Survey of Web Application and Internet Security Threats

Hesham Abusaimeh and Mohammad Shkoukani

Department of Computer Networks Systems, Faculty of Information Technology, Applied Science University,
Amman, 11931 Jordan

Abstract

Computer and network security are one of the most challenging topics in the Information Technology research community. Internet security is a significant subject that may affect a wide range of Internet users. People that use Internet to sell, buy and even to communicate needs their communications to be safe and secure. This paper is discussing the different aspects of Internet and networking security and weakness. Main elements of networking security techniques such as the firewalls, passwords, encryption, authentication and integrity are also discussed in this paper. The anatomy of a web applications attack and the attack techniques are also covered in details. The security of high-speed Internet as the growth of its use has stained the limits of existing network security measures. Therefore, other security defense techniques related to securing of high-speed Internet and computer security in the real world are studied as well such as, DNS, One-Time Password and defending the network as a whole. This paper is also surveyed the worm epidemics in the high-speed networks and their unprecedented rates spread.

Key words:

Web application Security, Network Security, Protection tools, SQL Injection, Firewall, and Intrusion Detection System.

1. Introduction

A fundamental fact in Internet security and web applications is that impossibility of 100 percent assurance that a computer system is reliable and confident. Internet security is the process of defending and conserving the resources and data of the private organization that are shared on the Internet. Internet security is one of the most important subjects that may affect a wide range of Internet Users. People that use Internet to sell, buy and even to communicate needs their communications to be authenticated, reliable, and safe.

The Web applications market importance appears from the increment of the number of organization that implement applications that wants to share on the internet for customers' services support or remote self-monitoring. This leads web application to become an environment to attract people and businesses, so it is a great target by attackers. Therefore, World Wide Web (WWW) has been developed from static web pages to dynamic platforms, which are linked to databases to provide different applications, known as web applications.

These web Applications is used in many field of businesses, it could be an informational website providing information about certain field or many fields, or an e-commerce website to let customers sell and buy items, or solution application on the extranet and /or the intranet of organizations. Web application can also be such as e-mail server or search engines. Computer-based systems are behind of all of these applications, and the security weakness is here. Once the attacker reaches the web application this may lead him to reach the computer-based system or the database, the server or implementation configurations, or the operating system settings then the companies will be in critical problem. If the attacker could not pass to the computer-based system, he might pass some wrong parameters, calculation, or send queries that injured hardware and software; leading to access unauthorized data, and disrupted business operations [1].

Many studies discussing the vulnerability of the web application, prove that almost all of the web application is not secure, some studies shows that half of the web applications have a high risk level and other shows that 80 % of the web applications have at least one critical security threats [2] [3].

Over the past years, there have been many technologies introduced by the U.S. government agencies and industry to protect their systems. These technologies should be enough to protect the electronic systems. However, they are not very efficient because of the lack of experimental tools that are trusted to protect these systems, and the lack of research and studies to improve developing and testing of the next generation security tools [1].

In addition, some studies believe that securing the high-speed Internet from viruses is an important factor at the present to protect the web applications. These studies also consider the benefits of the virus scanner tools to protect the personal computers, servers, proxies, and gateways from many known viruses and remove them from data, files and packets that will reach the web applications [4]. The high cost of security tools is also another important reason of insecure the web servers [5].

Viruses' danger was discussed by Thomas M. Chen in [6]. He wrote that since virus development has been grown to reach Macro viruses that affect the users of Microsoft applications, Viruses attacks become more critical and serious for all computer users.

Manuscript received December 5, 2012
Manuscript revised December 20, 2012

Comprehensive tools to auto protect the web applications and system might be the only way because of the high spread speed of the worm epidemics in the high-speed networks. However, these automated defense systems could cause many problem related to the limited accuracy and real time traffic reliability. The model of the epidemic spread of the worms through the high-speed networks was discussed in details.

In this paper we will survey the state of the arts related the Attacks types, methodology and the protection techniques. We will also focus on the professional security community techniques that can be used to take advantage of a web application that is vulnerable to SQL injection, and to make clear the correct mechanisms that should be put in place to protect against SQL injection and input validation problems in general. The SQL injection as a hacking technique, which is an important one, was also discussed in details [7].

2. Weakness of the Web Environment Security

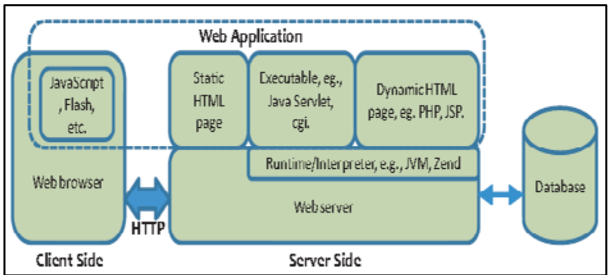


Fig. 1: Web Application Components [8]

In order to know the weakness of the web environment we should also know the components of the web application. The web applications consist of three main parts as shown in the Figure 1. The programming language is used to design the client side and to establish the queries of the database. The Hypertext transfer protocol (http), which is used to link the client side with the server side. In addition, to the business process which is the distinguish part of any web application [8].

