Bkav

RESEARCH

22% OF WEBSITES WORLDWIDE

have security vulnerabilities

November 2013 (Updated February 2014)

CONTENTS

Abstract

More complex and serious website attacks, information leaks are happening now than ever before. Such incidents have caused million dollars in loss for companies, organizations, and affected hundred millions of websites' users. In many cases, website attacks not only have economic purposes, but also derive from political conflicts.

July 2013, four Russians and one Ukrainian man were charged in what US Attorney Paul Fishman called the "largest hacking and data breach scheme ever prosecuted in the United States". In 7 years, from 2005 to 2012, these five hackers stole and sold 160 million of credit card numbers from more than a dozen companies, including some big retailing or financial units such as Nasdaq, Dow Jones, J.C. Penny, Visa Inc, 7-Eleven, Heartland paying system, Dexia Bank, Carrefour SA (CA) – France's biggest retailer.

By the beginning of 2013, a detailed report of Mandiant – US revealed the track of a group of Chinese hackers to a military unit of this country. Taking advantage of system vulnerabilities, for many years these hackers have dropped spyware with the aim to steal data from the systems of US companies and organizations.

Looking back further, by October 2010, WikiLeaks released hundreds of thousands of battlefield reports, diplomatic cables and a video of a U.S. helicopter attack that killed civilians. This largest leak of classified material in U.S. history was originally caused by US soldier Bradley Manning. Many believed the soldier was so easily able to dump data off of the networks because they weren't secure after all.

The increasing number and severity of such cyber security incidents have been called into question. Why are such crucial data leaked out of financial companies, well-known organizations, of which the systems are thought to be highly secured? Similarly, when conflicts arise among nations, political parties, why there are usually a series of website attacked in just a day? Bkav's experts state: the existence of website vulnerabilities might be the underlying cause. This inspired Bkav to carry out the research on vulnerabilities in websites all over the world.

Methodology

To conduct the research, Bkav set up a website security scanning system to find vulnerabilities. Before scanning, we made a list of websites of companies, organizations in many different countries. In each country, about 20 websites of units being in the top ranks of the stock market were chosen. We applied this criterion due to the belief that these are websites of big companies, organizations from each country so they must be best protected, while websites from others are less secured. Finally, 516 websites of big companies, organizations from 25 countries representing different areas in the world, such as US, UK, New Zealand, Korea, Japan, Mexico, South Africa, etc. were added to the list. (The detailed scanning data is in appendix 1)

Research period

The research was conducted in seven months, from July 2013 to February 2014, through 4 scanning phases on Bkav WebScan – Bkav's web security scanning system.

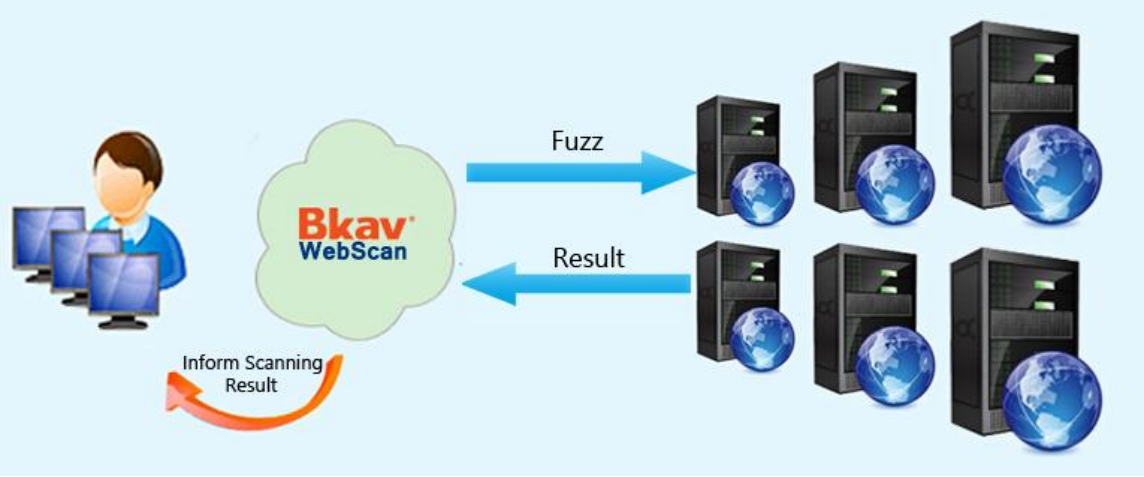
Research implementation

From the data of 516 selected websites, their addresses were added to the database of Bkav WebScan system. Then, the testing program was activated and automatically scanned to check and find out vulnerabilities in every website. With each website, Bkav WebScan tested many kinds of vulnerabilities such as: SQL Injection, Blind SQL Injection, XSS, and so on. From the websites' response, WebScan would produce report on the vulnerable components, kind and severity of the vulnerabilities. When the testing completed, the scanning result was exported into an HTML file. Bkav experts then analyzed the result.

