Network Security

Class 10

Lab 30

UNITED TRUST

bdeducation
Bangladesh Digital Education Research Limited
সময়ের পাঠশালা

Lab Objectives:

- Wireless Hijacking
- DDOS Attack
- Cross Site Scripting Attack
- SQL Injection Attack
- Pen Testing

wireless network

A wireless network is a set of two or more devices connected with each other via radio waves within a limited space range.

Wireless networks are widely used and it is quite easy to set them up. They use

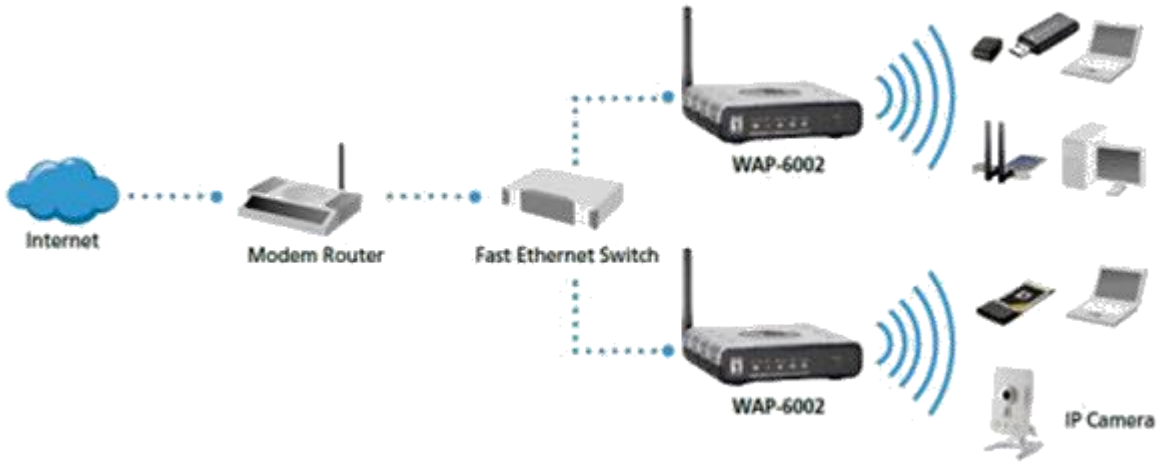
https://en.wikipedia.org/wiki/IEEE_802.11

standards.

A wireless router is the most important device in a wireless network that connects the users with the Internet.

A Wireless Router

In a wireless network, we have Access Points which are extensions of wireless ranges that behave as logical switches.



Although wireless networks offer great flexibility, they have their security problems. A hacker can sniff the network packets without having to be in the same building where the network is located. Most attackers use network sniffing to find the SSID and hack a wireless network.

