ISSN:0975-9646

Web Security and Classification of Different Types of Attack for Web

Shubham Srivastava

Faculty of Computer Science & Engineering, ITM GIDA,
Gorakhpur, UP, INDIA

Abstract: **The web is a vast and powerful attack surface that attackers can leverage to accomplish their goals of data and financial theft .The use of web application has become increasingly popular in our daily life as reading news paper, making online payments for shopping etc. At the same time there is an increase in number of attacks that target them. This paper presents a detailed review on various types of attacks and their classification regarding Web security. In this paper I am presenting a classification of attacks which must be deal for web security.**

Keywords: **Web Security, SQL Injection, Cross-Site Scripting (XSS), Remote File Inclusion (RFI), Phishing, Click jacking**

1-INTRODUCTION

Web security is an interesting topic. Ineffective Web security leads to all of the things that make us hate the Web: spam, viruses, identity theft, etc.

The web is a vast and powerful attack surface that attackers can leverage to accomplish their goals of data and financial theft. The use of web application has become popular day by day in our daily life as reading news paper, making online payments for shopping etc. At the same time there is an increase in number of attacks that target them given as below-

SQL injection attacks are possible because web application code is not secured during application development. SQL injection is a hacking method that is based on the security vulnerabilities of web application.

It is categorized as one of the top-10 2010 Web application vulnerabilities experienced by Web applications according to OWASP (Open Web Application Security Project).

Cross-site scripting is probably the biggest and most common problem. With it, an attacker injects JavaScript code into our document by adding it to the end of the URI as a parameter or in a form field.

Cross-site scripting (XSS) is a type of computer insecurity vulnerability typically found in Web applications that enables attackers to inject client-side script into Web pages viewed by other users.

Remote File Inclusion (RFI) is a type of vulnerability most often found on websites. It allows an attacker to include a remote file, usually through a script on the web server. The vulnerability occurs due to the use of user-supplied input without proper validation.

Phishing is a way of attempting to acquire information (and sometimes, indirectly, money) such as user names, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

Clickjacking is a terribly clever way to use CSS and inline frames to trick users into clicking something without knowing it.

2.0 CLASSIFICATION OF ATTACKS FOR WEB

Different Types of Attacks related to web are listed as below:-

- SQL Injection
- Cross-Site Scripting (XSS)
- Remote File Inclusion (RFI)
- Phishing
- Click jacking

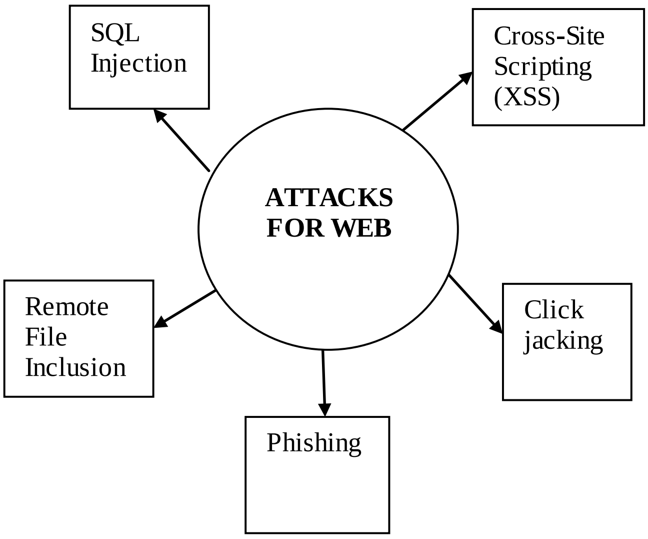

Fig.1 Web attacks

2.1 MEANING & IMPACT OF SQL INJECTION

There are some malicious codes that can be attached to the SQL called SQL Injection. SQL Injection is one of the many web attack mechanisms used by hackers to steal data from organizations. It is perhaps one of the most common application layer attack techniques used today. It is the type of attack that takes advantage of improper coding of our web applications.

