I.J. Information Engineering and Electronic Business, 2020, 5, 24-32
Published Online October 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2020.05.03

An Integrated Vulnerability Assessment of Electronic Commerce Websites

Issah Baako
Bagabaga College of Education, Tamale, Ghana
Email: issahbaako@bagabaga.edu.gh

Sayibu Umar
Bagabaga College of Education, Tamale, Ghana
Email: sumar@bagabaga.edu.gh

Received: 14 May 2020; Accepted: 04 June 2020; Published: 08 October 2020

Abstract: This paper examines the security issues on electronic commerce websites in Ghana using technical and nontechnical procedures. The study assessed e-commerce websites for the security tools employed to protect user data and other related privacy issues on the websites. It also analyzed e-commerce websites for encryption security tools that protect customer data and test e-commerce websites for the presence of security vulnerabilities that could threaten the security of the sites and their users using w3af. The study used a combination of three methods; web content analysis, information security audit and testing of the websites using w3af, a vulnerability assessment tool. Web application attack and audit framework (w3af) was used to test and identify possible vulnerabilities on the e-commerce websites that could be used by malicious users to steal customer data for fraudulent intent. The research focused to reveal the security vulnerabilities present on e-commerce websites that could affect the trust of clients, the satisfaction of clients, and patronage of e-commerce services by customers. The study found credit card number disclosures, full path disclosures vulnerabilities, cross-site request forgery vulnerabilities and social security number exposures of clients on the e-commerce websites. These security weaknesses in these e-commerce websites have been highlighted as findings in the study that would inform policy direction on electronic data collection, protection and use in the e-commerce industry in Ghana. The findings will also inform industry players in the e-commerce sector on the need to strengthen security on their websites and caution customers to be security conscious on all e-commerce websites. The major significance of the study is the fact that majority of the electronic commerce websites have a lot of vulnerabilities making them unsecure for customers to trust their private data into their care. This study as such informs the customer society and the electronic commerce industry of these security weaknesses and the urgent need to get them fixed. Some solutions have been suggested in the paper to assist in fixing these security vulnerabilities. These solutions have provided the best results. A diligent application of these methods in addressing the vulnerabilities would provide a more secure and less vulnerable e-commerce websites for users. The precautions suggested could assist protect customers and reduce cyber threats during online shopping.

Index Terms: E-commerce websites, w3af, security, vulnerabilities, data protection, XSS, injection

1. Introduction

Ghana has currently observed a surge in the number of e-commerce websites in the online retail space for a wide range of consumer products. A number of these websites were assessed for encryption security tools and the availability of security vulnerabilities that could affect users' privacy and security. There is a need to ascertain the safety level of these websites for online shoppers. Security and privacy are leading factors for establishing and maintaining customer trust among others in the electronic commerce industry. The security and privacy of customer data online either in transit or at storage in the server of e-commerce merchants need optimum protection. The general size of cybercrime isn't known. The measures of losses are critical however steady. People online face new dangers of extortion day by day which may result in substantial losses. Cybercrime has increased by approximately 13% in 2017 [1]. Computer Security Institute (CSI) survey in 2007 reported that 46% detected a security breach and 91% reported suffering financial loss as a result of breaches. It is for this reason that the study focused to ascertain if security breaches can be executed in e-commerce websites. The study investigated e-commerce websites on the security vulnerabilities that tend to cause security breaches that would potentially affect users. The objectives of the study were to assess the vulnerability levels of e-commerce websites that are of critical security risks to online shoppers; suggest technical and managerial solutions to enable e-commerce merchants to fix these vulnerabilities; and suggest precautionary measures for ensuring safe