Wireless Hacking Tools

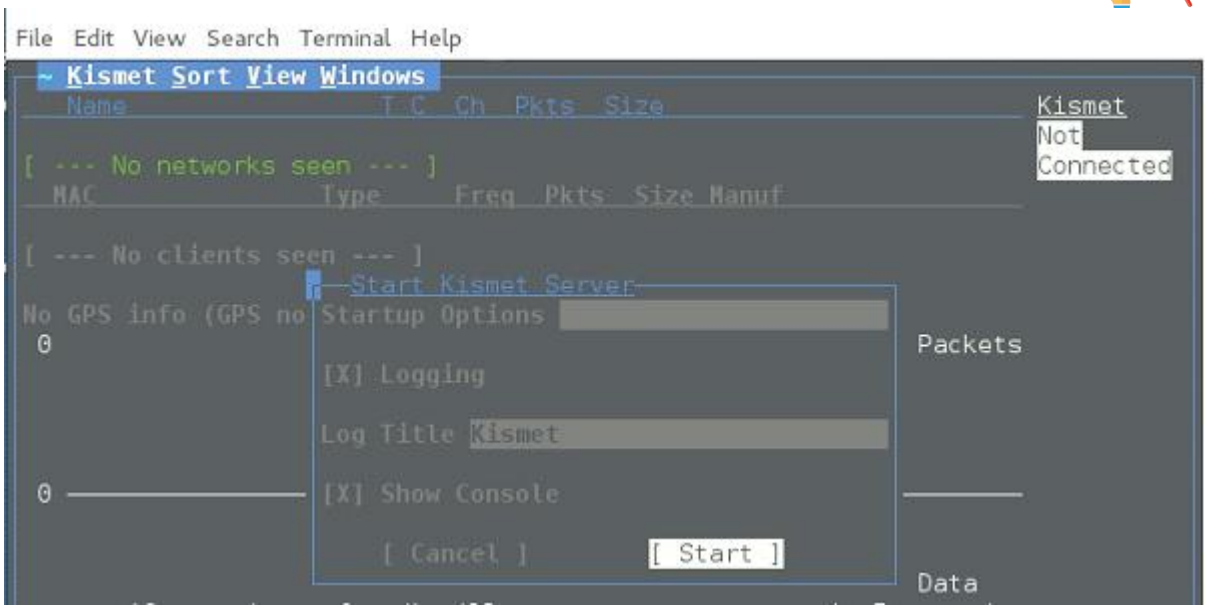
Kismet

Kismet is a powerful tool for wireless sniffing that is found in Kali distribution. It can also be downloaded from its official webpage

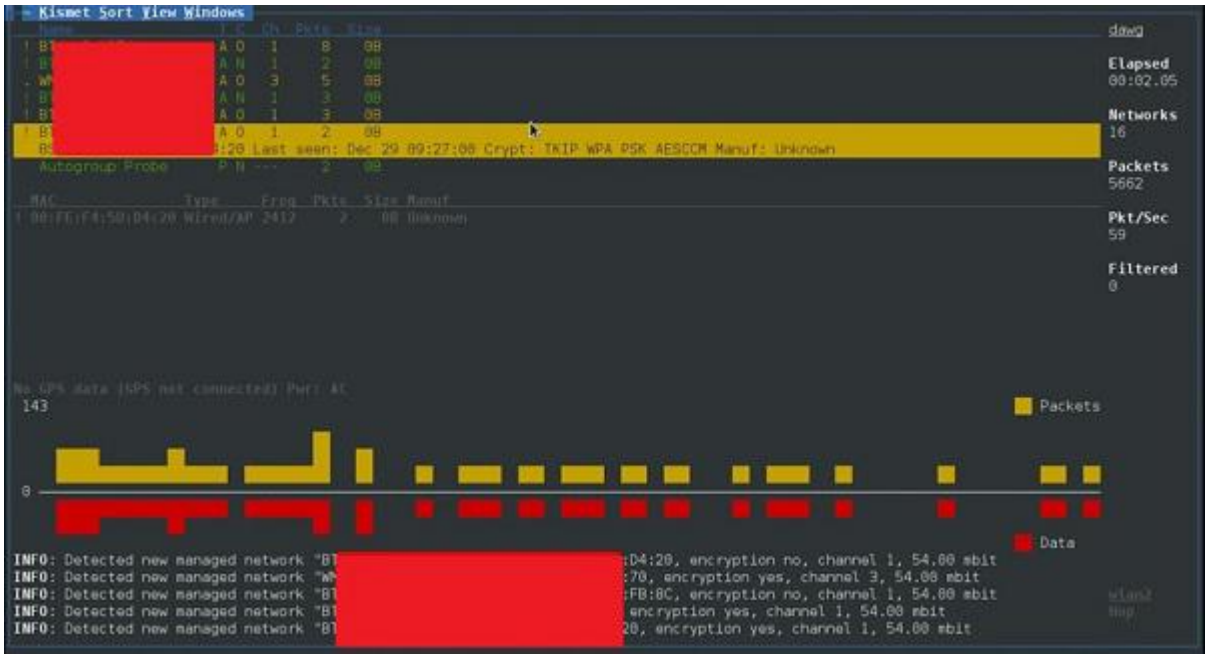
– https://www.kismetwireless.net/index.shtml

Let's see how it works. First of all, open a terminal and type kismet. Start the Kismet Server and click Yes, as shown in the following screenshot.

As shown here, click the Start button.



