Security Vulnerabilities in Web Application - An Attack Perspective.

S.Mirdula[1], D.Manivannan[2]
School of Computing, SASTRA University, Tirumalaisamudram,
Thanjavur, Tamilnadu, India -613401
1mirdu90@gmail.com
2dmv@cse.sastra.edu

Abstract:

Security is the essential and important topic in web applications. The choice of communication made the web technology a essential one in the environment. The importance of web application and its security increasing day by day, but traditional networks fails to provide security for web application. This paper discuss about some of the vulnerable online attacks commonly occurs in web applications and providing solution for preventing such attacks by using penetration tool BACKTRACK. The testing aspect of vulnerabilities is carried out for SQL injection. The various methodologies are also discussed.

Keywords: Web application, Attacks, Backtrack, SQL injection.

I. Introduction:

Web Security plays very essential role in day to day web application. Lack of security leads to major destructive causes in the society. There are two categories of web security namely web browser security and web application security [1]. Web browser security doesn't leads to major problem comparing to web application security. Web browser security is needed when the attacker attacked the web site. For example botnets, key logging, document theft, loss of data etc. web application security is more vulnerable than web site security, it leads to potential bugs, stolen credit cards, defaced site and also like SQL injection, cross cite scripting and Cross Site Request Forgery CSRF [2]. Web application interacts with the valuable and sensitive data. Attackers violate the web application worstly; this is mainly due to "improper validation of input variables". Web application is a complex task due to participating of multiple protocols and platforms. Web server can be accessed by web services, wireless devices and also browser can access the Server. The reason for the risk in web security is no proper deployment of security services along with the web application. In web application vulnerabilities occurs in platform, administration and in application. In platform, known vulnerabilities like script kidders get accessed. Vulnerability in the sense weakness of the system leads to the violation of system integrity, confidentiality, consistency, audit mechanism etc. To exploit the vulnerability, it must access security of an application through "auditing code" and "behaviour" of the security problems. There are two approaches one is negative approach which is vulnerability based and other one is positive approach which is behaviour based. Vulnerability based approach can be explained with Back track. In administration level, a quite riskier assessments like path truncation, backup checking, forceful browsing etc will occur. It leads to increased awareness and awareness should be in security flaws in content and configuration. In application level cookie manipulation, brute force, reverse directory traversal, buffer flow, SQL injection and Cross site scripting will occur [3]. Coding techniques used doesn't properly validate and hence in appropriate file calls reveals source code. Fig 1explains the types of work carried out in three levels.

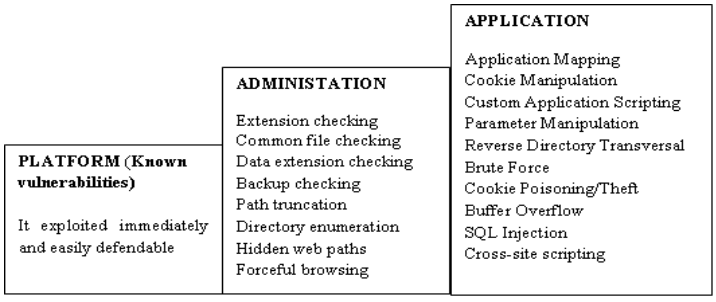

Fig1 Web Services

II. Related Works:

Security vulnerabilities carried out in two categories they are protocol stack and Web application technology.(Online attacks)

Protocol stack: In general attacks occurred in protocol stack are not attempt to serious tasks. It can be easily revealed using selected functionalities. It can be carried out in three layers such as network layer, transport layer and application layer. These are some of the attacks which occur in the protocol stack, they are less harmful and hence they are not taken into consideration. Fig 2 explains about attacks occur in protocol stack.