Another main threat in the internet security and web applications that the users browse via the default port number 80 using the http protocol and the port number 443 using the https secure layer protocol. The attacker starts using the web as a normal customer or user of the web site then these ports are used to attack the site and accessing the customers' data and files. The attack size depends on the importance of the data and the business of the companies that own these websites.

Many studies show that there are many managerial issues or administration errors, which lead to security threats such as:

1. The security threats are not clearly shown in the websites.
2. Security problems are usually solved via short-term recovery so the problems will appear again very rapidly.
3. Ignoring the fact that the information on the websites is costing money, in addition to losing the ability of estimate the information cost.
4. They do not understand that frequent security threats are causing decrementing the reputation of the organizations.
5. They depend on ready protection tool such as firewall or intrusion detection system without monitoring them regularly.
6. The relationship between the business problem and the information security is not totally understood from technical people.
7. Usually, information security tasks are requested from non- security expert people without giving them good training and enough time to do their tasks and fix the problems probably. Mainly this is happened, because most of the organizations need quick solutions to re-launch their websites again or to fix its application bugs.

All business websites will be attacked so it is when it will be attacked. In several examples as Western Union's site and Walt Disney Company, computers attackers used built in security problem in the web application to access the web data or get data from related systems or databases. It is also emphasized that using security prevention tools that we will explain later in this paper individually is not enough to secure a web application, these tools like:

1. Encryption and Decryption
2. Https or Secure Socket layer
3. Accounts and passwords
4. Listening or scanning programs
5. Firewall
6. Intrusion Detection System

3. The progression of the professional attacker

As Shown in Figure 2, the attacker will start using the web application as a normal user or customer. Then he can passes some of the prevention tools such as firewall or intrusion detection system until reaching the application layer where he will begin his attack. Usually, customers attackers are looking forward to get some privileges of normal users in order to collect or damage web information, while normal users attacker are trying to increase their privileges in order to get extra information and roles [9].

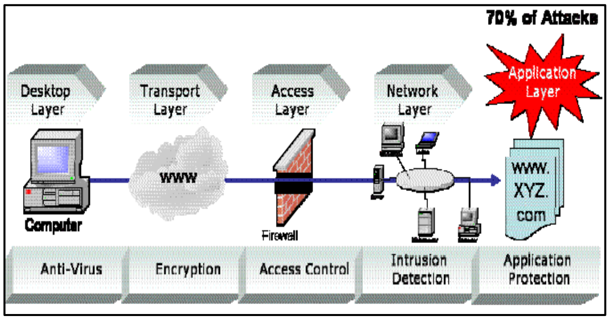


Fig. 2: The progression of the attackers [9]

4. How Do You Protect Your Site?

Security is not an easy thing that you only need to implement or apply. The cost of securing small static web sites for some organizations could be larger than the organization could pay or think to pay. This high cost came from that you do not only need to protect the customer data but also you need to protect your systems from frequent attacks which may cause to Denial of service attack, that make your web site down. These attacks can prevent some organizations that depend on e-business or e-commerce from doing their Job. Therefore, most of the companies' web applications are likely to be under the risk of attacks [5].

In order to protect these web applications, security experts must have the ability to detect the security threats and the back doors in their web application. After that, they can provide the solution starting with the urgent and highest priority problems such as Denial of service until covering all the security threats [10].

5. The Anatomy of Web Applications Attack

The structure of any attack goes through the following steps [11]:

1. Scanning: Initially most of the attackers begin with scanning all the open default ports on the web application IP address or the database starting with the default ports.
2. Gather information: After the scanning, the attacker try to know the versions and the edition of the web server and the Database Management System (DBMS) that are used in the targeted web application. Then the attackers try to use the public and default settings and passwords.
3. Code Testing: the attacker will start after that looking for any development errors that could let him attack the web application or increase his privileges, these errors can be found via running a normal testing process for the code and the script used in the web application.
4. Attack Planning: After all the previous steps, the attacker can design a complete plan in order to launch his attack on the web application.
5. Attack Launching: based on the gathered information and the putted plan the attacker attack the web site trying to damage all the data or get the data of the vulnerable we application [11,12].

