Recent Trends in Web Application Security Risks and Issues

K. R. Srinath

Associate Professor, Department of Computer Science, Pragati Mahavidyalaya Degree and PG College, Hanuman Tekdi, Koti, Hyderabad, Telangana, India.
k.r.srinathmtech@gmail.com

ABSTRACT

Security is the most important aspect while accessing Web application. Web application is a dynamic software program that provide communication medium between user and service provider. As popularity of web is increasing there are more possibilities of web application may be exposed to attacks. However web applications can offer good productivity and efficiency, there is also great chance, that they can easily be exposed to security threats. Those security threats may potentially be harmful for the organization. This happens because web developers are least concerned about the security of the application at developing stage. Since technology is taking faster advancement attackers are using new and automated way to attack the system. This paper surveys latest trends in attacks of web application. In recent years most of occurring web attacks are through SQL injections, DDoS attacks, and using automated botnets that uses artificial intelligence. This paper further discusses crucial security risks for web applications.

Keyword: - *Web Application, Security, Attacks, Web user, Security Risk, Vulnerabilities.*

1. INTRODUCTION

Past few years saw the popularity of Web applications advancement in order to face the demands and requirements of enterprises and users. They may be social media applications, health care applications, financial applications, educational, government applications etc. Whatever the type of web application its main purpose is to provide the platform for communication between web users and web service providers [5]. Web application is a software service that runs on web browser. And it allows dynamic access of software application to web users without downloading and installing the software through web browser over internet. Web application structure compromises of 3 layers (figure 1). In first layer web browser is used from client/user side. Second layer is operated by web server which generates dynamic web pages with required content with help of tools like Java, PHP, and ASP (Active Server Pages) etc. And the final layer is backend database operation which generates content from database called server database [9]. Cyber attacks are rising at rapid speed and taking most advanced and new forms as the fame of web is getting bigger. This is because most of the developers are not much focusing on security aspects while developing the web applications. And at times it is difficult to tough task to concentrate on security when developers need to provide more usability. Security is more crucial when providing best service to users. Web application may reveal sensitive data or allow access of the back-end systems to unknown sources when they are attacked. Web applications offers great functionality and productivity, but there is also a great chance of vulnerability towards security attacks, that could possibly be a potential risk to most of the enterprises. Most of hackers focus on applications that require user interaction functions registrations, user logging's, online payments, etc. all these tasks contains backend databases or Light Weight Data Access Protocols(LDAP) which stores or contains web users sensitive data and operates as basic communication medium between web user and infrastructure.

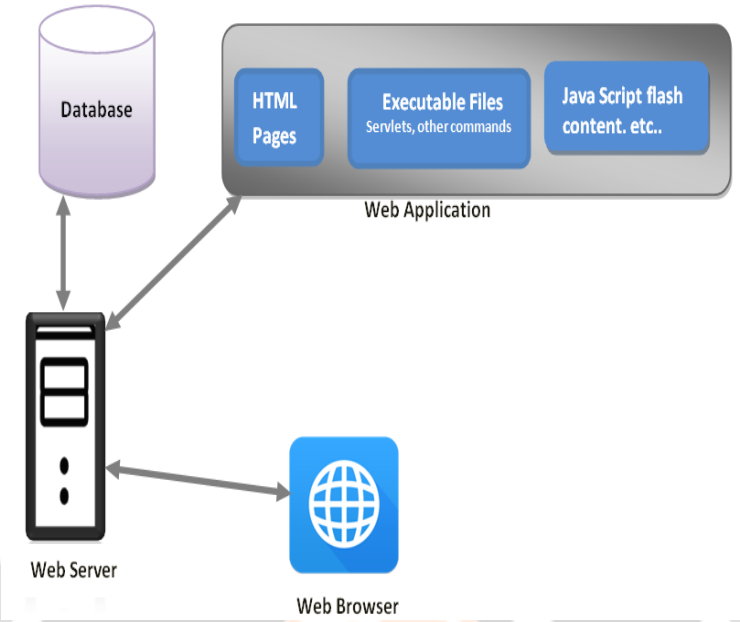

Fig -1: Web Application Structure

Malware attacks are most happening threats on Web application and Web application vulnerability is weakness of the application that can easily be exposed to threats. When compared to previous year attacks on Web applications increased 69% in Q3 2017 and when this percent is 30% higher when compared to Q2 of 2017. And is a serious problem to consider. Nearly all the attacks on web applications include phishing in which hackers lure the web application users and get the user information like bank details, and identity theft in hackers stoles the user credentials, DDoS (Distributed Denial-of-Service) attach in which hackers injects a Trojan over multiple systems in order to increase unnecessary traffic that causes denial of service. In the Past three months nearly 98 countries attacked by DDoS. SQL Injection is most dangerous and popular attack in which hackers get required sensitive data by injecting SQL queries. And malwares are programs that damage the entire system. Ransomware is a new type of issue in which attacker blocks access to the application or system and demands user or organizations to pay ransom amount otherwise exposes or destroys sensitive data. Although firewalls are used to defend against these attacks hackers are using most advanced and new ways attack the cyber systems. With advancement of technology attackers are using autobots called botnets or bots which uses artificial intelligence (AI) technology. Bots automatically operates themselves does the damage and they can spread automatically. A recent survey stated that almost 79% of organizations are not able to predict that their web traffic is coming from bots are human beings. The objective of this paper is to present a view of recent web application security attacks. The collected information is secondary data from various sources like journals, white papers, websites and articles.