online shopping. The fast development of e-commerce technologies within the last few years has made it necessary for organizations to extend their businesses and services online as well as invest in the security of their systems. However, the anonymity of the Internet and e-commerce transactions has a great impact on the trust that exists between the buyer and the seller and the security and privacy of the customer's data [2]. Customers in an e-commerce transaction are apprehensive about their personal information that could be stolen by criminals whilst making an online payment. Critical security concerns of customers bother on how e-commerce merchants can ensure integrity, authenticity, and confidentiality. Many e-commerce websites directly ask for users' personal information such as names, physical and e-mail addresses, phone numbers and credit/debit card details through forms. Some e-commerce websites also passively record data on users' browsing habits and match that data with personal and demographic information to create a profile of user preferences [3]. This data might end up in the hands of third parties who use it for other benefits other than the initial reason for which customers provided it. In a Business Week survey, only 40 percent of users have heard of cookies and only 25 percent could select the right definition on a multiple choice questionnaire [4]. Advocates of customer privacy believe that consumer discomfort with online monitoring would reduce the use of online resources on sensitive topics. Many in the financial sector still bear the brunt of e-crime. But the sector that witnessed the highest increase in attacks is e-commerce. Attacks in e-commerce are said to have risen by 15% from 2006 to 2007 [5] Customer privacy is an integral part of electronic commerce strategies and investments in privacy protection and has shown to increase customers' spend, trustworthiness, and loyalty. The study seeks to find out the level of safety of visitors to e-commerce websites. The major objectives of the study were to: i) assess e-commerce websites for the availability of security tools to protect security and privacy of customers; ii) find out the presence of security vulnerabilities on the e-commerce websites; iii) suggest effective technical methods of fixing identified security vulnerabilities. The study seeks to find out the level of safety of visitors to e-commerce websites. The development of information technology and the widespread of this knowledge on the Internet enable criminals to be more sophisticated in the deceptions and attacks they can perform. New and different attack strategies and vulnerabilities only really become known once a perpetrator has discovered and exploited them. Electronic commerce merchants must investigate several available security risks to significantly reduce the risk of attack and compromise on their systems. The awareness of customer risks and the use of multi-layered security protocols, detailed and transparent privacy policies and strong authentication and encryption measures would assure the customer of the safety of their transaction and personal data resulting in improved customer confidence. The protection of networks through the deployment of firewalls and protection of communication channels, servers and clients are sure strategies to ensure user confidence and security satisfaction. In recent times, several individuals and businesses have been riveted by the Advance Fee Fraud scam known as "4-1-9" that originates from many African countries particularly, Nigeria, Liberia, Sierra Leone and Ghana. The Internet Crimes Complaints Centre (IC3) Report for 2010 rated Ghana among the top ten (10) countries of global Internet fraud. The report is suggestive of the level and nature of Internet fraud in the country. The youth of these countries have an appetite for computer crime because it is inexpensive, ubiquitous, fast and physically anonymous. These issues which are always reported in the print and electronic media reveal the level of vulnerability in carrying out, particularly financial transactions online.

2. Related Works

Internet security is a serious concern for all Internet users, especially in electronic commerce transactions. Secure websites create safe connections between the website and the web browser for entered personal data by customers such as personal information, banking details, credit cards and debit cards not to be accessible to unauthorized users or third parties (Secure Your Website and Grow Your Business, 2016). To reduce the vulnerability of computers and customers in a network, organizations could choose from a variety of products or a combination of them to secure their networks [6]. These tools include encryption authentication mechanisms, intrusion detection, security management and firewalls [7]. Aside from electronic commerce websites with questionable practices, some online storefronts that are scammers posing as retailers to steal credit card and other personal information [8]. Experts as a result of the above stress the need for customers to identify and transact with only secured electronic commerce websites. There are several features that customers need to inspect before they could undertake shopping on electronic commerce websites. HTTP is the protocol through which data is sent between a browser and a website. HyperText Transfer Protocol Secure (HTTPS) is a secure form of HyperText Transfer Protocol (HTTP). The presence of 'S' in HTTPS means that communication between the browser and the website is encrypted. HTTPS protects confidential online transactions like electronic banking and electronic shopping [9]. Web browsers would display a padlock icon and precede the Uniform Resource Locator with "https". The benefit of HTTPS is to protect customer information like credit card numbers and personal information. This is relevant to the study to find out if electronic commerce websites employ HTTPS or HTTP. Customers could also verify and trust that their data is safe and the website is owned by a legitimate organization. [10]. Secure Socket Layer (SSL) is a standard security technology that establishes encryption between a web browser and a web server [11]. It ensures that data passed between the browser and the server is private and vital. It is an industry standard that protects several websites for online transactions with customers [12]. A web server requires an SSL Certificate to create an SSL connection. Certification Authorities issue SSL Certificates to organizations. Though the complexities and operations of SSL protocol are invisible to customers, their browsers would provide a lock icon to indicate that their data is protected

