COMPUTERS & SECURITY 58 (2016) 47–62

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A study on Web security incidents in China by analyzing vulnerability disclosure platforms

*Cheng Huang, JiaYong Liu *, Yong Fang, Zheng Zuo*

College of Electronics and Information Engineering, Sichuan University, Chengdu 610064, China

ARTICLE INFO

Article history:
Received 23 June 2015
Received in revised form 31 October 2015
Accepted 23 November 2015
Available online 14 December 2015

Keywords:
Web security
Machine learning
Vulnerability disclosure
Vulnerability management
Security response

ABSTRACT

Understanding the nature of a country's World Wide Web security can allow analysts to evaluate the security awareness of local organizations, the technology employed by researchers, and the defense capabilities of the whole country. In this paper, we put forward a new framework to evaluate the security situation in China with real vulnerability disclosure platforms. The focus of this research is to analyze the current situation of Chinese websites using 57,112 Web vulnerability incidents submitted by 5371 researchers from 2012 to 2015. The dataset is distributed into four types of organizations, including listed companies, government institutions, educational institutions, and startups. We present an approach, based on machine learning and natural language processing technologies, to classify the vulnerability type for each incident. Furthermore, our experimental results show that the vulnerability distribution and response speed toward important issues are so different among the four types of organizations that researchers at various levels of experience begin to take part in submitting vulnerabilities to public disclosure platforms. Based on the results, we propose security some best-practices for organizations and show that the security situation of Chinese websites has changed quickly in the last three years but is still facing several big problems.

1. Introduction

Since Web applications have become popular in recent decades, many traditional business and social activities have been put online. People spend a lot of time surfing the Internet and visiting different kinds of websites every day. It is well known that, while the Internet can be a source of useful information, it is also the cause of issues such as breaches in personal privacy and security. Specifically, security lapses among popular websites cause people to suffer a variety of inconveniences, from leaked personal photographs to the compromise of financial information or even loss of money. Frequently, those incidents are caused by common Web vulnerabilities, like Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), SQL injection, the exploitation of broken authorization, and session management. Attackers try to find weakness in popular websites in order to achieve their aims. The best solution is to find which kinds of vulnerabilities are most used, put more attention on these types of problems, and then fix them.

China has the largest population and the highest rate of economic development worldwide, but in technological terms China is growing much more slowly than other developed countries, especially in the area of security. Many companies and government websites have serious vulnerabilities, but they do not have security experts to help them test and fix these bugs. A new vulnerability disclosure platform, called Wooyun (Wooyun), was established five years ago. Wooyun focuses on building a communication platform between organizations and security researchers. The platform receives real vulnerabilities for all Chinese companies. It provides an opportunity for

* *Corresponding author.* Tel.: +8613668196693.
E-mail addresses: opcodesec@gmail.com (C. Huang), jylscu@gmail.com (J. Liu), yongfangscu@gmail.com (Y. Fang), leftzheng@gmail.com (Z. Zuo).
http://dx.doi.org/10.1016/j.cose.2015.11.006
0167-4048/

researchers to submit vulnerabilities to organizations as well as a learning environment for security researchers because all the vulnerability details are open to the public a month after submission. Three years later, a new platform called BuTian (360) put forward a new solution that offers money to individuals who collect security vulnerabilities from different organizations and content management systems (such as Wordpress, Joomla, Discuz, Drupal, etc.). A third, VulReport (VulReport), is another similar platform to Wooyun.

There are other Internet security testing platforms, such Bugcrowd (2012) (BUGCROWD), Vulbox (2014) (Freebuf), Sobug (2014) (Sobug), Secwk (2014) (JinlongSec), and HackerOne (2014) (HackerOne), which attract many top security researchers in the world and provide commercial security tests for organizations. However, these Internet security testing platforms only focus on paid service, do not make the detailed content of each vulnerability public, and only have a small percentage of the market. Without a doubt, Wooyun and BuTian have the biggest security incidents and vulnerability databases for Chinese websites.

Based on correlation with the Common Vulnerabilities and Exposures Database (CVE) (US-CERT) and the Exploit Database (EDB) (O. Security), Wooyun and BuTian platforms collect many kinds of real security incidents and vulnerability information for different organizations. Although BuTian currently limits the vulnerability details that it provides, a lot of useful information could be crawled from its websites. However, despite the availability of these data, some questions must be considered before performing an investigation into the security situation in the Chinese Web.

- Is it possible to get current security trends based on the history of incidents?
- How would we evaluate the Web security issues via vulnerability disclosure platforms?
- Is it necessary to do this research?

Although the open Web application security project (OWASP) has published many top 10 rankings in recent years, it focuses on the security issues of global websites. Different countries may have different security problems because of its technology and people. Additionally, if we want to evaluate the current Web security issues of Chinese websites, we must not only consider vulnerability types and trends, but also should take into account the technical abilities of the researchers that reported them, the number of organizations they affect, and the security response time toward globally important vulnerability incidents. Taking these factors into account will allow us to achieve a better analysis result.

Several prior investigations have been made into current security issues around the world. However, previous work is mainly focused on understanding the influence of specific vulnerabilities or getting an outline of the vulnerability from popular websites (i.e., by scanning the Alexa top 1 million domains). Instead, our work tries to use different measures to evaluate the state of security in Chinese websites. We study two platforms (Wooyun and BuTian), which provide high quality data sets for each vulnerability incident. The result showcases the real security situation, gleamed from actual vulnerability incidents.

To summarize, this paper introduces the following main contributions:

- We propose a system to analyze incident reports across different vulnerability reporting platforms. We focus not only on the vulnerabilities, but also consider other factors, such as researcher experience and important global incidents. Additionally, we investigate the trend of modern Chinese Web security issues, and the change in percentage of each vulnerability type over the last several years.
- We develop an automatic classifier model to recover elided vulnerability types using natural language processing and machine learning technologies.
- To the best of our knowledge, we compile the first assessment of security response from different Chinese organizations toward vulnerabilities, exploring the difference between four different classes of organizations. From this, we create a list of security suggestions based on the analyzed data for organization administrators and IT professionals, which we hope will increase awareness of web security issues.

The paper is organized as follows. An overview of related work is provided in Section 2. The framework design is described in Section 3. Section 4 compares the different vulnerability disclosure platforms, and introduces experiment data sets and vulnerability types. The research method used in our assessment is outlined in Section 5, where different aspects are presented to analyze our datasets. The results of our research are described in Section 6, with a discussion of the insights gleamed from our analysis discussed in Section 7. Finally, the conclusion is given in Section 8.

2. Related work

The security situation in certain places or areas has been studied for some time, and many models and methods have been proposed. The most relevant previous work will be highlighted here.

2.1. *Single vulnerability analysis*

There are many papers that focus on the evaluation of the security of a given nation by employing web scanning techniques. However, most of the past research on security issues has focused on analyzing the theory and effects of a certain common Web vulnerability in the wild. Appelt et al. (2014) developed a new SQL injection tool and used it to find vulnerabilities in common Web applications. Delamore and Ko (2014) proposed a large-scale SQL Injection detection tool to identify such vulnerabilities in the field. Lee et al. (2012) proposed a security testing technique based on a fuzzy method to detect known vulnerabilities of web applications using both static and dynamic analyses. Tripp et al. (2013) investigated a novel approach for enabling precise yet scalable static taint analysis, and developed a tool to help people find different kinds of bugs through source code analysis. While these tools have demonstrated their effectiveness, they have not been used to