2021 IEEE 8th International Conference on Adaptive Science and Technology (ICAST -2021), Nov. 25 – 26, 2021, Accra, GHANA

Vulnerability Analysis of Online Banking Sites to Cross-Site Scripting and Request Forgery Attacks: A Case Study in East Africa

Gifty Buah
Department of Computer Engineering
University of Ghana
Accra, Ghana
gbuah@ug.edu.gh

Scholastica Memusi
Information Technology
Carnegie Mellon University
Kigali, Rwanda
myrabel.memusi@gmail.com

John Munyi
Information Technology
Carnegie Mellon University
Kigali, Rwanda
wachirawamunyi@gmail.com

Timothy Brown
Electrical and Computer Engineering
Carnegie Mellon University
Kigali, Rwanda
timxb@cmu.edu

Robert A. Sowah
Department of Computer Engineering
University of Ghana
Accra, Ghana
rasowah@ug.edu.gh

2021 IEEE 8th International Conference on Adaptive Science and Technology (ICAST) | 978-1-6654-2717-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICAST52759.2021.9681978

***Abstract*—Web applications are prone to several attacks. Two common threats are cross-site scripting attacks and cross-site request forgery. With internet banking becoming more popular in East Africa, the level of security that online banking services offer has become an increasing concern. This paper presents an analysis of the safety of these applications used by many unsuspecting customers seeking convenience and determines ways to detect and prevent these attacks from taking place. We assumed that if people with a technical background in IT and information security are vulnerable to CSRF and XSS attacks, the public would be even more vulnerable. Out of 96 users, 35 answered our survey, 53.1% of the respondents said they do not check the URLs of online banking websites they visit to ensure they are not on a phishing site. Secondly, only 36.4% of users considered the security implications of clicking on links in emails or even on banking websites all the time. Based on the interviews done, testing and analysis conducted, there is a clear indication that Internet banking users are vulnerable to XSS and CSRF. Notably, close to 50 % of the Internet banking users we interviewed reported that they do not receive ample tips from the banks regarding security issues to look out for when transacting online. The findings from this research help make recommendations to banks and users to ensure that future online banking transactions are done more securely.**

Keywords— Cross-site scripting, cross-site request forgery, threats, attacks, internet banking

I. INTRODUCTION

Computer security involves all the measures that are put in place to protect sensitive resources in computer systems [1]. This includes ensuring the availability of the resources to authorized personnel and ensuring integrity and confidentiality of data on these systems. Worldwide, more people and resources are being dedicated to providing security in computing devices and networks due to the increased reliance on computing devices and the internet.

Vulnerability is a flaw in a computer system that allows an attacker to exploit the system [2]. These vulnerabilities can lead to unauthorized access of systems, unavailability, or decreased performance of computer systems. Identifying vulnerabilities in a computer system requires some vulnerability assessment. Vulnerability assessment tests the security of a computer system [3], and the outcome can lead to the identification of vulnerabilities in the system. From the software perspective, penetration testing is a significant way of identifying such vulnerabilities.

An essential service on the internet that has raised concerns about internet security is online banking. Online banking involves carrying out banking transactions using a home computer linked to a bank's computer via the internet or through a telephone link to a call center or a computerized system. Online banking is a necessary condition for the development of e-commerce and e-society. However, it comes with new security threats, drawing more attention to security for web-based applications.

The introduction of mobile money in East Africa was a game-changer, challenging banks to make banking a much more straightforward and convenient process. This spurred the growth of internet banking to compete with mobile money, thus giving customers a variety of options to choose from. Internet banking is a means by which customers access banking services via the internet [4]. We seek to investigate the safety of these web applications as they are prone to many threats such as cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks. Cross-site scripting is a vulnerability that allows attackers to inject malicious code into a benign website and therefore compromise the confidentiality and integrity of data transfers between the website and the client [5].

