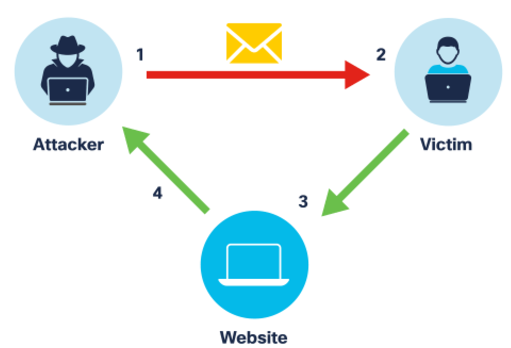
Application attacks

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)

It describes the **malicious exploit of a website where unauthorized commands are submitted from a user’s browser to a trusted web application**.

A malicious website can transmit such commands through specially-crafted image tags, hidden forms or JS requests - all of which can work without the user’s knowledge.

Race condition attack

Also known as a **time of check (TOC) or a time of use (TOU) attack**, a race condition attack happens when a computing **OS that is designed to handle tasks in a specific sequence is forced to perform two or more operations simultaneously.**

Ex. When two or more threads access shared data and try to change it at the exact same time, a race condition attack occurs

Improper input handling attack

**Data inputted by a user that is not properly validated can affect the data flow of a program and cause critical vulnerabilities in OS and applications** **that results in buffer overflow or SQL injection attacks**

Error handling attack

**Attackers can use error msges to extract specific info** such as the hostname of internal sys and directories or files that exist on a given web server - as well as database, table and field names that can be used to craft SQL injection attacks

Application programming interface (API) attack

An **API delivers a user response to a sys and sends the sys’s response back to the user**.

**An API attack occurs when a cybercriminal abuses an API endpoint**.

Replay attack

This describes a situation where a **valid data transmission is maliciously or fraudulently repeated or delayed by an attacker**, **who intercepts, amends and resubmits the data to get the receiver to do whatever they want.**

Directory traversal attack

Directory traversal **occurs when an attacker is able to read files on the web-server outside of the directory of the website.**

An **attacker can then use this info to download server config files** containing sensitive info, potentially expose more server vulnerabilities or even take control of the server

Resource exhaustion attacks

These attacks are **computer security exploits that crash, hang or otherwise interfere with a targeted program or system**.

Rather than overwhelming network bandwidth like a DoS attack, **resource exhaustion attacks overwhelm the hardware resources available on the target’s server instead.**

Spam

Also known as junk mail, is simply unsolicited mail. **In most cases, it is a method of advertising**. **However, a lot of spam is sent in bulk by computers infected by viruses or worms and often contains malicious links, malware or deceptive content that aims to trick recipients** into disclosing sensitive info, such as a social security number or band account info.

**Almost all email providers filter spam, but it still consumes bandwidth**. **And even if you have security features implemented, some spam might still get through to you**. Look out for the following indicators of spam:

- the email has no subject line

- it asks you to update your account details

- its text contains misspelled words or strange punctualtion

- links within it are long and/or cryptic

- it looks like correspondence from a legitimate business, but there are tiny differences - or it contains info that does not seem relevant to you

- it asks you to open an attachment, often urgently

Phishing

Its a form of fraudulent activity often used to steal personal info.

Phishing

It occurs when a **user is contacted** by email or instant msg or other way - **by smo masquerading as a legitimate person or organization**. **The intent is to trick the recipient into installing malware on their device or into sharing personal info**, such as login credentials or financial info.

Ex. U receive an email congratulating you for winning a prize. It looks like it was sent from a well-known retail store and asks you to click on a link to claim your prize. The link may redirect you to a fake site that asks you to enter your personal details, or it may even install a virus

Spear phishing

A highly targeted attack, spear phishing **sends customized emails to a specific person based on info the attacker knows about them** - which could be their interests, preferences, activities and work projects.

Ex. Cybercriminal discovers through their research that you are looking to buy a specific model of car. He then joins a car discussion forum you are a member of, forges a car sale offering and sends you an email that contains a link to see pictures of the car. When you click on the link, you unknowingly install malware on your device

Vishing, pharming and whaling

Criminals make use of a wide range of techniques to try to gain access to your personal info.

Vishing

Often referred to as voice phishing, **this type of attack sees criminals use voice communication technology to encourage users to divulge info, such as their credit card details.**

**Criminals can spoof phone calls using voice over internet protocol (VoIP), or leave recorded messages to give the impression that they are legitimate callers.**

Pharming

**This type of attack deliberately misdirects users to a fake version of an official website.**

Tricked into believing that they are connected to a legitimate site, users enter their credentials into the fraudulent website.

Whaling

Whaling is a **phishing attack that targets high profile individual**s, such as senior executives within an organization, politicians and celebrities.

Defending against email and browser attacks

There are many actions that you can take to defend against email and browser attacks. Some are:

- most internet service providers (ISPs) filter spam before it reaches the user’s inbox.   
 - many antivirus and email software programs automatically detect and remove dangerous spam from an email invox.

- organizations should educate employees about the dangers of unsolicited emails and make them aware of the dangers

- never assume that email attachments are sage, even when they come from a trusted contact.

- join APWG

More

Physical attacks

Physical attacks are intentional, offensive actions used to destroy, expose, alter, disable, steal or gain unauthorized access to an organization’s infrastructure or hardware.

Adversarial artificial intelligence attacks

Machine learning is a method of automation that allows device to carry out analysis and perform tasks without specifically being programmed to do so.

It powers many of the applications we use today, such as web searching, photo tagging, spam detection, video surveillance, fraud detection and security automation

This uses mathematical models to predict outcomes. But depend on data. If the data is tainted, it can have a negative impact on the predicted outcome

Supply chain attacks

Many organizations interface with a third party for their systems management or to purchase components and software. Organizations may even rely on parts or components from a foreign source.

Attackers often find ways to intercept these supply chains.

Cloud-based attacks

Rather than developing systems on their own premises, more and more organizations are making the move toward cloud-based computing, as we discussed earlier in this module.

The advantage is that the cloud provider will maintain the equipment but this also opens up an organization to a host of potentiial threats.