**Hacking Web Servers**

***Table of Contents Pages***

*Introduction………………………………………………...(1)*

*Web Server Vulnerabilities.……………………………….(2-3)*

*Types of Web Servers.………………………………………(3)*

*Types of Attacks Against Web Servers.……………………(3-4)*

*Effects of Web Attacks………………………………………..(4)*

*Web Servers Attacking Tools.………………………………..(4-5)*

*How to avoid Web Attacks?.…………………………………(5)*

*Citations.………………………………….……………………(6)*

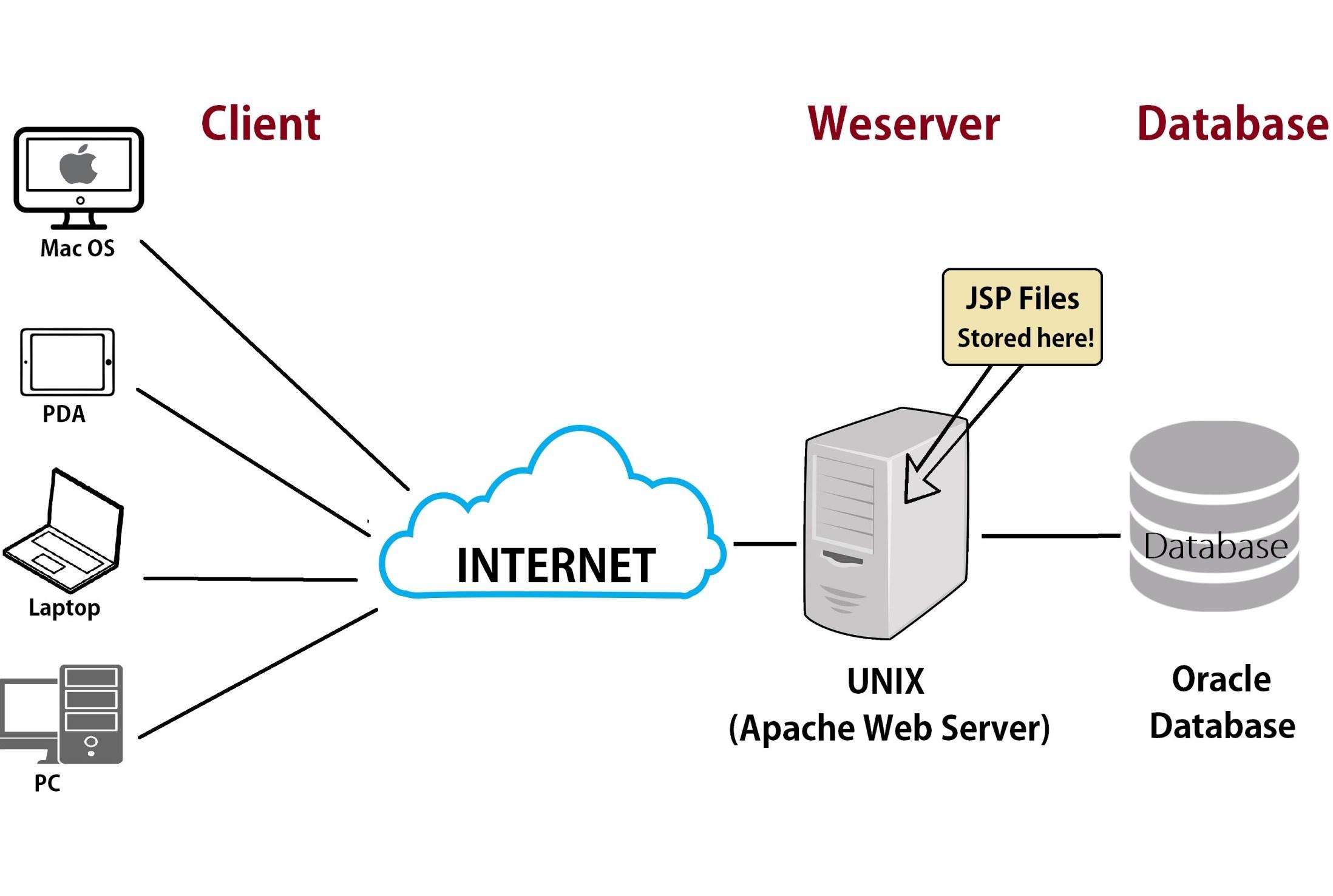
Daniel Rao

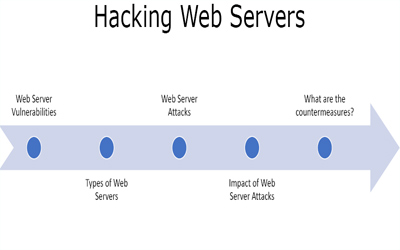
28th March, 2021

Vince Skinner

**Introduction**

In order to understand Hacking web servers we must first understand what are web servers? Web servers are basically any other ordinary computers used by businesses, corporations, government agencies and organizations. Web servers are usually responsible to handle multiple client requests and are a core component that holds clients sensitive information. For example, customers usually prefer the internet in order to get information and purchase products and services. Most of the organizations and businesses operate with a back-end website that are usually hosted by the web servers. These servers may store valuable information such as credit card numbers, email addresses, physical addresses, passwords and possibly medical records. This has made them prone to attackers. in order to defend against these kinds of attacks a good pen tester must identify end result vulnerabilities in order to secure their back-end web service.





