Sql Injection Assessment Of E-Commerce

Matin Katebi *, Milad Katebi **

* Master of Information Technology, Islamic Azad University of Bahar Branch, Iran matinkatebi@gmail.com
** Master student of Information Technology, University of Khaje Nasir Toosi (K.N.Toosi), Iran
mkatebi@kntu.ac.ir

Abstract: By increasingly development of electronic commerce and providing different electronic situations such as internet and mobile commerce, electronic commerce has been changed to one of important issues in 21 century. By development of electronic commerce related problems including keeping the security of information and transactions between seller and purchaser seems necessary. Every year attacks and financial and information losses resulted from these attacks are increased. So increase in efficiency of electronic business requires attention and practical measurements for keeping security and countering with possible risks by hackers of these programs. Most attacks are attacks to program level and today one of the most important attacks to this level is attack to data base of sites by the approach of SQL injection. In this paper it is tried to examine the SQL injection which leads to fetch and manipulating the information of data base. It is also tried to identify vulnerabilities in electronic commerce programs particularly sites which are based on business to customer (B2C) and finally while stating the strategies for managers of these sites for keeping their site in safe, approaches for encountering these attacks are introduced.

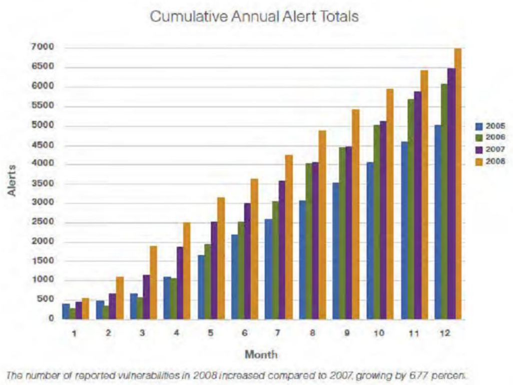
[Matin Katebi, Milad Katebi**. Sql Injection Assessment Of E-Commerce.** *N Y Sci J* 2012;5(12):73-79]. (ISSN: 1554-0200). http://www.sciencepub.net/newyork. 11

Keywords: SQLinjection, e-commerce, inband & outband attack, database hijacking

1. Introduction

The internet has changed business and trades a lot, and as a result buying and selling conditions and the relationships of the businessmen have changed. Mean while, new problems has created which have not existed before. One of the most important resulted problems is safety of information interchange. Although information technology is becoming universal in all societies, but The development and exploitation of it in addition to communications infrastructure development infrastructure related knowledge and safe and legal context is also dependent.because since at the same time of ever increasing developing of e-commerce web-sites and e-pay portals, different devices and methods of attacking are also increasing rapidly and everyone around the world can attempt to attack and harm virtual area of a country just in the case of having the ability of revealing and having necessary devices, expanding and exploiting the It depends on expansion of connection bases, those bases related to the knowledge and also legal and safe play ground. There for, security in e-commerce (e-security) has special importance among those who are expanding web-sites. This matter can be secured by rebuffing the vulnerability of the websites and facing threats to web applications precisely and correctly. So, each year every government and web-sites managers should spend some amount of their budget to assure web-sites securities and their e-pays. However, the number of attack reports and the amount & damages caused is increasing each year.

One of the main concerns of the security is weakness of web-sites programmers and Clumsily expansion of web applications. SQL injection attacks is one of the main attacks to the web applications databases and extracting its information. For the first time SQL piggybacking or SQL injection attack was brought up in late 1998 (Kachakil 2009). Studies have been done from 2002 to 2007 shows that more than 10 percent of the whole vulnerability is related to SQL injection and 20percent of these vulnerabilities is related to inputs validations (Thomas 2008). According to the recent investigations 16 percent of the websites are vulnerable to these attacks. Open web Application security project (OWASP) International organization of web Developers introduced SQL injection attacks as one of ten most vulnerabilities which web applications have (Halfond 2007) This article tries to investigate on these attacks in e-commerce web-sites especially the portals of B2C online selling and it examines ways of avoiding and contrasts them. In chapter 2 first SQL injection and their mechanisms are introduced, then their aims are stated and their main techniques are discussed. In chapter 3, the main parts of e-commerce portals which are connected to the database are mentioned and in each case new techniques of SQL injection attacks are explained and finally in chapter 4 a model are presented to confront these attacks in web-sites.