2. WEB APPLICATION SECURITY RISKS TYPES

With Security risk management is critical task for web application. The most common and critical web application security attacks specified by OWASP (Open Web Application Security Project) Top Ten 2017 are listed below. OWASP is a non profitable open organization which is focusing on providing security risk management to organization in world.

- **Injection:** Using drawbacks of security management hackers inject queries like SQL, Expression Language (EL) or Object Graph Navigation Library (OGNL), NoSQL, LDAP and OS Injections as part of commands or queries as when data is sent to web user. When this attack happens, the data supplied by user is not validated by security mechanism of organization. The data inserted by hacker into actual command can trick the interpreter into executing unintended commands or accessing data without proper authorization.

- **Broken Authentication:** web applications that are related with user authentication are exposed to this type of attacks. Attacker identifies session interruptions manually and attacks with automated password and

dictionary lists. When this attack occurs application denies user authentication and disconnects sessions abruptly to get user credentials like passwords bank related information, OTPs and highly sensitive data of organization etc.

- **Sensitive Data Exposure:** Most of the web applications are not able to secure sensitive data accordingly, that may contain personal, financial, healthcare and/or organizational sensitive information etc. That type of weak data may get into hands of hackers. This attack happens with no additional security mechanism is provided for sensitive data security, previously stolen passwords and man in the middle attacks.

- **XML External Entities (XXE):** Lots of Older XML processors evaluates URI during XML processing. Some XML process contain External entities contains sensitive data. By using this drawback of older XML processors, attackers extracts information, monitor system, apply DoS attack, execute commands remotely from the server, and also perform other attacks.

- **Broken Access Control:** By disrupting user sessions continually attacker hacks into the system. This happens when allow authenticated users try to access the application boundlessly. By using this drawback attacker can get access to functionality of application, modifies user credentials, access user sensitive data, and modify other user's data etc.

- **Security Misconfigurations:** This is popular issue regarding web application security. This may happen when default security configurations are not secure, defective secure configurations, open cloud storage, HTTP header misconfigurations, and error messages that contain sensitive information. To avoid this problem all the components including operating systems, frameworks, applications and system libraries must be configured securely and patching and upgradation must be done frequently.

- **Cross-Site Scripting (XSS):** This happens when web application contains data from untrusted sources in a webpage without proper authentication. Hackers executes their own commands on user's web page in order to get information about session, identity, website and redirect the users to malicious web sites.

- **Insecure Deserialization:** This attacks results in remote execution of application code. Impact of this type attack is unpredictable. Deserialization drawbacks also lead to injection, identity theft, and replay attacks.

- **Using components with known vulnerabilities:** Another reason for security breaches is using vulnerable system components. Attackers can easily hack into the system using these components. System is said to be vulnerable if we use outdated and un-supported software, like operating systems, web browsers, web application server, application, and database etc.

- **Poor logging and monitoring:** Monitoring and logging is major and crucial task in security management. Poor monitoring and lack of active response to attacks allows attackers to breach into the system. A recent study showed that most of the security breaches are occurring because of poor monitoring mechanisms of organizations.

3. RECENT TRENDS IN WEB APPLICATION SECURITY ATTACKS

Introduction SQL injection (SQLi) attacks are most frequent attacks that happened in this year stated in Akamai State of the Internet / Security Report 2017. The report further specified 47% of all web application attacks are SQL injection (SQLi) attacks. Reasons for popularity these types of attacks are they can easily find any vulnerable system to attack, they are easily scalable and automated. Second most popular attacks are Local File Inclusion (LFI) attacks and 38% of attacks happened on application layer are LFI attacks. Next popular attack is Cross-site scripting (XSS) attack, almost 9% of the attacks are XSS attacks. The source location for the most of the attacks is USA. Compared to last year 27% attacks are originated from America said the report. Report also found that three out of four web applications are vulnerable to threats. Mirai malware is used by cyber security breachers to attack the IoT devices. Attacks are taking new turn with help of technology. Botnet attacks combined with DDoS became more popular in this year. Recent Kaspersky Lab's DDoS Intelligence statistics report for Q3 2017 stated that from past three months 98 countries are victims of DDoS attacks. And in quarter of July-September 2017, 51.56% of all attacks originated from china. The report stated that South Korea is most affected by DDoS attacks. Ransomware attack, IoT Botnets,

Phishing and Whaling attacks, Business Process Compromise Attacks, and Machine Learning enabled attacks are latest web security threats listed in Intel's security report for 2017. Frequency of Ransomware attack is increased with rapid speed. Recently most of the countries suffered with Wannacry Ransomeware attack. Cost of Ransomeware attack in the year 2015 is USD 2.5 million and in 2016 it raised up to USD638 million. At end of 2016 massive number of DDoS attacks happened by Mirai Botnet which showed that most of service providers are incapable of dealing with cyber attacks. Business Process Compromise Attacks occurs when hackers are used to compromise the business process of a government organization in order to get the money. Recent Intel Security report stated that attackers using machine learning is for attacking social media application. With the data available on public platforms, attackers apply complex analysis tools on that data to select the victim. Akamai's State of the Internet Q3 2017 Security Report mentioned that India has become 7th target for web application attacks. World Bank stated that India has 462 million web users at present. There is need for security infrastructure.

