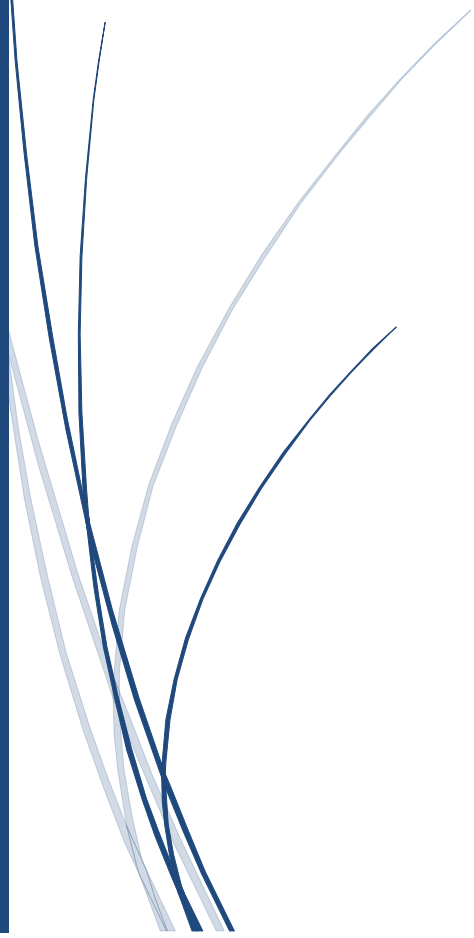
Chapter 13

Hacking web servers

Theory



Ethical Hacking

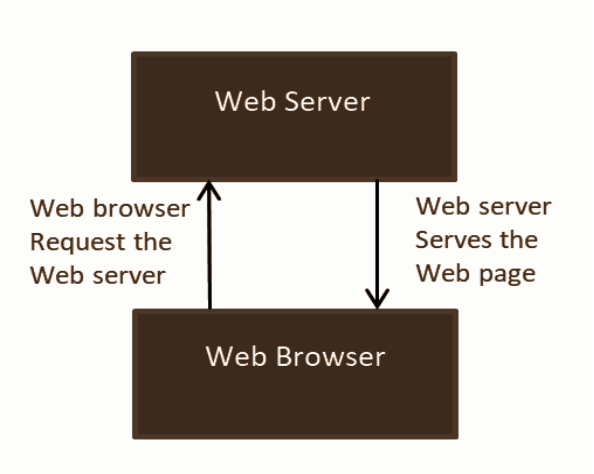
Web Server

Web Server is a computing system that runs on server OS to process the HTTP/HTTPS requests and serve the web pages on the world wide web. The pages delivered are HTML documents, which may include images and scripts in addition to the text content. Clients use a web browser to interact with the web server.

Any computer can be turned into a Web server by installing server software and connecting the machine to the Internet. There are many Web server software applications like Xampp, Apache, Nginx, IIS web server, etc.

How Web Servers Work?

When a user requests a web page hosted on the internet, the web server responds with that requested page. The below image represents this process.



Obtaining the IP Address from domain name: Web browser first obtains the domain name and resolves it to IP address. It can obtain the IP address in 2 ways:

1. By searching cache.
2. By requesting one or more DNS Servers.

After knowing the IP Address, the browser now demands a full URL from the web server. The web server responds, by sending the requested page to the browser, and if, the web page does not exist, then it will display an appropriate error message. The browser renders the response received from the server to display it on the screen.

List of popular web servers

The following are a list of the common web servers:

Apache – The commonly used web server on the internet. It is cross-platform application software, but it is usually installed on Linux. Most PHP websites are hosted on Apache servers.

Internet Information Services (IIS) – It runs on windows and is the second most used web server on the internet. Most websites built using ASP.Net are hosted on IIS servers.

Apache Tomcat – Java server pages (JSP) websites are hosted on this type of web server.

Other web servers – Novell's Web Server, IBM Lotus Domino servers, Cloudflare web server, Oracle web server, Lightspeed servers, Amazon web server, Google web server, Nginx, etc.

Footprinting Web Server

- Attackers use ID Serve, Netcraft, HTTP Recon, Whois tools to get details about the target server.
- Use robot's exclusion protocol, a standard used by websites to communicate with web crawlers and other web robots to gather some sensitive information.
- This file (robots.txt) will inform the web robot about which areas of the website should not be processed or scanned.
- By performing the DNS enumeration, we can get the dns records and types of servers.

Web Server Vulnerabilities

The following vulnerabilities are most commonly exploited in web servers:

- Improper file and directory permissions.
- Unnecessary services enabled, including content management and remote administration.
- Improper authentication with external systems.
- Default accounts with default or no passwords.
- Misconfiguration in web-server, operating system or network.
- Bugs in server software, OS or web application.
- Lack of security policy and procedures

Types of Attacks possible against Web Servers

Denial of Service Attacks – With this type of attack, the web server may crash or become unavailable to the legitimate users.

Domain Name System Hijacking – In this type of attack, the DNS settings are changed to point victims to the attacker's web server. All the traffic was supposed to hit a malicious server.

Sniffing – Unencrypted data sent over the network may be intercepted and used to gain unauthorized access to the web server.

Defacement – In this type of attack, the attacker takes advantage of vulnerabilities in the web server to replaces the organization's website with a different page that contains the hacker's name, images and may include background music and messages.

Impact of Web Server Attacks

- Easy to compromise user accounts.
- Gaining root access to other applications on servers.
- Access to confidential data (Data tampering/Data theft).
- Perform Web Application attacks.
- The compromised web server can be used to spread malicious software on the internet, which can infect users who visit the compromised website.
- Compromised user data can be used for fraudulent activities.
- An organization's reputation can be ruined.

Identify Vulnerabilities on Web Server

- Perform vulnerability scan to identify weaknesses in a network and determine if the system can be exploited.
- Use vulnerability scanners like Sparta, Nikto, HP Web Inspect, Acunetix Web Vulnerability Scanner to find out hosts, services, and vulnerabilities.
- Sniff the network traffic to identify vulnerabilities on active systems or network services.
- Test the web server infrastructure for any misconfigurations, outdated content, and vulnerabilities.

Countermeasures

- Scan for existing vulnerabilities, patch and update the server software regularly.
- Block all unnecessary ports, ICMP traffic, and unnecessary protocols.
- Consistently apply the latest software patches and update system software.
- If remote access is needed, make sure that the remote connection is adequately secured, by using tunneling and encryption protocols.
- Stop running vulnerable applications on the server, such as WebDAV. Unnecessary applications can be removed on a server by using Add/Remove Programs in the Windows Control Panel.
- Perform bound checking on input for web forms and query strings to prevent buffer overflow or malicious input attacks.
- Disable remote administration.
- Avoid printing error messages.

- Enable auditing and logging.
- Use a firewall between the web server and the Internet and allow only necessary ports (such as 80 and 443) through the firewall.
- Replace the GET method with the POST method when sending data to a web server.