6. Web Application Development Attack Techniques

Many attack techniques can be used against any web application. Some of them will be mentioned in this paper, but there are some techniques targeting the development layer of the web application such as the following [10, 11, 12]:

1. Passing Parameters: which means send some styles of parameters to the web application in order to get more data than the available on its pages. Passing parameters can be in a simple format and only pass the parameter to a web page in order to get some internal data or it could be hard format and send these parameters via the SQL queries in order to get more worthy data from the database.
2. Forcing a program: in this situation, the attacker force the web application to dead end in order to get some debugging and testing parameter then he can use it to see the hidden environment of the application or make the web down.
3. Accessing Cookie: some attackers are trying to access the contents of the cookies that have been transferred between the clients and the web application. The attackers may gain access to the restricted web application using information in the cookies.
4. Default Files Search: the attackers my query the default files of the programing environment that may stay accessible by the programmers. These files could be used to access unauthorized connection information.

7. Common Application Attack Methodologies

The way of implementing the attacks is called the attack methodology. Usually, we do have two main applications attacks methodologies, the static and dynamics attacks. The attacker usually used common and popular known attack methods in executing his attack in the static attack methodology. While, using complex and hard attacks methods that it is hard to prevent or even detect is called the dynamic attacks methodology [10].

7.1. Static Attacks Methodology

There are many well-known methods used in the static attacks methodologies such as the following methods:

1. Famous Methods or Exploits: in this static method, the attackers try to implement the well-known attack methods that have been used in attacking such a web application. The attackers try to get these methods from expert attackers or from the forums and the search engines.
2. Directory Enumeration: the attackers try in this method to get the map of the web application and the structure of the web directories in order to understand the hierarchy of the web application. In this method the attacker try to use a common hidden file and folders used in similar web structure in order to access the site critical information.
3. Debugging the Web Application: Discovering the backdoors and the code errors are used to get useful information to attack the web applications. Most of the web applications developer left code errors and backdoors in their applications.

7.2. Dynamic Attacks Methodology

The dynamic methods are more complex than the static method and they are changeable from one application to another. Such as the following methods [13, 14, 15, 16]:

1. Link Traversal: the attackers trace the URL of certain website to know some of the links and URLs that are no longer available or exist. These links may still reach some valuable information that is not removed yet of the web application.
2. Path Truncation: it is different from the link traversal because it is only care about the directories of the web application and the contents of these directories. Most of the web site error pages lead the attackers to know the structure of the directories in that web application.
3. Session Hijacking: the attacker captures the information and the parameters of the session's values in this method. Using this method, the attackers get permissions to unauthorized data.
4. Hidden Web Tracks: in this dynamic method, the attackers check the source code of the html code of certain web pages in order to know some of the hidden paths in the web application or old commented directories paths.
5. Java Applet Reverses Engineer: Some attacker decompiles the Java Applet code at the client site login. This reverse engineer gets unauthorized information from the web site let the attacker access the web site.
6. Checking the Backup Folders and the default files extensions: the attackers start the attack from the common files extension and backup folder names. Mainly the mirror of that web application including useful information about the website is available in theses folders.
7. Passing Parameters: Most of the Web applications allow its customer to submit parameters to their systems via web forms. The attackers submit invalid parameters via these forms in order to misuse the web application.
8. Executing Scripts: the attacker forces certain web server to execute a script, which is not implemented in its web application. The aim of executing these foreign scripts is to steal some information and user's cookies.
9. SQL injection, the most important dynamic methods is SQL Injection, where the attacker injects the web server with SQL statements and commands in order to attack the database and get useful information. More details about SQL injection will be followed in this paper.

8. Worm Epidemiology in the High-Speed Networks

Automated protection tools is used to auto protect the computer systems and the web server because of the high speed of worm propagation that can wait until be recovered by human. Most of these protection tools depend on detecting the worm after affecting the computer system. Moreover, using the high-speed computer and mobile networks has raised the risk of propagating the worms in many crossed systems and web applications.

The computer worm starts looking for vulnerable computer host. Then it start propagate and spread in the whole network in order to affect all the hosts in the entire systems servers of the network. Here is the difference between the worm and the virus, which that the worm spread faster in the network rather than stayed in the affected host system. Assuming that we have N computer systems or serves that are all vulnerable, but still clean from the worm infections. In addition, this worm propagate among the system in propagation speed equal to (β), then (It) the Number of the computer system that infected by the worm during with the (t) time can be calculated based on the following equation (1) [19].