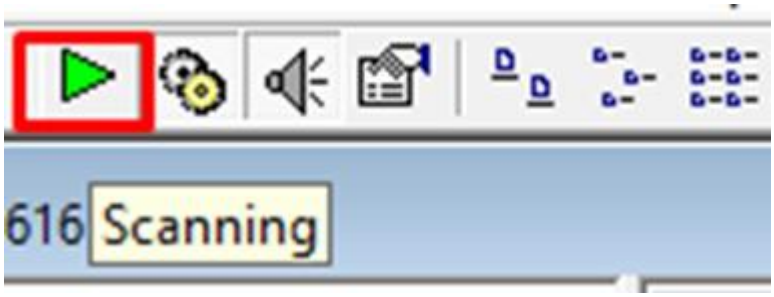
Now, Kismet will start to capture data. The following screenshot shows how it would appear –



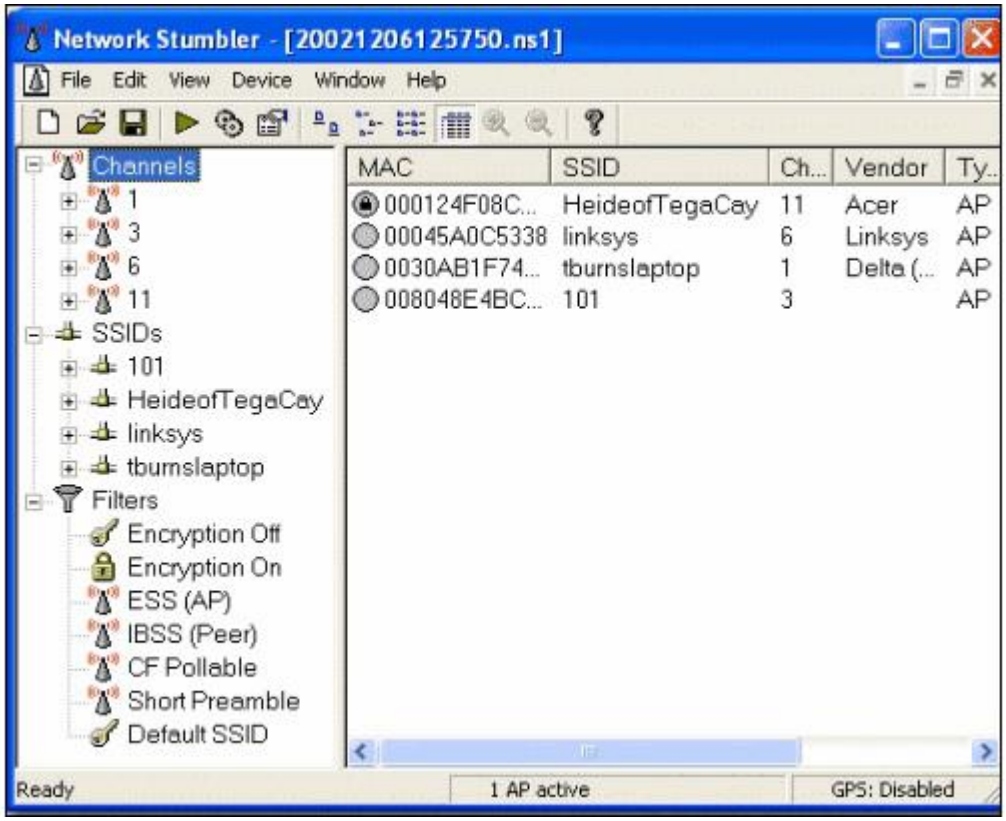
NetStumbler

NetStumbler is another tool for wireless hacking that is primarily meant for Windows systems. It can be downloaded from http://www.stumbler.net/

It is quite easy to use NetStumbler on your system. You just have to click the Scanning button and wait for the result, as shown in the following screenshot.



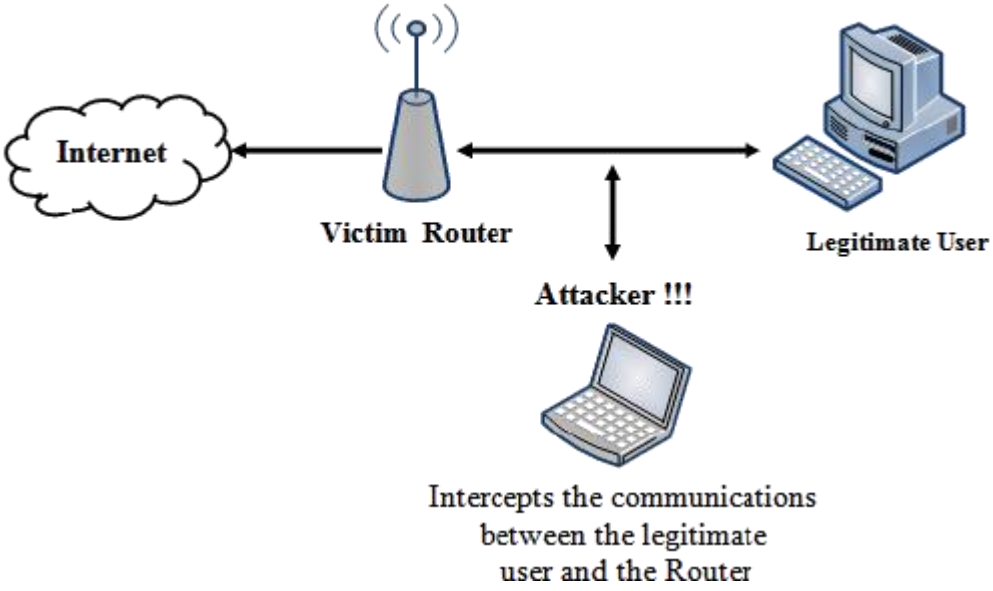
It should display a screenshot as follows −



