Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 298 – 306

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Empirical Analysis of Web Attacks

Daljit Kaur[a], Dr. Parminder Kaur[b]

[a]*Assistant Professor, Lyallpur Khalsa College, Jalandhar, India*
[b]*Assistant Professor, Guru Nanak Dev University,Amritsar, India*

Abstract

The web applications are becoming more popular and complex in today's era of Internet. These on-line applications provide rich benefits along with risk to organization, brand and data. Malicious attackers continue to exploit vulnerabilities in applications in order to steal sensitive information. The outlines of this paper is to analyze web attacks in recent years that have compromised web applications, its data or its users. This paper includes the web attacks analysis from Website Hacking Incident Database (WHID) and other information security and news websites. Also, it is an effort to analyze various attacks on major categories of web sites which is a guide to developers to take respective appropriate preventive measures in future. The top web attacks have been identified and also the top vulnerable categories of web applications are analyzed .

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: web attacks, web security, secure web development, web categories and web vulnerabilities.

1. Introduction

Over the past few years, a clear trend has emerged within the information security; web applications are under attack. Web applications continue to be a prime vector of attack for criminals, and the trend shows no sign of abating. Everyday there are new reports of highly organized cyber attacks on leading web sites. Application layer is the soft target for attackers because of vulnerabilities existing in web applications 1. Certainly, secure web development and writing secure code is the most effective method for minimizing web applications vulnerabilities 4. However, writing secure code and secure development is much easier said than done and involves various issues. Moreover, in today's competitive era of getting applications online in lesser time, security is not given the required importance during the development of many web applications. Also, implementing security using secure development life cycle takes more time, requires skilled staff and costs higher, which is not preferred by the small to medium sized organizations. Moreover, for some organizations spending more on secure development of web applications may not be a wise decision as they do not contain any sensitive information but brand security can be preferred by them. In other words, we can say that security is required for each web application but the level of security may vary from organization to organization and the type of web application as the primary goal of web applications is to gain some monetary or philosophical etc. To implement security, we must know what to secure and what are the loop holes. The objective of the study is to find the trend of attacks on web applications and the target of attackers i.e. to know what vulnerabilities are commonly at risk and using that analysis to develop more secure web applications in future .This paper analyses top web attacks on different web categories. It is also an effort to guide web developers to take preventive measures during development by looking insight the attack trends in recent years. Web developers can implement essential security features without wasting much time on finding security requirements and following a strict secure development life cycle. The research mainly focuses to answer the following questions:

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.057

What are the major attacks occurring on the web in recent years?
What type of web sites attracts maximum attackers?
What types of attacks are common on the major categories of web applications like finance, education, government etc. ?
Do all web categories observe the same types attacks and need the same security level?

The paper is organized as: Section 2 describes the research methodology, Section 3 reviews the literature and Section 4 analyses and compares the web attacks on yearly basis and also it briefs about these attacks. Section5 considers the ten major web categories and analyses attacks on each.

2.Research Methodology

To analyze the attacks of previous years for our research work, we have collected database of attack incidents on web applications from Web Hacking Incident Database, and following various national and international security and hacking news sites like hackread.com, news.softpedia.com, abcnews.go.com, infosecurity-magazine.com, sc-magazine.com, welivesecurity.com, itv.com, databreaches.net etc. The Web Hacking Incident Database (WHID), is a Web Application Security Consortium project dedicated to maintaining a list of web applications related security incidents. WHID's goal is to serve as a tool for raising awareness of the web application security problem and provide information for statistical analysis of web applications security incidents10. Also we have followed a blog, hackmageddon.com which shows the cyber attack statistics and timelines only after verifying each attack 5.