by an SSL encrypted session [13]. According to [14] the Transport Layer Security (TLS) protocol is a successor to Secure Socket Layer (SSL). TLS creates secure communication on the web for e-mail, Internet faxing and other data transfers. The TLS Handshake Protocol ensures that the server and client authenticate each other to negotiate an encryption algorithm and cryptographic keys for data to be exchanged [15]. During this server and client communication, TLS ensures that no third party eavesdrops or tampers with any message [15]. Penetration testing is a series of activities undertaken to identify and exploit security weaknesses [16]. According to [17], penetration testing is a security testing that attempts to circumvent the security of a system. Reference [18] views penetration testing as an effort to gain entry into a system to prove that its protection has weaknesses. It can also be said to be an analysis of an IT environment and a search for exploitable vulnerabilities in a system. Vulnerabilities refer to security weaknesses in the system requirements, design, and implementation, which attackers exploit to compromise the system [19]. According to [20], no system is 100% secure. However, the conduct of penetration testing is, therefore to inspect how secure or otherwise the system is in the perspective of a malicious user with the prime objective to compromise the system. Reference [21] posits that penetration testing is used to identify security gaps in a system, use exploits to get into the network of the target system and then gain access to sensitive data. Reference [17] believe that penetration testing aims to determine possible entry points into a system using common techniques and tools used by hackers. Many security exploits, however, argue that penetration testing is more than the simulation of hacker activities. Hence the goal of penetration testing is not to hack or break a company's IT system [22], but to provide solutions to finding vulnerabilities and expert security advice to help strengthen the security of the system [16]. Penetration testing helps organizations to assess the effectiveness or otherwise of the security measures they employed by explicitly revealing security weakness in the system [23]. Penetration testing could cause information disruption, denial of services, information leakage since testers are usually granted permission to a substantial amount of a company's sensitive information. Insecure software strongly undermines financial, healthcare, defense, commerce, and other critical information technology infrastructure. Information technology infrastructure is becoming increasingly complex and interconnected, making it difficult in achieving optimum application security [24]. Attackers could use different paths in a web application to harm a business or organization. In the recent past, XSS, and SQL Injection among other attacks have been leading the most threatening vulnerabilities lists despite the numerous countermeasures proposed by experts [25]. For instance, XSS is ranked second in the OWASP Top Ten vulnerability list and ranked first in the MITRE CWE/SANS Institute list of Top 25 Dangerous Software Errors. However, security vulnerabilities continue to exist due to the developer's lack of understanding of the problem and their unfamiliarity with current guarding strengths and limitations [25]. Injection vulnerability is untrusted data that is passed on to interpreters in a query or command results in Injection flaws like SQL, OS, and LDAP. Hostile data from attackers could deceive interpreters to execute unintended commands or access unauthorized data. Injection flaws are common in legacy code. They could also be found in Xpath, or NoSQL queries, XML parsers, SMTP Headers, and program arguments. Injection flaws are easy to discover during code examination but difficult through testing. Fuzzers and scanners are tools that assist hackers in finding injection flaws. An Injection could result in loss of data, data corruption, nonrepudiation issues or complete host take over. Manual inspection of codes is the surest method of finding out if the applications safely use interpreters. Security analysts use code analysis tools to find interpreter use and check data flow in applications. Penetration testers can craft exploits that confirm the existence of a vulnerability in an application. Automated dynamic scanning which exercises the application may provide insight into whether some exploitable injection flaws exist. Scanners cannot always reach interpreters and are weak in indicating if successful attacks. Poor error handling makes injection flaws easier to discover [24]. XSS flaws occur when applications send untrusted data to web browsers without proper validation or escaping [26]. XSS flaws aid attackers to run in the browsers of victims resulting in user sessions hijack, website defacement, or redirecting the user to untrusted sites [27]. XSS is the most predominant web application security flaw [28]. Testing or code analysis could be used to detect the presence of most XSS flaws in a web application. Complete coverage requires a combination of manual code review and penetration testing, in addition to automated approaches [29]. Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes [30]. They believe sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser. When crypto is employed, weak key generation and management, and weak algorithm usage are common, especially weak password hashing techniques [29]. Application functions that relate to authentication and session management are often not implemented correctly. This allows attackers to compromise passwords or session tokens, and exploit other implementation errors to adopt the identity of other users [31]. Attackers use leaks or flaws in the authentication or session management functions like exposed accounts, passwords and session IDs to impersonate users in this type of security risk [24]. Though developers often build session management schemes and custom authentication, it is difficult getting it rightly done. It results in errors at logout, password management, timeouts, remember me, secret question, account update, etc. Privileged accounts are mostly targeted and a successful attacker could do anything the victim could do.