Cross-site request forgery (CSRF) is an exploit. An attacker causes a user to visit a trusted server using a malicious URI, allowing the attacker to inject its authorization code. To answer the research question "How vulnerable are internet banking sites in East Africa to cross-site scripting and cross-site request forgery attacks?" we work on detecting XSS and CSRF attacks in web banking applications and focus on identifying appropriate prevention techniques that can be used. We also make recommendations to the banks based on our findings. The primary beneficiaries of this research are banks and their customers. Customers would like reassurance that their banking transactions are being done safely and that the bank is aware and capable of handling them in the event of a security breach.

The key focus of our research is web banking applications. We concentrate on inter-banking and intra-banking transactions and do not consider third-party-enabled transactions such as shopping online on a website with PayPal-enabled payment. We start by looking at popular banks in East Africa with online web banking applications and banks with a lot of traffic on their internet banking applications. The purpose of this is to determine if the most popular banks, based on their number of customers, take precautions and invest in any form of security to ensure their applications are safe to use. An assumption made is that the intended attacker has moderate resources, a graduate student studying at a university in the region with adequate knowledge on XSS and CSRF attacks. Also, we assume that the attack will be carried out using open-source scanning and attack tools. The prevention mechanisms recommended will be based on these assumptions as well. Other assumptions made about the attacker are that their motivation is to ruin the bank's reputation and bring to the public the flaws of the banks' online banking systems.

Even though this research considers banks based in East Africa, it can be related to other parts of Sub-Saharan Africa. Especially in Ghana, West Africa, even though the introduction of mobile money occurred a couple of years after its introduction in East Africa, the adoption and proliferation of mobile money and online banking are very similar in most African countries. Barclays Bank, now Absa, Ecobank, and Equity bank are major banks found throughout Africa, and the analysis covers these banks. The lessons and solutions proposed at the end of this research apply to all sub-Saharan countries since there is not much change in the underlying applications that power these systems.

II. Literature Review

As financial institutions reach more customers, the use of the Internet to transact has become more prevalent. XSS and CSRF attacks pose a considerable risk to customer data. According to Ernst and Young in [6], the East African market is served by over 100 different banks. It is estimated that over 70% of these banks offer internet banking. This research focuses on finding how secure are internet banking applications in East Africa. There have been over 10 reported internet banking fraud cases in 2018 as of this writing. Currently, most banks do not publicize security breaches nor explain what areas have been compromised. According to Kenya's Daily Nation newspaper, the National Bank of Kenya suffered a cyber-attack resulting in the loss of 29 million Kenya Shillings. Considering the above report, it is necessary to research and report findings to understand better how well-prepared banks are in East Africa when it comes to XSS and CSRF attacks. Across East Africa, particularly in Kenya, the legal framework addresses these issues through the Central bank of Kenya Act and the Kenya Communications (Amendment) Act [7].

Farah et al. in [8] conducted a study on cross-site scripting and cross-site request forgery vulnerabilities on websites in Bangladesh following an attack on the Bank of Bangladesh using XSS and CSRF techniques that cost the bank $100 million. From an analysis of 500 websites, 30% of the web applications were vulnerable to XSS and CSRF. 75% of the sites were vulnerable to CSRF attacks, and 65% of the sites were susceptible to XSS attacks. Out of the total number of vulnerable sites to XSS, 65% were DOM-based and reflected XSS, and 35% were stored XSS.

J. Mtsweni in [9] also analyzed the security posture of 70 websites in South Africa and then compared the results to that of 10 top global websites outside South Africa. Their focus was to investigate the defense mechanisms employed by the chosen websites. They checked client-side security policies that did not require actively scanning the selected websites to identify. From their results, over 67% of the analyzed websites unnecessarily expose server information. About 50% did not protect session cookies, and only about 30% of the websites used secure communications to transmit user information. It was also observed that some of the websites were using deprecated security policies.

Wangwe et al. in [10] assessed the readiness of the government of Rwanda, Tanzania, and Uganda to provide e-services to their citizens from an information security perspective. The results indicated that all three countries have an e-government policy that dictates minimum security standards. The results from the questionnaires sent out to government agencies revealed that fraud concerns were much higher than concerns of a network breakdown, with 50% of respondents expressing their internet fraud concerns.

To address the lack of a unified security framework in Africa, Kritzinger et al. [11] analyzed five major cyber safety concerns and proposed solutions to each of these concerns. The solutions were then used to create a comprehensive security framework that could be adopted in Africa. The concerns included security policies, security procedures, security awareness, security research, and technical security measures in Africa.

