Internet and Database Security

Pratima Bhalekar
Asst. Prof. , Department of Computer Science
Ashoka Center For Business and Computer Studies,Nashik

Sonali Ingle
Asst. Prof., Department of Computer Science
Ashoka Center For Business and Computer Studies, Nashik

Abstract: Internet web sites are increasingly using web applications to access database systems for information retrieval, transactions and publication. These Internet web applications are commonly being used for e-commerce, e-banking, and e-government to purchase goods, make reservations, pay taxes, enroll in classes, retrieve academic transcripts,acquire account balances and pay bills, to name a few. At the same time, related security issues will appear,but the fundamental security rules will remain the same. In this article, we briefly overview the advanced web and database securities, the security design principles and security methods.

I. INTRODUCTION

In recent years, with the frequent occurrence of security incidents, enterprises and organizations have now realized the importance of designing a safety information system. Today, information systems are heavily relied on web and database technologies, thus the risks and threats those technologies faced will also affect the security of information systems. Web and database security technologies can ensure the confidentiality, integrity and usability of data in information system, and can effectively protect the security and reliability of information system. Therefore, in order to better secure the information systems, we need to learn Web and database security-related knowledge.

This paper can be divided into three parts: advanced security threats, the principles of safety design and safety audit; Advanced security threats section contains cross-site scripting (XSS) attacks, AJAX and SQL injection attacks and other security threats, which will be presented in detail; the principles of safe design section describe the general safety design principles to help design information systems security; last section describes the manual and automatically audit methods, and general security audit framework to help readers to understand more clearly.

II. ADVANCED SECURITY THREATS

2.1 Web security threats :

2.1.1 AJAX security

As Web applications become increasingly complex, it is required for the performance of Web services is also increasing. AJAX (Asynchronous JavaScript and XML) (Garrett, 2005) technology is mainstream technology of Web2.0 that enables the browser to provide users with more natural browsing experience. With asynchronous communication, user can submit, wait and refresh mode freely, update partial page dynamically. So it allows users to have a smooth experience similar in desktop applications.

However, a variety of Web applications has brought us countless convenience, produced a series of security problems. When the introduction of AJAX technology, because of its inability to solve the security problems, the traditional Web security problems still exist, along with elements of the composition and structure of AJAX features, will lead to new security threats. In recent years, adding AJAX elements in sites has become a very popular trend, and most websites are typical AJAX-based applications. As most of the website builders just enjoy the conveniences of AJAX technology, little is known about its security threat, resulting in most of the AJAX application sites have different levels of security risks. Here, we summarize and analysis the AJAX security threats.

1. Security Threats of AJAX Technology

a. The Deficit of JavaScript Language

- JavaScript is a widely client-side scripting language, originally designed and implemented by Netscape, and it has been widely used to reduce the burden on the server. JavaScript scripting language features determine its presence in all kinds of security risks:
- JavaScript is an interpreted language. In the interpretation process, every error is a runtime error. Run-time error can only be found during runtime. If somewhere in the code the programmer has left a Bug,

but the logic of the code at run time is not running to the area, then the bug will not be found, which leaving significant risks to the application. To detect, locate the error position of interpreted language is quite difficult.

- JavaScript is a weak typing language. Weak typing languages do not need to declare variables at the time the programmer declare the variable. This flexibility often easily leads to many problems.
- JavaScript code has dynamic nature. It can be dynamically generated code, and used the eval-function dynamic execution; or you can directly modify the existing function.Once the attacker can gain control of the JavaScript code, he can overwrite the other user-defined methods and even the browser built-in method, thus cause many serious malicious behaviours.

b. Problems of Asynchronous

Asynchronous communication is the highlights and core idea of AJAX technology. But asynchronous will also introduce a series competition problems.

2. Issues of AJAX Framework

a. Explosion of Client-Side Logic

Programming client-side logic using JavaScript will bring the client-side logic to public. Users can easily through the browser's View Source feature to see the client code.

b. Incomplete Server

Most AJAX programmers validate user input at client-side, though it reduces the burden of server, it lefts room for security risks.