4. CONCLUSIONS

As security is at high risk with constant evolution of technology and popularity a strong secure defense system should be higher priority for organizations. This paper presented detailed overview of security risks and issues of web applications. With advancement of technology cyber security attacks are taking new and most dangerous turn. Attackers are using advanced technologies, like artificial intelligence and machine learning techniques for attacking the web. Organizations must secure their web infrastructure in keeping future in mind. Prevalence of attacks that those do not require tricking users is increasing. Wannacry, Emotet and Mirai Bot are few examples for that. To prevent cyber security risks organizations must employ mechanisms for monitoring web traffic frequently, efficient defense responsive system for security attacks, firewalls blocking unauthorized access, and frequent upgradation and patching of operating systems, software and other components.

6. REFERENCES

[1]. Edward Rolando Núñez Valdez, Oscar Sanjuán Martinez, Gloria García Fernández, Luis Joyanes Aguilar and Juan Ml. Cuevas Lovelle, "Security Guidelines for the Development of Accessible Web Applications through the implementation of intelligent systems",ijaiim, Vol. 1, No. 2.
[2]. Arunima Jaiswal, Gaurav Raj, Dheerendra Singh, "Security Testing of Web Applications: Issues and Challenges", ijca, Volume 88 – No.3, February 2014.
[3]. Hesham Abusaimeh and Mohammad Shkoukani, "Survey of Web Application and Internet Security Threats", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.12, December 2012.
[4]. Akamai State of the Internet / Security Report 2017.
[5]. Noorbasha Ahmad, E. Raveendra Reddy, "Detection of Harmful and Malicious Attacks in Social media Applications", SK International Journal of Multidisciplinary Research Hub, Volume 4, Issue 2, February 2017.
[6]. Cyber Security Report 2017, Telstra, 2017.
[7]. https://www.forbes.com/sites/gilpress/2017/11/26/60-cybersecurity-predictions-for-2018/#6d022c1773ff
[8]. Vamsi Mohan V, Dr. Sandeep Malik, "Detection and Prevention of SQL Injection Vulnerabilities in Web Applications: A Review", IARJSET, Vol. 4, Issue 9, September 2017.
[9]. Abdulrahman Alzahrani, Ali Alqazzaz, Nabil Almashfi, Huirong Fu, Ye Zhu, "Web Application Security Tools Analysis", Redfame Publishing, Vol. 5, No. 2; December 2017.
[10]. COGNIZANT, "A Multidimensional View of Critical Web Application Security Risks: A Novel 'Attacker-Defender' PoV", COGNIZANT 20-20 INSIGHTS, March 2017.
[11]. Gopal R. Chaudhari, Prof. Madhav V. Vaidya, "A Survey on Security and Vulnerabilities of Web Application", IJCSIT, Vol. 5 (2), 2014.
[12]. SANS Institute, "Security by Design: The Role of Vulnerability Scanning in Web App Security".
[13]. Savita B. Chavan, Dr. B. B. Meshram, "Classification of Web Application Vulnerabilities", IJESIT, Volume 2, Issue 2, March 2013.
[14]. Mr. K.Naveen Durai, K.Priyadharsini," A Survey on Security Properties and Web Application Scanner", IJCSMC, Vol. 3, Issue. 10, October 2014.
[15]. Sajjad Rafique, Mamoona Humayun, Zartasha Gul, Ansar Abbas, Hasan Javed, " Systematic Review of Web Application Security Vulnerabilities Detection Methods", Journal of Computer and Communications, 2015.
[16]. Susan Prescott," The top 10 web application security risks",AT&T.
[17]. https://www.apriorit.com
[18]. Nadiya UP, Maya Mathew, "Vulnerability Detection in Web Applications", ijircce, Vol. 5, Issue 3, March

2017.
[19]. Elizabeth Fong and Vadim Okun, "Web Application Scanners: Definitions and Functions", nist.gov.
[20]. Atefeh Tajpour , Suhaimi Ibrahim, Mohammad Sharifi," Web Application Security by SQL Injection DetectionTools", ijcsi, Vol. 9, Issue 2, No 3, March 2012.
[21]. Vandana Dwivedi, Himanshu Yadav, Anurag Jain, "Web Application Vulnerabilities: A Survey", ijca, Volume 108 – No. 1, December 2014.
[22]. Vignesh M, Dr. K. Kumar,"WEB APPLICATION VULNERABILITY PREDICTION USING MACHINE LEARNING", International Journal of Scientific & Engineering Research Volume 8, Issue 5, May-2017.
[24]. "Statistics for botnet-assisted DDoS attacks",Kaspersky Labs, Q3 2017.