ISSN 2278-7763

An Overview to SQL Injection Attacks and its Countermeasures.

Vishwajit S. Patil
Department of CSE
P.R.M.C.E.A.M Bandera, Amravati
vishwajit55@gmail.com
Dr. G. R. Bamnote
Professor & Head,
Department of CSE
P.R.M.I.T.& R. Bandera, Amravati
grbamnote@rediffmail.com

Abstract: Web applications are those applications which run in web browser. These applications are accept some data and send it to database for further processing. There are number of attacks on web application like cross site scripting, cross site request forgery but SQL injection attacks are the most prominent. Number of papers in literature has been projected ways to avoid SQL injection attacks by examining dynamic SQL query semantics at runtime in the application layer. This paper contains the study of SQLIA and its prevention techniques. SQL injection attacks on web application have become one of the most important information security concerns **[Pinzo'n C et al., 2010]**. These SQL injection attacks are extremely widespread and posses a serius security threat **[Khoury et al., 2011]**. In today's world SQL injection is one of the most dangerous security threats in database centric web applications **[Elia et al., 2010]** because this type of attack can comprise confidentiality and integrity of information in database **[Tajpour A et al., 2010].**

Keyword: web application attacks, XSS, CSRF, SQLIA, and SQLIV.

Literature survey of SQL injection

SQL injection is the attacks related to backend database results in unauthorized acess to private or confidential information stored **[Kiani M et al., 2008].** Also attacker intrudes to the web application data base to acess the data **[Tajpour & JorJor Zade, 2010].** Exploitation of SQL injection vulnerability (SQLIV) through successful attacks might results in authentication bypassing, leaking of private information etc **[Shahriar, H & Zulkernine, M]**. SQL injection attacks are very harmful as they targets interactive web application that employs database services. **[Wei & Muthuprasanna, 2006]**. The SQL injection attacks allow an attacker to access the underlying database, execute arbitrary commands at intent and receive a dynamically generated output **[Kosuga et al., 2007].**

If web application containing vulnerability can allows malicious users to obtain

IJOART

Copyright © 2014 SciResPub.

ISSN 2278-7763

unrestricted access to private and confidential information.This mechanism used by hackers to steal data from organization. It allows a hacker to gain control over the database of an application and consequently hackers may be able to alter data **[Shanmughaneethi et al., 2009].** An attacker can inject in the original SQL query and obtain, change or view data.

An overview of prevention techniques.

1. **AIIDA- SQL**

This prevention techniques works against SQL injection attacks and proposed by the author. They mentioned that SQL injection attacks are the most critical attacks from the web application. The techniques against SQLIA called Adaptive Intelligent Intrusion Detector Agent (AIIDA- SQL) According to author; the experimental results using this technique are good in real practice **[Pinzo'n C et al., 2010].**

2. Black Box Web Application Security Scanner

Standards security features are not enough to protect web application form hacking, threats, SQL injection, XSS, CSRF and hence black box testing is used. According to author sql injection is the most critical web application vulnerability. Author also mentioned that black box scanners are having some weaknesses. It is not good enough to identify vulnerable program that browses world wide web in a methodical, automated manner called as web crawling , user login etc. the black box testing tool had poor detection rate so that author proposed a set of recommendation that could enhance the rate of detection **[Khoury et al., 2011].**

3. Augmented attack tree modeling

SQL injection attacks are classified into seven types **[J. Viegas et al.,2006]**

a. Tautologies
b. Legal/Logical Incorrect queries
c. UNION query
d. Piggy – Backed Queries
e. Stored procedures
f. Inference and alternate encoding

There are two types of attack tree modeling **[Jie Wang et al., 2010]**

i. Conventional Attack trees
ii. Augmented Attack tree

These attack tree model not only applicable to SQLIA but also Cross Site Request Forgery

IJOART

Copyright © 2014 SciResPub.

ISSN 2278-7763

Attacks (CSRF). The method presented by author is generic and hence it can be applicable to other kinds of web based attacks.

4. Automated fix generator

SQL injection is example of taint based vulnerability that has been responsible for a large number of security failure to perform some promised act or obligation in recent years. Untrusted data from the user is tracked when it flows unsafely into a security critical operation and hence vulnerability is flagged. In SQL injection the user can add some additional conditions or commands to a database query, thus allowing the user to bypass authentication or alter data. Automated fix generator detects and fix sql queries that contains SQL injection vulnerability (SQLIV). For testing purpose author used phpBB v2.0 **[Dysart & Sherriff, 2008].** Anomaly Based Character Distribution Models

The anomaly detection process uses a number of different models to identify anomalous state for each basic block of a web application. A model is a set of procedure used to evaluate a certain features of a state variable associated with the block.