In essence, SQL Injection arises because the fields available for user input allow SQL statements to pass through and query the database directly.SQL Injection is the hacking technique which attempts to pass SQL commands (statements) through a web application for execution by the backend database. If not sanitized properly, web applications may result in SQL Injection attacks that allow hackers to view information from the database. Once an attacker realize that a system is vulnerable to SQL injection, he is able to inject SQL query or commands through an input form field.

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of our database and/or expose sensitive information. Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker.

Type of SQL injection attacks :

- Stored procedure
- Piggybacking
- Tautology
- Union
- Logically incorrect query attacks

Table 1- Summary of SQLIA's

Sno.	Type of Attack	Description
1	Stored procedure	Stored procedures are stored on the server side, they are available to all clients. Once the stored procedure is modified, all clients automatically get the new version.
2	Piggybacking	In this attack type, an attacker tries to inject additional queries along with the original query, which are said to "piggy-back" onto the original query.
3	Tautology	The basic goal of this attack is to inject code into one or more conditional statements so that they always evaluate to true.
4	Union	Using this technique, an attacker can trick the application into returning data from a table different from the one that was intended by the developer.
5	Logically incorrect query attacks	This type of attack lets an attacker gather important information about the type and structure of the back-end database in a Web application.

2.2 CROSS-SITE SCRIPTING (XSS)

A cross-site scripting vulnerability may be used by attackers to bypass access controls. It is the biggest and most common problem. With it, an attacker injects JavaScript code into our document by adding it in a form field. Cross-site scripting (XSS) is a type of computer insecurity vulnerability typically found in Web applications that enables attackers to inject client-side script into Web pages viewed by other users. Cross-site scripting carried out on websites accounted for roughly 80.5% of all security vulnerabilities.

Once we have successfully injected JavaScript, we will be able to do following things-

- Read out cookies
- Open forms that ask the user to enter their passwords or credit card details
- Execute viruses, worms etc.

The reason is that JavaScript is not bound by any security model. This is a big security problem with JavaScript.

XSS is a very common problem. It can be classified as below-

- Non-persistent (or Reflected)
- Persistent
- Traditional (caused by server-side code flaws)
- DOM-based (in client-side code)

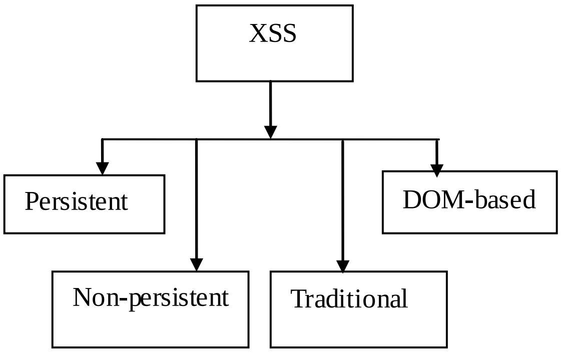

Fig. 2 Classification of cross site scripting

A reflected attack is typically delivered via email. If the trusted site is vulnerable to the XSS vector, clicking the link can cause the victim's browser to execute the injected script.

The persistent (or stored) XSS vulnerability is a more devastating variant of a cross-site scripting flaw: it occurs when the data provided by the attacker is saved by the server, and then permanently displayed on "normal" pages returned to other users in the course of regular browsing, without proper HTML escaping.

Traditionally, cross-site scripting vulnerabilities would occur in server-side code responsible for preparing the HTML response to be served to the user.

DOM-based vulnerabilities occur in the content processing stages performed by the client, typically in client-side JavaScript. The name refers to the standard model for representing HTML or XML contents which is called the Document Object Model (DOM).

2.3 REMOTE FILE INCLUSION (RFI)

Remote File Inclusion (RFI) is an attack that targets the computer servers that run Web sites and their applications.

In RFI an attacker uses a flaw in our website to inject code from another server to run on ours. It is in the same family as XSS but much more problematic. Remote File Inclusion (RFI) is a type of vulnerability most often found on websites. It allows an attacker to include a remote file, usually through a script on the web server. Remote File Inclusion (RFI) is caused by insufficient validation of user input provided as parameters to a Web application. Parameters that are vulnerable to RFI enable an attacker to include code from a remotely hosted file in a script executed on the application’s server.