It is important to note that your card should support monitoring mode, otherwise you will fail to monitor.

Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is a security protocol that was invented to secure wireless networks and keep them private. It utilizes encryption at the data link layer which forbids unauthorized access to the network.



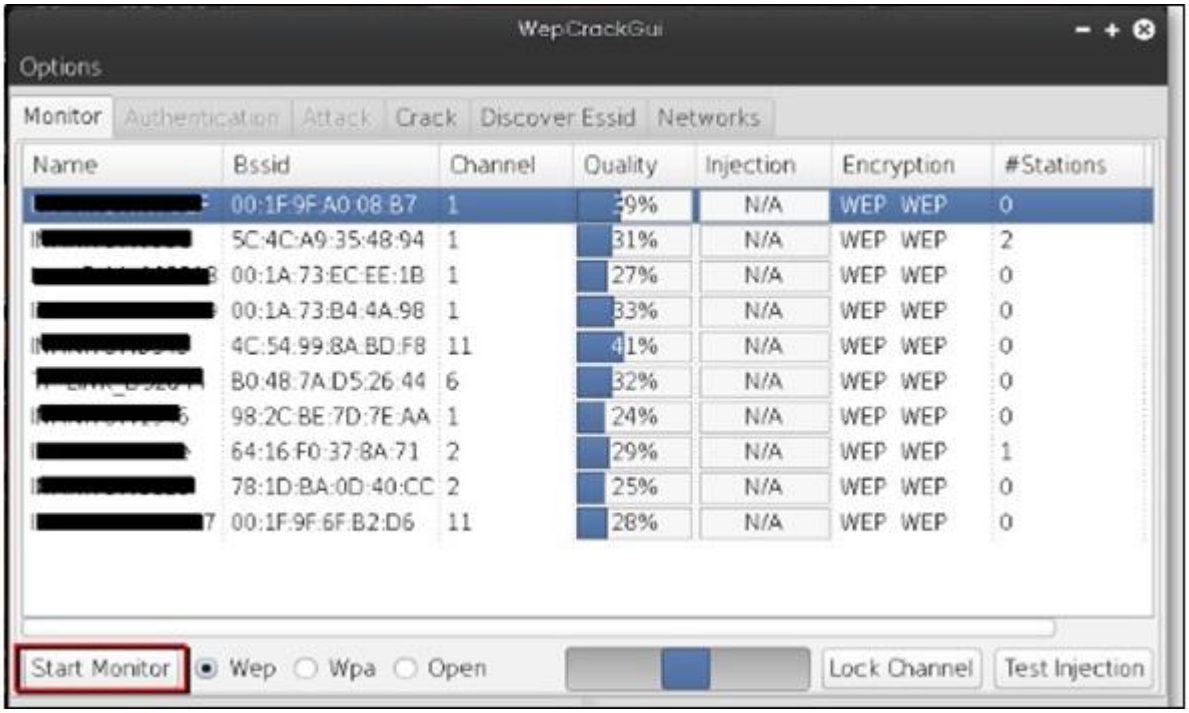
Note that WEP is not entirely immune to security problems. It suffers from the following issues −

√ It is vulnerable to dictionary attacks.

√ WEP is vulnerable to Denial of Services attacks too.