The number of reported vulnerabilities in 2008 increased compared to 2007, growing by 677 percen.

Figure1. Number of vulnerability in years

2. Introducing SQL Injection Attacks

This attack is one of the injection attack types. It is based on this fact that hacker may fills entry parts of a web site with appropriate SQL characters or he may inject some words in SQL statements and define a new structural statement (Thomas 2008) to change the main SQL commands, or affect their execution and get access to the database information by different ways. In such cases, the hacker is presented with the chance of changing and defining the information.

Among the effects of SQL Injection on web Application are defining the data in a database (Insert, Update, Delete), executing managerial efforts on a database (such as shut down DBMS), regaining the content of files which are presented for DBMS, and in some cases commanding the operating system. Stealing e-mails, database credits, and users' other important information, are among the destructive aims of this attack. For instance in 2006, in a company which was aimed to process credits cards, 40 millions of credit cards were stolen and millions of dollars were defrauded as a result of being vulnerable to SQL injection Also, SQL injection vulnerability in the help desk system in Missouri university caused 22000 students information to be stolen in 2007.

SQL injection attack presents different techniques to Penetrate e-commerce web-sites, each of them can be used through different mechanisms of SQL injection attack and then the aims of such attacks are going to be studies and in section 3.2 different types of SQL injection attacks will be named and their aims and mechanisms will be examined one by one.

2-1. Injection Mechanisms

To the web application, can be penetrable in different ways. In this section the vulnerable parts and each of the entrance mechanism are going to be discussed.

2-1-1. Injection to the user's entrance

SQL is a DML (Data Manipulating Language); there for, these different sentences as select, insert, update, delete and select union can be changed and be applied to web-sites in the title of users' log in and can gain different information from databases. (chric 2002) In lots of SQL attacks, user inputs comes from those form submissions which are sent to the web application by HTTP get or post request. (Halfond 2006).

2-1-2. Attacks to cookies

Cookies are those files which contain person's user account in a web-site, and are stored by the browser in the local computer. When the user login the same web-site for the second time, his information can be read from the cookies and can be set. In the case that a web application uses cookies content to build SQL queries, the attacker can easily manage an attack by adding some codes to the cookies. (Halfond 2006).

2-1-3. Injection to the server variables

A set of variables, including environmental variables, HTTP network, and Headers, are called server variables. Web applications use these variables in different ways including logging usage statics and defining the browsing process. In the case that these variables enter the database without evaluation, SQLIA vulnerabilities are caused. (Halfond 2006) In this way hackers can put their queries in Http and network headers and thus when queries are logged to the server variables which are issued to the database, so the attack in this header is happened.

2-1-4. Second order injection

The aim of this attack is different from the aim of regular injection attacks. This mechanism is an undirected SQLIA type, since the hacker's login to the system and the database, may lead to an attack not just in the same minute, but it is happened while this log in used later by the system. (Halfond 2006). In some cases it is possible that some limitations (such as escape, type check, filtering the log in) be maintained by the programmer of the web application to stop the hackers, and in this way he makes sure about the safety of the program; But when the data is used in another meaning or when different queries are made, some of these methods can be cheated. For instance, if' is omitted from received logins by the programmer in a way that each " "is replaced with " ' ' " ' in a query, while the hacker get a username called admin using previous method and enters admin' --, according to the limitation set by the programmer can not succeed in penetrating the system. In this case in order to penetrate he can register a user as admin' --

in registration part and then the following query can be entered in login page and password of admin user can be changed:

SQL="update users set password='"+new password+"' 'where username=' "+rso("username")+"'.'

Among other limitation is limiting the login length in login parts this limitation can also be broken using special soft wars. Other methods also can be considered to avoid different kinds of limitations. Since injection point is different from the point in which the attack can be recognized, second order injection attacks cannot be easily found and avoided.

2-2. Attack Aim

Attacking web applications are based on different aims. These attacks in a general grouping can be divided to four main characterizes of web application. These attacks can be grouped as followed:

2-2-1. Attacking to the reliability.

When SQL database keeps important data, loosing its reliability causes lots of problems in SQL injection vulnerability.

2-2-2. Attacking to the authentication:

If SQL commands which are used to evaluate the usernames and passwords are not assured enough, it is possible for a hacker to penetrate the system as a user without knowing its password.

