

Chapter 38

Auditing Defense Against XSS Worms in Online Social Network–Based Web Applications

Pooja Chaudhary

National Institute of Technology Kurukshetra, India

Shashank Gupta

National Institute of Technology Kurukshetra, India

B. B. Gupta

National Institute of Technology Kurukshetra, India

ABSTRACT

Nowadays, users of Online Social Network (OSN) are less familiar with cyber security threats that occur in such networks, comprising Cross-Site Scripting (XSS) worms, Distributed Denial of Service (DDoS) attacks, Phishing, etc. Numerous defensive methodologies exist for mitigating the effect of DDoS attacks and Phishing vulnerabilities from OSN. However, till now, no such robust defensive solution is proposed for the complete alleviation of XSS worms from such networks. This chapter discusses the detailed incidences of XSS attacks in the recent period on the platforms of OSN. A high level of taxonomy of XSS worms is illustrated in this article for the precise interpretation of its exploitation in multiple applications of OSN like Facebook, Twitter, LinkedIn, etc. We have also discussed the key contributions of current defensive solutions of XSS attacks on the existing platforms of OSN. Based on this study, we identified the current performance issues in these existing solutions and recommend future research guidelines.

1. INTRODUCTION TO ONLINE SOCIAL NETWORK (OSN)

Nowadays, the utilization of Online Social Network (OSN) [Fire et. al. (2014), Haddon et. al. (2011)] has escalated abruptly since such networks have entered into daily routine life of people in the form of virtual gathering locations that ease communication. With the advent of smart phone technology and the development of many digital devices, the usage of OSN-based Web applications (like Facebook