2.4 PHISHING

Phishing is a way of attempting to acquire information (and sometimes, indirectly, money) such as user names, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

Phishing is the technique of fooling people into entering information into a bad website. We show end users an interface that looks legit (for a bank or what we have) but that in reality sends their information to our database.

The trick with phishing is to make the form really look like it comes from a website we trust.

Types of Phishing Attacks:

Different types of phishing attacks have now been identified. Some of them are listed below-

Deceptive Phishing- The term "phishing" originally referred to account theft using instant messaging but the most common broadcast method today is a deceptive email message. Messages about the need to verify account information, system failure requiring users to re-enter their information, fictitious account charges, undesirable account changes, new free services requiring quick action, and many other scams are broadcast to a wide group of recipients with the hope that they will respond by clicking a link to or signing onto a bogus site where their confidential information can be collected.

Malware-Based Phishing refers to scams that involve running malicious software on users' PCs. Malware can be introduced as an email attachment, as a downloadable file from a web site, or by exploiting known security vulnerabilities- a particular issue for small and medium businesses who are not always able to keep their software applications up to date.

Keyloggers and Screenloggers are particular varieties of malware that track keyboard input and send relevant information to the hacker via the Internet. They can embed themselves into users' browsers as small utility programs known as helper objects that run automatically when the browser is started as well as into system files as device drivers or screen monitors.

Session Hijacking- It describes an attack where users activities are monitored until they sign in to a target account or transaction and establish their bonafide credentials. At that point the malicious software takes over and can undertake unauthorized actions, such as transferring funds, without the user's knowledge.

Web Trojans pop up invisibly when users are attempting to log in. They collect the user's credentials locally and transmit them to the phisher.

Hosts File Poisoning- When a user types a URL to visit a website it must first be translated into an IP address before it's transmitted over the Internet. The majority of users PCs running a Microsoft Windows operating system first look up these "host names" in their "hosts" file before undertaking a Domain Name System (DNS) lookup. By "poisoning" the hosts file, hackers have a bogus address transmitted, taking the user unwittingly to a fake "look alike" website where their information can be stolen.

System Reconfiguration Attacks modify settings on a user's PC for malicious purposes. For example: URLs in a favorites file might be modified to direct users to look alike websites. For example: a bank website URL may be changed from "bankofabc.com" to "bancofabc.com".

Data Theft- Unsecured PCs often contain subsets of sensitive information stored elsewhere on secured servers. Certainly PCs are used to access such servers and can be more easily compromised. Data theft is a widely used approach to business espionage. By stealing communications, design documents, legal opinions, employee related records, etc., thieves profit from selling to competitors.

DNS-Based Phishing - Pharming is the term given to hosts file modification or Domain Name System (DNS)-based phishing. With a pharming scheme, hackers tamper with a company's hosts files or domain name system so that requests for URLs or name service return a bogus address and subsequent communications are directed to a fake site. The result is that users are unaware that the website where they are entering confidential information is controlled by hackers and is probably not even in the same country as the legitimate website.

Content-Injection Phishing describes the situation where hackers replace part of the content of a legitimate site with false content designed to mislead the user into giving up their confidential information to the hacker.

Man-in-the-Middle Phishing is harder to detect than many other forms of phishing. In these attacks hackers position themselves between the user and the legitimate website or system. They record the information being entered but continue to pass it on so that user's transactions are not affected. Later they can sell or use the information or credentials collected when the user is not active on the system.

Search Engine Phishing occurs when phishers create websites with attractive offers and have them indexed legitimately with search engines. Users find the sites in the normal course of searching for products or services and are fooled into giving up their information. For example, scammers have set up false banking sites offering lower credit costs or better interest rates than other banks.