2-2-3. Attacking to the authorization:

If authorization information are stored in the database, these information can be changed as a result of an appropriate use of SQL injection vulnerability.

2-2-4. Attacking to the integrity:

If integrity of a database is not assured, It is possible to read and change its data using a SQL injection attack. In this section SQL injection attack aims are mentioned based on their objectives. In each case the processes

2-2-5. That should be done in the happened attack are stated:

Finding Injectable parameters: The hacker should find users' login fields and those parameters which are vulnerable to SQLIA, in order to Attack.

2-2-6. Performing database finger-printing:

A hacker used to know the version and type of the database of a web application to inject his queries and to be able to do his attacks based.

2-2-7. Performing database finger-print: Since each

Database react to queries differently, a hacker should know the type and version of the database of the web application to injection his queries and then to do his attacks based on that database. A simple way is using several special grammars.

2-2-8. Determining database schema:

To gain true information from a web application database, hackers usually need to know some information about qualities of the database such as tables' names, columns' names, and type of columns' data.

2-2-9. Extracting data:

The main aim of lots of attacks is finding the amount and values from a database. Based on web application type, these information can be sensitive and appropriate for the attack.

2-2-10. Adding or modifying data:

The aim of this attack is adding or changing the database information.

2-2-11. Performing denial of service:

This kind of attack is used to shutdown the database or to lock and drop tables of web application database. So, they destroy users' accessibility and the possibility to service them.

2-2-12. Evading detection:

These attacks are used to avoid checking up and recognizing the mechanisms of protecting the system.

2-2-13. By passing authentication:

The aim of this kind of attack is database Passing the mechanisms of authentication in web application and databases and changing the users' level of accessibility. These kind of attacks causes the hacker to have complete accessibility a special user has.

2-2-14. Executing remote commands:

This kind of attack perform arbitrary commands, like store procedures or the functions in the database.

2-2-15. Performing privilege escalation:

These attacks are used to limit the accessibility by abusing errors or executing special logical errors in the database. To face the attacks to pass getting identity, this attack focus on exploiting users' privilege of the database. (Halfond 2006).

3. Vulnerable parts of the ecommerce portal against SQL injection

Nowadays, the Internet plays the most important role as a means for ecommerce. There are lots of web-sites which are working just for trades. Among these website, are retail sites, C2c and B2c markets. These web- sites are active to sell the company's productions, either directly or as a broker. Apart from the kind of activity which is done by the web-site, the way it interact with the user, and its user interface, there are some main principles for these kinds of communications. Among them we can mention parts related to registering user name, his or her entrance to the website, selecting the product, buying, payment, and etc. These activities need a permanent connection to the database. As it was mentioned before, SQL injection attack is the main attack to the database. This kind of attack aims at today's most important databases including SQL server, my SQL, oracle, and etc. In this part, the most important parts of these website which are connected to the database are mentioned and then, in the case of existence, themain techniques of SQL injection is going to be mentioned. In each part, first the mechanism of the attack will be presented, then the aim of the attack will be explained and finally some cases of SQL injection attacks, which act in this way, will be stated.

3-1. Registration, Entrance, editing information

E-commerce websites have a part for the user's contacts including user's registration, entrance from, editing information, and etc. These parts are designed to the web- site, to produce satisfaction, contacts managements, special offers, etc. One of the most vulnerable parts of the websites is these parts and attacking them is among the attacks to the clients. One of the main damages to SQL injection will be done in the some way. Approximately in every ecommerce websites, there is login page and everybody can use it.

However, it is one of the most vulnerable parts of the website, and mostly all techniques of SQL injection attacks happen for it. Since this from has access to the user's accounts, the attacks to it is very dangerous.

3-1-1. Registration, editing information:

Injection mechanism: injection to the users entrance, second order injection, by the use of this mechanism, as it was said in chapter 2, by the means of registering a user using special methods in this part, some of the limitations that the programmer has designed can be defrauded. The attack aim: recognition of injection parameters, detecting the schema of database, addition or definition of the data, bypassing authentication, Executing remote commands.Some cases of attacks: piggy backed query, union query, functions, and etc.

3-1-2. Entering User information

Injection mechanism: inject to the users entrance,second order injection The attack aim: All the mentioned in section 2.2 Some cases of the attack: All the attacks can happen, especially those which use inference.