3. Methodology

This study used explorative and experimentation study approaches to explore e-commerce websites to identify the presence or otherwise of encryption security. Exploratory research has the advantage to afford a researcher to better explore and better understand the problem to identify the critical issues and focus on them. The websites were grouped according to the presence of encryption security to protect users. Web application attack and audit framework (w3af) was used to scan each website to identify vulnerabilities that could be present to be exploited. W3AF is a penetration tool that is supported on all network operating systems and compatible with windows network operating system. It is an extremely popular, powerful and flexible framework for web assessment and exploitation. The security risk levels of the identified vulnerabilities were analyzed manually using OWASP Top Ten 2017 Vulnerabilities in web applications.

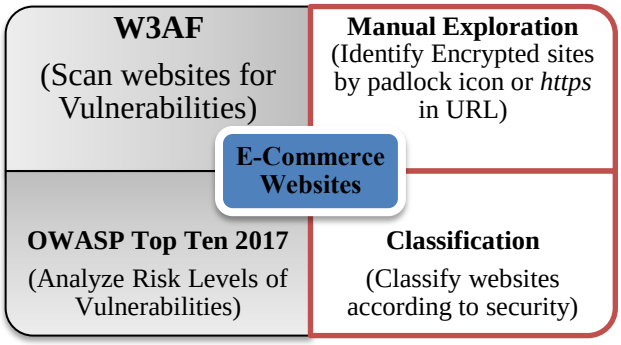

Fig. 1. Methodology for the study

Fig. 1 shows the approach that was used to conduct the vulnerability assessment. The e-commerce websites were manually explored to identify encrypted sites and then classified according to their secure levels. The w3af penetration testing tool was then employed to automatically scan the websites for vulnerabilities. These identified vulnerabilities were then analyzed using the OWASP Top Ten 2017 security vulnerabilities. The objective of the approach was to collect unbiased results that would closely represent the true security state of e-commerce websites. The purpose of penetration test is to identify vulnerabilities in the web application that can be exploitable to an outside attacker. The rapid changes in web application require a newer approach of combining a manual and automation penetration testing. These two methods have proven not to be mutually exclusive. In-depth manual and automated penetration testing as used in this study has the benefit of improving security knowledge, extend the depth and coverage of test. The researchers applied a qualitative and quantitative research survey approach with a sample size of 15 e-commerce websites that were active at the time of the study and the findings are presented in the mixed format of quantitative and qualitative analysis.

1) Manual Exploration and Web Content Analysis

Each sampled e-commerce website for the study was carefully explored to find out the security technologies deployed to ensure the security and privacy of customer data in electronic commerce websites. This was to find out the availability and type of security provided on the websites that would prevent the activities of hackers. This approach aided in exploring the security architecture of the websites.

Conducting Manual Exploration to Check Website Security

Check the left of **URL**
If
Padlock icon or ***https*** is present
Then
Website is ***Secure*** (User information submitted is safe)
Else
Warning icon*/information* icon and ***http*** present
Website is ***Unsecure***
Implies Information submitted can be seen or intercepted by malicious users.
Click on ***lock icon*** to view ***Security Overview***

Click on ***View Certificate*** (General tab) to reveal
Issuer of Certificate
Webserver certificate is issued to
Validity period of Certificate

Fig. 2. Procedure to conduct Manual Exploration

On each e-commerce website, the above procedure was used to check the security of the website and the type of security deployed, issuer of certificate and the validity period.

The profile of issuers of security certificates was verified to ascertain their level of trustworthiness.

2) Conducting Web Application Attack and Audit Framework (W3AF) Scan

W3af performs the functions of auditing and scanning for vulnerabilities in web applications and tries to exploit the vulnerabilities that are found in the application.

The researchers used the w3af at this stage to scan the e-commerce websites to identify web application vulnerabilities present in the chosen e-commerce websites. The results would inform if customer data and transactions are secure on this e-commerce websites.

Web Application Attack and Audit Framework (w3af) can identify almost all web application vulnerabilities using more than 130 plugins to scan target websites. It uses tactical exploitation techniques to discover new URLs and vulnerabilities. It can exploit SQL injection, OS commanding, remote and local file inclusion, XSS and unsafe file uploads. The plugins find the vulnerabilities and exploit them.

Table 1. The functions of each selected plugin for the test.

Plugin	Description/function
Audit	Audit plugins use the knowledge created by discovery plugins to find vulnerabilities on the remote web application and the web server.
bruteforce	Bruteforce plugins will bruteforce logins. These are basic authentication and form logins.
Grep	Grep plugins analyze every request and response to find vulnerabilities on errors, cookies, mails, comments and much more information about the target web application.

The researchers selected *audit*, *bruteforce* and *grep* to configure w3af to scan the website for exploitable security vulnerabilities.