For this research work, we have collected the web attacks incidents database from January 2012 to June 2015, then found the top attacks on web applications and major web categories those are at high risk of these attacks **.**

3.Literature Review

Since the development of Internet and World Wide Web (WWW), web applications have become very popular, and, nowadays, they are used in almost every environment. With rise in number of web applications and the sensitive information they are containing, web attacks have also become common. The previous web site security statistics report of WhiteHat depicts that, 86 percent of web sites that they have tested, have had at least one serious vulnerability and the average number of serious vulnerabilities are 16.7 8. And the work done by W.Du, K.Jayaraman finds that the root cause of unique vulnerabilities is stateless nature of web 3. Application vulnerabilities Trends Report by cenzic has shown the trend of vulnerabilities in 2012 to 2014, which indicates the drop of vulnerabilities with time 1. It also says that the drop in number of vulnerabilities does not mean hackers are less persistent and web applications are more secure. In fact, hackers fire power is increased and there are more powerful attacks in 2014. Secure web applications are only possible when a Secure SDLC (Software Development Life Cycle) is followed. In our previous research work, we had proposed a Secure SDLC that implements security from the beginning process of development from Requirement Analysis to Design, Coding, Testing and Implementation phase 6. According to 4, with the increasing complexity and interconnections in digital infrastructure, difficulty of achieving security is increasing exponentially and the work done by Garg and Singh explains the five common security problems like SQL Injection, XSS (Cross Site Scripting), etc and their countermeasures in SDLC. In our another paper, we had also mapped the 20 common web vulnerabilities to the actions needed to take during development process which provide help to developers to avoid common vulnerabilities 7. Lot of work is done on these common vulnerabilities. As Savita B.Chavan and Dr. B.B. Meshram has classified the attacks and weakness that can lead to the compromise of website,its data or its users. They have classified vulnerabilities on the basis of development phase of web applications2.

It is obvious that implementing security in SDLC takes more time, requires skilled staff and costs higher, which is not preferred by the all clients. Moreover, for some organizations spending more on secure development of web applications may not be a wise

decision as they do not contain any sensitive information but brand security can be preferred by them. It was realized that security is required for each web application but the level of security may vary from organization to organization and the type of web application. Developers may choose the vulnerabilities to avoid for a web site, depending upon the trend that may better secure it in less time and efforts. This research work is an effort to look insight the security level requirements for various web categories by analysing attack trends on these categories.

4. Web Attacks Analysis

Web applications are the continuous target of hackers. Web attacks data is collected from Jan 2012 to May 2015 and also the major attack categories are realized on the basis of frequency of these attacks. Table I shows the attacks in previous years, which indicates the drop in most attacks but it does not mean that web sites are more secure than previous as the attacks are more powerful and dangerous in terms of information lost, risk and cost.

Table1. Web Attacks Data

Attack	Jan – Dec 2012	Jan – Dec 2013	Jan –Dec 2014	Jan- June 2015
SQLi	352	185	112	71
DDoS	151	178	85	30
XSs	68	34	6	02
A/c Hijacking	30	106	88	34
Defacement	74	120	135	57
Unauthorized access	10	14	11	1
Direcory traversal	0	3	2	1
Phishing	9	2	2	0
PoS/Malware	11	29	74	31
BruteForce	0	4	4	0
Malicious Code injection	0	1	5	0
DNS Hijacking	6	29	15	5
Server Vulnerabilities	1	0	2	0
Others	97	132	129	35
Unknown	265	208	183	68
Total	1074	1045	853	335

The attacks in 2014 are decreased by 20.6 percent as compared to 2012 and the negligible decrease in the year 2013 is seen. Only the attacks Defacement and Malware are increased drastically in the years 2013 and 2014 comparative to 2012. Malware based attacks are increased almost 2.6 times in each year and 82 percent rise seen in defacement attacks from 2012 to 2014. Also, the current year is showing the similar attack trends in its first half as the previous year.