3-2. Interaction with the bank of holding account, recording information.

In most of the e-commerce website, there is a possibility to pay online, using Internet account card. In such cases, website firstly should get users account information and then contact the counterpart bank and after passing some bank processes, the same amount of money will be withdrawn from the person's account. As person's important information is put in this part, destructive penetrators hackers try more to get information and penetrate to the website; so this part is one of the sensitive and important parts which need more protection against damages, and its safety is very crucial. Since the prices are given from website, s database, there is a possibility for SQL injection to attack it. Injection mechanism: changing users entrance, second order injection.

Attack aim: Recognizing injection parameters, detection the schema of database, addition or defining data, bypassing authentication, executing remote command, evading detection. Some cases of attacks: piggy backed query, union query. functions, Illegal/ logically Incorrect Queries, and etc.

3-3. Cookies

In most of the e-commerce website cookies are used to recognize previous customers, for the comfort of the users, or recording other information. Cookies are appropriate places for different kinds of attacks. The hacker by having access to user's cookies can have the same access to the information. Since cookies information is the same as having access to the person's user account information, and thus leads to interaction with database, SQL injection attack is possible, while working with cookies. Injection mechanism: attacking cookies, if they contain private information. Attack aim: performing privilege escalation, bypassing authentication, getting the amount of data.Some cases of the attacks: piggy backed query, tautology and etc.

3-4. URL

It is not necessary to mention that all of the websites in the world need their own URL-URL is used to make connection between other pages. Sometimes database reads its information from the URL, and writes on it, too. In fact, in this case query string is used. Lots of the attacks aim at URL. Among these attacks, there are SQL injection attacks. Injection mechanism: injection to the server's variables.

Attack aim: To understand the database version, finger print database, the database schema, recognizing injection parameters, getting the amount of data, performing denial of service. Some cases of attack: tautology, union query, legal/ logically Incorrect Queries, piggy back query, using time delays.

3-5. choosing shopping item and shopping cart

Lots of e-commerce to comfort the user and the possibility to choose several shopping item, arrange shopping carts user adds each shopping item to his cart by choosing it. Adding shopping item and its price to the shopping cart is done in an interaction with database so can be one of the aims of an attack. Injection mechanism: injection to the user's entrance.

Attack aim: Adding and changing commands, executive remote commands, defining injectable parameters.Some cases of the attacks: union queries,functions, store procedures.

3-6. Price offer, putting comments, contact us, discussing subjects, private message.

In lots of the website, including e-commerce website, there is the possibility for the users to contact website managers through putting some comments or contacting them.

In lots of others there is also the possibility to comment about an especial shopping item. Sometimes the from possibility is also added. Since the information are recorded in the database, so there is the possibility to executing other command of the database in a destructive way. Injection mechanism: injection to the user's entrance.

Attack aim: adding and changing data, executing remote commands. Some cases of the attack: functions, and store procedures.

3-7. Searching shopping item.

Web-sites for the comfort of their users, and helping him finding subjects have a part named search, in which by entering subjects keyword, concerned maher is found. In lots of the e-markets there is the possibility to search the shopping item. Since this search is done in the database, SQL query can be entered from this part. injection mechanism: injection to the users entrance.

Attack aim: detecting the schema of database, getting the amount of the data, performing denial of service. Some cases of the attacks: union queries, piggy backed query, using time delays known names

4. Present a model to contrast with the SQL injection

As it was mentioned SQL injection attack is one of the most important attacks to e-commerce web-sites. In order to encounter SQL injection attacks various methods should be considered.

The best way to avoid these attacks is preventing them. Since the attack of e-commerce site is irreparable damage, Maintaining the security requirements is more important, Because Ecommerce without security, privacy and protect sensitive information (of) seller and buyer is impossible. so in this section try to Provide a model to indentify all type of SQL Injection attacks and prevent them. As can be seen in figure 2, Components of this model includes different levels. In each level Methods to prevent again SQL Injection attacks are described.