Based on the scanning result of Bkav WebScan, the following main issues can be identified:

- The total number of vulnerabilities in each website
- Severity of the vulnerabilities
- The existence of critical website vulnerabilities such as: SQL injection, XSS, Xpath injection, etc.

WebScan operating model



Bkav WebScan system scans for website security vulnerabilities through black box approach. Specifically, the system's core sends fuzz data to the website hosting server or directly accesses the website's URL with faulty data, then sends the response to the analyzer before producing conclusion about the vulnerability.

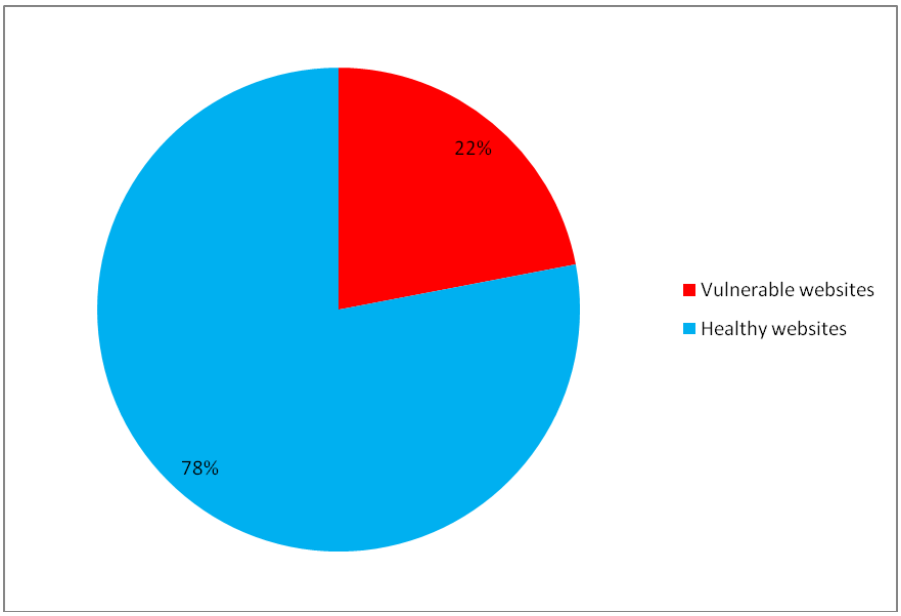
Fuzz data is a collection of identifying data, it is combined with some parts of URL or data processed by the website. Fuzz data used in this research is collected from our years of practical experience in vulnerability researching, checking and fixing. It ensures the accuracy for the identifying of vulnerabilities with Bkav WebScan.

With each kind of bug, the testing system is meticulously built from experience of Bkav's security experts. For instance, Bkav WebScan's number of samples for XSS bug only reaches above 40. With normal web programmers, validating input data is not really necessary because most of them focus on building websites which run

smoothly rather than secured ones. On the other hand, with an expert in cyber security, getting a large enough number of samples (of about 40) for only one XSS is not easy and requires years of experience.