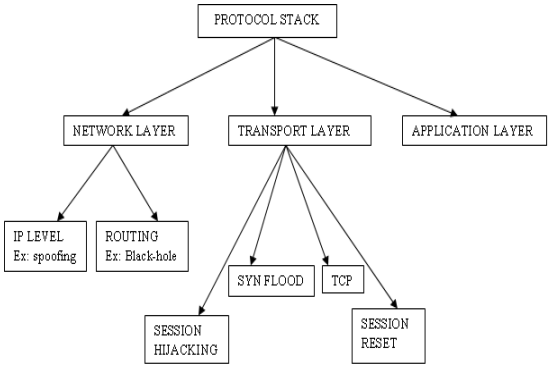

Fig 2 Attacks occur in protocol stack

Online Attacks: There are numerous online attacks which affect the web security, among them some of the attacks are categorized and preventive measures are analyzed using a penetration tool. Attacks taken for consideration are Denial of service & Distributed Denial of service, SQL injection technique, Cross site Technique, phishing & pharming, and finally IP Spoofing [4]. This paper aims to explain the vulnerabilities due to these attacks and the remedial measures to be taken to prevent those attacks.

III. Online Attacks

A. Denial of service attacks:

Denial of service makes use of service un accessible to the user and it aims at distracting the authorized user of the system application. Overloading of server or the network leads to the denial of service attacks. It is a malicious attempt by a single person or group of the people to cause the node to repudiate service to the customers. The idea behind the Denial of service attack is the modification of data, vandalism, and closing the site permanently. The direct impact of this attack is on the services and obstructing the communication between the user and the system. In simple denial of service, a single host attack the victim site by creating enormous amount of traffic and hence there will be no access of services to the users. PING OF DEATH is one of the finest example for DOS attack, in which disrupting the service by continuously pinging the spoofed request. Types of DOS attacks are Classical DOS, flooding, Penetration, and Eaves dropping. Figs 3 discuss about the DOS attack types.

Ping of death is the example of classical DOS, as described above it disrupts the service by continuous pinging of request. TCP and ICMP packets are example for flooding in which, continuous sending of TCP request block the system and hence server get hacked.

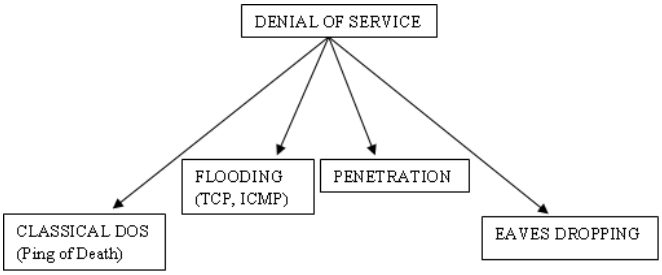

Fig 3 DOS Types

Eaves dropping or network sniffing listens to the packet transmitted from other network in order to hack the secret passwords. This denial of service is similar to transport layer in protocol stack and hence it can be easily prevented. Remedial measures to be taken for preventing this attack is “BACK SCATTER ANALYSIS”. This qualifies the prevalence of denial of service attacks. [5]

*B. DDOS (Distributed Denial of service***)**

It employs multiple attackers to attack the host. It installs malicious backdoor programs to create the botnets. Example of DDOS is Triple Flood Network (TFN). Zombies is nothing the group of backdoor programs, it can be of Handler zombies and agents zombies. The handler zombies carried out the malicious code from attacker and transfer to agent zombies, in which agent zombies attack the target system. The remedial measure to prevent DDOS is “SLASH DOT EFFECT”.[6]

C. Phishing & Pharming

Phishing is highly effective vulnerable attack, used to acquire the sensitive information like bank accounts, credit card details, username, and passwords details by masquerading through mails as well as phishing web sites. Phishing website is nothing but the fake site, which resembles similar to the original websites with minute changes in advertisements and logo, which is just misplaced. “Deception” is the major reason for hacking the personal information. Pharming aims to redirect the web site traffic to another website; it is used with the Phishing to steal the identity information. A preventive measure of this is “Anti-pharming measures”.