Several techniques have also been proposed to detect and protect web-based applications from some of these attacks. Oppliger et al. [12] discussed various client-side attacks in internet banking, and protection mechanisms that are being implemented and researchers have suggested. Wurzinger et al. [13] proposed detecting and preventing cross-site scripting attacks by employing a server-side solution, SWAP: Secure Web Application Proxy, which is deployed to the reverse server without significant modification to the original web application the user is accessing. More advanced, machine learning-based methods are proposed by [14] uses unsupervised learning to detect malicious javascripts, while [15] uses feature analysis of scripts to determine whether they are malicious or not.

This paper aims to investigate the level of security of selected internet banking applications. Based on the results obtained, recommendations will be made to the banks on detection and prevention mechanisms for XSS and CSRF attacks to protect customers' data and money. This research is vital to different industry sectors. The public at large is possible fraud victims and will benefit from our study by learning how to protect themselves and what to look out for during online banking transactions. Customers also need the guaranteed safety of their data and money. In a case where a successful attack happens, the bank's reputation is at stake, and the trust built in the business is at risk. The bank could lose money. Researchers will also be interested in the findings since we address current security loopholes in web banking applications in relation to XSS and CSRF. Our research aims to share results; hence, our report will serve as a good consolidation of knowledge to a security professional and

software firms selling patches and fixes for the vulnerabilities we aim to expose. These groups of people are the intended audience.

III. Methodology

To answer the research question, two aspects of information security are considered. First are the technical measures put in place by banks to protect their customers from XSS and CSRF. Second, are the operational measures for preventing and recovering from XSS and CSRF attacks. Nine banks in East Africa are chosen as our sample space for an in-depth study of their online banking applications and security procedures. The nine banks were selected based on the following criteria:

- The number of customers: Results from the study must apply to as many of the banking population in East Africa as possible. The banks with the largest customer base are therefore considered.
- Level of activity on their online banking systems: Banks with high online banking usage will be considered when choosing the final six.

Based on the technical measures and the operational procedures mentioned earlier, the research question was broken down into two problems.

A. Technical measures

For the technical measures, we first considered whether banks in East Africa have any security measures to prevent and recover from cross-site scripting and cross-site request forgery? This was to provide information on the level of security of the web applications. The method for answering this question was broken down into two: conducting a survey with information security personnel of six of the targeted banks and performing penetration tests on their web banking applications to determine whether there were any security measures in place against XSS and CSRF. Data collection through the survey was based on the security personnel's answers to the two main questions:

- Does the bank consider cross-site scripting and cross-site request forgery as part of their security model?
- Has the bank been able to detect or recover from an XSS or CSRF attack, and what was the duration of the response?

Penetration testing on the web banking applications was also done to collect more data. The experiments were carried out using OWASP's Zed Attack Proxy (ZAP) and XSSer, which are included in the Kali Linux software. These are open source XSS and CSRF vulnerability checking tools and require the web application URL to be provided for scanning. Scanning was done in intruder mode so that we could have the results a potential attacker would have if they launched such an attack.

B. Operational and procedural measures

The operational measures to mitigate cross-site scripting and cross-site request forgery are as necessary as technical security measures. Several actions on the user's part can lead to an infection of the client's computer with malicious scripts that collect sensitive banking information. We assessed how vulnerable clients are by analyzing the ease with which an attacker could infect the application with malicious scripts by exploiting the user. In this, we identified the sub-question: How informed are users about XSS and CSRF? The methodology for tackling this sub-question was through a survey. This survey, given to information security personnel of banks, provided us with data on the effort made by the banks to educate their internet banking users about XSS and CSRF. The survey focused on answering the questions:

- How often do users check the URL of the banking site to be sure they are on the right website?
- How often do users consider the security implication before clicking on a link in an email supposedly sent by their banks?

Fig. 1 summarizes the methodology for answering the research question.

IV. Results and Discussion

Two different surveys were prepared for users and IT personnel from banks. Results from the penetration tests are also analyzed.