Key Findings

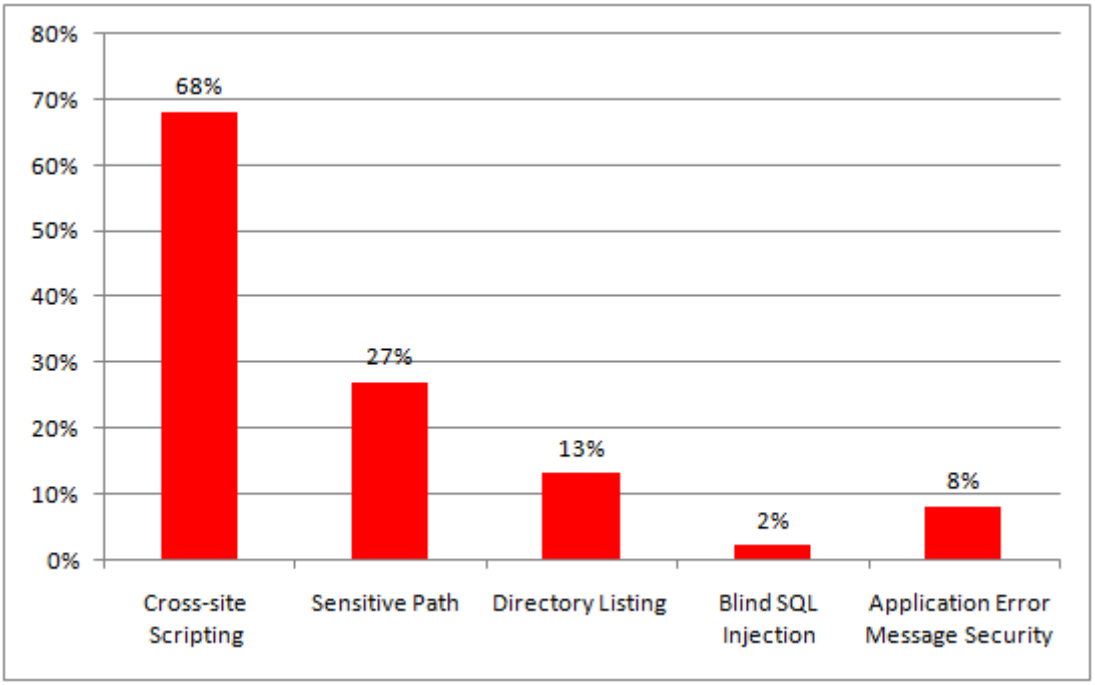
Finding 1: 22% of scanned websites have vulnerabilities



114 out of 516 scanned websites, about 22%, are vulnerable. This is really a high rate; and if a website is vulnerable, it normally has more than one bug. According to the data by Bkav WebScan system, the highest number of vulnerabilities in a website is 407, and the average ranges from 10 to 20.

22% of websites having vulnerabilities constitute a "fertile land" for any hackers with even basic IT knowledge to intrude into website systems of companies, organizations. Based on successful intrusion, hackers can escalate privilege to steal information. Furthermore, normal users might be affected because when a website is attacked and dropped with malware, accessing it might make users' computers become victims. August 2013, the New York Times was under DNS attacks and its readers could not access the website for some hours. This is an evidence for the fact that, besides directly affecting companies, organizations which own the victim websites, the attacks do have impact on normal users.

Finding 2: Five kinds of vulnerabilities detected



There are 5 kinds of main vulnerabilities: Cross-site Scripting, Sensitive Path, Directory Listing, Blind SQL Injection and Application Error Message Security. The scanning result shows that 78 websites (68% of vulnerable websites) have **Cross-site Scripting** (XSS). This is one of the most popular vulnerabilities and one important security issue to web developers and users. Any websites permitting users to upload information without carefully checking the existsence of dangerous code have the potential for XSS bug. XSS bug is among the basic and popular kinds of vulnerability that engineers usually meet when programming websites. Hackers can exploit XSS vulnerabilities to take control of the admin page.

Ranking second is **Sensitive Path,** which appears in 31 websites (27% of the vulnerable websites). This kind of bug can cause the disclosure of sensitive links. In case the revealed links lead to simple information, the damage might not be serious. However, it will be really dangerous if the paths are admin or configuration links. The worst is that hackers can access websites' configuration page or log in administration page.

