A Survey on different Web based attacks

Harsh A Bhatt[1], Prof. Tejendra Thakur[2]
[1, 2] Department of Computer Engineering
[1] GTU PG School, India
[3] UCET, GTU, India

Abstract- *Web application is one of the most powerful communication channel and service providers for information delivery over internet today. Securing web is like securing our nation. So, internet security is very much encouraging task for us. OWASP top 10 vulnerability list that resulted more number of attacks in the website in the few years. In this paper we are discussed the different types of web application attacks like Cross Site Scripting attack(XSS), DOS attack, SQL Injection Attack. Survey of such attacks happening in last three to four years. To find out such security weakness or vulnerabilities Penetration testing method is used.*

Keywords- OWASP Top 10, Web application, Cross Site Scripting – XSS, SQL Injection, DOS attack, Penetration testing

I. INTRODUCTION

Now a days Web applications are widely used everywhere in the world. So, the web application security is the biggest issue all around the world. The world is extremely dependent on the Internet. Open Web Application Security Project (OWASP) Top 10 vulnerability gives the different attacks in the website. XSS, SQL injection, Sniffing, Request Encoding and DOS attacks which poses an enormous threat to the availability of the Internet. An existence of these attacks on the web damages or completely interrupt services to authentic users by expending communication and/or computational resources of the target.[1] A Web application (Web app) is an application program that is stored on a remote server and delivered over the Internet through a browser interface. Currently to achieve security of web application is a leading task for any organization including the most modest types of e-commerce, banks and even large state systems. Web application security is crucial part of corporate world. A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent authentic users from accessing the service.[5] Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise gentle and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. [6] Penetration testing (also called pen test) is the practice or process of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. The main objective of penetration testing is to determine security weaknesses. [2] Web application stores the sensitive information such as financial and health, ethical and legal consequences and also to evaluate and identify the potential vulnerability for future research in this area. This paper will provide the survey of different web application attacks.

II. SURVEY OF DIFFERENT WEB ATTACKS

There are many different types of attacks are occurred due to vulnerabilities in web software or application. Some of the attacks are given below:

A. Cross Site Scripting (XSS) attack:

XSS is also called CSS (Cross Site Script), Cross Site scripting attacks, it refers to a malicious attacker inserts malicious Html code into the Web page, when users browse the page, the Html code embedded in Web will be executed, which would allow an attacker to control the display contents of a Web page, or on behalf of the attacker to perform certain actions, it can be used for stealing privacy, Phishing and other malicious attacks. The technology that XSS attack used is mainly HTML and Javascript.

There are basically two major types of XSS vulnerabilities:

1. Reflected (Non-Persistent) Attack – In a reflected XSS attack, the attacker influences a victim to click on a specially created link that makes a request to a vulnerable web- server. This enables the attacker to run arbitrary code in the victim’s web-browser. In this type of attack, the attacker has to target each victim individually.
2. Stored (Persistent) Attack – In a stored attack, the attacker inserts the malicious or harmful code in a web-page or other data stored on a vulnerable server. Further, the attacker’s code will then run in the browser of everyone who visits the compromised web-page. Due to the underlying potential to exploit multiple victims

with minimal effort, stored attacks are generally considered to be more dangerous than reflected attacks.

Cross-site scripting (also known as XSS or CSS) is generally believed to be one of the most common application layer hacking techniques.

B. SQL Injection attack:

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. This is a serious threat to any database driven site and web applications might allow an attacker to gain access to database if it is vulnerable to such attacks. Due to this, the database could be taken complete control of and it could be corrupted. [3]

C. Denial Of Service(DOS) attack:

In computing, a denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. A distributed denial-of-service (DDoS) is where the attack source is more than one–and often thousands of-unique IP addresses.

Following are the figures which are come into picture while looking towards stories of attacker in the last three to four years. 22% of UK companies surveyed experienced a disruptive attack in 2012, compared to 35% of respondents in a recent Neustar North American survey. Overall, UK respondents claimed that over a third (37%) of these attacks lasted more than 24 hours.