A. User Survey

A survey was conducted to get users' views on the level of security of online banking systems. This survey was also intended to study users' actions and behavior online, making them vulnerable to XSS and CSRF. A survey with 10 questions was sent out to the Carnegie Mellon University Africa 2018 and 2019 students, 96 students in all. CMU Africa students were chosen for this interview because of their level of education and knowledge about security. It would help us know how people with knowledge about security in East Africa perceived the security of online banking applications. An assumption made was that if people with a technical background in IT and information security came out as vulnerable to CSRF and XSS, the public would be even more vulnerable. Out of 96 users, 35 answered our survey. As shown in Fig. 2, 53.1% of the respondents said they do not check the URLs of online banking websites they visit to ensure they are not on a phishing site. Secondly, only 36.4% of users considered the security implications of clicking on links in emails or even on banking websites all the time. It may sound surprising that several users in such an academic institution do not critically check URLs and links. However, it is normal that online banking users behave this way since security is naturally not the focus of their visit to the online banking website. Even for people with knowledge in security, this is true. But this behavior of users puts them at risk of XSS and CSRF as malicious scripts can be easily inserted into their browsers by clicking on malicious links. 42.4% of respondents said their banks did not educate them on online banking security. This is a significant proportion, and users are at risk if they do not have basic information on the necessity for security in online banking. 9.1% of people have been victims of theft due to stolen credentials. Even though users are at risk of XSS and CSRF, attackers have not taken advantage of the situation. The low number of reported cases of credential theft is likely why users do not seem bothered by the risk of their behavior online. They may be quite optimistic that nothing of the sort could possibly happen to them since it rarely does anyway.

B. Bank Personnel Survey

We reached out to IT professionals working in 6 banks across the region. The questions we asked were centered

around the safety of their internet banking web application. Four responses were received from Barclays Bank, Banque Populaire du Rwanda, Equity Bank, and National bank of Kenya. When asked to rate the safety of their internet banking applications, all respondents rated it to be very good. With this response, we believed that the banking application would be free from prevalent attacks like XSS and CSRF. We also inquired whether they educated their customers on internet banking security and responded that they all do. They indicated that they educate their users through text messages, emails, and other communication media. The response on whether their online banking applications had ever been attacked yielded a 100% no. The exciting thing was when asked how long it took for them to recover from an attack if they had been attacked, 66.7% out of 3 respondents said it took 1-3 days. We did not understand how they could have possibly recovered from an attack if there had been none. A summary of the results is shown in Fig. 3.

From this, we inferred that there was information being withheld from us. We made this conclusion because they were also very reluctant to tell us some of the tools they were using to generate their one-time passwords. All respondents pointed out that they do indeed have a system that detects any attack attempts on their application and regularly scans their system to ensure it is certainly secure. However, as of this writing, none of us had been approached and questioned about scanning their websites even though we did not mask our IP addresses during the scanning. One of the 4 banks interviewed admitted to not having a threat model for their online banking system despite having rated its security very high. Without a threat model, how could the personnel ensure that their internet banking application was safe from any threats?

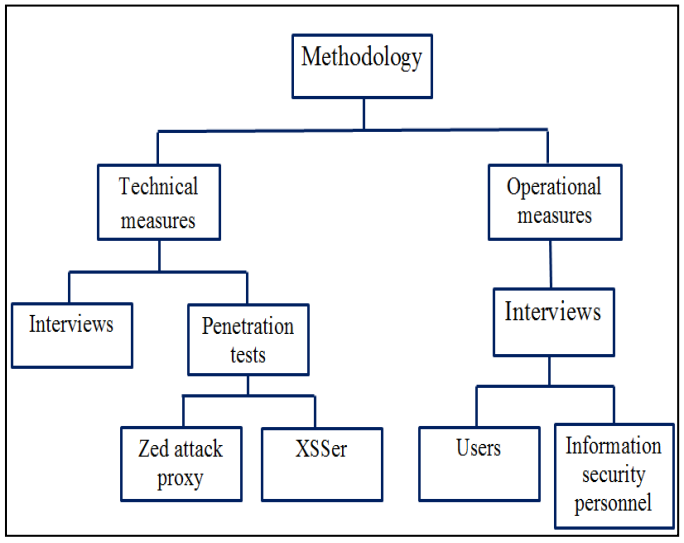

Fig. 1 Summary of methodology

C. Penetration tests

Seven out of the nine online banking applications were scanned using XSSer and Zed Attack Proxy. Out of these, only Barclays bank and Ecobank had no detected XSS or CSRF vulnerability. It is noteworthy to mention that Ecobank had some other vulnerabilities which were not XSS or CSRF related. The major XSS and CSRF related vulnerabilities detected were:

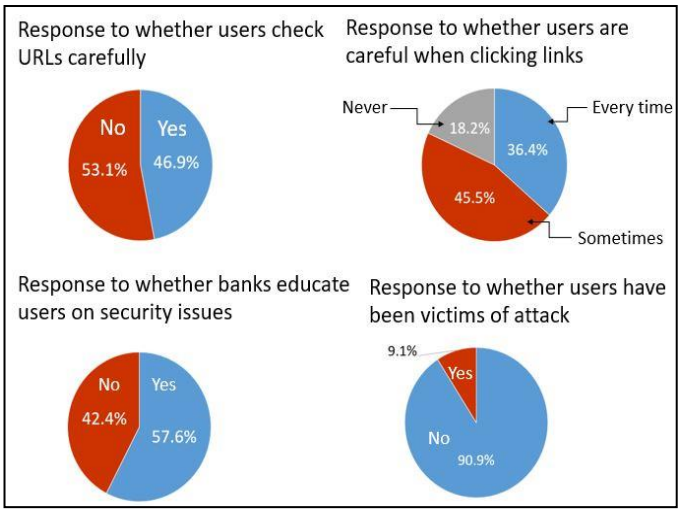

Fig. 2 Summary of users' response to survey

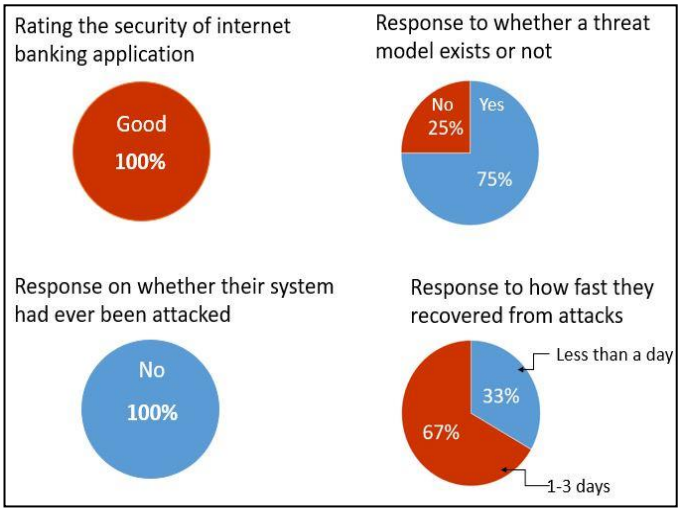

Fig. 3 Summary of bank personnel's response to survey

- Cookie without secure flag: This vulnerability means that cookies from users could be sent over unsecured connections. For example, if the online application communicates with a third-party website that was not SSL enabled, any user data shared with that server will be in the clear: username, password, and all!
- Cookie without HTTP only flag: This vulnerability means that a script can get access to using cookies. XSS attackers mainly insert scripts into browsers to steal users' data. Without the HTTP-only flag, a script inserted by an attacker can easily get access to a user's cookies.
- XSS protection disabled: The XSS protection field, when enabled, automatically stops a webpage from loading if a potential attacker script or XSS vulnerability is detected. Having this disabled means, a compromised webpage will still load and execute the malicious script.

The banks and the respective vulnerabilities detected are shown in Table 1. In the table, the symbol x represents the presence of a vulnerability. A significant surprise encountered was with the National Bank of Kenya. The HTTPS certificate for their online banking application was invalid at the time of the analysis, but users were still being asked to enter their passwords. This means that all data collected during this period was not encrypted.

