A Holistic Evaluation of E-Commerce Payment Security Through Automated and Manual Analysis

Urvashi Kishnani, Briana Whalen, Andrew Burris, Sanchari Das
Ritchie School of Engineering and Computer Science, University of Denver

ABSTRACT

With increasing online transactions, questions regarding customers’ privacy and security are increasing and need to be addressed. These online transactions, by necessity, involve personal and sensitive information, including Personally Identifiable Information (PII) such as name, address, SSNs, and banking information. This information also changes hands several times from the end user, online platform, banking platform, and, if necessary, to a transportation company for shipping fulfillment.

Thus, to understand the current security and privacy aspects of these platforms, we performed a holistic evaluation of 91 e-commerce websites. We also conducted a literature review to understand better e-commerce and what is involved in a payment platform.

Through a combination of hands-on and automated tool-based analysis, along with the study of relevant literature, we evaluate the current state of online payment platforms from the view of technical security and user privacy. Our literature review highlights the most discussed privacy and security associated with e-commerce platforms and makes some gaps in the literature.

The website analysis focuses on the website’s privacy policy, cookies, payment, and other security measures and highlights both the divergence from or adherence to expected outcomes. Finally, we propose suggestions for both users to make informed decisions and for companies to increase the security and privacy front of their e-commerce website products.

OVERVIEW

We selected and performed a thorough evaluation of 91 different e-commerce websites. After that, we looked at the security and privacy details of the website from several angles. Our analysis was performed using both automated and manual evaluation.

We utilized the PrivacyCheck tool, which collects data points for 20 different subcategories from lengthy privacy policies, 10 of which are under user control and the remaining under GDPR.

Each of these 20 subcategories has an associated question that the tool answers and gives a score of 0-10. In addition, another tool, CookieServe, was used to determine the number of default cookies used by each website and their specific purpose, whether necessary, analytical, or advertisement.

We conducted a hands-on evaluation of the payment platform’s security by looking at five key factors: website security, where we looked for the use of Hypertext Transfer Protocol Secure (HTTPS) and the presence of a valid digital certificate; authentication, where we checked for Multi-Factor Authentication (MFA) options and guest checkout; payment security where we checked for the use of a secure payment processor and association with a trusted financial institution; input validation where we checked whether incorrect card details and addresses were being detected; and user confidence where we looked if the website allowed for customer ratings and reviews on their products.

RESULTS – LITERATURE REVIEW

Each website collected about 38.5 cookies, with one having as many as 115 cookies. Most of the cookies were used for advertising purposes, which they implied were not deemed necessary or used for analytical, functional, performance, or advertisement purposes. Necessary and functional cookies were the least in number. In the privacy policy, we note that the average score obtained for user control is only about 53.5%, which indicates that most websites only give users partial control over the data collected or tracked by them.

REFERENCES & ACKNOWLEDGEMENT


We thank Ashton Foster, Oscar Jane Tighe, IC McManus, Neil G Dewhurst, Liliana Chis, and John Justine S Hastings, Brigitte C McManus, Neil G Dehghani, Liana Oh, and John MacInnes. 2013. The standard error of measurement is a more appropriate measure of quality for pragmatic medical assessments than reliability: an analysis of MRCGP LR examinations. BMC medical education 13 (2013), 1-5.


We thank Ashton Foster, Oscar Jane Tighe, IC McManus, Neil G Dewhurst, Liliana Chis, and John Justine S Hastings, Brigitte C McManus, Neil G Dehghani, Liana Oh, and John MacInnes. 2013. The standard error of measurement is a more appropriate measure of quality for pragmatic medical assessments than reliability: an analysis of MRCGP LR examinations. BMC medical education 13 (2013), 1-5.

We thank Ashton Foster, Oscar Jane Tighe, IC McManus, Neil G Dewhurst, Liliana Chis, and John Justine S Hastings, Brigitte C McManus, Neil G Dehghani, Liana Oh, and John MacInnes. 2013. The standard error of measurement is a more appropriate measure of quality for pragmatic medical assessments than reliability: an analysis of MRCGP LR examinations. BMC medical education 13 (2013), 1-5.