D. IP Spoofing

IP Spoofing is another vulnerable attack, in which attacker send forged IP address to the victim site, it resembles as the request from the trusted host , so the victim accept the request and the system gets blocked. In this technique, hacker uses two sets of IP, one is the IP address used within the range and other one is from the authorised external IP address. Basic concepts of IP Spoofing are explained with the following Fig 4

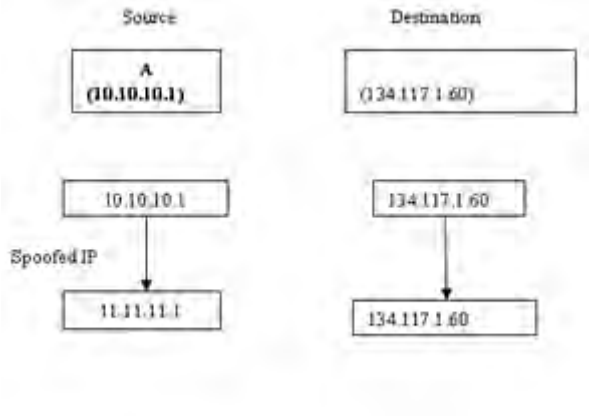

Fig 4 IP Spoofing

In this example, ‘A’ refers to the source with the IP address of 10.10.10.1 and destination is the Shelton website, its IP address is 134.117.1.60. Attacker by knowing the trusted IP address spoof the original source IP address to Spoofed Hacking address and sent to the destination so, the website is hacked by the hacker. There are two types of IP spoofing, one is Non-binding spoofing and other one is Binding Spoofing.

E. Non-binding Spoofing

In this method, hacker attacks the website if the target machine and the subnet is similar configuration. If the target and subnet is similar, then sequence and acknowledgement are in same phase. Victim is waiting for the data receiving from partner, during this the unknown hacker (sender) send the data packets with spoofed IP address and so the victim site gets blocked. Fig 5 shows the overview of Non-binding spoofing.

F. Binding Spoofing

In this method, attackers send numerous packets to target machine, in order to violate the victim site. Due to this sequence number and acknowledgment are un reachable. Victim site get confused that from which sender its getting data packet, since it doesn’t send any request to any of the partner. Fig 6 shows the overview of binding spoofing.

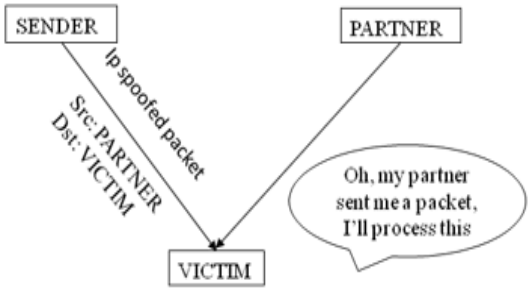

Fig 5 Non-binding Spoofing

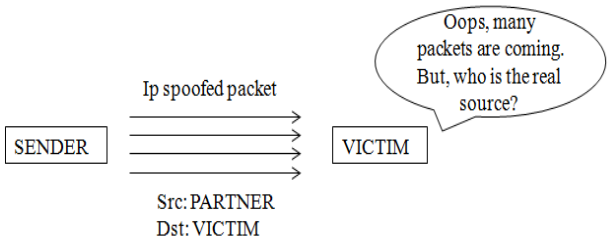

Fig 6 Binding spoofing.

G. SQL Injection

This technique makes use of code to exploit the vulnerability in the database. It adds or removes the content in the site but doesn't waste the resource utilities accessing of database by using SQL commands. This is due to improper validation of input data or incorrect filtering of input data. Blind SQL is one of the type of SQL, in which attacker cant able to visit the results. This can be preventing by proper input validation with SQL query commands [7].