$$It = \frac{I0N}{I0 + (N - I0)\, e^{\beta N t}} \qquad (1)$$

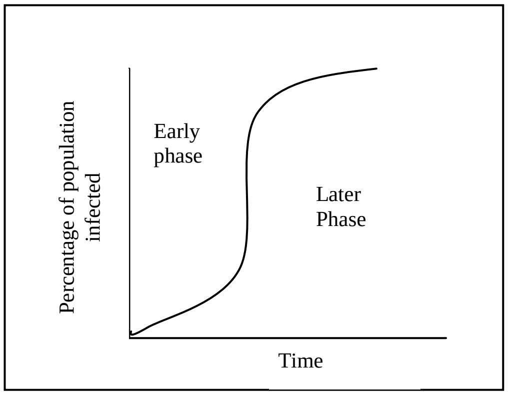


Fig. 3: Worm propagation in the web application

When a computer system infected the worm stay ready for a certain trigger in order to launch its attack with this time, the worm can spread among the other computer system through the time shaping this S figure that is shown in Figure 3.Which has the familiar S-shape shown in Figure 3. At the early level of the infection time, the number of infected system will be very few. This number of infected systems will be increased with the propagation rate (β). This increment will be very fast until most of the systems become infected with the worm and the later phase [19].

Figure 4 shows the random propagation of worms through infected random hosts. In the early phase, the worm on the infected host looking for a number of vulnerable systems to be its next hosts. Then the worms on these hosts will rescan the network looking for new hosts causing exponential increment in the number of hosts. The process of scanning the network will be very efficient and easy because of the huge number of systems that can be hosts of the worm.

The size of scanning system raises the number of infected hosts, resulting in network congestion similar to a denial-of-service (DOS) attack. The worm may also affect the application layer protocol [15].

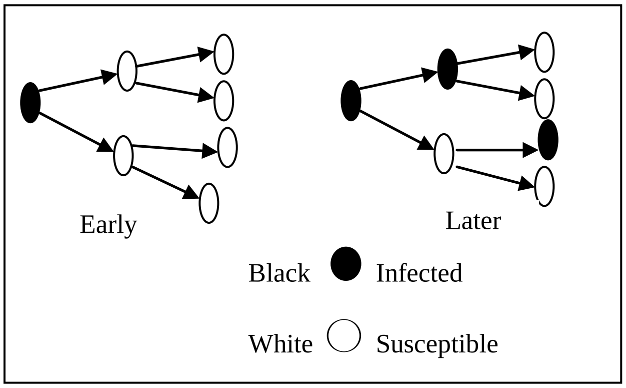


Fig. 4: Showing the Infection speed of the web application

9. Web Applications and SQL Injection

The relation between the database and the web applications is very strong, because most of the web applications are designed to retrieve and store the customer data in the databases. Therefore, SQL injection becomes a major attack on the web application to retrieve or store data without authorization or access permission. The SQL injection is a method of inject the web application with fault parameter via the SQL statements in order to get unauthorized access. The SQL injection is mainly depend on the client side of the web application [17, 18, 19].

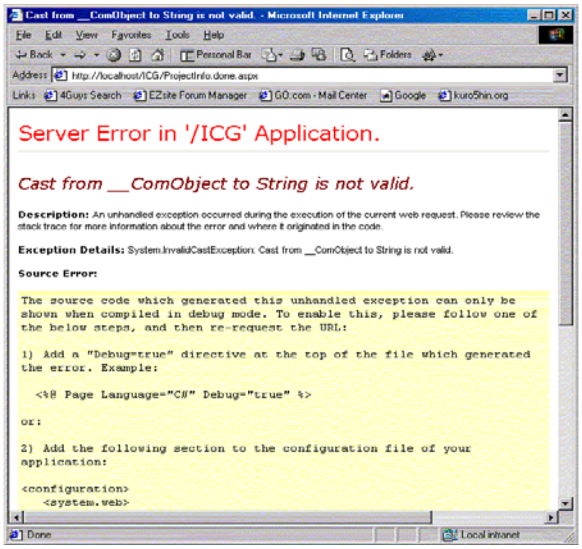
The SQL injection can be used through the following two stages:

1. Testing for Vulnerability

In this stage, the attackers are looking for web application that can insert SQL statement to it. Then that attacker makes script or SQL statements in order to pass them via the parameters from the web application to the database [20]. Therefore, the developer of the web application must validate all the parameters passed to their classes and functions. In addition, all the development team should cooperate among them in order to validate their parameters for their function because these parameters will be passed cross the system [20, 21].

2. Evaluating Results

Some SQL injection attacks are based on result appears on the server such as Open Database Connectivity (ODBC) errors as shown in Figure 5, http sessions syntax, and some code comments that may appear in the error pages. These errors can be used by the attacker in order to launch the SQL injection attack [21].


