Intrusion Detection for Web Application: An Analysis

N.Sakthipriya, K.Palanivel

Abstract— Web applications are becoming the dominant way to provide access to online services and also a valuable target for security attacks. As the use of web applications for critical services has increased, the sophistication of attacks against these applications has grown as well. To protect web applications several intrusion detection systems have been proposed. In this paper, several techniques which are meant for detection of web application related attacks and their advantages and disadvantages are presented. Furthermore, the common web application attacks which are vulnerable to the web application are discussed. Finally, this study concludes with an analysis of challenges to overcome for the detection of web application attack that still remain to be resolved.

Index Terms— Web Application, Intrusion Detection, Attacks, Tools

1 Introduction

THE Internet services and use of web applications are increasing tremendously around the world. But unfortunately it has been found easy to disturb the functionality of Internet by attacking its infrastructure taking advantage of Internet services and protocols. The vulnerability of web application has attracted the attention of malicious hackers to exploit and access to sensitive information which might lead to enormous gain. The security of web-based applications should be addressed by means of careful design and thorough security testing. Unfortunately, this is often not the case. For this reason, security conscious development methodologies should be complemented by an intrusion detection infrastructure that is able to identify the attacks and provide early warning about suspicious activity. Intrusion detection is the process of monitoring events occurring in a system and reporting them accurately to the proper authority when the suspicious activity occurs. There are two main types of intrusion detection methods. The one is anomaly detection which is based on finding deviations from normal user behavior are considered intrusive. The next one is misuse detection, it characterized as a' pattern' or 'signature' that IDS looks for. Pattern or signature might be a static string or a set sequence of actions.
The Intrusion detection system provides the following:

- Monitoring and analyzing of user and system activity.
- Auditing of system configurations and vulnerabilities.
- Assessing the integrity of the files and critical system.
- Statistical analysis of activity patterns.
- Abnormal activity analysis.
- Operating system audit.

2 COMMON WEB APPLICATION ATTACKS

2.1 SQL Injection

The SQL Injection attack is abusing Web pages which allow users to enter text in form fields which are used for database queries. Hackers can enter a disguised SQL query, which changes the nature of the query. Hence the queries can be used to access the connected database and change or delete its data.

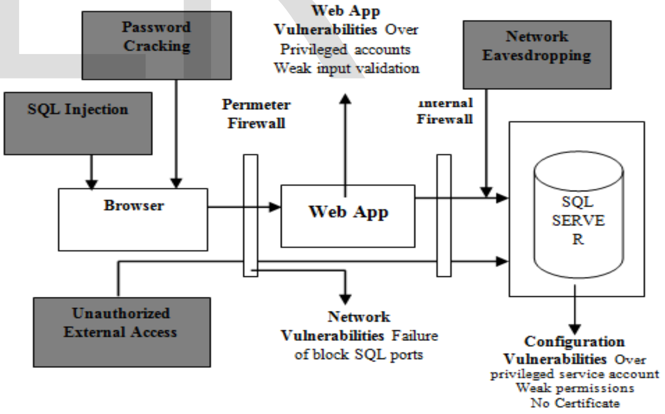
Password Cracking
Web App Vulnerabilities Over Privileged accounts Weak input validation
Network Eavesdropping
SQL Injection
Perimeter Firewall
ınternal Firewall
Browser
Web App
SQL SERVE R
Unauthorized External Access
Network Vulnerabilities Failure of block SQL ports
Configuration Vulnerabilities Over privileged service account Weak permissions No Certificate

Fig (1): SQL Injection Attack

2.2 Cross Site Scripting

Cross site scripting is an attack targeted towards the hosting web application underlying OS, and often back-end database. An attacker will often attack web application that does not filter scripts from form fields submitted to web application.

Attackers are often able to insert code which gets executed by the user's browser. This code will attempt to steal browser cookies that include banking session data, password etc. Session cookies are then used by the attacker to emulate a legitimate user session to a banking site, email account, etc.