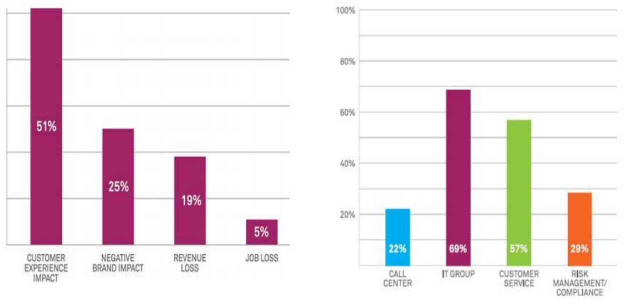

Figure 1 Figure 1 Fig. Financial loss in various sectors due to DOS attack & Areas of Greatest Cost Increases in a DDoS Attack

Sony Hacked in April to June 2011, Sony is by far the most famous recent security attack. After its Playstation network was shut down by LulzSec, Sony reportedly lost almost $171 million. The US carrier was hacked last year, but said no account information was exposed. They said they warned one million customers about the security breach. Money stolen from the hacked business accounts was used by a group related to Al Qaeda to fund terrorist attacks in Asia. According to reports, refunding costumers cost AT&T almost $2 million. [1]

Following figure represents the survey of web applications that are most vulnerable to XSS attack and SQL Injection attack.

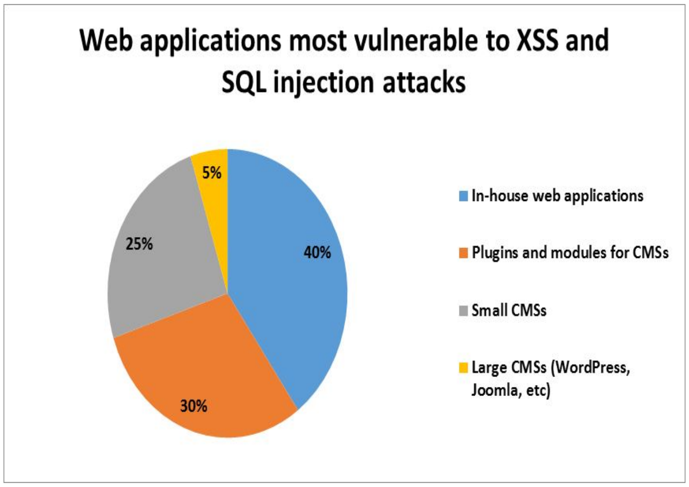

Figure 2: Web applications most vulnerable to XSS and SQL attacks

Cross-site scripting (XSS) is increasingly common in the cloud computing world, up more than 160% in the fourth quarter of 2012 from the previous three months, a security firm is warning. The company warns that both XSS and SQL injection attacks have become even more prevalent since the third quarter of 2012.

Following are some graphical representation of Cyber Crime:

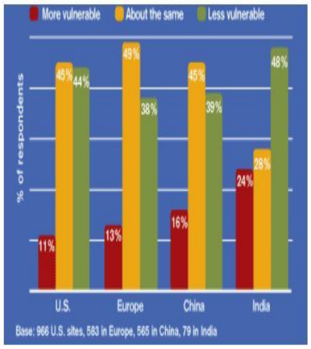

Figure: 3 Amount of Vulnerability Comparison Chart

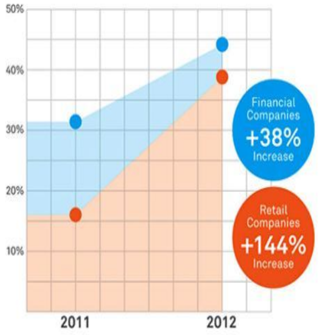

Figure: 4 Comparison Chart of Cyber Crime in 2012 & 2013

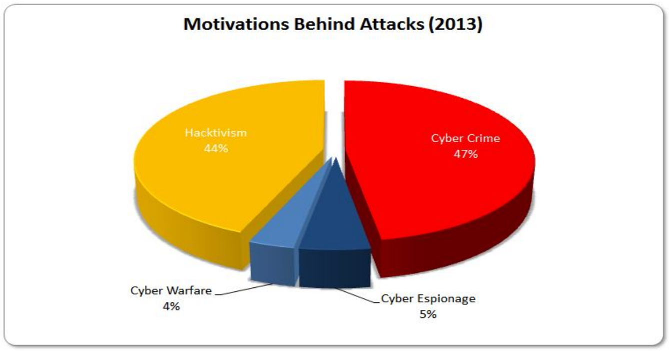

Figure: 5 Comparison of Attacks

Following are some measures:

- 42% increase in targeted attacks in 2012.
- 31% of all targeted attacks aimed at businesses with less than 250 employees.
- One waterhole attack infected 500 organizations in a single day.
- 14 zero-day vulnerabilities.
- 32% of all mobile threats steal information.
- A single threat infected 600,000 Macs in 2012.
- Spam volume continued to decrease, with 69% of all email being spam.
- The number of phishing sites spoofing social networking sites increased 125%.
- Web-based attacks increased 30%.
- 5,291 new vulnerabilities discovered in 2012, 415 of them on mobile operating systems

There are many other web application vulnerabilities given by OWASP Top 10 2013 like Cross-Site Request Forgery (CSRF) attack, Broken Authentication and Session Management, Insecure Direct Object References, Security Misconfiguration, Sensitive Data Exposure, Missing Functional Level Access Control, Using Components with Known Vulnerabilities, Unvalidated Redirects and Forwards.