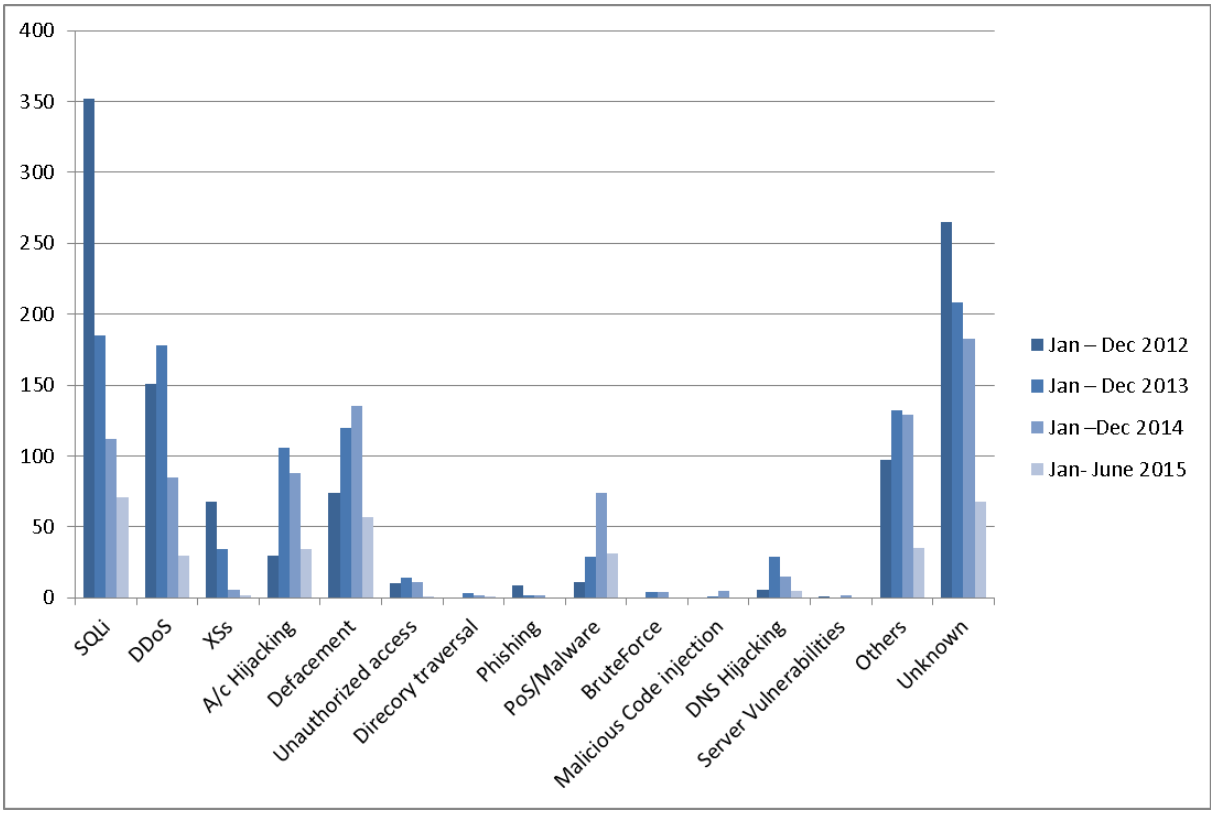

Fig. 1

The comparative chart of the three years is shown in Fig. 1.It reveals the fact that most attacks are reduced in number while few attacks like Defacement, Malware, DNS /Account Hijacking are increased than previous years.

The top five categories of the web attacks are SQLi (SQL Injection) , DDoS (Distributed Denial of Service), Defacement, Account Hijacking and Malware. SQLi attacks are dropping in number but still it is most occurring attack on web applications. Defacement and Malware based are growing and attacks like Account Hijacking, DDoS, XSS (Cross Site Scripting) are popular among hackers. These attacks cause security and monetary risk to organization, brand and data as well as inconvenience and insecurity to users. Many attacks are popular among hackers for a particular set of web applications depending on the services provided by it. Next section identifies various categories of web applications and attack trends on them.

.