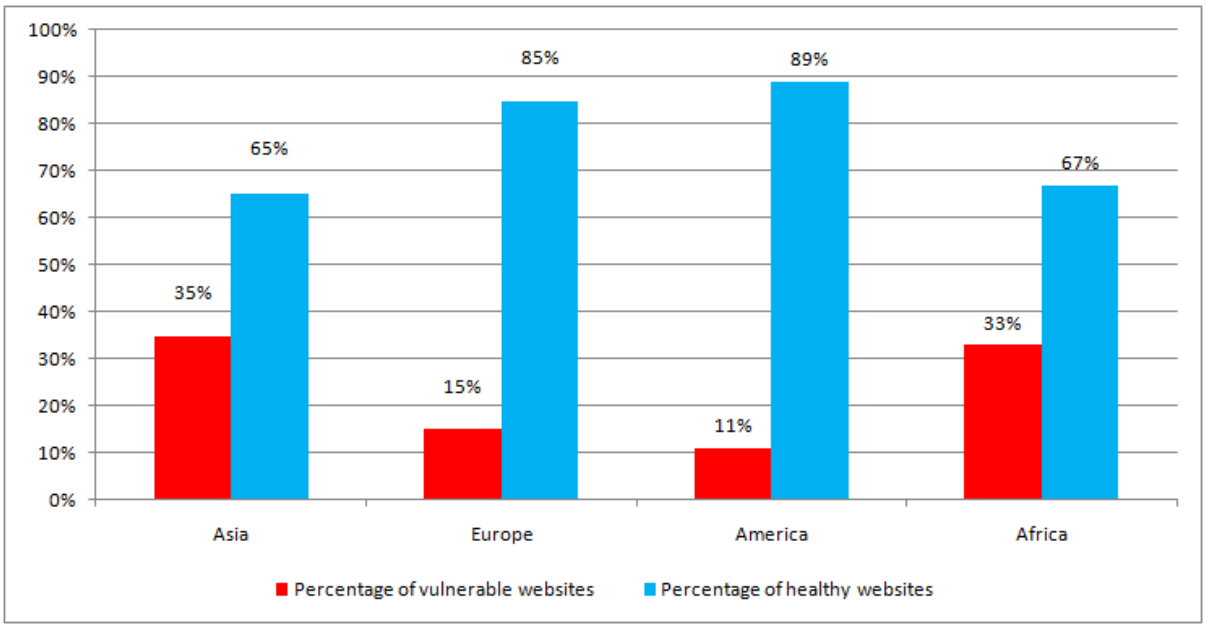
Directory Listing appears in 13% of vulnerable sites. This kind of security hole comes into existence if administrators do not configure the web server to prevent the listing of directories. If users access a victim website's link which leads to a folder (*http://abc.com/folder/*), all files in this folder will appear on the browsers of users. Although the bug is not too dangerous, the results might be unpredictable if the folder contains secret files that administrators do not want to show to normal users such as log, configuration, or sensitive files.

Application Error Message Security in 8% of vulnerable websites results from the fact that web server's messages are exposed during programming or debugging. Although Application Error Message Security does not pose direct threat to websites, it is a stepping stone to exploitation of other dangerous bugs.

2% of vulnerable websites have **Blind SQL Injection**. Programmers' failure to validate the input parameters of queries to database is the main cause of this kind of hole. Hackers can utilize Blind SQL Injection to insert unexpected commands to take control of website, destroy database, steal secret information such as credit card information or customer accounts. Even though appearing in just a small number of websites, Blind SQL Injection poses the greatest and most direct threat to its victims because exploitation does not require any intermediate steps like other vulnerabilities.

Bkav states these are basic and popular bugs. However, their threats are great because hackers can easily find them by simple tools or even by chance. The underlying reason might lies in the inadequate awareness of website developers as well as in the lack of website security testing procedure. Hackers can exploit these very basic vulnerabilities to carry out attacks against websites, directly affecting operation of companies, organizations as well as their users.

Finding 3: The density of vulnerabilities is different among areas



According to the data collected by Bkav WebScan, America is the area with the highest rate of safe websites. 11% of websites there have vulnerabilities, and 89% are indentified to be safe. Then, Europe and Africa rank the second and third, with invulnerable websites accounting for 85% and 67%. The diagram above also shows that Asia is the area with the highest rate of unsafe websites, 35%. The figures are quite homologous with the development of science and technology or the level of IT application in different areas in the world.

Conclusion and Recommendations

1. Conclusion

This result does be in line with expectations of Bkav. The rate of more than one fifth of scanned websites having vulnerabilities is no doubt the reason for spillage of information such as credit card details, business secrets, confidential political information, etc. This has called into questions the security of websites all over the world. Great diversity in kind and severity of vulnerabilities creates a favorable environment for hackers with even very basic knowledge. Threats coming from website security holes are not troublesome to a certain company or organization only, but to the whole world as well.

From years of experience in network security, Bkav's experts identify that basic website vulnerabilities appear because of two main reasons. Firstly, companies, organizations do not have regular website security testing procedure to detect existing risks in their websites, so as to have timely solution. Secondly, website developers do not have adequate knowledge of security; hence they might make basic mistakes when developing websites.