- *N.Sakthipriya is currently pursuing master's degree program in Computer Science &Engineering in Pondicherry University, Pondicherry, and India PH-09488549639. E-mail: priya.sakthi43@gmail.com*
- *K.Palanivel is currently working as System Analyst in Pondicherry University, Pondicherry, India, and PH-09488824888. E-mail: kpalani@yahoo.com*

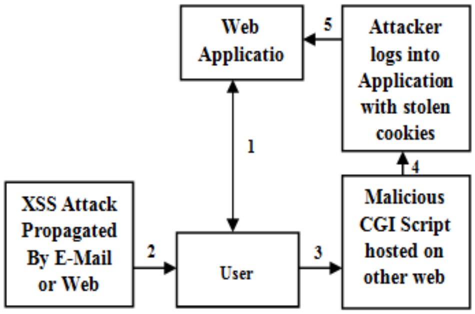
Web Applicatio
5
Attacker logs into Application with stolen cookies
1
4
XSS Attack Propagated By E-Mail or Web
2
User
3
Malicious CGI Script hosted on other web

Fig (2): XSS Attack Hijack Scenario

2.3 Session Hijack

Session hijacking attack is mainly aimed at the web server side. An attacker takes over the web server and therefore hijacks all subsequent legitimate user sessions to launch attacks. By hijacking other user sessions, the attacker can listen in, send spoofed replies and drop user requests. There are two types of session hijacking.

- Active session hijacking.
- Passive session hijacking.

Active session hijacking involves hijacking an already authenticated session. The original user has logged in his account profile and then the attacker steals the cookies to hijack the active session and then disconnect the original user from the server.

In passive session hijacking, attackers does not hijack active session instead they capture the login credentials while the original user is trying to establish a new connection with the server and the attacker is sitting silently on the same network and recording the login credentials.

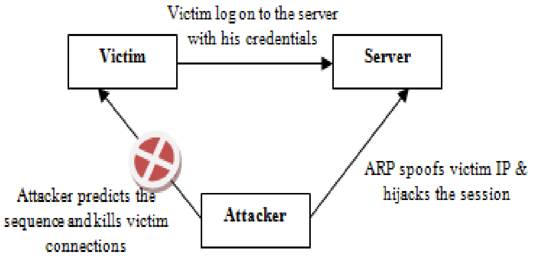
Victim log on to the server with his credentials
Victim
Server
Attacker predicts the sequence and kills victim connections
Attacker
ARP spoofs victim IP & hijacks the session

Fig (3): Session Hijacking

2.4 Remote Code Execution

This vulnerability allows an attacker to run arbitrary, system level code on the vulnerable server and retrieve any needed information contained therein. Improper coding errors lead to this type of vulnerability.

2.5 Cross Site Request Forgery

Cross site request forgery is an attack which forces an end user to execute unwanted actions on a web application in which legitimate user is currently authenticated. With the help of email an attacker may force the users of a web application to execute actions of the attacker's choosing. A successful CSRF exploits can compromise end user and operation in case of normal user. If the targeted user is the administrator account, this can compromise the entire web application. The malicious website causes a user's browser to send a request to a trustable site. The trustable site sees a valid and authenticated request from the browser and does what is asked.

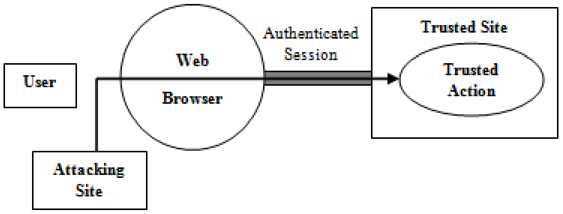

Fig (4): CSRF Attack Scenario

2.6 Sophisticated HTTP attacks

Sophisticated HTTP attacks are among the most popular hacking techniques. Hacker's mainly target HTTP requests and manipulates or modifies the requests to cause the requisite damage. The attacks are usually performed using HTTP port 80 or other HTTP communication.

Sophisticated HTTP attacks result in easy access into the web server for the hacker, allowing him to cause immense damage. Hackers can delete information, steal data, or add info. They can cause interminable harm to a website. If a website gets affected, it can result in serious damage to its online business, spoil the website's image, or cause the financial loss to the business.