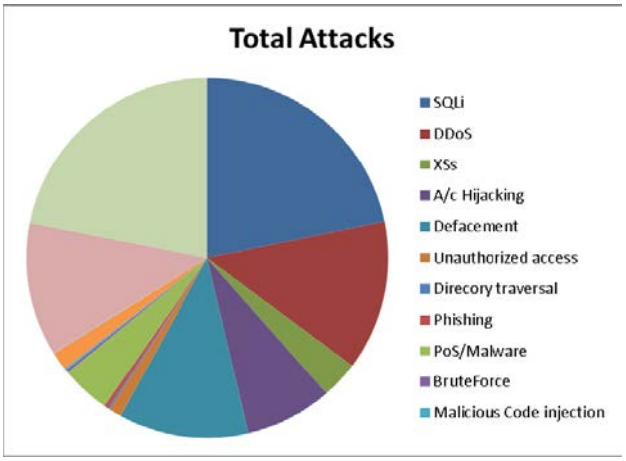

Fig. 2

5. Web Application Categories

Every web application that we see falls into a web category and here we have identified the major ten categories of the web applications and these include financial, government, education, news, tourism, entertainment, health, social networking, e-commerce and software/video games. Then we have analysed the identified attacks in the previous years, depending on the category they belong and they have shown the similar trend as shown in Table 2 and graphically represented in Fig. 3. It is seen that government web sites are leading with huge difference in compromising with attacks in the years 2012, 2013 and 2014. Also according to a report in an IT newspaper, Tech Gateway's Feb 2015 issue, government sites are maximum vulnerable to attacks 9.

The other web applications that have significant number of attacks in the previous three years are Educational, Social Networking, Finance and the web sites that provide software to download, use or video games. Tourism related web applications have faced least number of attacks, as shown in Table 2. Trend of the attacks on the web application categories are similar year wise as the major four vulnerable categories are government, Education, Social networking and software/video games in all the three years with consistent and highest vulnerable Government websites.

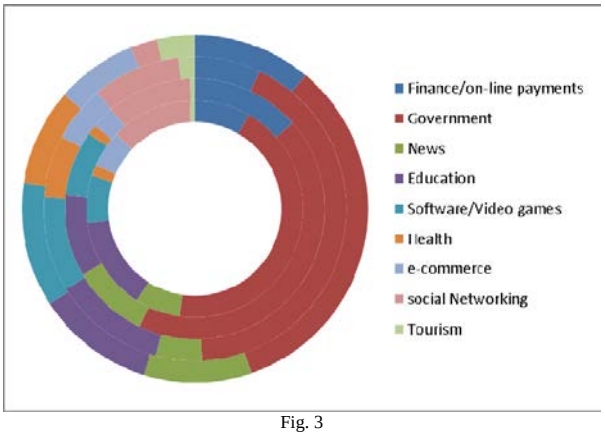

Fig. 3

Table 2 Web Categories

Web Application Categories	2012 Attacks	2013 Attacks	2014 Attacks	2015 Attacks	Total Attacks
Finance/on-line payments	47	98	33	22	200
Government	248	315	197	67	827
News	38	69	23	20	150
Education	78	73	56	22	229
Software/Video games	40	59	47	23	169
Health	9	9	31	18	57
e-commerce	31	20	28	15	94
social Networking	69	77	44	5	195
Tourism	4	4	8	7	23
On-line entertainment	31	17	9	10	67

Now, each web application category was analysed for the last three years attacks and result are shown in Table3 . Government web sites are leading in almost each type of attacks.

Table 3 Attack trends on web categories

Category	**SQLi**	**DDoS**	**Defacement**	**A/C Hijacking**	**Malware**	**Unauthor. Access**	**DNS Hijacking**	**XSS**	**OTHERS**	**UNKNOWN**
Finance/on-line payments	30	70	12	1	9	2	1	2	20	53
Government	132	186	232	28	16	5	3	24	107	113
News	39	27	13	29	1	1	3	9	23	17