The author used anomaly based approach to detect SQL injection attacks and it is superior to existing model which works against SQLIV **[Kiani M et al., 2008].** VIPER tool for penetration testing **[Angelo Ciampa]** .

According to authors, they have suggested a tool called VIPER to perform penetration testing of web applications. This tool relies on a knowledge base of heuristics that guides the generation of the SQL queries. This tool first identifies the hyperlink structure and its input form.

5. Hidden web crawling **[Xin et al., 2010].** SQLIV are the most prominent issues in today's World Wide Web. Many traditional vulnerability scanners are available but they are unable to fulfill the requirements. Author proposed a mechanism based on hidden web crawling to achieve the goal. The authors also compare their tool with other traditional scanners and tested on the public web sites. The results show that the proposed tool is good over the traditional web scanners.

IJOART

Copyright © 2014 SciResPub.

ISSN 2278-7763

6. High interaction Honeypot System **[Jiao Ma et al., 2011]**

Honeypots are a very original approach to computer security. The honeypot are classified in two categories

a. Low interaction : fake services
b. High interaction : complete access

Here authors proposed a high interaction honeypot system against SQLIV. They used two approaches.

a. Modifying PHP extension for mysql to intercept data based request
b. Adopting exception based and signature based detection techniques.

The results show that this system is very efficient against SQLIV.

7. MUSIC

Many vulnerability are discovered after the deployment of software implementation such as buffer overflows, sql injection and format string bug are the most commonly occurring security flaws in software implementation **[Shahriar, H & Zulkernine, M]**. In 2004 the denial of service exploitation alone cost more than 26 million dollar in financial losses to business organization **[L. Gordon et al., 2004]**. MUSIC –mutation based SQL injection Vulnerability checking proposed by the author which is good enough to protects such types of attacks which is not address by the existing testing approaches. The discovered vulnerabilities can be fixed and the losses incurred by end user can be prevented.

8. **Preventing SQL injection attacks in stored procedures**

This prevention mechanism proposed by the authors. According to authors stored procedures acts as a medication against SQL injection attacks. A stored procedure is nothing but a subroutine available to application that accesses a relational database system. The techniques proposed in this paper by author to eliminate the occurrence of such attacks are a permutation of static application code analysis with runtime validation

Conclusion

9. SQL injection is most powerful and easiest attack method on web application **[Pinzo'n C et al., 2010]**. The effects of these attacks may turn into loss of private and vital information. From this paper we have studied that different authors

IJOART

Copyright © 2014 SciResPub.

ISSN 2278-7763

proposed a number of countermeasures against SQLIV and SQLIA. The VIPER tools performs the penetration testing**[Angelo et al.]** by using SQL injection AIIDA-SQL tool, black box scanners, augmented attack tree modeling, automated fix generator, hidden web crawling etc.

From this paper we can conclude that several solutions are exists to prevent SQL injection attacks but no concrete solution is presents.

References

[Angelo et al.] Angelo Ciampa, Corrado Aaron Visaggio, Massimiliano Di Penta :"A heuristic-based approach for detecting SQL-injection vulnerabilities in Web applications".

[Dysart & Sherriff, 2008] Dysart, F.; Sherriff, M.; , "Automated Fix Generator for SQL Injection Attacks," Software Reliability Engineering, 2008. ISSRE 2008. 19th International Symposium on, vol., no., pp.311-312, 10-14 Nov. 2008

[Elia et al., 2010] Elia, I.A.; Fonseca, J.; Vieira, M.; "Comparing SQL Injection Detection Tools Using Attack Injection: An Experimental Study," Software Reliability Engineering (ISSRE), 2010 IEEE 21st International Symposium on, vol., no., pp.289-298, 1-4

[J. Viegas et al., 2006] J. Viegas, W. Halfond, and A. Orso. A Classification of SQL-Injection Attacks and Countermeasures. In International Symposium on Secure Software Engineering, 2006.