3. Traditional Web Security Threats of AJAX

AJAX framework gives users a good experience in desktop's application, users no longer have such a long wait for the server to response and refresh the page. However, this feature also poses a problem: the user does not know what the current request was sent, did not even know the current request was sent. This feature allows many of the traditional Web attacks in a more intimate manner. Main traditional Web security threats are (Razvan & Maria, 2010):

- AJAX framework of SQL injection;
- AJAX framework of XPath injection;
- AJAX framework for cross-site scripting attacks (XSS);
- AJAX framework for cross-site request forgery attacks (CSRF);
- AJAX framework of denial of service attack (DOS).

4. Security Threats Introduced by AJAX

The introduction of AJAX, initially to solve the user to submit a request in the browser when the server response is required after a long wait, refresh the entire page to the next step of the problem. But AJAX technology to bring convenience, but also introduces some security threats.

a. JSON Injection and JSON Hijacking

JSON (JavaScript Object Notation) (Crockford, 2006) is widely used lightweight data transmission and exchange format in AJAX. JSON is based on a subset of JavaScript and developed from JavaScript Array and Object, and the adopted text format is completely independent with language. The data of JSON and can be transmitted cross-platform. Therefore, JSON Injection and JSON Hijacking are current two aspects of security threats.

b. Trust Crisis of AJAX Proxy

For security reasons, JavaScript code is limited to running in a sandbox, JavaScript also prohibit access to third-party domain. But sometimes you need to call in the AJAX thirdparty services, such as components Mashuop procedures. Solution to this is to build an AJAX proxy that the Web server to create a Web service, only forwarding calls to third-party Web service request. AJAX proxy allows the client calls the Web service as a third party may also have to provide AJAX proxy servers and third-party server, a crisis of confidence. First, the attacker can access through the AJAX proxy direct access to many previously unavailable resources. Meanwhile, the attacker via AJAX proxy attack on third-party Web server, you can also hide the source of the attack, showing up as if from the AJAX proxy attack (Anley, 2002).

c. Disclosure of User Data

AJAX technology gives users a better browsing experience, but some AJAX-based application inadvertently brought the disclosure of user data. AJXA technology is widely used in such situations: a user registers a mailbox, enter the account he wants to use, after he moves to the next input section, the browser prompts the user name input box: the account that you are applying has been applied, please re-apply. This design reflects good humanbased design rule, the user does not have all the information before being prompted to fill out and submit the account has been to apply for. But in this way the user data will be leaked in the unconscious. False malicious attacker by entering any letters, numbers, combined to form the account, you can immediately know whether the mailbox has been registered. If you know the mailbox already exists, there may occur spam, or send e-mail containing the malicious XSS code may be so. Enumeration by simple repetition, the attacker can even know the mail server name of all existing accounts, which will undoubtedly bring great threats.

2.1.2 Cross site scripting

Cross-site Scripting (also known as XSS or CSS) occurs when dynamically generated Web pages display input that is not properly validated. In XSS, malicious attackers acted as normal visitors upload Malicious Script as JavaScript codes etc. to Web server by utilizing the bugs of utility programs or codes in the Web server. Attackers also send URL links including malicious script to objective users. When Web users visit the pages containing malicious script or open the received URL links codes in the Web sites, users' browsers will auto-load and execute the malicious script codes. This attacking procedure indicates that XSS is actually a simple attack technology. In most cases, malicious attackers attack users indirectly by utilizing Web server, and direct attack occurs merely.

XSS is a passive attack. First of all, by utilizing the XSS bugs in the Web programs, alicious attackers construct a trap page and the malicious script can be saved in the page content or URL. The URL of this page is then announced in the BBS after embedding to e-mails or disguising attractive titles. If the users visit ULR, the JavaScript will be executed by
attackers' browser. The procedure of XSS attack is shown in fig. 1.