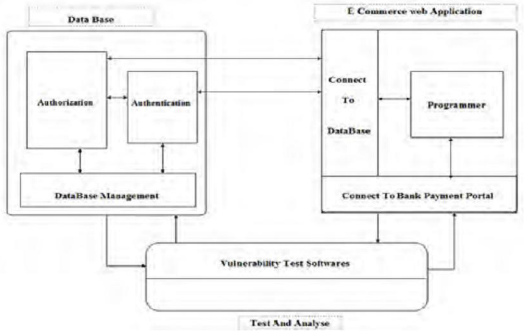


Figure2. A model against SQL injection

4-1. database management

4-1-1. Putting a safe database driver

One of the ways to prevent. this attack can be obtained by putting a safe database driver between web application and underlying connection of database management system. To recognize an attack, the driver uses SQL queries and following stack to create SQL statement and finally it can recognize inject able query from the right query. The driver is not dependent in a special web application and can be added to every system (Mitropoulos 2008).

4-1-2. lock down in SQL server

The most important point here is that SQL server must be locked down In the fallowing there is a list of the points that should be done while creating a SQL server: Methods of connecting server should be identified: It should be checked that just in the use network libraries be active.In order to bo that network utility can be helpful. It should be checked that which user accounts exist: user account with low level of access can be created to use the programs. Those user accounts which are unnecessary should be deleted. It should be assured that all of the user accounts have strong password: lots of the extended stored procedures can be omitted without any damage. If it is done, also those DLLs which contain the codes of extended stored procedures should be omitted.All of the sample data banks and examples which are presented in the program as presupposed should be omitted. It should be checked that each user account can have access to which subjects or objects: A user account which uses a program to access the database, should necessarily has the least permission to access its needed objects. 1. Patch level of the sever should be checked: There are several attacks of buffer overflow and format string type and also several security problems in the patches themselves. So the serve always should be kept update from the viewpoint of patches. It should be checked that what can be logged out and what happens to them.

4-2. Connect to Database

4-2-1. Using prepare statements

Lots of the programmers think that using a managed code can prevent SQL injection vulnerability, but this idea is not right. one of the best ways to prevent this vulnerability is using prepare statement. These statements have static structure and usually are designed to improve the database connection. In a low level, those statements, separate user data from SQL commands. so, in the case of appropriate use user's login never can be transferred as a SQL
command

4-2-2. Compatibility of the error message

When a database error is occurred, a message should be shown, but it is possible not to show the whole SQL error messages. when a web application is faced with an error, the program should answer the error by an ordinary page or returning back to a standard place.Thus, debugging information or other details can be hidden to prevent possible hackers.

4-2-3. Using store procedures

Process in a database should only be done by the store procedures, and these procedures should have the least level of accessibility and should utilize a parameterized API which greatly helps with the sanity checking of user data.

4-3. Web Programming E-Commerce

In this step Most systematic and principled way to act is that encryption and programming standards that need to do is this case, and should be applied. Visits can be a code for identifying each species will be useful to vulnerable

4-3-1. Inputs validation

Lots of the vulnerabilities of SQL injection are a result of weak inputs validation (Fong 2007). Most of the SQL injections can be recognized by checking user login, and then they can be prevented. Different methods of creating validity can be classified as followed:

1. The efforts to process the data and modifying them, in a way they become valid. In this case SQL statements can be written in a way tha instead of using characters like (, =, &, space, >, <) equivalent cases be used.

2. Rejecting and refusing those logins which are know as harmful logins. In order to do that the entrance of some characters link (, &, space, …) or some keywords like (insert, drop shutdown, select union, …) by the user can be prevented.

3. limiting data type; for example if a login should be in numeral type, the user should not be able to enter un-numeral values (Cannings2008)4. Limiting the entrance length according to the needs.

4-4. Access management to the database

4-4-1. Links with the least accessibility

The web-site manager to safeguard the database should use user accounts with least necessary accessibility for applications and never use systemic or managerial user accounts like "sa", "dba ", " admin " and the same this.

4-4-2. Not accessing systemic files

As far as possible the managers should limit SQL server accessibility to systemic files and interactive commands like cmd. exe.

4-4-3. Disable Adhoc

Must disable ADHOC report through OLEDB from SQL server. ADHOC from OLED provider controls by determining Disallow Adhoc Access in registry. (Cerrudo 2008).

4-5. Process test and analyst

One of the efforts which can be done by a web –site manager is using different devices to recognize vulnerable parts of the web – site. For instance, SQLbrute (it can recognize the vulnerable parts in blindly attacks), SQLninja, SQLbf (the device to check SQL server username), SQLexec (For system commands which use xpcmdshell), absinthe, acnnetix web vulnerability scanner.