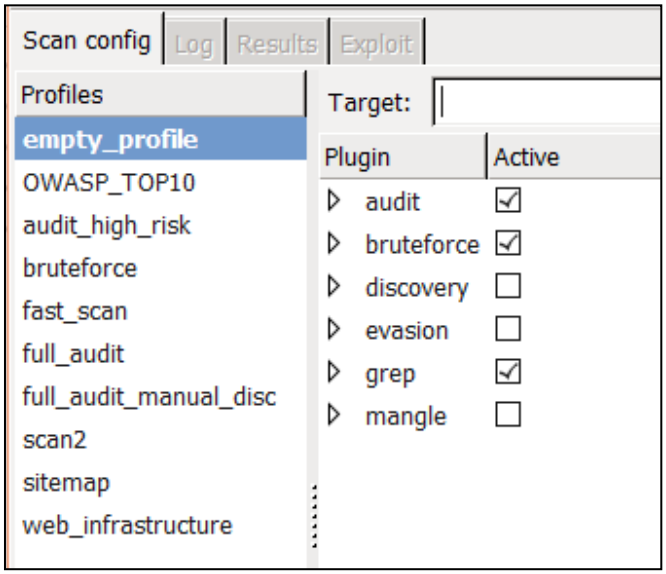

Fig. 3. Configured w3af ready for target and scan

The web addresses for each e-commerce website was supplied in the ***Target*** text box and the ***Start*** button used to initiate the scan for flaws and vulnerabilities present in the websites.

4. Results and Discussions

The web application audit and attack framework (w3af) identified vulnerabilities that could compromise the safety of user data in the e-commerce websites. The findings of w3af are shown in the figures as screenshots.

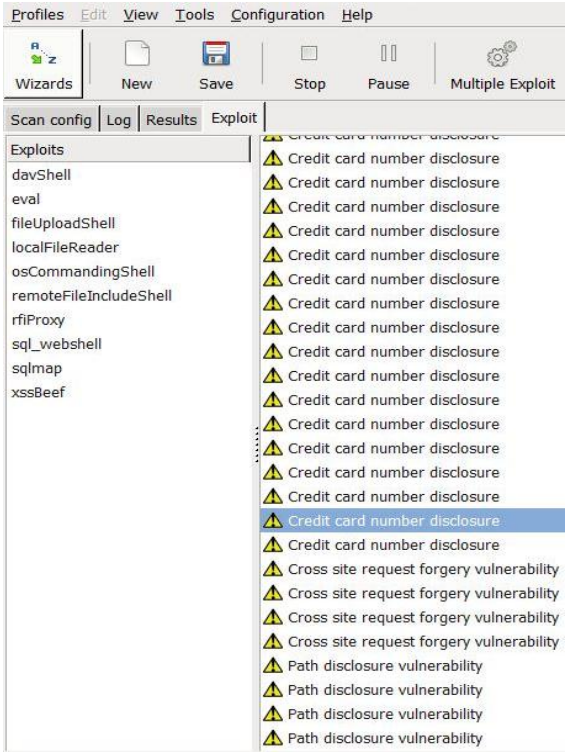

Fig. 4. Security threats identified on e-commerce website

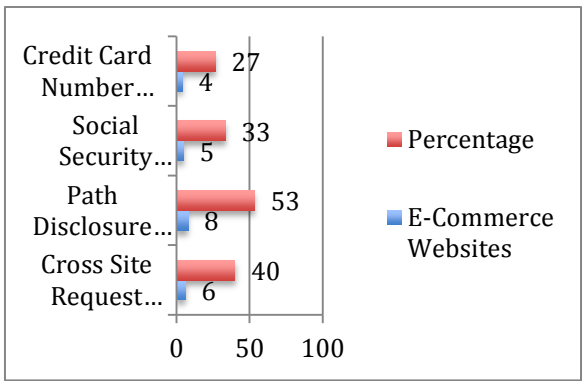

Fig. 5. Vulnerabilities identified from w3af scan

These vulnerabilities have been classified and discussed under the following headings.

1) The HTTP Methods GET and POST

These are HTTP methods used to allow communication between servers and clients. The web browser is the client and the application that hosts the website on a computer is the server. The POST and GET methods are for request-response between servers and clients. The GET method causes data sent to be part of the URL. Sensitive information and passwords sent are visible to everyone in the URL. The GET method features include requests that are visible in browser history, able to bookmark, used to retrieve data, and can be cached.