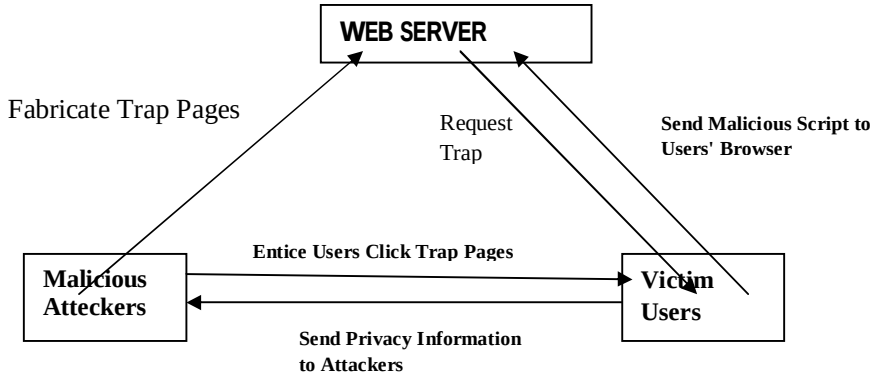

Fig. 1. The Process of Cross Site Scripting Attack

2.2 Database security threats

Database security relates to two parts: data visiting and data recovery. The first part can be realized by using a suitable authorization to make sure that the legal users can get their right data and reject all exceeding authority at the same time. The latter part means that database can recover the data securely and completely. Recently, database is facing the problem of security hole e.g. privilege elevation, SQL inject,XSS, data leakage and improper error processing.

2.2.1 SQL inject

1. SQL Inject Principle

SQL Inject refers that the attackers deceive database server to execute unauthorized wilful inquire and illegal operation through adding extra SQL statement element to the end of predefined inquire statement in application programs. The essence of SQL Inject is utilizing the bugs caused by the programmers who did not detect or incomplete detect the database inquiry request, submitting malicious SQL statement and cheating server executes malicious inquiry. At last, the attackers can get the sensitive data or control the whole website. The main reason for SQL injection attack to succeed is that when dynamically generating SQL statement commands, websites only directly using the subscribers inputted data without any verification.

2. Process and Methods of SQL Attack

In SQL attack process, the attackers firstly trial the SQL inject bugs in application programs by design inputs. The executive SQL statements are then imported to control implement programs. After obtaining the database information, the attackers acquire the administration authority of server system.

a. Discovery of SQL Inject Bugs

Discovery of SQL inject bugs brings necessary information to further attack. Before SQL attack, the attackers need to identify the aim database platform and decide what SQL attack statements or methods should utilize (Halfond et al., 2006).

b. SQL Inject Bugs Utilization

- After finding out the bugs, attacks including illegal inquire database, obtaining secret information and users data, controlling database and server system occur.
- Speculating table name and field name. Attackers take advantage of SQL statement, such as `and (select count(*) from TestDB.dbo.tablename)>0;` to guess table name. If the table name have existed, the webpage returns to regular.
- Obtaining field value. After getting table name and column name, field value is generated by utilizing ASCII word-by-word decoding. After these two steps, the attackers can get data, user name, password and information in database.

III. SECURITY DESIGN PRINCIPLE

3.1 Web security design principle

We should obey the following principle when designing and deploying computer network security.

1. Balance Analysis Principle of Demand, Risk and Cost:

According to the existing technology, there is hardly a perfect Safety network. We should do some qualitative and quantitative analyse to threaten and possible risk network faced. The standards and measures are then made to confirm security policy of system.

2. Principle of Comprehensiveness and Integrity:

We can analyse security issues of network and formulate specific measures by using views and methods of system engineering. Multi-methods make a prefer security measure. A computer network including links of human being, device, software and data take an important role in network security, and only analyse and treat in whole view can they obtain valid and executive measures.

3. Consistency Principle:

Consistency Principle means that network security issues should concurrent exist with the whole network operating cycle, and security architecture should keep in line with network security. Actually, network security strategies should taken into consideration in the beginning of network construction rather than at the end of this procedure with characters of facility and low cost.

4. Principle of Security and Reliability:

Guarantee of system security is very important. In procedure of design and implement, specify measures are adopted to ensure security of information secure product and technology proposal. By strict technology administration and redundancy configuration of device, quality of product and reliability of system can be guaranteed.

5. Principle of Advanced Technology:

Advanced technology system and standard technology are required in security design.

6. Principle of Easy-operation:

Security measures are manually completed. Complexed measures can always lead to high requirement for administrators, and low security. Otherwise, the measures should be friendly to operation of system.

Methods as installing fire wall, setting up isolation region for protected resource, encrypting the sensitive information being stored and transmitted, providing identity authentication and building secret passage, providing digital signature for audit and tracking to software without any security guarantee are adopted to ensure Web service security.

1. Install Fire Wall

The most popular security method is providing an isolation region to LAN or website. Firewall of LAN is a function module inside computer or network equipments between innernet and Internet. Its purpose is to provide security protection to an innernet or host and control access objects, so it can also called access control technology. There are two operation mechanisms for fire wall e.g. packet filtering and agency. Packet filtering aims at the service provided by host of special IP address. Its basic principle is to intercept and capture IP packet of IP layer in network transmission, then find out resource address and destination address, source port and destination port of IP packet. Whether to transmit IP packet is based on fixed filtering principle. Agent is achieved in the application layer, the basic principle is to construct an independent agent program for Web

services, and client program and the server can only exchange information by their own agent programs rather than allow them to interact directly with each other.