Cast from __ComObject to String is not valid. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Personal Bar Folders
Address http://localhost/ICG/ProjectInfo.done.aspx
Links 4Guys Search EZsite Forum Manager GO.com - Mail Center Google kuro5hin.org
Done
Local intranet

Server Error in '/ICG' Application.

Cast from __ComObject to String is not valid.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.InvalidCastException: Cast from __ComObject to String is not valid.

Source Error:

```
The source code which generated this unhandled exception can only be
shown when compiled in debug mode. To enable this, please follow one of
the below steps, and then re-request the URL:

1) Add a "Debug=true" directive at the top of the file which generated
the error. Example:

  <%@ Page Language="C#" Debug="true" %>

or:

2) Add the following section to the configuration file of your
application:

<configuration>
   <system.web>
```

Fig. 5: ODBC error message in web application

Executing the SQL injection attack can be in many forms, the following are the major attack techniques of the SQL injection [22, 23, 24]:

a. Passing Parameter to gain authentication: the easiest SQL injection technique is to send parameter to any input form such as login form which most the web application has. The attacker here tries to pass parameters that make the conditions of the expected SQL statement at the server side becomes true and retrieve the correct data [25].

b. Used Information from the error message appeared on the web application pages: Sometime error messages show part of the SQL statement that has the error. Then the attacker start to build up his message based on the information he got from the error message. The attacker may also recompile the error message in order to redesign the script or the code that include the SQL statement in order to inject it with fault parameters [24, 25, 26].

c. Select Statement Union Attack: some web application forms retrieve its data based on filters inserted from the users. These filters are fields in a where conditions of select statement. The attacker may use these filters especially if they are inserted filters such as search engine where you can add any word to filter your data, to add Union All other select statement to the original select statement. The input result, which will be passed to the database, is two select statements union each other. The output of this will be the execution for the first statement and the second on even if the condition of the original one is wrong [26].

d. Parenthesis attack: missing SQL statement parenthesis "( )" may be one the syntax errors that can be used to inject a parenthesis in different location and return fault records [27].

e. Like Queries and percent sign '%': most search functions use like clause with percent sing in the select statement in order to return any record that have a field or part of field like the condition field [28].

f. Using insert command: Adding information to the database is done using the insert command. The attackers may use the insert statement in order to fill the database with a fault rows. Other attacker my take advantages of the page after the insert form page in order to edit or retrieve the data from the database. The attacker may fill the values of the insert statement by other select statement. Therefore, he can show information from the database in indirect way [25].

g. Using SQL server stored procedure: stored procedures include set of SQL statements. Most of the databases management system have default installed stored procedures such as Microsoft SQL server has thousands of stored procedures. Attacks on stored procedures can be critical security threats for all the web application that based on databases. Injection of SQL procedure is mainly easier than SQL statement injection because it is based on execution the stored procedure not adding any part of the statements in the stored procedures [29].

h. Wrong Column order Number: if the attacker could inject the SQL statement, then the next step before getting the data would know the number of columns in the original select statement and their order. In order to know the number of columns and their order the attacker may keep trying until not reaching any error message [25].

i. Add extra where column: the attacker may not add union all select statement as already mentioned here. If he can know the structure of the table, then he will add more where condition to the original statement and condition using the and sign '&' in order to filter the data or change the condition [22].

j. Accessing tables and fields names: if the attacker can know the structure of the database, the table names and the names of the fields in each table then he can easily design SQL injection attack. Some DBMSs save the name of the table and columns in its structure files and some are store in the database itself such as the SQL server where all the tables are stored in the table sysobject and all the columns of the tables are stored in the table syscolumns [27, 28].

k. Single record cycling: some web applications such as search tools are already developed to return as many rows as you want. In addition, other web application only returns the records that met your condition. Using the comment '- - ' sign to ignore all the condition fields will return you more than the single record that should return using the condition [25].

l. Dead End: after all these injection techniques the attacker may not affect the web application and get unauthorized data because that the select statement where he run his injection is already a sub statement in another SQL statement. Then the attacker in these situations will get error message after error message without knowing what to do [28].

10. Two recommended phases in order to secure the web application form the SQL injection

10.1. Data Sanitization

All the inputs data that have been read from the customer of the web application should be checked carefully and validate that it is out of any strings or characters or even SQL statements that may affect the database. This validation process should be done at the web application side not only in the SQL statements. Regular expression are the best technique for filtering the input string in order to allow only the kind of character that is allowed for example the following regular expression : s/[^0-9a-zA-Z]//\ allows only the numbers and letters to be entered to the system with any special characters. If you want to allow the clients to enter some symbols you must specify the certain symbols which are allowed and the location in the string same as the '@' in the e-mail address fields. [30].