Following figure shows the Top 10 source countries for web application attacks, Q1 2015

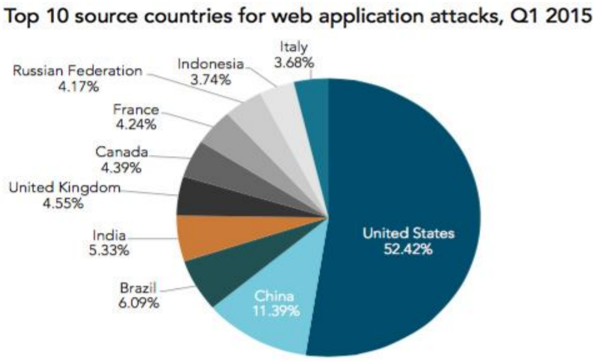

Figure 6: Top 10 Source countries for web application attacks, Q1 2015

III. TECHNIQUES AND TOOLS TO IDENTIFY WEB APPLICATION VULNERABILITIES

Following are some techniques to identify web application vulnerabilities:

A. Penetration Testing

The main objective to evaluate the security of an IT infrastructure by attempting to exploit system vulnerabilities such as OS or service, application flaws and even risky end-user behaviour. There are several main phases of penetration testing like Information gathering, Scanning, Vulnerability identification, exploitation and reporting.
Penetration tests can be conducted in several ways:

1. Black-Box Testing: The pen tester has almost no information about the surface to be tested.
2. White-Box Testing: The pen tester knows a lot about the infrastructure or application.
3. Gray-Box Testing: The pen tester has limited knowledge of the internal details of the program or application.

B. Tools to detect web application vulnerabilities

There are many different tools are available to detect web application vulnerabilities. Some of the open source tools are listed below:

1) Nmap
Nmap is a free and open source utility for network discovery and security auditing. The software provides a number of features for investigative computer networks, including host discovery and service and OS detection.

2) Metasploit
Metasploit is a powerful open source framework that performs difficult scans against a set of IP addresses. It provides information about security vulnerabilities and helps in penetration testing and IDS signature development.

3) W3af
W3af stands for Web application attack and audit framework. W3af is an open source web application security scanner. It help you to secure your web applications by finding and exploiting all web application vulnerabilities.[7]

4) OpenVAS
OpenVAS stands for Open Vulnerability Assessment System. OpenVAS is a frame work of several services

and tools offering a vulnerability scanning and vulnerability management solution.

5) Nikto
Nikto Web Scanner is a Web server scanner that tests Web servers for risky files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received.[8]

Fuzzing technique is also used to discover software vulnerabilities using different fuzzing tool like Webfuzz tool provides a frame which could create an effective analysis to test web software.[4]

IV. CONCLUSIONS

This paper is the basic reference paper which involves a basic survey of different web attacks that happens all around the world. The different statistics data images should also give the ratio about the different attacks so that we will measures which attack is more harmful. From this survey we will conclude that we have got the idea and scenario of the different web attacks. We have also shown tools and techniques to detect the web application vulnerabilities. We will develop some techniques to prevent such types of attacks with using different tools in future.

REFERENCES

[1] Rajesh M. Lomte, Prof. S. A. Bhura Computer Science & Engineering Department, BNCOE, India. "Survey of different Web Application Attacks & Its Preventive Measures" IOSR Journal of Computer Engineering (IOSR-JCE)e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 14, Issue 5 (Sep. - Oct. 2013), PP 46-51 www.iosrjournals.org

[2] Gabriel Avramescu, Mihai Bucicoiu, Daniel Rosner, Nicolae Ţăpuş Faculty of Automatic Control and Computers, University Politehnica of Bucharest, Romania "Guidelines for Discovering and Improving Application Security" 2013 19th International Conference on Control Systems and Computer Science

[3] A.Pramod , A.Ghosh, A. Mohan, M.Shrivastava and Dr. R. Shettar, “SQLI Detection System for a safer Web Application ” , 2015 IEEE International Advance Computing Conference (IACC)

[4] Li Li, Q. Dong, L. Zhu, and D. Liu, “The Application of Fuzzing in Web software security vulnerabilities Test” , 2013 International Conference on Information Technology and Applications.

[5] https://www.techopedia.com/definition/24841/denial-of-service-attack-dos

[6] https://www.owasp.org/index.php/SQL_Injection

[7] http://w3af.org/

[8] https://en.wikipedia.org/wiki/Nikto_Web_Scanner