2.7 Buffer Overflow

A buffer overflow is an exploit that takes advantage of a program that is waiting for an input of the user. There are two types of buffer overflow attacks:

- ➢ Stack based attack
- ➢ Heap based attack

Heap based attacks flood the memory space reserved for a program, and it is a rarely used for performing such an attack due to its difficulty.

Stack-based buffer overrun, the program being exploited uses a memory object known as a stack to store user input.

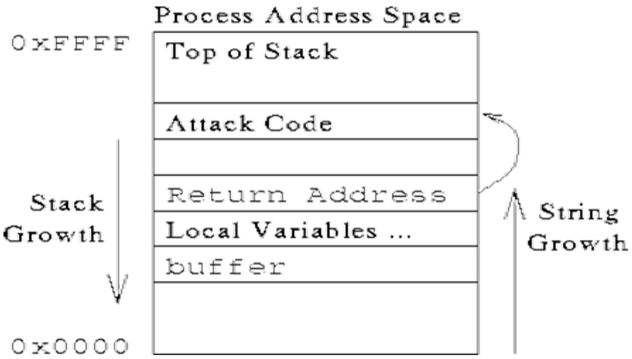

Fig (5): stack based buffer overflow attack

3 TOOLS FOR IDS

3.1 SNORT

Snort is open source intrusion detection and prevention system excels at traffic analysis and packet logging on IP network. Combining the benefits of signature, protocol and anomaly based inspection. Through protocol analysis, various pre-processors, snort detects a large number of worms, port scans, vulnerability exploiting attempts and other suspicious behavior. Snort uses a rule based language to describe traffic that it should collect or pass and a modular detection engine.

3.2 OSSEC

OSSEC is an open source Host based Intrusion Detection system that performs log analysis, policy monitoring, root kit detection, file integrity checking, real time alerting and active response. Because of its powerful log analysis engine, ISPs, several universities and data centers are running OSSEC to monitor and analyze their firewall, web server and authentication logs.

3.3 SQUIL

SQUIL's main component is an intuitive GUI that provides access to real-time events, session data and raw packet captures. It facilitates the practice of network security monitoring and event driven analysis.

3.4 OSSIM

OSSIM is an open source Security Information and Event Management comprising a collection of tools designed to assist network administrators in computer security, intrusion detection and prevention system. It also provides a strong correlation engine with low, mid and high level visualization interfaces as well as reporting and incident managing tools.

3.5 TRIPWIRE

Tripwire is a software security and data integrity tool useful for monitoring and alerting on specific file changes on a range of systems.

It functions as a host based intrusion detection system but preferably attempting to detect intrusions at the network interface level, it detects changes to file system objects. It is useful for detecting intrusions after the event. It can also serve many other purposes such as change management, integrity assurance and policy compliance.

4 RELATED WORKS

Many researchers have introduced various techniques to defend against various attacks.

C. Kruegel and G. Vigna [6], presented an intrusion detection system that uses a number of different anomaly detection techniques to detect attacks against web servers and web based application. The system correlates the server side programs referenced by client queries with the parameter contained in the queries. The system derives automatically the parameter profiles associated with web application data.

M. Cova, D. Balzarotti, V. Felmetsger, and G. Vigna [1], they present Swaddler, a novel approach to anomaly based detection of attacks against web application. Swaddler analyzes the internal state of web application and learns the relationship between the applications critical execution points and the application internal state. Swaddler is able to identify the attacks that attempt to bring an application an inconsistent anomalous state such as a violation of the intended workflow of web application

G. Vigna, W.K. Robertson, V. Kher, and R.A. Kemmerer [8], presented WebSTAT, an intrusion detection system that analyzes web requests looking for malicious behavior and it provides a sophisticated language to describe multi-step attack in terms of the states and transaction. It operates on multiple event streams and it is able to correlate both network and operating system level events with entries contained in the server logs.

M. Auxilia, D. Tamilselvan [2], proposed a negative security model based on misuse of web application is used. This negative security model provides a web application firewall engine with a rule set, to ensure censorious protection across every web architecture. WAF's are deployed to establish an increase external security layer to detect and prevent attacks before they reach web applications.