10.2. Secure SQL Coding for your Web Application

There are also a few directions exact to SQL injection coding. Firstly, validate and verify all the clients input data, even if the data is numeric. Secondly, increase the privileges and permission of the database to limited users. Then do not have the full permission user or the admin user to access all the default stored procedures and system tables. Do not have any removable disk drive on the data base server and install update scanner tool such as anti-viruses tools. Keep the database server updated redundantly and periodically in order to enhance the security level of the server [30, 31].

11. Protection Techniques

11.1. Intrusion Detection System

The Intrusion Detection System (IDS) is used to detect many kinds of attacks behavior that can compromise the security of the web application system. These kinds of attacks that can be detected by the IDS include Worms, Viruses, unauthorized logins, access to sensitive files and folders, increase access privileges [32].

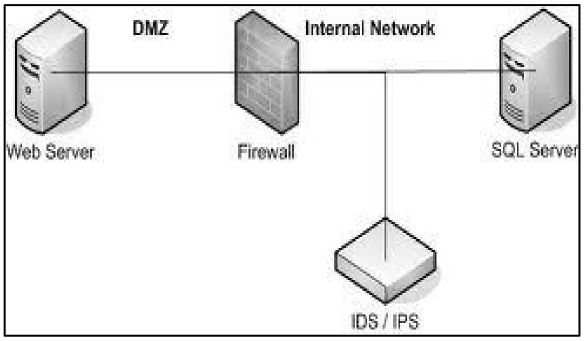


Fig. 6: Intrusion Detection/prevention Systems

11.2. Intrusion Prevention System

Another automated protection tools is called the Intrusion Prevention System (IPS). The IPS is usually a device that monitors the network in order to study the behavior of the authorized user in the network. Therefore, the IPS will prevent unauthorized users from access the web application and the network resources. [33].

11.3. Passwords

The passwords strength of security is depending on the users who create them and the combination of characters, letters and numbers. Generally, the easiest method to access a password of web application defenses is with inside knowledge. The attacker may track someone profile of social web site in order to get information about him to guess his organization web application password [34]. Nowadays, most of the web application that server clients try to show the clients the complexity level of their password when creating their accounts or after that. Other web application also choose a default random password that is very complex and hard to remember from the users themselves, which make them write it down anywhere cause another threat possibility. Password itself cannot be the only protection technique that a company uses.

11.4. SSL and Data Encryption

The Socket Secure Layer (SSL) protocol and data encryption may secure the customer data during the transmission of these data from the web server to the client machine. However, the server and the client system need to decrypt these data once they want to read it or modify it [35]. Data encryption same as password cannot be work alone without other protection technique. Usually this encryption and decryption are based on shared key that both the client and the server need to know. Therefore, distribution of this shared key should be also run through a secure process.

11.5. Firewalls

As shown in Figure 6 the firewall is like a barrier inside the network to allow only the people who have authorized access to pass through this gate. Firewall can be either hardware device or software tool that can be configured to allow and block certain users, packets, ports, or even Internet Addresses (IPs). The attacker may make a huge process in order to convince the firewall that he is an authorized user to pass through it and this is what usually happens in the Trojan horse virus [36]. In the computer networks, a firewall is working with a router. The firewall scans each network packet to decide whether to forward it toward its destination inside my company network or forbidden its pass. A firewall also includes or works with a proxy server that creates network requests on behalf of the users systems. A firewall is often installed in a specially designated computer separate from the rest of the network so that not any arrived packet can get directly at the servers system in the company network.

11.6. Standard Scanning Programs

The known attacks and security threats are stored in automated tools to scan all the programs and packet sent or received on the clients system. Most of these automated scanners protect the organizations network from known attacks made before on hardware devices and software. Most of these scanners secure your systems from fixed list of threats. Therefore, there is no guarantee to protect your applications and systems from new expected kind of attacks that did not happen before. Sometimes they can alert they users that doing some actions or accessing some file will be vulnerable and security risk. Usually these applications require daily update for its libraries in order to update the list of threats to include the new threats that just happen to other computer systems[37].

11.7. Internet Service Provider

Most of the protection techniques is mainly to guarantee securing the systems and data inside an organization. However, what about the internet service providers (ISPs). Most of the ISPs do not care about security same as the application productions companies. Security is not their business. Nevertheless, nowadays most of these third parties start looking for security improvements in order to enhance or keep their reputation in the IT markets [38].

11.8. Code Implementation

Programmers are not security experts that why they do not consider that much the security threats while developing an application. Some huge development companies apply security testing for their applications after the development phase. While the most of these companies only deals with security after their applications face an attack. However, in order to protect your system you should not only test the code but you need to implement all the validation and verification required in the code development phase. In addition, to secure all the servers and databases that is worked in the background of these applications. Tester mainly are not attacker that why he cannot imagine the complete way of attacking the system. Therefore, companies should start looking for hiring attacker in their quality assurance departments [39, 40].