WEPcrack

WEPcrack is a popular tool to crack WEP passwords. It can be downloaded from – https://sourceforge.net/projects/wepcrack/

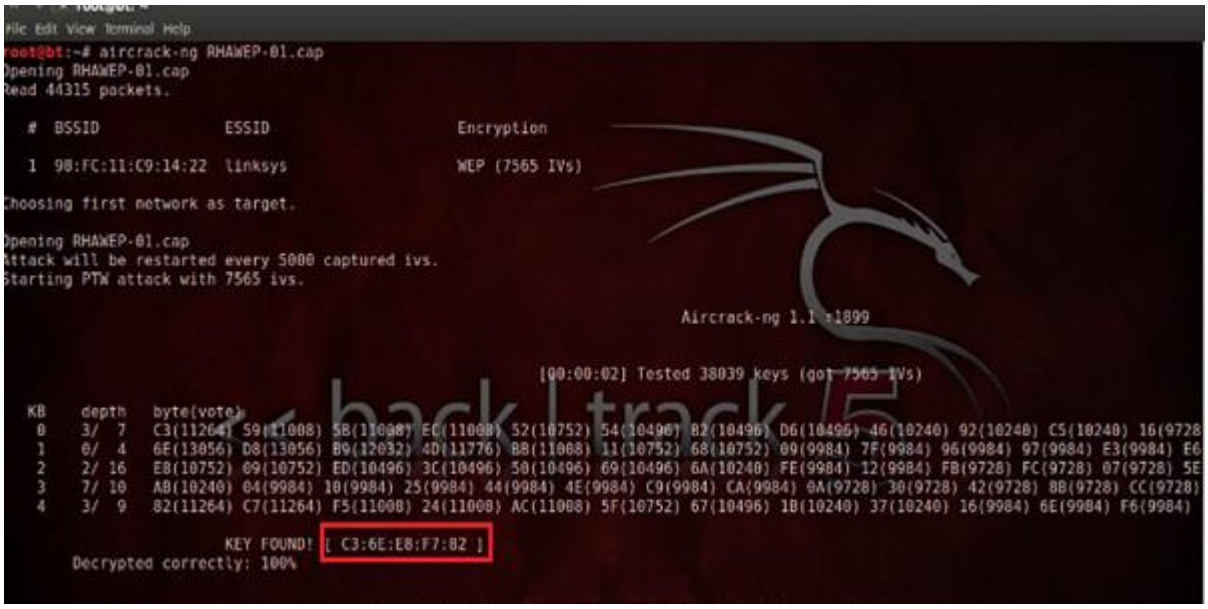


Aircrack-ng

Aircrak-ng is another popular tool for cracking WEP passwords. It can be found in the Kali distribution of Linux.

The following screenshot shows how we have sniffed a wireless network and collected packets and created a file RHAWEP-01.cap.

Then we run it with aircrack-ng to decrypt the cypher.



Wireless DoS Attacks

In a wireless environment, an attacker can attack a network from a distance and therefore, it is sometimes difficult to collect evidences against the attacker.

The first type of DoS is Physical Attack. This type of attack is very basic and it is in the base of radio interferences which can be created even from cordless phones that operate in 2.4 GHz range.

Another type is Network DoS Attack. As the Wireless Access Point creates a shared medium, it offers the possibility to flood the traffic of this medium toward the AP which will make its processing more slow toward the clients that attempt to connect. Such attacks can be created just by a ping flood DoS attack.

Pyloris is a popular DoS tool that you can download from – https://sourceforge.net/projects/pyloris/

Low Orbit Ion Cannon (LOIC) is another popular tool for DoS attacks.

Quick Tips

To secure a wireless network, you should keep the following points in mind –

√ Change the SSID and the network password regularly.

√ Change the default password of access points.

√ Don't use WEP encryption.