2. Encryption for Confidential Information

This method is particularly effective to protect confidential information, which can prevent wiretapping and hacking. Transmission encryption in Web services is in general achieved in the application layer. When WWW server sends confidential information, firstly, it selects keys to encrypt the information, based on the receiver's IP address or other identification; After browser receives the encrypted data, it decrypts the encrypted data according to source address or other identification of the information in IP packet to get the required data. In addition, transmission, encryption and decryption of information at the IP layer also can be achieved by encrypting and decrypting the whole message to ensure information security at the network layer.

3. Provide Identity Authentication for the Client / Server Communication and Establish A Secure Channel

Currently some network security protocols e.g. SSL and PCT have appeared, which are based on the existing network protocol. These two protocols are mainly used for not only protecting confidential information but also preventing other unauthorized users to invade their own host. SSL protocol is a private communication and includes technology of authentication, signature, encryption for the server, which can not only provide authentication for the server but also provide authentication for the client according to the options of the server.

4. Digital Signatures for the Software

Many large companies use digital signature technology for their software, and claim that they are responsible for the security of their software, especially e.g. Java applets, ActiveX controls, which will bring risks to Web services. Digital signatures are based on public key algorithms, using their private key to sign its own released software, and are authenticated by using the public key. Microsoft's Authenticode technology is used to identify a software publisher and prove that it has not been damaged. Authenticode is software for client, which monitors the ActiveX control, Cab files, Java applets, or download of executable file, and look for the digital certificate to verify in these files, and then show warning words, the certificate organization's name and other information to the user for possible security problems. Digital signature can protect the integrity of the software, and it is sensitive to illegal change of the software in the transfer process.

3.2 Database design principles

Users enter into the database system through the database application program when users firstly access the database, database applications deliver the username and password which is submitted by the user to the database management system for certificating, after determining their legal status, users are allowed to enter. They also must pass the authentication when operate objects, tables, views, triggers, stored procedures etc. in the database. How can users operate in application and database is depended on rights allocation and constraints of accessing control.

1. Secure Database System Model

Criteria based on security database, you can create a simple security database system model which is divided into four layers: system layer, including data access, encryption and decryption algorithm; function layer is the key to the whole system, including key distribution mechanism, fast indexing mechanism and derive control; interface layer is directly user-oriented, which includes the function of user authentication, authorization management, database maintenance and query management; At application layer, users can manage database through not only interactive ways but also command mode.

2. Management Strategy of Database

a. Access Control

Access control is the rights control of user access to all kinds of resources of the database, which is divided into two stages: one is security account identification, the other is the access permission identification. In the security account authentication phase, the user logins for the authentication, if it's successful, he can connect to the SQL Server, otherwise it will reject the connecting requirement. Access license verification refers to that after the user connect to SQL Server, the system determine whether they have license to access to the database according to the user account stored in the database and correspond to server login identification. Access control can prevent the illegal users.

b. Database License

After the legal users access to the server and database, the database access mechanism will control the legal users to operate the data objects. First of all, statements in the database license will limit the database user to

carry out some SQL statements. Secondly, objects in the database license will limit the database user to carry out some tasks of the database objects.

c. Establish Data Security by Using System Stored Procedures
As the database administrator, if you want a user to have a select right rather than the delete right, at this time you can achieve the goal by establishing stored procedures, thus protecting the safety of the data.

d. Establish Data Security by Using the View
If the administrators give users the permission to access the database tables and form a too large user access area, it will cause threats brought by users to data security of the database. To avoid this situation, you can achieve data security view through the way of establishing data view.

e. Establish Data Security by Using the Database Role
This role is used for setting license at a time that number of database users can access to the database, if permission is not deployed properly, it will threat data in the database directly. As an administrator, you should be very careful when you give permission to the public role.

f. Data Backup
Data backup is principal work in the course of daily management of the database. When the server or database system breaks down, the original data is difficult to recover without a backup strategy. Therefore, the database should be installed in security zone of their intranet, and cannot be connected to the Internet directly. In addition, different computers should implement backup strategies to protect data security when people deal with abnormal failure.

g. Database Encryption
Database encryption requires that database cryptography changes plaintext into cipher-text, and cipher-text data stored in the database. Cipher-text is decrypted to get clear information when queries, so data will not be leaked even if the hardware store is stolen, thus the database system security is greatly improved, of course, the cost also increases. Response to attacks from the network level, the database mainly uses many ways e.g. installing a firewall, doing intrusion detection etc. to improve its safety performance. Firewall resists the incredible connections from outside. Intrusion detection systems are generally deployed in firewall, and detect abnormalities on the network and the host through Network packet interception analysis or Analysis of log.