H. Cross cite scripting

This is similar to SQL injection but it executes java scripts. Attacker makes use of malicious java script to hack the client side. Scripting execute the commands in the HTML page. It causes web page modification, steal access credentials etc. Fig 7 explains how the cross site scripting occurs. Initially attackers sends malicious code, server stored the message. Users request the server the server for the data, server responds to the user, and user execute the script, the malicious code attack the client. Client access gets denied [8].

Back track is a penetration tool used to exploit vulnerabilities of harmful online attacks. It provides assessments tools and vulnerability tests for preventing the attacks. It has 12 categories of tools used to detect attacks.

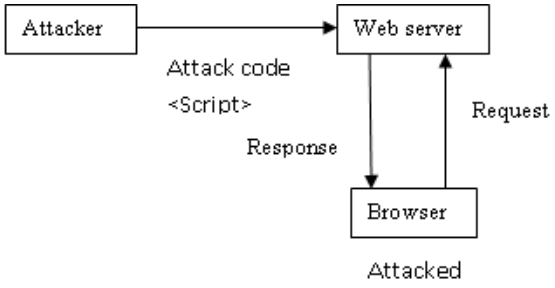

Fig 7 Cross cite scripting

IV. Backtrack

The general methods of performing the tests are gathering the information, vulnerability assessments, target accessing and maintenance, and finally track clearance. The steps given below are to explain how to prevent the SQL injection by using Backtrack.

Procedure for carrying SQL injection using Backtrack

The code shows how the SQL injection attacks can be detected using Backtrack with the help of web exploitation tools. With the help of SQL map, this can be carried out. Initially clear the existing procedures applied in the penetration tool by opening the terminal window, type **root@root:/pentest/web/scanners/sqlmap# clear**.

root@bt: ~# cd/pentest/webscanners/sqlmap

root@bt:/pentest/web scanners/sqlmap#sqlmap.py.u http://junicc.com.ar/noticia.php?id=1

After clearing the pre-existing procedures have to select the corresponding URL. Open new word file using **gedit** for saving the database contents. While executing that, will get the database information in the terminal window, copy and paste the DBS name and DB'S in that word file. From the database copy the "junincc junincc". Now open the terminal

root@bt:/pentest/web/scanners/sqlmap#python sqlmap.py.U http:// junincc.com.ar/noticia/php?id=1 junincc junincc".

Tables and columns displayed in the terminal window, copy the last table name Usuarios. In the first line initialize table name as **T Usuarios.** Open the terminal window, column is displayed in that. In that column and table login id and password displayed.

Idusuario, Usuarios, and clave- column name. Open the terminal window, to use the dictionary attack.

Data is displayed in the terminal window…**Clave** is the password and uses MD5 cracking.

