International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 4, Issue 08, August-2018

STUDY OF VARIOUS ATTACKS AND TOOLS FOR WEB APPLICATIONS SECURITY

Neha Bhateja, Dr. Sunil Sikka

Amity School of Engineering & Technology
Amity University Haryana, Gurgaon (India)

Abstract: In today's era of hyper connected world, Web applications provide us a convenient way to access information. Major business and commercial transactions are now performed via these web applications. To name a few areas, web applications are used in Banking, Retail, Healthcare, Automobile, Education etc domains. Securing the user data and transactions on these web applications becomes the utmost important goal for any organization. The applications are becoming more complex as the user demand is increasing for more functionality. This has resulted in possible security flaws being exposed to potential hackers. The attacks are being carried out in multiple layers of the web applications including client side and server side and vary from SQL Injection to XSS, DOS etc. In order to avoid any data theft or modification, additional measures are required to detect and prevent any breach to the web applications security. This paper presents the various kinds of attacks possible on a web application and the tools available to handle such attacks. Every tool has its own capabilities and set of limitations. The paper discusses about the attacks in detail and maps each tool with the features it provides.

Keywords: Web Applications, Security, SQL Injection, Cross-site Scripting.

Introduction

Now a day's, users are highly dependent on the internet to access the information related to them. The information that is stored over the internet on the web servers can be access through the web applications. A web application is program or say an interface between the users and the web servers. All the large organizations, whether it's a business related, commercial or an education, provides the online facility to their users with these web applications. users can use them to communicate with others, sharing the information, doing inline shopping, online transactions, bill payments, all these tasks are performed on these web applications[1,2,4].
The information accessed by the users are stored on the database on the server side. the users can send a request to the web servers to get the information and if they are authorized then server can respond to the users.

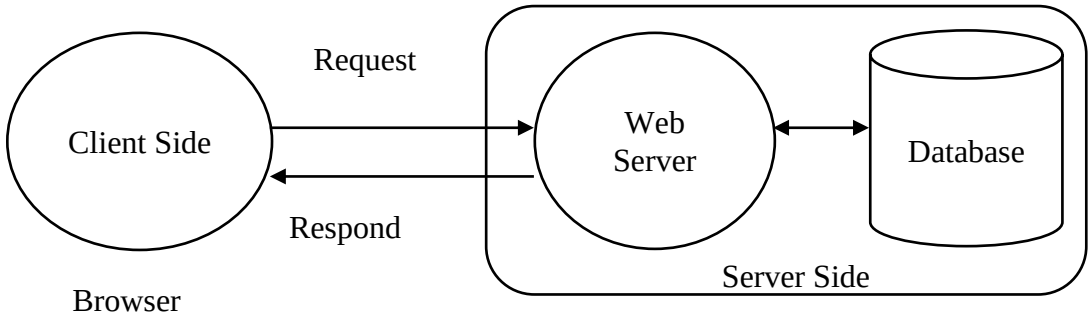

Fig1: Web Application

The useful information pass to the end users from the database by the web applications. the security concerns are also related to the applications. if these applications are not secure or if the security features are not implemented well while designing the web applications, then malicious users can theft the data or information from the database. The attackers can attack the database by various ways.

Types of Attack
Various types of attacks are performed on the web applications[4,5]:

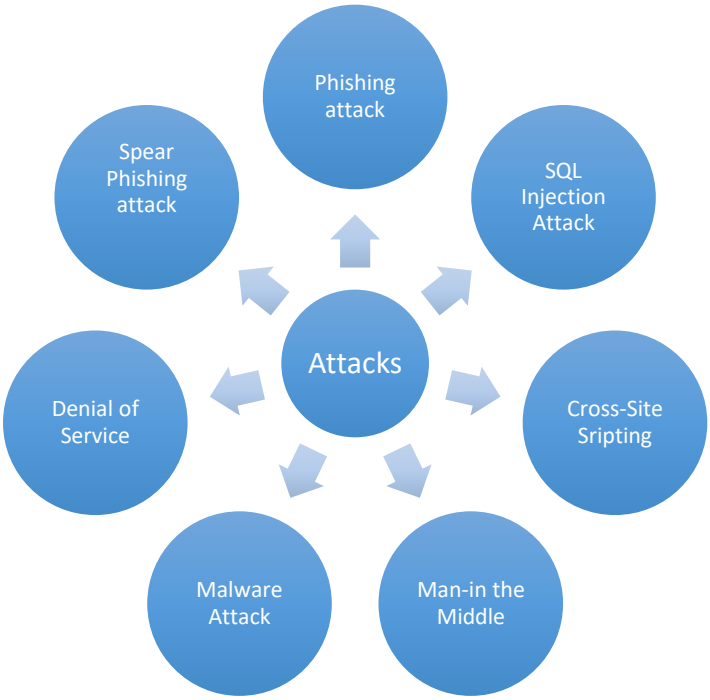

Fig 1: types of web application attack

S.No.	Name of the Attack	Description
1	Phishing Attack	Phishing is an act to obtain confidential information through internet users. This is mostly done through emails, voice scams, text messages. The attacker uses this technique to acquire the personal information of the victim such as name, location, login credentials, bank account information and many other useful details. Phishers can use social websites to track the information like Facebook, Instagram, Linkedln. For example, a person is sending an email to the official id of Amazon, but in return he receives reply from an unauthorized mail id and also from Amazon, so here the fake email is done using Phishing technique.
2	SQL Injection Attack	SQL stands for Structural Query Language. It is a programming language which is used to deal with the database for creation, inserting or updating the data. The attacker can inject the malicious code in the queries by reconstruct the queries (SELECT, CREATE, INSERT, UPDATE) and get the authorized access to fetch the data from the database. SQL injection attack can be performed by many methods like Tautologies attack, union attack, Boolean-based SQL injection, Time-Based SQL injection.
3	Cross-Site Scripting Attack	This type of attack is performed at the client side. The malicious users attack the target scripts that are embedded in a web page by injecting the malicious scripts in form of code or links. XSS attack is performed to access the useful information of the user that is retained by the browser and access the cookies also. Types of XSS attack are as follow: 1. Reflected XSS 2. Stored XSS 3. DOM (Document Object Model) XSS
4	Man-in the Middle Attack	In Man-in-the-middle attack, malicious user enters into communication process which is going between the two users to get the access to that information which is transferred by them to each other. This type of attack performs on the communication that goes online like web surfing, email etc. Time when MITM attacks can happen: - 1. Between login and authentication on financial websites. 2. Networks which are supposed to be secured by keys (public or private). Data gathered from an attack can be used for things like unapproved fund transfers, identity theft or a change in password. MITM attack avoidance: - 1. Do not use wifi networks which are not password protected. 2. By logging out of secure websites when they are not in use.

5	Malware Attack	Malware is the short form of malicious code which defines various different harmful software. There are various ways to perform the malware attack on the web sites like worms, virus, Trojan horse, Adware, Spyware. Once the malware attack injected into the web applications, the attacker can gain the unauthorized access to steal the information, change the system configuration, disturbing the communication process, and hijack's the system.
6	Denial of Service Attack	In DoS, the aim of the attacker is to prevent the users to use the services provides by the web sites or unavailable the services to the users. Denial of service attack is performed by two ways: first, by sending the excessive requests to the server to increase the traffic over the network (Flooding). Flood attack includes: 1. ICMP Flood (also known as PING Flood) 2. SYN Flood and second, execute the code that leads to crash the system.
7	Cross-Site Request Forgery	Cross-Site-Request-Forgery(CSRF) is known as sea-surf, session riding or XSRF. It is an attack where an attacker forces the user to execute the malicious code on an authorized web application, where the user is currently login. The attackers can perform this attack with aim to stolen the session cookies, information theft, change passwords.

Web Application Firewalls

The web application firewalls are used to detect and prevent the web applications from various attacks. The following table represents a list of application firewall (Open source and commercial both) [7,8,9].

S. No.	Name of Tool	Feature
1	Iron Bee	Denial of Service (DoS), SQL Injection, CSS, Cookie Attack
2	AQTRONIX (Web Knight)	SQL Injection, Denial of Service (DoS)
3	Guardian @ Jumper Z.NET	SQL Injection, Cross-Site Scripting
4	FortiWeb	SQL Injection, Cross- Site Scripting, Cross-Site Request Forgery
5	ModSecurity	SQL Injection, Cross- Site Scripting, Command injection
6	BinarySec	SQL Injection, Cross-Site Scripting, Buffer Overflow
7	Shadow Daemon	SQL Injection, Cross-Site Scripting, Command Injection
8	Citrix	Denial of Service (DoS), SQL Injection, Cross- Site Scripting
9	Barracuda	Denial of Service (DoS), SQL Injection, Cross- Site Scripting
10	Imperva Secure Sphere	SQL Injection, Cross- Site Scripting, Cross-Site Request Forgery
11	Web Castellum	SQL Injection, Cross-Site Scripting, Command Injection

Conclusion:

To conclude, we have reviewed multiple types of attacks possible on a web application and mapped them against the tools that provide for their detection and prevention. There is no single tool which provides a protection layer against all the different possible attacks. Every tool has its own set of capabilities. In order to be shielded against any possible attack, it is better to use a combination of tools which provide security at different layers of the web application. Some are best suited for firewalls, some for client side and others for server side. Securing web application is never enough as the hackers are also adding to their capabilities to create and deploy new forms of attacks.

Reference:

[1] Hesham Abusaimeh and Mohammad Shkoukani. Survey of Web Application and Internet Security Threats", International journal of computer science and network security, Volume.12, No.12,December – 2012.

[2] Nadya EIBachir EI Moussaid and Ahmed Toumanari. "Web Application Detection: A Survey and Classification. International Journal of Computer Applications", Volume 103 – No.12, October – 2014.

[3] Yousra Faisal Gad Mahgoup Elhakeem , Bazara I. A. Barry," Developing a Security Model to Protect Websites from Cross-site Scripting Attacks Using Zend Framework Application", International Conference on Computing, Electrical and Electronics Engineering (ICCEEE), August 2013, PP. 624-629

[4] Research On SQL Injection Attack And Prevention Technology",Authors: Li Qian, Jun Lu, 2015 International Conference on Estimation, Detection and Information Fusion(ICEDIF-2015)

[5] Gopal R. Chaudhary and Prof. Madhav V. Vaidya. "A Survey on Security and Vulnerabilities of Web Application". International Journal of Computer Science and Information Technology, Volume 5(2), 2014.

[6] Imran Yusof, Al-Sakib Khan Pathan, 2014. Preventing Cross Site Scripting Attack By Applying Pattern Filtering Approach. IEEE 5 th International Conference on Information and Communication Technology for The Muslim World (ICT4M), pp: 1-6.
[7] MichaelMeike , Johannes Sametinger and Andreas Wiesauer, "Security in Open Source Web Content Management Systems", Journal IEEE Security and Privacy archive Volume 7 Issue 4, July 2009.
[8] Open source web application firewall.
https://geekflare.com/open-source-web-application-firewall/
[9] Open Web Application Security Project. http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project