Zhang, Yuqing; Liu, Qixu; Luo, Qihan; Wang, Xiali

XAS: cross-API scripting attacks in social ecosystems.

Summary: With the rapid development of online social networks, various Web application programming interfaces (APIs) on social platforms are released to share profitable social data with all kinds of third-party online services. However, it also brings new risks to social networks once Web APIs are insecurely designed, implemented, and invoked. The focused topic in this paper is security analysis of a new type of cross-site scripting (XSS) which is based on Web APIs in new complicated social ecosystems which consist of social networks, third-party apps, and other online services. In this paper, we refer to Web API-based XSS as cross-API scripting (XAS). For the first time, we take typical XAS attacks in diversified context as cases to demonstrate the new exploiting opportunities and threats in social ecosystems. Also, we design a tool to identify the design and implementation flaws of Web APIs in 11 popular social networks. We discover several security flaws of API via our experiment. According to the results, we conclude causes of XAS flaws in depth. We also examined 143 Web-based apps and verified the prevalence of XAS flaws. Finally, we proposed preliminary measures both in social networks and third-party applications to alleviate XAS.

Keywords: Web security; social network; Web apis; cross-API scripting; cross-site scripting
doi:10.1007/s11432-014-5145-1