The results indicated statements: "*The URL [**url here**] is vulnerable to cross site request forgery*" and "*Attackers can exchange the method from POST to GET when sending data to the server"*.

2) Credit Card Number Disclosure (OWASP Top 10 - 2017 A3)

This security vulnerability was identified in twenty-seven percent (27%) of the e-commerce websites. This type of vulnerability is categorized under Sensitive Data Exposure in OWASP Top Ten Web Application Security Vulnerabilities - 2017. This is a situation where a web application ineffectively protects sensitive data like credit cards, debit cards, user authentication details or personal data. Sensitive data exposure covers data display, data in transit and data at rest. Attackers can steal or alter such weakly protected data to conduct credit card fraud, identity theft or other crimes. Sensitive data need extra protection whether in transit or at rest in the server or browser since customers give

credit/debit card details and personal information online. Customers who shop on these e-commerce websites risk their credit/debit card information and personal details.

3) Cross Site Request Forgery (CSRF/XSRF) Vulnerability (OWASP Top 10 – 2017 A7)

CSRF/XSRF was identified on forty percent (40%) of the e-commerce websites. CSRF forces the browser of a logged-on victim to send a forged HTTP request together with a session cookie and others automatically included authentication information to a vulnerable web application. The vulnerability allows attackers to force the victim's browser to generate requests the vulnerable application believes are legitimate requests from the victim.

Attackers use social engineering tricks on web application users to execute malicious actions. A successful CSRF attack can force ordinary users to transfer funds and change an email address. With administrative account users, the entire web application system can be compromised.

4) Full Path Disclosure (FPD) Security Vulnerability (OWASP Top 10 - 2017 A3)

This vulnerability enables the attacker to see the path to the *webroot/file*. As shown in Figure 4, w3af revealed that this vulnerability was present in fifty-three percent (53%) of the websites. Some vulnerability requires attackers to have the full path to the file they wish to view. An example is the SQL injection attack executed on web servers. Attackers could use FPD to produce various outcomes. If the webroot of a system is getting revealed, attackers could use this information with file inclusion vulnerabilities to access configuration files in the web application or operating system.

5) Social Security Number Exposure Vulnerability (OWASP Top 10 - 2017 A3)

This vulnerability is grouped under A3 – Sensitive Data Exposure in OWASP's 2017 top ten security vulnerabilities indicating the level of risk and damage it can cause to user data. It is a situation where malicious users can easily identify the social security number of a client in a web application. Social Security Numbers could be used in identity theft by attackers. Many organizations such as government institutions, medical facilities and financial agencies use Social Security as their primary identifier in record-keeping applications.

From the findings, customers risk having their personal and credit or debit card details stolen by hackers on e-commerce websites with vulnerabilities due to software defects, system defects and configuration defects or flaws. The impact of a security breach on e-businesses is heavy as systems could be hijacked, customer data stolen or entire database deleted.

5. Conclusion and Suggested Solutions

1) Credit Card Number Exposure

E-commerce merchants need to provide encryption technology for all sensitive data both at storage and in transmission in ways that defend against insider attack, external user and man-in-the-middle attacks. They must not store sensitive data on servers unnecessarily. Unavailable data can not be stolen online.

The use of algorithms (*bcrypt*, *PBKDF2* or *scrypt*) would protect passwords. Customers must deactivate caching for any page that store private data. Users must not use public computers or devices (Internet café) or shared office computers to transact online business.

2) Cross Site Request Forgery (CSRF)

Electronic commerce websites must include an unpredictable token in each HTTP request to be unique to each user session. Electronic commerce websites must use a CSRF guard like OWASP's CSRF Guard to automatically include tokens. Electronic commerce websites must require users to re-authenticate themselves or prove their identity (for example, *CAPTCHA*).

3) Exchanging POST to GET method

Allowing the POST request to go over an ***https*** connection could solve this vulnerability. All forms that lead to POST methods must be loaded over ***https***.

4) Full Path Disclosure (FPD)

Network administrators of electronic commerce websites can stop this vulnerability by disabling the display of error messages in PHP's ***php.ini*** file, Apache's ***httpd.conf*** file or through the PHP script.