Education	76	4	21	10	15	5	--	11	20	60
Software/Video games	47	30	7	14	5	1	2	9	20	46
Health	4	1	1	12	11	3	--	2	11	22
e-commerce	37	4	1	8	11	--	--	5	4	24
social Networking	55	38	13	13	3	3	24	5	19	21
Tourism	8	0	1	2	3	--	--	--	2	6
On-line entertainment	14	11	2	15	2	2	--	5	1	8

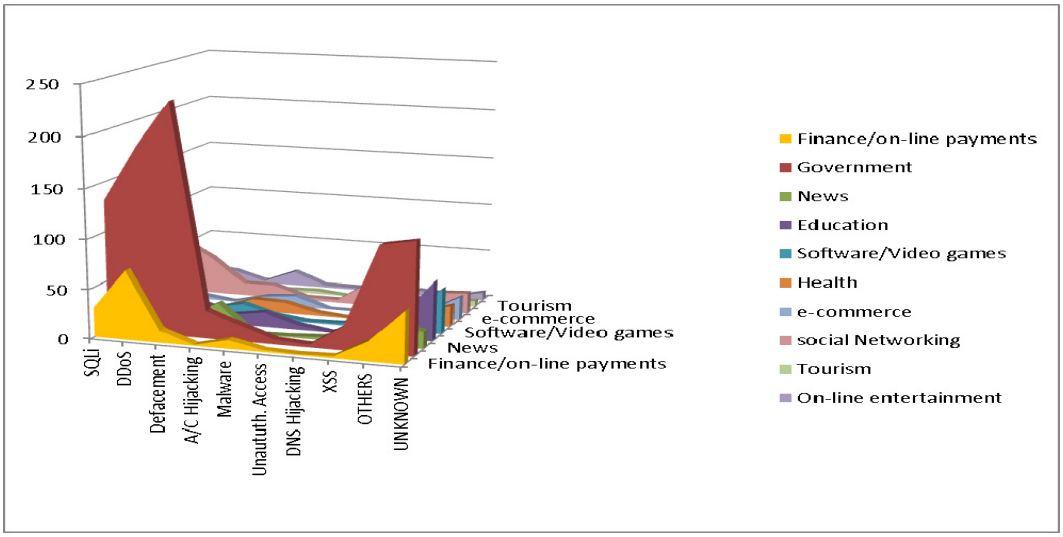

Fig. 4

Figure 4 shows the top two categories of the web applications and the different attacks distribution. Maximum attacks on government sites are Defacement attacks followed by DDoS, SQLi, XSS and others. Educational web sites have maximum SQLi attacks followed by DNS Hijacking, Defacement and Malware attacks. Government websites have least attacks of type DNS Hijacking and Unauthorized Access. Different web sites categories have different types of attacks distribution. We have identified the top attacks on each category as shown in Table 4.