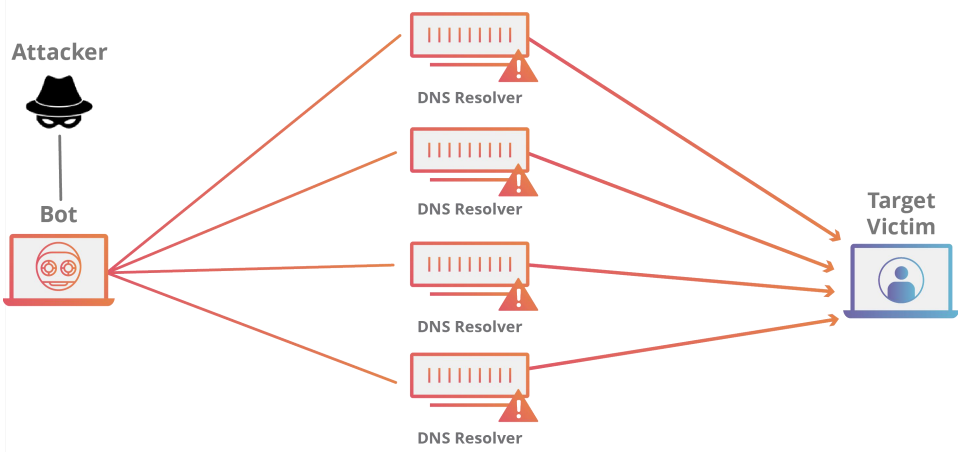
√ Turn off guest networking.

√ Update the firmware of your wireless device.

Some Other Important Hacking Methods

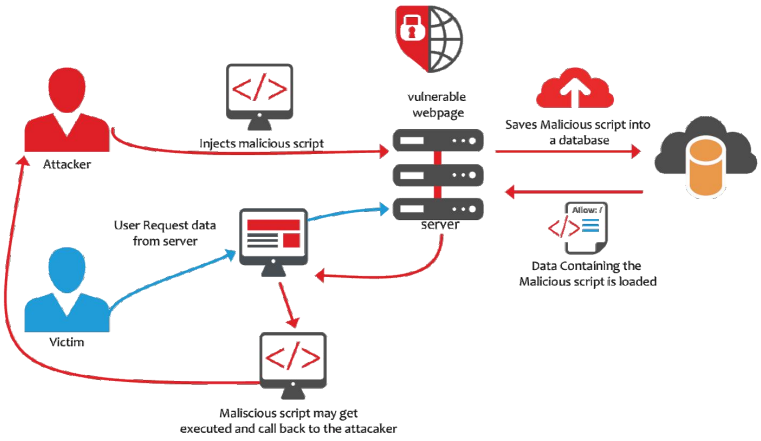
DDOS Attack

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service or a website unavailable by overloading it with huge floods of traffic generated from multiple sources.



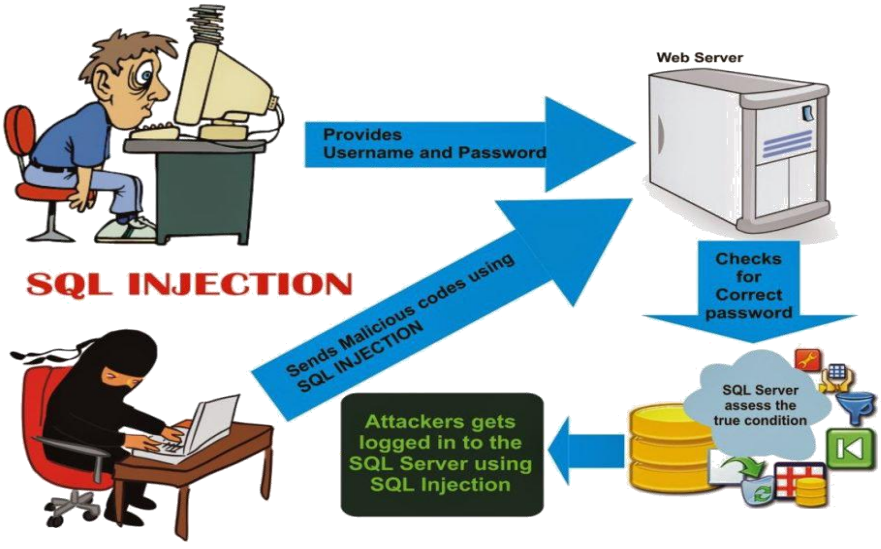
Cross Site Scripting

Cross-site scripting (XSS) is a code injection attack that allows an attacker to execute malicious JavaScript in another user's browser.



SQL injection

SQL injection is a set of SQL commands that are placed in a URL string or in data structures in order to retrieve a response that we want from the databases that are connected with the web applications. This type of attacks generally takes place on web pages developed using PHP or ASP.NET.



Penetration Testing

Penetration Testing is a method that many companies follow in order to minimize their security breaches. This is a controlled way of hiring a professional who will try to hack your system and show you the loopholes that you should fix.