IV. SECURITY AUDIT

4.1 Definition of security audit
Security audit is based on certain security policy, improving system's performance and safety by recording and analyzing historical events and data. Security audit includes all actions and instruments, e.g. testing, assessing and analyzing all of the weak links in the network information system to find the best ways to let the business run normally, based on the maximum guarantee of safety. It is to ensure the safe operation of network systems and prevent confidentiality integrity and availability of the data from being damaged, prevent intentional or unintentional human error and detect criminal activity on the network. The network status and processes can be targeted to recorded, tracked and reviewed by using the audit mechanism, and find safety problems. In addition, the audit can provide the basis of making filtering rules for online information, if the harmful information is found in the website, it will be added into the list of route filtering, to reject all information of IP addresses on the filtering list through information filtering mechanism.

4.2 Execution of security audit
4.2.1 Key technologies of network security audit system
1. Analysis of Data Source of Network Security Audit System
For security audit system, selection of incoming data is the key problem to be solved, data source of the security audit can be divided into three categories: Based on the host, based on network and other channels. In order to select the appropriate data sources, it analyzes each class of data source respectively as follows.
a. Data Source Based on the Host
Data sources of the network security audit based on the host , including audit records of the operating system, system log, log information of application system and information based on the target.
b. Data Source Based on the Network
Network data is the most common source of information in the current network security audit system and commercial intrusion detection system. The basic principle is that when the network data stream transmitting in the network, using a special data acquisition technology to collect the data transmitted in network as the data source of security audit system.

c. Other Data Source

Data source from other safe products mainly refers to log files produced by safe products e.g. firewall, authentication system which are operated independent in the target system. These data sources also should be considered by security audit system. Data source from network device e.g. a network management system, using information provided by SNMP (Simple Network Management Protocol) as data source. Out-of-band data source refers to data information provided by the artificial way, which is contrived and non-systematic, e.g. recording what happened in system environment manually, including hardware error information, system configuration information, system crash, other kinds of natural hazard events etc. Out-of-band data source may play an important role for later analysis.

In general, it will improve the performance of security audit system if active log of the network and its safe device are used as audit data source.

3. Network Security Audit System Architecture

Network security audit system mainly consists of three modules.

a. Data Collection Module

Data collection module acquires network packet of users' operation by monitoring and core filtering technology depending on imaging feature of switchers and user-defined strategies. The key to realize this module is to acquire accurate and complete packet. Data integrity of data acquisition modules is determined by the exactness and completeness of audit results.

b. Packet Processing Module

Protocol analysis is a key step in the data packet processing. Main job of packet processing module is to capture the data packets and determine the protocols e.g. TELNET, FTP and other protocols it belongs based on their header information. According to the formats, transmission mode and message content, it make the user's operation to restructure, restore, and finally it restore user data and submit to the audit module.

c. Data Audit Module

According to the rules defined format, the achieved user information e.g. TELNET and FTP commands, SQL statements, manipulate objects, operating keywords will match with the user-defined strategy in rule base. Responses are made according to the matching results, and the audited data are recorded into audit logs. The rule base is generated based on the visit strategy deployed by authorized administrator. The authorized administrators formulate or modify the strategy, and issue it to the next rule base. In process of utilizing audit system, administrators gather experience and add novel strategies constantly according to the issues in system usage making the rule base more and more abundant.

4.2.4 How do security audit

1. Establish Audit System

An audit system which leads to excellent audit should to be developed to ensure that auditors do their work on a regular basis. In the audit system, auditors should clearly know what the audit objects are. The main focus is the enterprise's information protection e.g. the server, backbone switches, routers and security devices.