G. Vigna, F. Valeur, D. Balzarotti, W.K. Robertson, C. Kruegel, and E. Kirda [7], proposed the system composed of a web based anomaly detection system, a reverse HTTP proxy and a anomaly database detection system. The serially composing a web based anomaly detector and a SQL query anomaly detector increase the detection rate of the system. To address the system's capacity for producing false positives, they additionally present an approach to provide differentiated access to a website based on the anomaly score associated with web requests.

Meixing Le, Angelos Starou, Bret ByungHoon Kang [9] , proposed Double Guard an IDS system that models the network behavior of user sessions across both back end database, by monitoring both web subsequent database requests, the system able to find attacks that independent IDS would not be able to identify. That quantifies the limitations of any multitier IDS in terms of training sessions and functionality coverage

Juan Jose Garcia Adeva, Juan Manuel Pikatza Atxa [3], Intrusion detection software component based on text mining techniques attempts to detect either unauthorized access or misusing a web application and by using text categorization, it is capable of learning the characteristics of both normal and malicious user behavior from log entries generated by web application server and therefore the detection of misuse in a web application is achieved.

Viktoria Felmetsger, Ludovico Cavedon, Christopher Kruegel, Giovanni Vigna [5], proposed a novel approach to identification of class of application logic vulnerabilities, in the context of web application is presented. And this approach uses a composition of dynamic analysis and symbolic model checking to identify invariants that are a part of the intended program specification but are not enforced on all paths in the code of a web application.

Christopher Krueger, Giovanni Vigna, William Robertson [4], presented an intrusion detection system proposed that uses a number of different anomaly detection techniques to detect attacks against web servers and web based application. The system analyzes client queries that reference server side program and create models for a wide range of different features of queries. The system derives automatically the parameter profiles associated with the web applications and relationships between queries from analyzing data.

R. Sekar [10], presented a new technique called taint inference and it operates by intercepting requests and responses from this application. For web applications, this interception may be achieved using network layer interposition or library interposition. They developed a class of policies called syntax and taint aware policies that can accurately detect and block the most injection attacks.

Table 1: Analysis of various intrusion detection techniques

Sl. No	Title	Advantage	Disadvantage	Attack class
1	Anomaly Detection of Web based attacks	Support detection of new attacks and cannot be evaded by attempting to hide malicious code inside a string.	Header data of GET request are not taken into account its rely on web access logs, attacks that compromise the security of the web server.	Buffer overflow, Directory traversal, cross site scripting, Input validation & Code Red
2	Swaddler : An approach for the anomaly detection of state violations in web application	Detect the attacks that cannot be identified by examining the external flow of request and response.	Vulnerable to mimicry attack.	Workflows violation attacks.
3	A stateful Intrusion Detection system for Word Wide Web Servers	The expressiveness of the language allows the attack modeler to describe timing relationship and this approach is one to detect more complex attacks.	Vulnerable to denial of service attacks.	Web crawler, Pattern matching, Cookie Stealing, Buffer overflow, Document root escape.
4	Anomaly detection using Negative security model in web Application.	Provided a rule set for detecting the attacks , HTTP traffic can be monitored in real time in order to detect and prevent attacks from reaching web applications.	Does not provide a unique rule for detection of all attacks.	HTTP attacks, SQL injection, Cross site scripting.
5	Reducing errors in the anomaly based detection of web based attacks through the combined analysis of web requests and SQL queries.	When the attack is detected it does not block anomalous request immediately but its attempt to serve them through a web server with restricted access to sensitive information thereby reducing the false positive.	Vulnerable to distributed DOS attack.	SQL injection, Command injections, Information tampering, Cross site scripting.
6	Double Guard : Detecting Intrusions in multi-tier web application	The causal mapping can identify the attack even in normal network traffic, 100 % detection accuracy with 0 % & 0.6% false positive for static and dynamic web page.	Cross site scripting attack is possible, Vulnerable to mimicry attack, Not designed to mitigate DDOS attacks.	Privilege escalation, Hijack future session attack, Injection attack, Direct DB attack
7	Intrusion detection in web application using text mining	Log information generated by the system does not need any particular format, Does not require any explicit programming for machine learning.	The system cannot detect the new attack; Focus only on access control, The false positive is high.	Access control.
8	Toward Automated detection of logic vulnerabilities in web applications	They focused on the fact that many invariants that relate to import concepts of web applications were not identified	Vulnerabilities identification is limited.	Application logic vulnerabilities (authorization)
9	A multi model approach to the detection of web based attacks	The reduced number of false positives, able to detect a high percentage of attacks with a very limited number of false positives.	Relies on web access logs, The direct instrumentation of web servers introduces unwanted delay.	Buffer overflow, Directory traversal, cross site scripting, Code Red, Input validation.
10	An Efficient Black box technique for defeating web application Attacks	Effective in detecting a broad range of attacks on application written in multiple languages, Low overheads.	A false negative may occur due to parsing error, policy error or incompleteness.	SQL injection, Command injection, Path traversals, crosses site scripting.

