12/15/website-of-registrar-generals-department-hacked/. [Accessed 03 May 2015].

[8] BBC, "Ghana election commission website hit by cyber-attack," 2016. [Online]. Available: http://www.bbc.com/news/world-africa-38247987. [Accessed 3 January 2017].

[9] D. Vandana, Y. Himanshu and A. Jain, "Web Application Vulnerabilities: A Survey," International Journal of Computer Applications, vol. 108, no. 1, pp. 25-31, 2014.

[10] H. Nemati, "Information security and ethics: concepts, methodologies, tools, and applications: concepts, methodologies, tools, and applications," IGI Global, pp. 73-75, 2008.

[11] P. Svenhard and A. Radaslic, "A penetration test of an Internet service provider," School of Information Science, Computer and Electrical Engineering, 2012, pp. 5-25.

[12] HKSAR, "Web Application Security," The Government of the Hong Kong Special Administrative Region, Hong Kong, 2008.

[13] R. Johari and P. Sharma, "A Survey on Web Application Vulnerabilities (SQLIA, XSS) Exploitation and Security Engine for SQL Injection," International Conference on Communication Systems and Network Technologies, pp. 453-458, 2012.

[14] M. E. Whitman and H. Mattord, Principles of Information Security, Fourth Edition ed., 2012.

[15] J. Vacca, "Computer and Information Security Handbook," Elsevier Inc, 2009, pp. 63-70.

[16] BiztechAfrica, "Annual security roundup report, "2016 Security Roundup," 2017. [Online]. Available: http://www.biztechafrica.com/article/trend-micro-2016-security-roundup-reveals-748-incr/12235/. [Accessed 2 March 2017].

[17] R. Lehtinen and G. T. Gangemi, "Computer Security Basics, 2nd Edition," O'Reilly, Ed., 2011, pp. 24-26.