Use the following to prevent Full Path Disclosure:

php.ini:
display_errors='off'

httpd.conf/apache2.conf:
php.flag display_errors off
PHP script:
Ini set ('display_errors', false:

Fig. 6. Code to prevent Full Path Disclosure

5) Safety Precautions for Online Shoppers

Encrypted websites provide the safest condition for online shopping. Potential shoppers must identify encrypted websites by the presence of a padlock symbol on the URL bar. The URL of e-commerce website must start with '*https'* rather than '*http'*. Online shoppers must not use the same password for different e-commerce accounts. This would ensure that the accounts on the other websites would be safe if one account were compromised. The surest way to keep accounts safe is to regularly change passwords every six months. This reduces the effect of damage a compromised account could cause an online shopper. A better way to stay safe online is by using effective Internet Security programs. Security features such as real-time anti-phishing and identity theft protection are excellent tools that can ensure the safety of online shoppers. Most public Wi-Fi hotspots do not encrypt data and information can easily be picked on them. Its use would set one up for identity theft. Online shoppers must use networks that are better secured to stay safe online. It is also a good practice to frequently check credit card statement especially after shopping online to ensure that there were no hidden charges or over deductions.

References

[1] Khoirunnisaa, Alfi Zuhriya, Lutfi Hakim, and Adhi Dharma Wibawa. "The Biometrics System Based on Iris Image Processing: A Review." *2019 2nd International Conference of Computer and Informatics Engineering (IC2IE)*.IEEE,2019.DOI: 10.1109/IC2IE47452.2019.8940832

[2] Kome, Ivan Marco Lobe. *Identity and consent in the internet of persons, things and services*. Diss. Ecole nationale supérieure Mines-Télécom Atlantique, 2019.

[3] Zimmermann, Verena, et al. "Assessing Users' Privacy and Security Concerns of Smart Home Technologies." *i-com* 18.3 (2019): 197-216.

[4] Gribing Arlfors, Christian, and Simon Nilsson. "Tracking the cookies: A quantitative study on user perceptions about online tracking." (2019).

[5] Mittal, Sangeeta, and Shivani Tyagi. "Computational Techniques for Real-Time Credit Card Fraud Detection."*Handbook of Computer Networks and Cyber Security*. Springer, Cham, 2020. 653-681.

[6] Cordova, Ronald S., Rolou Lyn R. Maata, and Alrence S. Halibas. "Blowfish Algorithm Implementation on Electronic Data in a Communication Network." *2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*. IEEE, 2019.

[7] Khandare, Laxman, Desai Karanam Sreekantha, and K. V. S. S. S. S. Sairam. "A Study on Encryption Techniques to Protect the Patient Privacy in Health Care Systems." *2019 Innovations in Power and Advanced Computing Technologies (i-PACT)*. Vol. 1. IEEE, 2019. DOI: 10.1109/i-PACT44901.2019.8960235

[8] Hanees, A. L. "Phishing e mail detection in e Banking using data mining techniques." (2019).

[9] Rescorla, Eric, and A. Schiffman. "The secure hypertext transfer protocol." *IETF Request for Comments, RFC* 2660 (1999).

[10] Bhiogade, Mittal S. "Secure socket layer." *Computer Science and Information Technology Education Conference*. 2002

[11] Kant, Krishna, and Prasant Mohapatra. "Scalable Internet servers: Issues and challenges." *ACM SIGMETRICS Performance Evaluation Review* 28.2 (2000): 5-8.

[12] Shinozaki, Jin, and Masayuki Arai. "Secure Socket Layer Visualization Tool with Packet Capturing Function."*International Journal of Future Computer and Communication*3.3 (2014): 187.

[13] Turner, Sean. "Transport layer security." *IEEE Internet Computing* 18.6 (2014): 60-63.

[14] Dierks, Tim, and Eric Rescorla. "The transport layer security (TLS) protocol version 1.2." (2008): 5246.

[15] Ke, Jiun-Kai, Chung-Huang Yang, and Tae-Nam Ahn. "Using w3af to achieve automated penetration testing by live DVD/live USB." *Proceedings of the 2009 International Conference on Hybrid Information Technology*. 2009.

[16] Goel, Jai Narayan, and B. M. Mehtre. "Vulnerability assessment & penetration testing as a cyber defence technology." *Procedia Computer Science* 57 (2015): 710-715.

[17] Cohen, Fred. "Managing network security—Part 9: Penetration testing?." *Network Security* 1997.8 (1997): 12-15.

[18] Massacci, Fabio, Marco Prest, and Nicola Zannone. "Using a security requirements engineering methodology in practice: The compliance with the Italian data protection legislation."*Computer Standards & Interfaces* 27.5 (2005): 445-455.

[19] Zhao, Jensen J., and Sherry Y. Zhao. "Opportunities and threats: A security assessment of state e-government websites." *Government Information Quarterly* 27.1 (2010): 49-56.