Table2- Summary of various "Phishing attacks"

SNO.	TYPE	DESCRIPTION
1	Deceptive Phishing	Most common broadcast method today is a deceptive email message. Messages about the need to verify account information, system failure requiring users to re-enter their information etc.
2	Malware-Based	It refers to scams that involve running malicious software on users' PCs.
3	Session Hijacking	It describes an attack where users activities are monitored until they sign in to a target account
4	Hosts File Poisoning	When a user types a URL to visit a website it must first be translated into an IP address before it's transmitted over the Internet. By poisoning the hosts file, hackers have a bogus address transmitted, taking the user unwittingly to a fake "look alike" website where their information can be stolen.
5	Content-Injection	This type of phishing describes the situation where hackers replace part of the content of a legitimate site with false content designed to mislead the user into giving up their confidential information to the hacker.
6	Man-in-the-Middle	In these attacks hackers position themselves between the user and the legitimate website

2.5 CLICKJACKING

Clickjacking also known as a "UI redress attack". It occurs when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the the top level page. It is a terribly clever way to use CSS and inline frames to trick users into clicking something without knowing it. **e.g.** The victim tries to click on the button x but instead actually clicked on the invisible button y. In essence, the attacker has hijacked the user's click, hence the name 'Clickjacking'. By using clickjacking an attacker can create a circumstance where the victim is subversively giving access to the attacker.

3.CONCLUSION

It is obvious from above description that web attacks are one of the largest class of security problems. In this paper we have reviewed the most popular existing classes of web attacks related issues. This paper presents a brief description of various types of web attacks and their classification. Figure and tables support the document, which make the concept more clear.

ACKNOWLEDGMENT

I am feeling so glad to express my sincere thanks to my Parents, colleagues and all those persons who helped me directly and indirectly to complete this paper.

REFERENCES

[1] Indrani Balasundaram, E.Ramaraj "An Authentication Scheme for Preventing SQL Injection Attack Using Hybrid Encryption PSQLIA-HBE"(ISSN 1450-216X Vol.53 No.3 (2011),pp.359-368)

[2] William G.J.Halfond and Alessandro Orso "AMNESIA:Analysis and Monitoring for Neutralizing SQL-Injection Attacks"

[3] M.Mutuprasanna, Ke Wei,, Suuraj Kothari' Eliminating SQL Injection Attacks - A Transparent Defense Mechanism

[4] William G.J.Halfond ,Jeremy Viegas, Alessandro Orso "AClassification of SQL injection Attacks And Countermeasures"

[5] Shaukat Ali, Azhar Rauf, Huma Javed "SQLIPA:An authentication mechanism Against SQL Injection"

[6] K. Amirtahmasebi, S. R. Jalalinia, S. Khadem, "A survey of SQLinjection defense mechanisms," Proc. Of ICITST 2009, vol., no., pp.1-8, 9-12 Nov. 2009

[7] Shubham srivastava,"A Survey On: Attacks due to SQL injection and their prevention method for web application" (IJCSIT) Vol. 3 (1) , 2012, 3225-3228

[8] http://searchsecurity.techtarget.com/definition/phishing

[9] http://www.microsoft.com/security/online privacy/phishing-symptoms.aspx

[10] https://www.owasp.org/index.php/Clickjacking

[11] http://en.wikipedia.org/wiki/Clickjacking

[12] https://www.owasp.org/index.php/Cross- site_Scripting_(XSS)

[13] http://en.wikipedia.org/wiki/Cross-site_scripting

[14] http://www.imperva.com/resources/glossary/ remote_file_inclusion.html

Shubham Srivastava is currently working as a Lecturer of (Computer Science & Engineering) at Institute of technology and management, GIDA, Gorakhpur. He received his **B.Tech.** (Computer Science and Engineering) degree from ITM, GIDA,Gorakhpur, Uttar Pradesh Technical University, Lucknow (U.P.), INDIA, in 2005. And Completed his **M.Tech.(CSE)** from Teerthankar Mahaveer University, Moradabad, UP, INDIA in 2010-2011 Batch. He has research interest in the area of data & network security

.