A Survey of Intrusion Detection System for Web Application

Piyushkumar A. Sonewar
PG Student, Department of Computer Engineering,
Sinhgad Technical Education Society's, Smt. Kashibai Navale College of Engineering
Pune, Maharashtra, India

Nalini A. Mhetre
Asst. Prof. Department of Computer Engineering,
Sinhgad Technical Education Society's, Smt. Kashibai Navale College of Engineering
Pune, Maharashtra, India

Abstract

Web applications provide massively large facilities to the users. As the usability and popularity of the web applications have increased so as various types of attacks over it. In this paper we discuss various attacks like SQL injection attacks, Cross Site Scripting attacks, Privilege Escalation attack etc. and some of the methodologies to overcome it. Attacks are possible in on any web applications due to various reasons like ambiguous coding methods, design level flaws, web application configuration errors, validation error in user input etc. Different approaches have been implemented based on signatures of these attacks. Even though various intrusion detection systems are present, attacks continues to prevail.

1. Introduction

In the age of fast growing internet Web applications are the crucial part for users. These applications uses and manages personal information of these users. To cope up with this increased use, web applications are being designed on the basis of multi-tiered architecture. In multi-tiered architecture a web server resides in between clients and database server. In such scenario attacks are possible over web server as well as database server. Different approaches have been implemented to identify such attacks on each side individually and also on both sides i.e. web-server as well as database server combined [3].

Most of the IDS approaches are directed towards signature based detection mechanisms. Well-defined patterns of any well-known attack are used for comparison. To this various pattern matching algorithms can be applied to detect attacks to the system. As per Open Web Application Security Project OWASP [8] four attacks amongst top ten attacks happens due to faulty input validations. Even a simple application logic error gives opportunity to hackers to get into the system.

In this paper we are defining some basic terminologies in first section followed by the various works that has been done to this issue and so on up to the conclusion.

1.1 Web Applications

A web application is an application developed using programming languages that uses web browser to retrieve data and interact with contents of the web application. Simply put web applications are meant for users to access contents offered to the clients via web browser. All standard web application is based upon three logical points viz. presentation logic, data access logic and business logic. Combining these three things produces tiered architecture for web application. In a typical three tier architecture all these layers are independent and does not reveal any implementation dependencies if present.

Attacks are possible on each of these layers. Attackers look for any design flaws, application logic error or vulnerabilities in coding of web application. Strict input validation of the user requests is must. The attackers and valid users are the same until they initiates some varied requests to the web application.

1.2 Intrusion Detection System (IDS)

Confidentiality, Integrity and Authentication are the three most basic security issues. Any activity that threatens any of these parameters is categorized as

intrusion. An IDS refers to a system that detects an abnormal activity in either a network, system or web applications that may cause harm to the security of the system. IDS is generally categorized in two types viz. Anomaly Detection and Misuse Detection.

A. Anomaly Detection:

In this type of IDS a well-defined behaviour of user application is known on the first hand. Any random actions are considered as a threat. A predefined pattern is associated with some type of attack. Any unconventionality from the normal conduct is detected as an anomaly to the system. Previously unknown attacks can be detected but there is a high chance of false positive. Anomaly detection is somewhat difficult for dynamic applications.

B. Misuse Detection:

Principally misuse detection defines the attack description and matches them against audit data stream. It searches for any of the known attacks. Verifying against audit data excellently detects the attacks with very less false positive but this scheme is ineffective for undefined attacks.

Once intrusion has been detected, there are many ways in which the administrator can be alerted. Depending upon the urgency of the situation an email or a mobile message to the administrator can be sent, or an alarm can be raised to alert the guards. A counterattack against the intruder is also possible in which the attacker can be traced out and attack on one's system can be mounted but there is a possibility of collateral damage.

1.3 Attacks

Enormous categories of attacks are possible on all type of web application. This section introduces the attacks under consideration in brief. Privilege escalation attack, SQL injection attack, Direct DB Attack, Cross Site Scripting (XSS), these attacks are being disused here.

A. Privilege escalation attack:

This attack takes advantage of design flaws or programming errors of the web applications to get into the system. In this attacks scenario the attacker enters the system as a normal user and by manipulating programmer's logic the attacker escalates his/her privileges. For example attacker can log in to the web application as a normal user and boom its privileges to administrator level by completely annihilating programmer's design logic.

This attack is categorized into two types viz. vertical and horizontal. In vertical privilege escalation attack, attacker grants himself higher privileges. While in horizontal privilege escalation attack attacker has same privileges but attacker may pose as a different user.

B. SQL injection attack:

SQL injection is one of the most used attacks in case of web application. In this type of attack, attacker exploits security vulnerabilities of the web application to alter the valid SQL query designed by the programmer. The impact of this attack varies according to the SQL queries being injected. It ranges from being as simple as an information retrieval to remote code execution. SQL injection can be so severe that the complete system can be compromised.

C. Direct DB Attack:

Some attacker may directly attack the database server to get any crucial information stored at the database server. Some attackers may avoid webserver and go for database server directly in this attack, or it may be the case that webserver has already been compromised.