[20] Yeo, John. "Using penetration testing to enhance your company's security." *Computer Fraud & Security* 2013.4 (2013): 17-20.

[21] Midian, Paul. "Perspectives on Penetration Testing—Black Box vs. White Box." *Network Security* 2002.11 (2002): 10-12.

[22] Shah, Sugandh, and Babu M. Mehtre. "An overview of vulnerability assessment and penetration testing techniques."*Journal of Computer Virology and Hacking Techniques* 11.1 (2015): 27-49.

[23] OWASP, Top. "Top 10-2017." *The Ten Most Critical Web Application Security Risks. OWASP™ Foundation. The free and open software security community. URL: https://www. owasp. org/index. php/Top_10-2017_Top_10* (2017).
[24] Rodrigues, Douglas, et al. "Engineering secure web services."*Crisis Management: Concepts, Methodologies, Tools, and Applications*. IGI Global, 2014. 203-223.
[25] Wassermann, Gary, and Zhendong Su. "Static detection of cross-site scripting vulnerabilities." *2008 ACM/IEEE 30th International Conference on Software Engineering*. IEEE, 2008.
[26] Patil, Vishwajit S., Dr GR Bamnote, and Sanil S. Nair. "Cross site scripting: An overview." *IJCA Proceedings on International Symposium on Devices MEMS, Intelligent Systems and Communication*. No. 4. 2011.
[27] Fonseca, Jose, Marco Vieira, and Henrique Madeira. "Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks." *13th Pacific Rim international symposium on dependable computing (PRDC 2007)*. IEEE, 2007.
[28] Wichers, Dave. "Owasp top-10 2013." *OWASP Foundation, February* (2013).
[29] Song, Fuyuan, et al. "Efficient and Secure k-Nearest Neighbor Search Over Encrypted Data in Public Cloud." *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 2019.
[30] Davidson, Alex, et al. "Privacy pass: Bypassing internet challenges anonymously." *Proceedings on Privacy Enhancing Technologies* 2018.3 (2018): 164-180.

Authors' Profiles

Issah Baako, born in 1977. M. Sc. Information Technology and TUTOR at Bagabaga College of Education, Ghana. He has worked as a SUBJECT TEACHER at the basic school level in Ghana where he taught Mathematics. He has also served as a STATISTICS OFFICER at the Northern Regional Education Directorate, Tamale, Ghana. His main research interests include E-commerce Security, cyber security, cyber-insurance and E-Learning technologies.

His publications are: 1) Issah Baako, Sayibu Umar, Prosper Gidisu, "Privacy and Security Concerns in Electronic Commerce Websites in Ghana: A Survey Study", International Journal of Computer Network and Information Security (IJCNIS), Vol.11, No.10, pp.19-25, 2019. DOI: 10.5815/ijcnis.2019.10.03.
2) Umar Sayibu, Frimpong Twum, Issah Baako, "Delivering a Secured Cloud Computing Architecture and Traditional IT Outsourcing Environment via Penetration Tools in Ghana", International Journal of Computer Network and Information Security (IJCNIS), Vol.11, No.11, pp.46-59, 2019. DOI: 10.5815/ijcnis.2019.11.06

Umar Sayibu, born in 1973 and a Tutor at Bagabaga College of Education Tamale - Ghana. He holds an M.Sc. degree In Information Technology from Kwame Nkrumah University of Science and Technology, Kumasi – Ghana in June 2018. He received his BA degree in Information Studies in 2010 from University of Ghana Accra - Ghana. His research area of interest is Cloud Computing, Information Systems and Computer Networks.

His publications are: 1) Issah Baako, Sayibu Umar, Prosper Gidisu, "Privacy and Security Concerns in Electronic Commerce Websites in Ghana: A Survey Study", International Journal of Computer Network and Information Security (IJCNIS), Vol.11, No.10, pp.19-25, 2019. DOI: 10.5815/ijcnis.2019.10.03.
2) Umar Sayibu, Frimpong Twum, Issah Baako, "Delivering a Secured Cloud Computing Architecture and Traditional IT Outsourcing Environment via Penetration Tools in Ghana", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.11, pp.46-59, 2019. DOI: 10.5815/ijcnis.2019.11.06

How to cite this paper: Issah Baako, Sayibu Umar, " An Integrated Vulnerability Assessment of Electronic Commerce Websites", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.12, No.5, pp. 24-32, 2020. DOI: 10.5815/ijieeb.2020.05.03