Unlike in real life where human is protected by strict laws, in online world nowadays, the outstanding development of technology means that risks from unsafe systems meet no geographical barriers. Hackers can sit in this country and attack websites in others. Laws seem to fail to follow the rushing development of technology. Therefore, cyber attacks, system intrusions, data breaches, which are happening more now than ever before, do not merely have economical purposes. They now also aim to obtain certain political goals. This requires a change in awareness from governments, organizations, or even in knowledge of website developers, coders.

Based on practical experience combined with observation, summarization and analysis of the results by Bkav WebScan system, Bkav has conducted this research to help

people understand more about website security situation around the world. The data is automatically recorded by Bkav WebScan system, so the above results may not stand for the whole situation. The practical figures might be even much greater if the testing is directly carried out by security experts. The research was carried out by Bkav independently, its data does not aim to assess the security level of websites of any companies or organizations.

Through this research, we also have a number of recommendations with the aim to help website administrators of strengthen information security for their companies, organizations.

2. Recommendations

It's advisable to have and implement website security testing before official launching. Besides, regular checks are necessary, so that bugs are fixed timely, ensuring safety for your website system. Furthermore, companies and organizations should have training courses for developers and coders to strengthen their secure programming knowledge. When coding websites, engineers must analyze all possible cases to avoid potential vulnerabilities. Bkav recommends that companies and organizations should use professional services provided by security firms for their website systems to stay safe. In Bkav, periodic training courses for engineers, periodic hole testing on our websites with Bkav WebScan system and security testing by security experts have helped to ensure the best information security.

About Bkav

Established in 1995, Bkav Corporation is the leading firm in network security, software, smartphone manufacturing and smarthome. In the field of network security, antivirus and mobile security softwares of Bkav have been present in more than 100 countries all over the world. The leading technology research and advisory firm Gartner has listed Bkav among "Cool Vendors in Emerging Markets".

Bkav has preeminent security experts. The corporation is known as the security firm to discover the first critical flaw in Google Chrome just days after its launch in 2008. Bkav was also the firm to trace the master server in Britain of unprecedentedly massive DDoS attacks targeting US and Korean governments' websites in July, 2009.

Bkav Corporation is known as a manufacturer of security appliances such as intrusion prevention system Bkav Network Inspector, Bkav Antispam GW, Bkav WebSecurity Scan. Bkav is also providing collaboration software products (messenger, workflow management, mail, video conference).

In electronics industry, Bkav is a smartphone and smarthome manufacturer. With Bkav SmartHome, every equipment in your house will be connected and controlled automatically based on smart context scenarios via touch screen or tablet, hence creating a convenient, safe and energy-saving living environment.

Contact Information

Bkav USA

800 El Camino Real, Mountain View, California, 94040

Telephone: (+1) 202 386 6779
Website: www.bkav.com

Email: Bkav@bkav.com

Appendix 1

Data collected by Bkav WebScan

No.	Nation *(Alphabetically sorted)*	Number of vulnerable websites	Number of invulnerable websites
1.	***Belgium***	2	18
2.	***Bulgaria***	4	16
3.	***Cambodia***	9	12
4.	***Croatia***	3	17
5.	***Czech***	2	18
6.	***Finland***	3	17
7.	***Hungary***	4	16
8.	***Indonesia***	3	17
9.	***India***	6	14
10.	***Japan***	6	14
11.	***Korea***	8	12
12.	***Malaysia***	8	12
13.	***Mexico***	1	19
14.	***New Zealand***	2	18
15.	***Pakistan***	4	19
16.	***Poland***	5	15
17.	***Serbia***	8	13
18.	***South Africa***	7	13
19.	***Taiwan***	4	15
20.	***UAE***	5	17
21.	***UK***	3	21
22.	***Ukraine***	2	18
23.	***USA***	4	21
24.	***Venezuela***	5	15
25.	***Vietnam***	6	15

Reference

1. Emily Jane Fox, "CNN", <http://money.cnn.com/2013/07/25/pf/credit-card-hacking-scheme/index.html>, 25th August 2013

2. Five people charged for stealing and selling 160 million credit/debit card numbers, United States District Court, District of New Jersey, Criminal No. 09-626 (JBS) (S-2) <https://www.documentcloud.org/documents/739951-indictment-for-hacking-corporations.html>

3. Mandiant Report, <https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/>, 20th March, 2013

4. Chris Plesance, Dailymail <http://www.dailymail.co.uk/news/article-2412465/Chelsea-Bradley-Manning-requests-Wikileaks-pardon-president-Barack-Obama.html>, 5th September 2013