12. Conclusion

Securing all web applications is a great challenge in the computer security research. There many benefits of attacking web applications such critical banking information and credit cards details, which make these web applications always under risk of attacking. There are many internet security techniques to protect the web applications, which have been surveyed in this paper. The attacker methodology of launching the attack and the progression of the executing the attack have also been studied in this paper. This paper also gave special attention to SQL Injection because of the importance of this attacking method in retrieving the data from the DBMS. Worms and Viruses have been also discussed in this paper for their importance.

Acknowledgments

The authors are grateful to the Applied Science Private University, Amman, Jordan, for the financial support granted to cover the publication fee of this research article.

References

[1] Verizon 2010 Data Breach Investigations Report, “http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_enxg.pdf”.

[2] Web Application Security Statistics, “http://projects.webappsec.org/w/page/13246989/webapplicationsecuritystatistics”.

[3] WhiteHat Security, “WhiteHat website security statistic report 2010”.

[4] Peder Jungck, and Simon S.Y. Shim, “Issues in High Speed Internet Security”, Computing Practices published by the IEEE Computer Society, 2004 IEEE.

[5] Butler W. Lampson, “Computer security in the real world”. IEEE Computer 37, 6 (June 2004), pp. 37-46.

[6] T. Chen, J-M. Robert, "Worm epidemics in high-speed networks," IEEE Computer, vol. 37, June 2004, pp. 48-53.

[7] Kevin Spett, “SQL Injection”, Whitepaper, 2002 SPI Dynamic Inc.

[8] Xiaowei Li and Yuan Xue, “A Survey on Web Application Security”, Technical report, Vanderbilt University, 2011.

[9] C. C. Palmer, “Ethical Hacking”, IBM SYSTEMS JOURNAL, VOL 40, NO 3, 2001

[10] Caleb Sima, “Security at Next Level”, Whitepaper, 2004 SPI Dynamic Inc.

[11] Sean-Philip Oriyano, “Anatomy of a Web attack: Understanding the most common attack types”, © Copyright IBM Corporation, 2009

[12] Steve Petite, “ANATOMY OF A WEB APPLICATION: Security Considerations”, White Paper, Sanctum Inc., July, 2001

[13] Feng Zhao, Heqing Huang, Hai Jin, and Qin Zhang, "A hybrid ranking approach to estimate vulnerability for dynamic attacks", Computers & Mathematics with Applications, Volume 62 Issue 12, December 2011, Pages 4308-4321

[14] Rahul Johari and Pankaj Sharma, " A Survey on Web Application Vulnerabilities (SQLIA, XSS) Exploitation, Proceedings of the 2012 International Conference on Communication Systems and Network Technologies Pages 453-458

[15] Jingguo Wang, Nan Xiao, and H. Raghav Rao, "Drivers of information security search behavior: An investigation of network attacks and vulnerability disclosures", ACM Transactions on Management Information Systems (TMIS), Volume 1 Issue 1, December 2010.

[16] David Watson, " Web App Attacks: Web application attacks" Network Security, Volume 2007 Issue 10, October 2007, Pages 10-14.

[17] Tajpour, A, Masrom, M. , Heydari, M.Z. , and Ibrahim, S., "SQL injection detection and prevention tools assessment", Proceeding of 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010, pages 518-522.

[18] Elia I.A., Fonseca J., and Vieira M., " Comparing SQL Injection Detection Tools Using Attack Injection: An Experimental Study", Proceeding of 21st International Symposium on Software Reliability Engineering (ISSRE), 2010 IEEE, pages 289-298.

[19] Tao Li, Zhihong Guan, and Yuanmei Wang, " The stability of a worm propagation model with time delay on homogeneous networks", proceeding of International Conference on Intelligent Control and Information Processing (ICICIP), 2010 IEEE, pages 753-755.

[20] Shijia Gu, Weihai Li, and Zhao Long, " Improved vulnerability testing mode based on syntax analysis and regular expressions test cases generation", proceeding of 3rd International Conference on Broadband Network and Multimedia Technology (IC-BNMT), 2010 IEEE, pages 90-94.

[21] Shahriar H. and Zulkernine M., " Automatic Testing of Program Security Vulnerabilities", proceeding of 33rd International Conference of Computer Software and Applications (COMPSAC), 2009 IEEE, pages 550-555.

[22] Tajpour A., Massrum M., and Heydari M.Z., " Comparison of SQL injection detection and prevention techniques", Proceeding of 2nd International Conference on Education Technology and Computer (ICETC), 2010 IEEE, pages 174-179.

