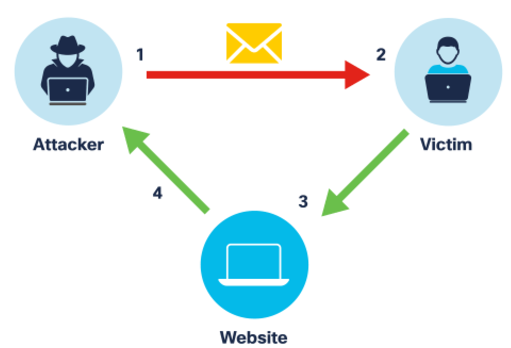
Application attacks

Cross-site scripting (XSS)



Common vulnerability found in many web applications

This is how it works:

1. Attacker exploits XSS by **injecting scripts containing   
    malicious code into web page**
2. The **web page is accessed by the victim, and the   
    malicious script unknowingly pass to their browser**
3. The **script can access** any **cookies, session tokens or other   
    sensitive info** about the user, **and is send back to cb**
4. Armed with this info, **the cb can impersonate the user**

Code injection

**Most modern websites use a database [SQL,XML…] to store and manage data.**

***Injection attacks seek to exploit weaknesses in these databases***.

XML injection attack

**Can corrupt the data and threaten the security of website.**

It works by **interfering with an application’s processing of XML data or query entered by a user**

*Cb can manipulate this query by programming it to suit their needs*. This will grant them access to all of the sensitive info stored on the database and allows them to make any number of changes to the website

SQL injection attack

**Cb insert a malicious SQL statement in an entry field**

This attack takes advantage of a **vulnerability in which the application does not correctly filter the data entered by a user** for characters in an SQL statement

As a result, the *cb can gain unauthorized access to information stored on the* *database*, from which they can spoof an identity, modify existing data, destroy data or even ***become an administrator*** of the database server itself.

DLL injection attack  
 a Dynamic link library (DLL) file is a **library that contains a set of code and data for carrying out a particular activity in Windows**. Applications use this type of file **to add functionality that is not built-in,** when they need to carry out this activity.

DLL injection **allows a cb to trick an application into calling a malicious DLL file, which executes as part of the target process**.

LDAP injection attack

The Lightweight Directory access protocol (LDAP) is an **open protocol for authenticating user access to directory services**.

An LDAP injection attack **exploits input validation vulnerabilities by injecting and executing queries to LDAP servers**, giving cb an opportunity to extract sensitive info from an organization’s LDAP directory.

Buffer overflow

**Buffer = memory areas allocated to an application**

**A buffer overflow = occurs when data is written beyond the limits of a buffer.**

By **changing data beyond the boundaries of a buffer, the application can access memory allocated to other processes.**

**This can lead to a system crash or data compromise, or provide escalation of privileges.**

These memory flaws can **also give attackers complete control over a target’s device**. For example, an attacker can change the instructions of a vulnerable application while the program is loading in memory and, as a result, can install malware and access the internal  
 network from the infected device.

Remote code executions

It allows a cb to **take advantage of application vulnerabilities to execute any command with the privileges of the user running the application on the target device**.

**Privilege escalation exploits a bug, design flaw or misconfiguration in an OS or software application to gain access to resources that are normally restricted.**

Metasploit project

Is a *computer security project that provides info about security vulnerabilities and aids in*  *penetration testing.*

Among the tools they have developed is the metasploit framework, which can be used for developing and executing exploit code against a remote target.

Meterpreter

Is a **payload within metasploit that allows users to take control of a target’s device by writing their own extension and uploading these files into a running process on the device**. **These files are loaded and executed from memory**, so they never involve the hard drive. ***This means that such files fly under the radar of antivirus detection.***

It also has a module for controling a remote sys. Webcam. Once meterpreter is installed on a target device, the metasploit user can view and capture images from the targets webcam.

Other application attacks

Evety piece of info that an attacker receives about a targeted sys or application can be used as a valuable weapon for launching a dangerous attack

Cross-site request forgery (CSRF)

Race condition attack

Improper input handling attack

Error handling attack

Application programming interface (API) attack

Replay attack

Directory traversal attack

Resource exhaustion attacks