Fig 8 Selecting SQL map in Backtrack

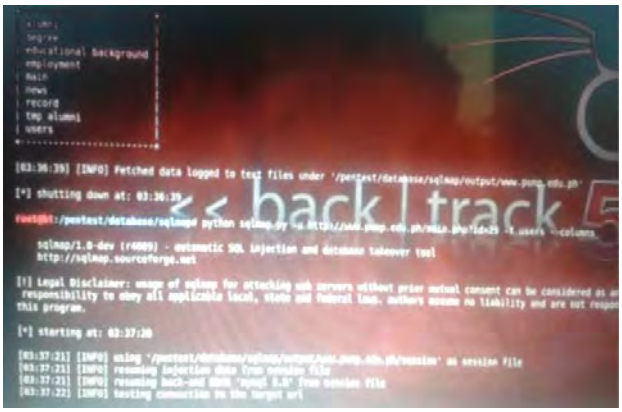

Fig 9 Database Creation using backtrack

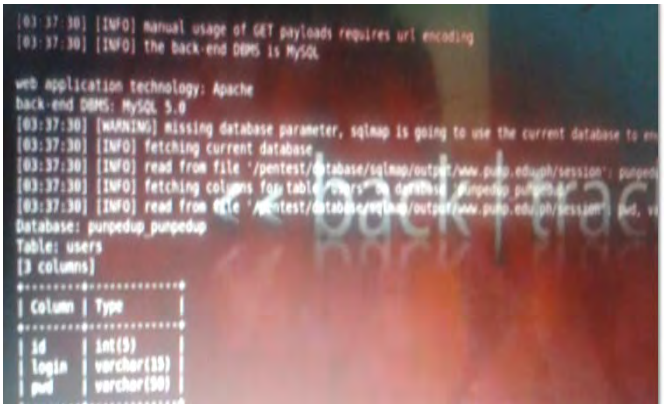

Fig 10 Getting Login id & password

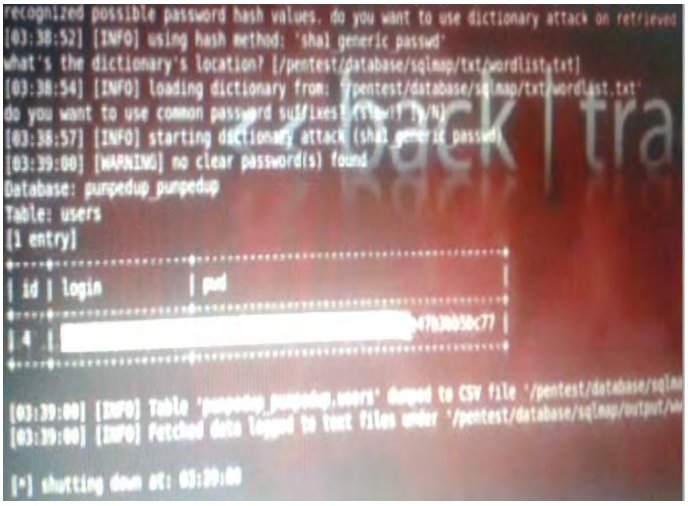

Fig 11 Login id & password displayed in Table & column

V. Conclusion:

In this paper, some of the vulnerable online attacks of web servers and its preventive measures are discussed. Since the traditional networks are failed to provide security to web application, Linux based penetration tool with back search algorithm is provided in order to prevent the attacks. SQL injection is taken in to consideration and processed using backtracks. Similarly all kind of vulnerable attacks can be prevented using this penetration tool.

V References

[1] D. Balzarotti, M. Cova, V. Felmetsger, et.al.,Composing static and dynamic analysis to validate sanitization in web applications. In IEESymposium on Security and Privacy, 2008.

[2] A. Barth, C. Jackson, and J. Mitchell. Robust A. Barth, C. Jackson, and J. Mitchell.” Robust defenses for cross-site request forgery”. In proceedings of ACM CCS '08, 2008.

[3] S. Fogie, J. Grossman, R. Hansen, A. Rager, and P. Petkov. XSS Exploits: Cross Site Scripting Attacks and Defense. Syngress, 200.7.

[4] Gilgor, V. A note on the Denial-of-Service Problem. Proceedings of Symposium on Security and Privacy (SP'83), Oakland, CA, USA, ,. IEEE Computer Society, Washington, DC, USA., pp. 139-149,1983.

[5] Furuya, F., Matsuzaki, T., and Matsuura, K. Detection of unknown DoS attacks by Kolmogorov-complexity °uctuation. Lecture Notes in Computer Science, pp 3822, 395-406, (2005)

[6] Li, L. and Lee, G. DDoS attack detection and wavelets. Telecommunication Systems, pp 435-451.,(2005

[7] Yaashuwanth .C, Dr. R. Ramesh,” Attacks in WEB Based Embedded Applications”, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 6, November 2010

[8] Jayamsakthi Shanmugam1, Dr. M. Ponnavaikko2,” Cross Site Scripting-Latest developments and solutions: A survey”, Int. J. Open Problems Compt. Math., Vol. 1, No. 2, September 2008