**Web server vulnerabilities**

Open server is a program that stores usually fires and makes them accessible via Network or Internet. web servers require both hardware and software. attackers usually Target DS voice and the software to gain authorized entry to the server. attackers may gain authorized entry to the server. Some of the common vulnerabilities that an attacker maybe able to take advantage of are as follows:

* **Default settings:** settings that are usually default such as user ID and passwords which can be easily guessed by the attackers.This is a very dangerous vulnerability as it may allow the attacker to run commands on the server which can be exploited quite easily.
* **Bad configuration:** certain configurations allow attackers to execute commands on the server which can be dangerous if the user does not have a good password.
* **Bugs in the operating system and web servers:** bugs that are discovered in the operating system or web server software using pentesting can also be exploited to gain unauthorized access to the system.
* **Lack of skill security and proper procedures:** Lack of security and proper procedures are one of the leading causes of attacks. this involves things such as not updating antivirus software such as not matching the operating system and a web server software on time or not installing a good firewall on the system. This can create a big loophole in their security which can be easily exploited by the attackers.

**Types of web Servers**

Some of the most common web servers are Apache and internet information services also known as IIS. Apache is the most commonly used web server on the internet. it is usually installed on Linux. Most PHP websites are hosted on Apache servers.

Another is the IIS, which is developed by Microsoft. It runs on Windows and is the second most used web server on the internet. Most aps and aspx websites are hosted on IIS servers.

**Types of Attacks against Web Servers**

* **Directory traversal attacks:**  does the type of attack exploits bugs in the web server to gain unauthorized access to files and folders that are not publicly available. once the attacker is able to gain access, they may be able to download and steal valuable information, execute codes and install malicious software on the server.
* **denial-of-service attack:** did this type of attack, the web server may crash or could possibly become unavailable to legitimate users.
* **DNS hijacking:** with this type of attack, the DNS setting may be changed to point to the attackers web server so that all the traffic That was supposed to be sent to the web server is now redirected to the attackers machine.
* **Phishing:**  this type of attack in person is the website and direct traffic to the fake website. This is mainly a client-side attack where the legitimate users may be tricked into submitting sensitive data such as login details, credit card numbers to the attackers machine.
* **Pharming:** Type of attack, the attacker compromises the DNS server on the user's computer so that the traffic is directed to the malicious website.

**Effects of Web Attacks**

* **Reputation:** the organization's reputation may be ruined if the attacker is able to obtain valuable information about its customers data.
* **Ruining System or privacy:** The web servers can be used to install malicious software on the client's machine. as they're using the compromise website the malicious software downloaded onto the visitors machine can be a virus such as Trojan or botnet softwares.

**Web servers attacking tools**

Some of the most common web server attacking tools are as follows:

* Metasploit: this is an open source tool for developing and testing using exploit code. it can be used to discover vulnerabilities ended up servers and write exploit that can be used to compromise the servers.
* Mpack: this is a web exploitation tool. It Was Written in PHP and is backed by SQL as a database engine once a web server has been compromised using mpac, all of the traffic is redirected to malicious download websites.
* Zeus: this tool can be used to turn a compromised computer into a bot or zombie. A botnet is a compromised computer which is used to perform internet-based attacks. A botnet is a collection of compromised computers. The botnet is used mainly in denial of service attacks or sending spam mails.
* Neosplit: This tool is mainly used to install or delete programs.

**How to avoid attacks on Web Servers?**

* **Patch management:** this involves installing patches regularly to help secure the server what's up patches and updates that fixes the bug in the software. The patches can be applied to the operating system and the web server system.
* **vulnerability scanning systems:**  these include programs such as Nmap or Zenmap to quickly identify and resolve on their vulnerabilities that are present in the web server system.
* **Antivirus:**  installing a good antivirus is a must in order to have a secure system.
* **Firewalls:** Installing a good firewall can simply stop the attacks by blocking all traffic coming from the source IP.
* **Ports:** Shutting down unnecessary ports is really important when it comes to securing a web server system.
* **Default Passwords:**  updating default passwords is a must in securing the web service system.

**Citations**

<https://www.greycampus.com/opencampus/ethical-hacking/web-server-and-its-types-of-attacks>

<https://www.guru99.com/how-to-hack-web-server.html>