**Branch :- Computer Sci. & Engg. Class :- Final Year**

**Subject :-System and Software Security Lab manual Sem :- VII**

**Teacher Manual**

**PRACTICAL NO 02**

**Practical no. 2**

**AIM:-** Illustrate different types of vulnerabilities for hacking a websites / Web Applications.

**THEORY:-**

# Reasons for Attacking Web Applications

Currently there are many privacy risks in web applications. Today too many websites are hacked by anonymous. They target website because of different types of reasons. They are mentioned in table 1.

|  |  |
| --- | --- |
| **Attack Goal** | **%** |
| Stealing Sensitive Information | 42% |
| Defacement | 23% |
| Planning Malware | 15% |
| Unknown | 08% |
| Deceit | 03% |
| Blackmail | 03% |
| Link Spam | 03% |
| Worm | 01% |
| Phishing | 01% |
| Information Warfare | 01% |

# Table 1: Reasons for Attacks

**Web Application Vulnerability**

There are several different types of attacks used by hackers. These types of attacks and its usage are mentioned in following Table 2.

|  |  |
| --- | --- |
| **Attack/Vulnerability Used** | **% of use** |
| SQL Injection | 20 % |
| Unintentional Information Disclosure | 17 % |
| Known Vulnerability | 15 % |
| Cross Site Scripting (XSS) | 12 % |
| Insufficient Access Control | 10 % |
| Credential/Session Prediction | 08 % |
| OS Commanding | 03 % |
| Security Misconfiguration | 03 % |
| Insufficient Ant automation | 03 % |
| Denial Of Service | 03 % |
| Redirection | 02 % |
| Insufficient Session Expiration | 02 % |
| Cross Site Request Forgery(CSRF) | 02 % |

# Table 2: Types of Attacks

This all are the Vulnerability types and how much it’s usage. The SQL Injection and Cross Site Scripting are the most famous vulnerabilities in web application. Generally web servers, application servers, and web application environment are affected to following types of vulnerabilities. The OWASP (Open Web Application Security Project) listed all security vulnerability at

.There are two types of attacks which are frequently used by hackers namely SQL Injection attack and XSS (Cross Site Scripting) Attack. The following are the brief explanation of each type of attack.

# SQL Injection Attack

Injection means tricking an application into including unintended commands in the data sent to an interpreter. Here what interpreters do? They take strings and interpret them as command. (SQL, OS Shell, XPath, LDAP etc.) Any web application which accepts the user input as a basis of performing database query may be vulnerable to SQL Injection. It uses loopholes in the web application that interact with database. In this attacker exploits input vulnerability and attempt to send incorrect command or SQL query to the web application. These queries can fraud the interpreter to display unauthorized data to hacker. By this attack hacker can Read the important information related to user (user name, password, email) from database. Access admin account and perform all the operation which is done by only admin. Hacker can also modify data by passing query. He run operating systems command on database server. There are also some parts in SQL Injection;

* + - * Union Based SQL Injection
      * String Based SQL Injection
      * Error Based SQL Injection

# Cross Site Scripting (XSS)

XSS is also one of the danger attacks. In this attack hacker simply inject script in WebPages. These pages are returned to client and malicious code will be executed in the browser of client with alert popup. And by simply responding the web application hacks. (Ex. Attacker sets the trap – update my profile then victim views page – see Attacker profile and script silently sends attacker victim’s session cookie). Hacker can Access cookies, session tokens, do remote code execution and get sensitive data. We can classify XSS into two classes’ server XSS and client XSS. There are three types of XSS;

* + - * Stored XSS
      * Reflected XSS
      * Dom based XSS

Stored XSS also known as persistent XSS .This occurs when hacker stored malicious script permanently in target server like database, visitor log, and comment field or in URL. Reflected XSS occur when hacker insert inject script into some input field.

# Broken Authentication / Session Management

This attack also like bypass authentication. Authentication is method utilized by web application to verify that whether the user is authorize or not. Valid user’s password and username stored in to database. This is a most frequent system for web application. Various actions can break the authentication no matter its strong. If the user authentication system of website is weak then Hacker can take full advantage he can change the password, modify account information, and get sensitive information.

# Cross site request forgery (CSRF)

This attack also like a XSS but there is one difference that is here attacker create forged http request (e.g. Update account, login – logout, purchase process) and forced victim in to submitting malicious action via image tags, XSS, or other techniques. In which he is authenticated such as submitting http request through alert box or with other techniques. If the user is authenticated the attack succeeds. By this attack attacker can steal all the information or get the password or username.

# Insecure Direct Object References

When developer expose references to initial implementation object like file, dictionary, database key. Without access control check or other protection attacker can manipulate these references to access an authorized data hacker who is unauthorized simply changes a parameter value that directly refers to the system object to another object the user isn’t authorized for .

# Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server and platform. In these types of attack hacker accesses default accounts, unused pages, un-patched flaws, unprotected files and dictionaries to gain unauthorized access or for the knowledge of the system.

# Sensitive Data Exposure

Many applications do not properly protect important information like credit card; tax ID’s, authentication Ids. Hacker may steal or change such weekly protected data to conduct credit card fraud, id theft or other crimes. Hacker generally does not break cryptography. They break something else such as steal keys, do man in middle attacks or steal clear text data of the server while transit or from user’s browser.

# Using Components with Known Vulnerability

Components like frameworks or software module always run with full privileges. If vulnerable component exploited then attack can facilitate important data loss. In this hacker search a weak component by scanning. He customizes the exploit as need and executes the attack.

# Invalidated Redirects and Forwards

Generally web application redirects users to another page or website and use un-trusted data to consider designation pages without proper validation. Hacker can redirect victim to phishing site. Hacker links to redirect and forced victim to click. Since the link is to a valid site. Attacker targets unsafe forward to bypass authentication.

# Missing Function Level Access Control

Mostly web applications verify function level rights before making that visible in the UI. Application need to perform the same access control checks on the server when each function is accessed. If request are not verified hacker, it will be able to forge requests in order to access functionality without proper authorization. Hacker who is authorized user simply changes the URL or a parameter to privileged system. He can also access private functions that aren’t protected.

**CONCLUSION:-** In this way, we have illustrated different types of vulnerabilities for hacking a websites / Web Applications.