TABLE I. SUMMARY OF BANKS AND VULNERABILITIES DISCOVERED ON THEIR ONLINE BANKING APPLICATIONS

Bank	**Vulnerabilities**				
	Cookie w/o secure flag	***Cookie w/o HTTP only flag***	***XSS protection disabled***	***SQL injection detected***	***HTTPS certificate invalid***
Equity Bank	x				
Commercial Bank of Africa		x			
National Bank of Kenya	x		x	x	x
Banque Populaire du Rwanda			x		
Bank of Kigali	x	x			
Ecobank					
Barclays Bank					

V. CONCLUSION

This research aimed to find if Internet bank users in East Africa are under any threat to cross-site scripting and cross-site request forgery. Based on the interviews, testing and analysis conducted, there is a clear indication that Internet banking users are vulnerable to XSS and CSRF. Notably, close to 50 % of the Internet banking users we interviewed reported that they do not receive ample tips from the banks regarding security issues to look out for when transacting online. Possible vulnerabilities were also identified with two users reporting the loss of money due to credential theft. This shows that attacks on users are not prevalent, but vulnerabilities can be taken advantage of. We recommend that banks ensure that, HTTPS certificates are active, HTTP-only flag and secure flag of cookies are enabled and XSS protection is also enabled for all online banking websites. More resources should be invested in educating users about the security of online banking applications. For future work, we propose that extensive analysis using advanced tools such as the browser exploitation framework (beEF) be used for the analysis to help find the vulnerabilities that the open-source tools we used might have missed. Also, more banks should be included in the analysis.

REFERENCES

[1] D. Gollmann, "Computer security," Wiley Interdisciplinary Reviews: Computational Statistics, vol. 2, pp. 544-554, 2010.

[2] Y. Khera, D. Kumar, and N. Garg, "Analysis and Impact of Vulnerability Assessment and Penetration Testing," in 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), 2019, pp. 525-530.

[3] S. Nagpure and S. Kurkure, "Vulnerability assessment and penetration testing of Web application," in 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), 2017, pp. 1-6.

[4] J. Jansen, "Studying Safe Online Banking Behaviour: A Protection Motivation Theory Approach," in HAISA, 2015, pp. 120-130.

[5] R. Kissel, Glossary of key information security terms: Diane Publishing, 2011.

[6] E. a. Young, " Eastern Africa banking sector," 2013.

[7] C. B. o. Kenya, "Central Bank of Kenya Act CAP 491," 2014.

[8] T. Farah, M. Shojol, M. Hassan, and D. Alam, "Assessment of vulnerabilities of web applications of Bangladesh: A case study of XSS & CSRF," in 2016 sixth international conference on digital information and communication technology and its applications (DICTAP), 2016, pp. 74-78.

[9] J. Mtsweni, "Analyzing the security posture of South African websites," in 2015 Information Security for South Africa (ISSA), 2015, pp. 1-8.

[10] C. K. Wangwe, M. M. Eloff, and L. M. Venter, "E-government readiness: An information security perspective from East Africa," in Proceedings of IST-Africa 2009 Conference, 2009, pp. 1-6.

[11] E. Kritzinger and S. Von Solms, "A framework for cybersecurity in Africa," Journal of Information Assurance & Cybersecurity, vol. 2012, p. 1, 2012.

[12] R. R. R. Oppliger, and T. Holderegger "Internet Banking: Client-Side Attacks and Protection Mechanisms Computer," Computer (Long. Beach. Calif), vol. 42, pp. 27-33, 2009.

[13] C. P. P. Wurzinger, C. Ludl, E. Kirda, and C. Kruegel, "SWAP: Mitigating XSS attacks using a reverse proxy," ICSE Workshop on Software Engineering for Secure Systems, pp. 33-39, 2009.

[14] S. Goswami, N. Hoque, D. K. Bhattacharyya, and J. Kalita, "An Unsupervised Method for Detection of XSS Attack," Int. J. Netw. Secur., vol. 19, pp. 761-775, 2017.

[15] S. Lalia and A. Sarah, "XSS Attack Detection Approach Based on Scripts Features Analysis," in World Conference on Information Systems and Technologies, 2018, pp. 197-207.