2. Focus on Safety Auditors fostering

Safety audit involves massive products and wide content. The basic information of the audit come from operating system, network systems, security devices, applications system etc. Security auditors are not only necessary to understand the operating system knowledge, but also should be familiar with network protocols, database, virus infection mechanism. Moreover, auditor should understand the basic situation of application systems as well as master the work principles of servers, switches and security devices, especially the understanding a variety of security policies of information systems deeply. Thus, in the audit processing, the analysis of massive information can be developed and the observing and thinking ability can be cultivated. However most of the enterprise information system security audit work is just begin without any own professionals. Although security audit can be conducted by professional security company or buying excellent audit software, it is still harmful in term of the safety and longterm development. The audit process involves a number of important enterprise information especially the system security weaknesses. Serious threaten will occur when criminals turn up or the workers are in low ability to analyze the weak links. From the above analysis, the security audit work should be accomplished by the professionals in the enterprises. From the angles of security audit requirement for auditors and situation enterprise internal personnels, the enterprise should lay emphasis on the foster of information system administrators, network administrators, security guards especial the safety audit personals. Because all security policy, security system and security measures are developed by human beings, personnels with high quality and ability are required in developing management standards of enterprise information system and ensuring enterprise information security.

3. Reasonable Structure of the Security Audit System

The premise of improving the safety audit is to build a security audit system in line with business needs. In building a security audit system, the follow issues should be considered:

a. The profundity and scope of audit. The audit profundity and scope determine the complexity of the audit system, which are also the basis of audit products selection.
b. Problems of data sources. An audit system operation is based on data from the system at all levels, and how to obtain the data sources of audit system is the most critical issue.
c. Relationship with the original systems. To ensure the normal operation of the original system go smoothly in the realization of the audit, and the least modification and the minimum impact on system performance make the audit perfect.
d. Eliminate of audit function ignore. If the audit system is easily bypassed, it would lead to serious problems.
e. Effective utilization of audit data. In establishing an audit system, the lack of deep utilization of audit data will lead to weak audit system effection.

Network security is accompanied with the production of computer, especially the present popular network, security problem is emphasized by at all levels of sectors and industries especially the area of intranet security. Network security is a huge and complex dynamic system, hardware equipments provide basic security for the network, but a system which continues to improve can find a kind of dynamic equilibrium only with the help of network security audit system by doing real-time audit and effective evaluation to the system which has been established and discovering the potential safety hazard in time. These problems will become hot spots for future security research in building a solid and reliable network security audit system.
Computer network security audit is a very complex and extensive research subject, as an indispensable part in integrity security framwork, it is a complement for a firewall system and a intrusion detection system. It involves a wide range of knowledge. With the complexity of computer operating system and network communication technology increasing, the complexity of network security audit is also increasing. How to improve network security audit system performance of various technologies and how to build a strong network security audit system need to further constantly explore and research.

V. CONCLUSION

Web and database technologies are in a rapid evolution roadmap, for example web3.0 and graph database (Angles, 2008) are getting more and more attention. At the same time, related security issues will appear, but the fundamental security rules will remain the same. In this chapter, we briefly overview the advanced web and database securities, the security design principles and security audit rules and methods. Due to the limitation of chapter length and variable programming languages, most contents in each section are general guide lines and rules. When deploying practical information systems, we need to map those rules to real implementation. Information systems can be more secured if we know and apply those technologies.

REFERENCES

[1] Jesse James Garrett (Feb 2005). Ajax: A New Approach to Web Applications. Available from http://adaptivepath.com/ideas/ajax-new-approach-web-applications
[2] Raducanu Razvan & Moisuc Maria (2010). The security of Web 2.0 and digital economy. *Recent Advances in MATHEMATICS and COMPUTERS in BUSINESS, ECONOMICS, BIOLOGY & CHEMISTRY*. pp.168-170, ISSN: 1790-2769
[3] D. Crockford (July 2006). The application/json Media Type for JavaScript Object Notation (JSON). *RFC 4627*, July 2006Anley C. Advanced SQL Injection in SQL Server Applications. *Next Generation SecuritySoftware Ltd*. 2002.
[4] Halfond W G ; Viegas J and Orso A (2006). A classification of SQL-injection attacks and countermeasures. *Proceedings of the IEEE International Symposium on Secure Software Engineering*, Mar. 2006 Renzo Angles, Claudio Gutierrez. Survey of graph database models. *Journal ACM Computing Surveys*, Volume 40 Issue 1, February 2008