[Jiao Ma et al., 2011] Jiao Ma; Kun Chai; Yao Xiao; Tian Lan; Wei Huang; , "High-Interaction Honeypot System for SQL Injection Analysis," Information Technology, Computer Engineering and Management Sciences (ICM), 2011 International Conference on , vol.3, no., pp.274-277, 24-25 Sept. 2011

[Jie Wang et al., 2010] Jie Wang; Phan, R.C.-W.; Whitley, J.N.; Parish, D.J.; , "Augmented attack tree modeling of SQL injection attacks," Information Management and Engineering (ICIME), 2010 The 2nd IEEE International Conference on ,

IJOART

Copyright © 2014 SciResPub.

ISSN 2278-7763

vol., no., pp.182-186, 16-18 April 2010

[Khoury et al., 2011] Khoury, N.; Zavarsky, P.; Lindskog, D.; Ruhl, R.; , "An Analysis of Black-Box Web Application Security Scanners against Stored SQL Injection," Privacy,
security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom) , vol., no., pp.1095-1101, 9-11 Oct. 2011

[Kiani M et al., 2008] Kiani, M.; Clark, A.; Mohay, G.; , "Evaluation of Anomaly Based Character Distribution Models in the Detection of SQL Injection Attacks," Availability,
Reliability and Security, 2008. ARES 08. Third International Conference on , vol., no., pp.47-55, 4-7 March 2008

[Kosuga et al., 2007] Kosuga, Y.; Kernel, K.; Hanaoka, M.; Hishiyama, M.; Takahama, Yu.; , "Sania: Syntactic and Semantic Analysis for Automated Testing against SQL Injection," Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual , vol., no., pp.107-117, 10-14 Dec. 2007

[L. Gordon et al., 2004] L. Gordon, M. Loeb, W. Lucyshyn, and R. Richardson., "Ninth CSI/FBI computer crime and security survey", Technical Report RL32331, C.S.I. Computer
Security Institute, 2004. Accessed from
www.theiia.org/iia/download.cfm?file=9732 (January 2008).

[Pinzo'n C et al., 2010] Pinzo´n, C.; De Paz, J.F.; Bajo, J.; Herrero, A.; Corchado, E.; , "AIIDA-SQL: An Adaptive Intelligent Intrusion Detector Agent for detecting SQL Injection
attacks," Hybrid Intelligent Systems (HIS), 2010 10th International Conference on , vol., no., pp.73-78, 23-25 Aug. 2010

[Shahriar, H & Zulkernine, M] Shahriar, H.; Zulkernine, M.; , "MUSIC: Mutation-based SQL

IJOART

Copyright © 2014 SciResPub.

ISSN 2278-7763

Injection Vulnerability Checking," Quality Software, 2008. QSIC '08. The Eighth International Conference on , vol., no., pp.77-86, 12-13 Aug. 2008

[Shanmughaneethi et al., 2009] Shanmughaneethi, S.V.; Shyni, S.C.E.; Swamynathan, S.; , "SBSQLID: Securing Web Applications with Service Based SQL Injection Detection," Advances in Computing, Control, & Telecommunication Technologies, 2009. ACT '09. International Conference on, vol., no., pp.702-704, 28-29 Dec. 2009

[Tajpour A et al., 2010] Tajpour, A.; Massrum, M.; Heydari, M.Z.; , "Comparison of SQL injection detection and prevention techniques," Education Technology and Computer (ICETC), 2010 2nd International Conference on , vol.5, no., pp.V5-174-V5-179, 22-24 June 2010**[Tajpour & JorJor Zade, 2010]** Tajpour, A.; JorJor Zade Shooshtari, M.; , "Evaluation of SQL Injection Detection and Prevention Techniques," Computational Intelligence, Communication Systems and Networks (CICSyN), 2010 Second International Conference on , vol., no., pp.216-221, 28-30 July 2010

[Wei & Muthuprasanna, 2006] Wei, K.; Muthuprasanna, M.; Suraj Kothari; , "Preventing SQL injection attacks in stored procedures," Software Engineering Conference, 2006. Australian, vol., no., pp. 8 pp., 18-21 April 2006

[Xin et al., 2010] Xin Wang; Luhua Wang; Gengyu Wei; Dongmei Zhang; Yixian Yang; , "Hidden web crawling for SQL injection detection," Broadband Network and Multimedia Technology (IC-BNMT), 2010 3rd IEEE International Conference on , vol., no., pp.14-18, 26-28 Oct. 2010

IJOART

Copyright © 2014 SciResPub.