D. Cross Site Scripting (XSS):

XSS is a web application attack where attacker crafts a Uniform Resource Locator (URL) in such a way that it seems to be legit, but in fact it is not. It's like a trap attack, in which once the user visits this crafted URL the attacker executes some malicious code in user's browser. There are two types of XSS viz. persistent XSS and Non persistent XSS attacks.

i. Persistent XSS attacks:

In persistent attack, the attacker will give the input to some part of the web application and in future this input will be available to other users via which the attack will be successful.

ii. Non persistent XSS attacks:

In these attacks, the data input by the malicious user is encountered by the users directly. There is no intermediate persistent storage involved in it. This attack generally takes place in the form of abnormal URL being sent to the victims. The attacks take place only if such links are visited by the users.

2. Related Work

Security threats discussed above have been under scanner for long. There are variable solutions for these attacks but such attacks are still occurring. In this section we will be overlooking some of the previous approaches. Attack classification scheme, providing foundation for evaluation of ID, need to be mutually exclusive, complete and unambiguous. Sanctum Inc.

has categorized web threats. Sanctums classification scheme is useful in developing general understanding of common threats to web services and possible consequences [7].

This paper presents a five phase model to overcome SQL Injection and XSS types of attacks at some level. It starts with detecting attacks using API (Application Programming Interface) and IDS, followed by preventing attacks using IDS, Making log of attack database, mining of web log using WAPT (Web Access Pattern Tree) and finally making reports using P chart techniques. This approach is effective for JSP, ASP.NET. An ID maintains details of application in database and if any threats are found it is stored in intrusion log. WAPT algorithm generates reports using intrusion log [4].

According to Das, Sharma and Bhattacharyya in this approach HTTP attacks are identified in three steps. Web layer log file matching, clustering and labelling applied over the value of packet arrival rate. This approach uses supervised text matching and unsupervised clustering approach to detect intrusion [5].

Skaruz,Seredynski have used Gene Expression Programming to classify attacks over web applications. SQL queries are classified on the basis of each query's individual structure. These are divided into distinct parts called as tokens. GEP is able to find good quality solution very quickly. But this model limits the SQL queries to be in the form of only 36 tokens in all. And rate of false alarm is also somewhat high [6].

Chandrasekhar and Raghuveer proposed a model is based upon combination of several techniques. K-mean clustering technique clusters the given dataset, neuro fuzzy logic used to train k neural networks generated in previous step. Vectors are generated by passing each of the data generated through nuero fuzzy classifier and at last classification based on redial SVM (Support Vector Machine) is done to detect intrusion [1].

Meixing Le, Brent ByungHoon Kang have defined a single IDS approach to detect intrusion at both webserver and database server. This approach eliminates the need of two IDS, generally required for detecting intrusions. Lightweight virtualized containers are used to distinguish between the requests coming from each individual client. XSS have capability of evading this system [3].

3. Proposed Approach

Considering all the systems studied there are some approaches that eliminate the risk of intrusion at great extent. Our approach depends upon web services. Web services plays crucial role in web applications. Our approach includes a service provider that allocates available web service to the requesting client. Clients will be getting a response from database server via these web services. Each client is individualized based on web services available. Scheduling can be done to assign free web services to the requesting client.

Attacks are identified based on mapping model between queries and predefined signatures. Categorization of each attacks is done and preventive measures are applied to the restrict attacks.

4. Conclusion

In this paper, brief overview of various security techniques have been presented. As per the referred papers no IDS can provide 100% security to web application but it provides security to great extent. The success of any IDS depends upon the available attack database and its accuracy. This study is directed towards the attacks over web application and use of different approach to overcome such intrusion.

5. References

[1]. A. M. Chandrasekhar, K. Raghuveer "Intrusion Detection Technique by using K-means, Fuzzy Neural Network and SVM classifiers", 2013 International Conference on Computer and Informatics(ICCCI-2013) Jan04-06,2013,Coimbatore, INDIA

[2]. Ashwini D. Khairkar, Deepak D Kshirsagar, Sandeep Kumar, "Ontology for Detection of Web Attacks",2013 International Conference on Communication Systems and Network Technologies

[3] Meixing Le, Brent ByungHoon Kang, "DoubleGuard: Detecting Intrusions in Multitier Web Applications", IEEE Transaction on Dependable and Secure Computing Vol. 9, No. 4, July/August 2012

[4]. R.Priyadarshini, Jagadiswaree.D, Fareedha.A, Janarthanan.M, "A Cross Platform Intrusion Detection System using Inter Server Communication Technique" , IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011 IEEE MIT, Anna University, Chennai. June 3-5, 2011

[5] Debasish Das, Utpal Sharma, D K Bhattacharyya, "A Web Intrusion Detection Mechanism based on Feature based Data Clustering", 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009

[6] Jaroslaw Skaruz, Franciszek Seredynski "Detecting Web Application Attacks With Use of Gene Expression

Programming", 2009 IEEE Congress on Evolutionary Computation (CEC 2009)

[7]. Jeongseok Seo, Han-Sung Kim, Sanghyun Cho and Sungdeok Cha, "Web Server Attack Categorization based on Root Causes and Their Locations ", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC04)

[8]. https://www.owasp.org/index.php/Top_10_2013-Top_10