5 CONCLUSION

The undeniable existence of vulnerabilities in the web application prevails the attacker to exploit through various attacks. In order to detect the existence of attacks, the Intrusion detection system has been emerged. However, there are still many challenges to overcome because of the occurrence of new attacks. This study presents a survey of various techniques for defending against various attacks. Our review finds that the existing techniques have its relative merits accompanied by a set of demerits.

From this analysis, it is inferred that the data complexity of application has been increased, the web application adapted to multi-tier design. As discussed above, the Intrusion detection model for multi-tier web application need a proper input validation mechanism as a additional defense for detecting attack such as cross site script attack and this challenge is yet to be resolved.

REFERENCES

[1] M. Cova, D. Balzarotti, V. Felmetsger, and G. Vigna, “Swaddler: An Approach for the Anomaly-Based Detection of State Violations in Web Applications,” Proc. Int’l Symp. Recent Advances in Intrusion Detection (RAID ’07), 2007.

[2] M. Auxilia, D.Tamilselvan, “Anomaly Detection Using Negative Security Model in Web Application,”IEEE 2010.

[3] Juan Jose Garcia Adeva, Juan Manuel Pikatza Atxa,” Intrusion Detection in web applications using text mining,” Journal of Artificial Intelligence - Elsevier 2006.

[4] Christopher Kruegel, Giovanni Vigna, William Robertson,” A multi model approach to the detection of web based attacks”, Journal of Computer Networks - Elsevier 2005.

[5] Viktoria Felmetsger, Ludovico Cavedon, Christopher Kruegel, Giovanni Vigna,”Towards Automated detection of logic vulnerabilities in web applications “, USENIX Security'10 Proceedings of the 19th USENIX conference on Security, 2010

[6] C. Kruegel and G. Vigna, “Anomaly Detection of Web-Based Attacks,” Proc. 10th ACM Conf. Computer and Comm. Security (CCs’03), Oct. 2003.

[7] G. Vigna, F. Valeur, D. Balzarotti,W.K. Robertson, C. Kruegel, and E. Kirda, “Reducing Errors in the Anomaly-Based Detection of Web-Based Attacks through the Combined Analysis of Web Requests and SQL Queries,” J. Computer Security, vol. 17, no. 3, pp. 305-329, 2009.

[8] G. Vigna, W.K. Robertson, V. Kher, and R.A. Kemmerer, “A Stateful Intrusion Detection System for World-Wide Web Servers,” Proc. Ann. Computer Security Applications Conf. (ACSAC ’03), 2003.

[9] Meixing Le, Angelos Starou, Bret ByungHoon Kang,” Double Guard: Detecting Intrusions in Multitier Web Applications,” IEEE Transactions On Dependable and Secure Computing, Vol. 9, NO. 4, July/August 2012.

[10] R. Sekar,” An Efficient Black box Technique for Defeating Web Application Attacks”, Proc. Network and Distributed system security sump.(NDSS),2009.

[11] http://www.ossec.net/

[12] http://www.snort.org/

[13] http://sguil.sourceforge.net/

[14] http://www.tripwire.com/

.