[23] Kindy D.A. and Pathan A.K., " A survey on SQL injection: Vulnerabilities, attacks, and prevention techniques", proceeding of 15th International Symposium on Consumer Electronics (ISCE), 2011 IEEE, pages 468-471.

[24] Tajpour A., and JorJor Zade Shooshtari M., " Evaluation of SQL Injection Detection and Prevention Techniques", proceeding of 2nd International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), 2010 IEEE, pages 216-221.

[25] Yeole A. S. and B. B.," Analysis of different technique for detection of SQL injection", proceeding of the International Conference & Workshop on Emerging Trends in Technology (ICWET), 2011 ACM, Pages 963-966.

[26] Steven Palmer, " Web Application Vulnerabilities: Detect, Exploit, Prevent", Syngress Publishing, 2007, ISBN:1597492094 9781597492096.

[27] Raducanu Razvan, "Over the SQL injection hacking method", Proceedings of the 3rd International Conference on Communications and information technology (CIT), 2009, pages 116-118.

[28] Yakkala V. Naga Manikanta, "Protecting web applications from SQL injection attacks by using framework and database firewall", Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2012 ACM, pages 609-613.

[29] Dejan Sunderic, " Microsoft SQL Server 2005 Stored Procedure Programming in T-SQL & .NET", Osborne/McGraw-Hill Berkeley, CA, USA , 2006 , ISBN:0072262281 9780072262285.

[30] Ali Amiri, "Dare to share: Protecting sensitive knowledge with data sanitization", Journal of Decision Support Systems, Volume 43 Issue 1, February, 2007, Pages 181-191

[31] Mina Askari, Reihaneh Safavi-Naini, and Ken Barker, "An information theoretic privacy and utility measure for data sanitization mechanisms", Proceedings of the second ACM conference on Data and Application Security and Privacy (CODASPY), 2012 ACM, pages 283-294.

[32] Fernando Esponda, "Immune System Inspired Digital Data Representations: Storing all but the valuable data", VDM Verlag Saarbrücken, Germany, 2009, ISBN:3639174534 9783639174533

[33] Phurivit Sangkatsanee and Chalermpol Charnsripinyo, "Practical real-time intrusion detection using machine learning approaches", Journal of Computer Communications, Volume 34 Issue 18, December, 2011, pages 2227-2235.

[34] Beate Grawemeyer and Hilary Johnson, "Using and managing multiple passwords: A week to a view", Journal of Interacting with Computers, Volume 23 Issue 3, May 2011, pages 256-267.

[35] Kyu Ho Park and Ki-Woong Park, "ACCENT: Cognitive cryptography plugged compression for SSL/TLS-based cloud computing services", Journal of ACM Transactions on Internet Technology (TOIT), Volume 11 Issue 2, December 2011, Article No. 7.

[36] Alex X. Liu, "Firewall policy change-impact analysis", Journal of ACM Transactions on Internet Technology (TOIT), Volume 11 Issue 4, March 2012 , Article No. 15.

[37] Marjan Korosec and Joze Duhovnik, "Identification and optimization of key process parameters in noncontact laser scanning for reverse engineering", Journal of Computer-Aided Design , Volume 42 Issue 8, August, 2010 , pages 744-748.

[38] Serguei Netessine and Nils Rudi, "Supply Chain Choice on the Internet", Journal of Management Science, Volume 52 Issue 6, June 2006, pages 844-864.

[39] Lingli Zhang and Chandra Krintz, "The design, implementation, and evaluation of adaptive code unloading for resource-constrained devices", Journal of ACM Transactions on Architecture and Code Optimization (TACO), Volume 2 Issue 2, June 2005, pages 131-164.

[40] Mu-Woong Lee, and Sunghun Kim, "Integrating code search into the development session", Proceedings of the 27th International Conference on Data Engineering, 2011 IEEE, pages 1336-1339.

Dr. Hesham Abusaimeh received his B.Sc. degree from Applied Science University, Amman, Jordan in 2003, and M.Sc. degree from New York Institute of Technology in 2004, both in computer His Ph.D. degree in computer science in the field of wireless sensor networks communication and routing protocols from Loughborough University, UK in 2009. His research interests include Network and Controls, Routing Protocols, Network Lifetime and Consumption Energy, wireless sensor networks, and web applications security.

Dr. Mohammad Shkoukani received his B.Sc. degree from Applied Science University, Amman, Jordan in 2002, M.Sc. and PHD degrees from The Arab Academy for Banking and Financial Sciences, Amman, Jordan, in 2004, and 2009 respectively, all in Computer Information Systems. His research interests include Agent Oriented Software Engineering, System Analysis and Design, and Electronic Commerce Applications.