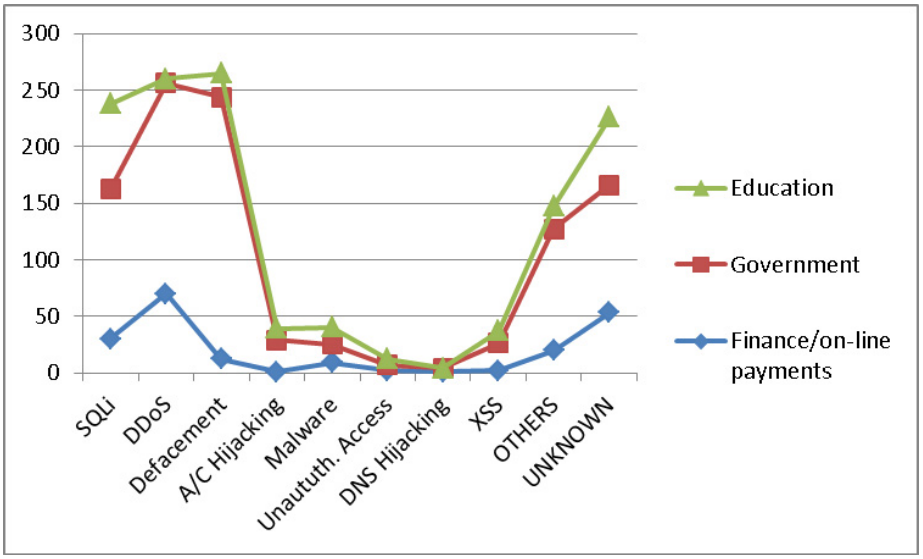

Fig 5

Table 4

Category	Attack 1	Attack2	Attack3	Attack4	Attack 5	Attack 6
Govt	Defacement	DDoS	SQLi	Unknown	Others	XSS
Education	SQLi	Unknown	Others	Defacement	Malware	XSS
social N/w	SQLi	DDoS	DNS Hijacking	Unknown	Others	Defacement
Finance	DDoS	Unknown	SQLi	Others	Defacement	Malware
S/W or Video Games	Unknown	SQLi	DDoS	Others	A/c hijacking	XSS
News	SQLi	DDoS	A/c hijacking	Others	Unknown	XSS
E-commerce	SQLi	Unknown	A/C hijacking	Malware	XSS	DDoS
online Entertainment	SQLi	A/c Hijacking	DDoS	Unknown	XSS	Malware, Unauthorized Access
Health	Unknown	Others	A/c Hijacking	Malware	Unauthorized Access	SQLi/XSS
Tourism	SQLi	Unknown	Unauthorized Access	----------	----------	

So, in order to develop a web site we can see the attack trends and make it more secure just by following the countermeasures of the vulnerabilities that are making those attacks successful. The preventive actions of top twenty vulnerabilities are given in our previous work 7. Developers may follow those preventive actions during development life cycle of web applications and avoid dangerous attacks. Different web applications need different level of security and there is no need to spend more efforts than they deserve. It may save development time, cost

and still more secure.

6. Conclusion and Future Work

Web applications reach out to a larger, less-trusted user base than legacy client-server applications, and yet they are more vulnerable to attacks. Many companies are starting to take initiatives to prevent these types of break-ins. This paper gives the empirical analysis of the web attacks and their occurrences on different web categories. Though 100% security is not possible in this insecure world of Internet but this analysis may help the developers to concentrate on the avoidance of some major occurring attacks during the development phases of that they are going to develop. It has been not specified in this paper that what actions in SDLC should be taken to avoid the corresponding vulnerabilities. The occurrence phase of each vulnerability in SDLC can be found by looking insight it and respective actions in development, coding and testing phase can be taken. The proposal of model is not given at this stage as each attack needs to be case studied for that. In future, a framework or model for the secure development of web applications can be designed and tested on the basis of trend of web attacks on different web categories revealed from this analysis.

References

1. Application Vulnerability Trends Report , *Cenzic Report*, 2014.
2. S.B. Chavan and B.B. Meshram, Classification of Web Application Vulnerabilities, *IJESIT* Volume 2, Issue2, March 2013.
3. W. Du, K. Jayaraman, Tan, X. Luo and T. Champin. Why Are There So Many Vulnerabilities in Web Applications, The New Security Paradigm Workshop(NSPW), 12-15 September, 2011.
4. A. Garg and S. Singh. A Review on Web Application Security Vulnerability, *IJARCSSE*, volume 3, Issue 1, January, 2013.
5. P. Passeri, Cyber Attack Timelines from www.hackmageddon.com
6. D. Kaur, P. Kaur and H. Singh , Secure Spiral: A Secure Software Development Model, *Journal of Software Engineering*, DOI:10.3923/jse.2012.10.15 pp.10-15
7. D. Kaur, P. Kaur , Case Study: Secure Web Development, Designing Engineering and Analyzing Reliable and Efficient Software , *IGI Global*, 2011 pp. 239-250.
8. Website Security Statistics Report , White hat Security, 2013.
9. Government websites are more vulnerable, article published in weekly Tech gateway newspaper, Volume 2 , Issue 3
10. R.Barnet: Web-Hacking-Incident-Databse retrieved from http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database on Nov 20,2015