4-6. Recommendation to the website manager

It should be noted that complete security is not guaranteed in any time, therefore, Mangers of Ecommerce sites must be adhered to another principles.The most important recommendation is ensure that any SQL Injection vulnerability not exist, because even if all the problems identified and solved, the new problems are created daily.To prevent SQL injection attack is recommended to use parametric reports.

Also recommend that know the new protocol of electronic payment system and update their usages protocol. Also they have to figure on from security of bank payment portal. In addition, familiar with legal rules can in many cases due to possible damage to compensate for the attack. As last prevention and precaution, configuration and testing the firewall filters to block out unnecessary traffics control. Do not only causes the databases are more secure but are the entire network is safe (Cerrudo 2008).

5. CONCLUSION

Fast and ever-increasing changes of IT and connections in addition to really important gains including e-commerce, have caused new threats to national securities of the countries there fore, the discussion about securing virtual world especially e-commerce websites gain enormous importance so that whole regular and legal possibilities should be used together with technical possibilities to prevent crimes. Most of the penetrations which happen in a web application are a result of the weakness and gaps in programming and also weakness in databank. In recent years the main attacks to data bases are about those web-sites with e-pay possibility and credit cards of SQL injection attacks. Thus, this article have tried to introduce SQL injection attack mechanism and aim to attack the e-commerce programs databases, and also it briefly mentioned several techniques of this attack, vulnerable parts of an e-commerce web-site in connection with its database, and those attacks that in each part can be performed were investigated and finally a model to prevent these attacks was presented to be used by managers and web developers of e-commerce web sites and the ways to confront them have been presented.

References

[1] *Malware Detection,* 2007,Chapter2,Halfond W And Orso A,"*Detection And Prevention Of SQL Injection Attacks",* Springer Us, Volume 27, Isbn978-0-387-32720-4 (Print) 978-0- 387-44599-1 (Online)

[2] Cannings R, Dwivedi H, Lackey Z, 2008, *Hacking Exposed™ Web 2. 0: Web 2. 0 Security Secrets And Solutions*, Mcgraw- Hill Companies.

[3] Kosuga Y, Kono K, Hanaoka M, 2007, *Sania: Syntactic And Semantic Analysis For Automated Testing* Against SQL Injection, 23rd Annual Computer Security Applications Conference, Ieee, Isbn: 978-0-7695-3060-4

[4] Stuttard D, Pinto M, 2008 "*The Web Application Hacker's Handbook*", Wiley Publishing, Inc, Indianapolis, Indiana.

10/5/2012

[5] Fong E, Okun V, 2007," *Web Application Scanners:Definitions And Functions*", Proceedings Of The 40th Hawaii International Conference On System Sciences

[6] Ullrich J, Lam J, January 2008, Defacing *Websites Via SQL Injection*, Network Security, Volume 2008, Issue 1

[7] Thomas S, Williams L, Xie T, 2008, *On Automated Prepared Statement Generation To Remove SQL Injection Vulnerabilities*, Information And Software Technology, Volume 51, Issue 3

[8] Mitropoulos D, Spinellis D, 2008, *Sdriver: Location-Specific Signatures Prevent SQL Injection Attacks*, Compute R S & S E C U R I T Y Xx X (2 0 0 8).

[9] Muthuprasanna M,Wei K,Kothari S,2006,*Eliminating SQL Injection Attacks - A Transparent Defense Mechanism,* IEEE International Symposium on Web Site Evolution

[10] Chris A, 2006, *(More) Advanced SQL Injection*, An Ngssoftware Insight Security Research (Nisr) Publication,

[11] Chris A, 2002,*Advanced SQL Injection*, An Ngssoftware Insight Security Research (Nisr) Publication

[12] Grossman J, "Website Security Statistics", Founder And Cto, Whitehat Security, August 2008.

[13] Kachakil D, 2009, *Sfx-SQLi (Select For Xml SQL Injection*)

[14] Cerrudo C, 2008,"*Manipulating Microsoft SQL Server Using SQL Injection*", Application Security, Inc. Web: Www. Appsecinc. Com Halfond W, Viegas J, Orso A,2006,*A Classification of SQL Injection*