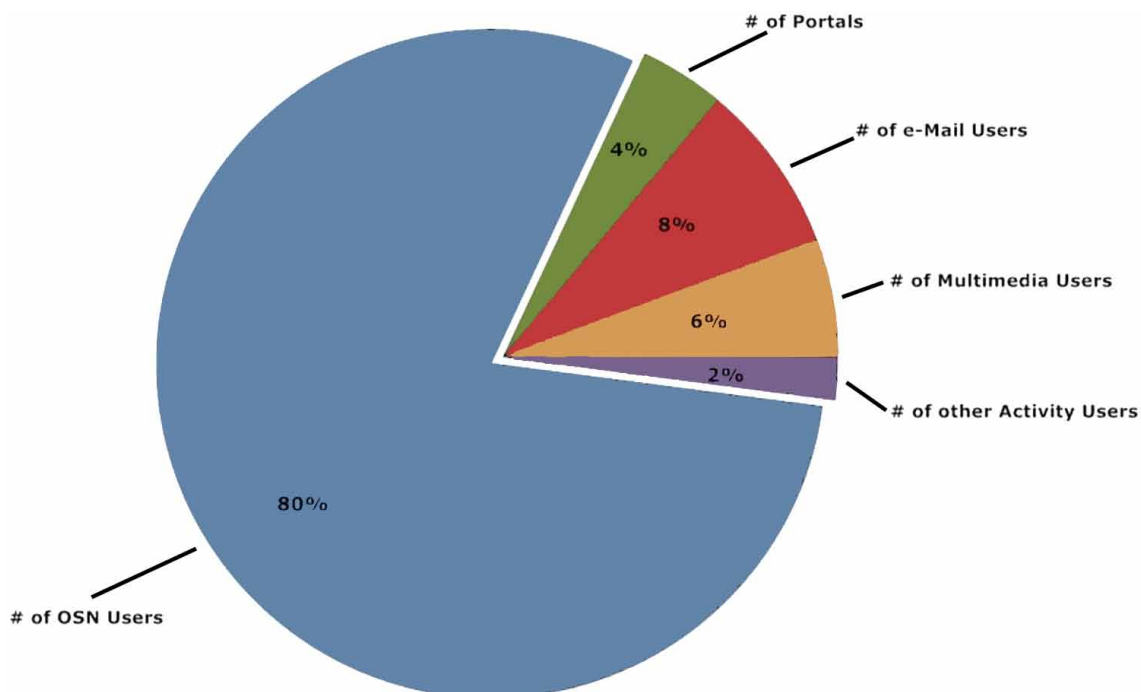
DOI: 10.4018/978-1-5225-3422-8.ch038

[Facebook, (2013)], Twitter [Twitter, (2014)], LinkedIn [LinkedIn, (2014)], etc.) has been tremendously increasing after the development of Web 2.0. Such Web application comprises billions of daily online active users. Figure 1 highlights the statistics of different community of online users in OSN i.e. its popularity among Internet users. OSN basically provide a digital virtual place to users for sharing their information including relationship status, qualification, DOB and many more. Users establish new social connection with their loved ones and re-establish the lost connections. In other words, OSN facilitates socialization. User can interact with other user through posts, messages, photos, and videos. Facebook is the most popular OSN site with 1.23 billion active users [Haddon, (2011), Facebook (2014)]. Other popular OSN-based Websites are Google+ with 200+ million active users [Google+, (2014)]; Twitter has more than 160 million users [Twitter, (2014)] and LinkedIn with more than 150 million users [LinkedIn, (2014)].

As the use of OSN sites is greatly embedded into the lives of general people, to provide privacy to their personal information is a challenging task before the developers and researchers. Users' information may be used by the OSN admin and by commercial companies to know the users preferences and to identify the audience for their advertisement and product usage. So all this leads to the violation of users' privacy and security. According to a survey done by Facebook in December 2013 [Facebook, (2014)], Facebook is having 556 million daily active users on mobile devices, shown an increase of 49% year per year. OSN usage is not popular among adults only but it is also most popular among teenagers also.

According to survey done in 25 European countries among 25000 participants [Haddon, (2011)] it has been observed that 60% of the children in age group of 9-16 are daily users of OSN sites and 59% of those maintain their personal profile on any of the OSN site (26%- 9-10, 49%- 11-12, 73%- 13-14 and 89%- 15-16). Besides this, 30% of children surveyed maintained social connection with person they

Figure 1. Popularity of OSNs among users



29 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/auditing-defense-against-xss-worms-in-online-social-network-based-web-applications/188239

Related Content

Preferential Selection of Software Quality Models Based on a Multi-Criteria Decision-Making Approach

Ankita Verma, Anushka Agarwal, Manisha Rathore, Sneha Bisht and Deepti Singh (2023). *International Journal of Software Innovation* (pp. 1-13).

www.irma-international.org/article/preferential-selection-of-software-quality-models-based-on-a-multi-criteria-decision-making-approach/315739

AI-Driven Virtual Simulation for Packaging Customization

Lei He (2022). *International Journal of Information System Modeling and Design* (pp. 1-10).

www.irma-international.org/article/ai-driven-virtual-simulation-for-packaging-customization/313580

Issues and Aspects of Open Source Software Usage and Adoption in the Public Sector

Gabor Laszlo (2009). *Software Applications: Concepts, Methodologies, Tools, and Applications* (pp. 1577-1591).

www.irma-international.org/chapter/issues-aspects-open-source-software/29465

Dealing With Noise and Partial Volume Effects in Alzheimer Disease Brain Tissue Classification by a Fuzzy-Possibilistic Modeling Based on Fuzzy-Genetic Initialization

Lilia Lazli and Mounir Boukadoum (2019). *International Journal of Software Innovation* (pp. 119-143).

www.irma-international.org/article/dealing-with-noise-and-partial-volume-effects-in-alzheimer-disease-brain-tissue-classification-by-a-fuzzy-possibilistic-modeling-based-on-fuzzy-genetic-initialization/217396

Configuration Management and Documentation

(2017). *Model-Based Design for Effective Control System Development* (pp. 278-296).

www.irma-international.org/chapter/configuration-management-and-documentation/179504