12.1.4 Web Server Attack Facts

Many of the attacks presented so far can be applied to a web server. Web servers are attacked because they are publicly accessible, are easy to find, and can inflict a lot of damage.

This lesson covers the following topics:

- Server attack types
- Web server hacking methodology
- Web server attack tools

Server Attack Types

Attacks specific to a web server are described in the following table.

Attack	Description
Website defacement	Website defacement is a fairly unique type of attack in which a website is vandalized or defaced in an attempt to humiliate, discredit, or even just annoy the victim. In response to ethical or political actions, hacker groups will often initiate defacing attempts to promote or support various agendas. Hacktivists typically replace the web content with their own logo or poster along with a statement explaining why they have targeted the organization. In some instances, instead of changing a site's appearance, the attacker will change the site's content. The impact of this type of attack may not be immediately obvious. Instead of a flashy alteration, smaller, more subtle changes are made to descriptions, pictures, product costs, or statements that have been posted to a site.
Directory traversal	A directory traversal attack is an HTTP exploit that can provide attackers access to restricted areas of a web server. This attack is generally used on older servers that have vulnerabilities and misconfigurations. The hacker targets directories and executables that should be restricted. Anyone accessing the web server from the internet should be able to access only web pages and information stored in the root directory. An attacker can use the command line, a browser, or a vulnerability tool to search for restricted files outside of the root directory.
Cross-site scripting (XSS)	A cross-site scripting attack takes advantage of web applications' scripting defects. An attacker alters the XSS to send malicious code to a user. The target's web browser is unaware that the code is malicious and executes the script. The malicious script allows the hacker to access sensitive information such as cookies, session tokens, and private information.
DoS/DDoS attacks	In a DoS/DDoS attack, a hacker causes the web server to generate a large number of responses to requests, causing it to slow down, crash, or become otherwise inaccessible to authorized users. High-profile web servers, such as those owned by banks, credit card companies, or government services, are frequently targeted with these attacks.
DNS server hijacking	In a DNS server hijacking attack, a hacker changes the DNS settings on the DNS server so that all requests are rerouted, typically to the hacker's malicious server.
Man-in-the-middle attack	A man-in-the-middle attack is used to intercept communications between an authorized user and the web server. The hacker can then gain access to sensitive information or alter the information.
Phishing attack	In a phishing attack, a user is tricked into clicking a seemingly legitimate link to complete a request for information. Instead, the user is redirected to a malicious website that steals the user's login information or other sensitive data.
HTTP response splitting attack	This attack involves header response data being added to the input field, causing the server to split the response into two parts. The attacker is able to manipulate the second response and can redirect the user to a malicious website.
SSH brute force attack	SSH is used to create a encrypted tunnel between hosts. An SSH brute force attack is used to gain unauthorized access to the tunnel by a brute force attack on the SSH login credentials. The tunnel can then be used to transmit malware and other malicious items without detection.
Web server password cracking	A attacker uses various weaknesses to hack into seemingly secure passwords. Attackers can use social engineering, phishing, spoofing, keystroke logging, viruses, wiretapping, or other methods to crack these passwords. Passwords can be cracked manually or with tools.

Web Server Hacking Methodology

The web server methodology provides a step-by-step list of the actions needed to perform an attack against a web server. This methodology combines many of the techniques from previous lessons.

Step	Description
Information gathering	During the information gathering step, the attacker gathers information about the target using the internet, Whois, traceroute, and Active Whois.
Footprinting	During the footprinting steps, the attacker gathers system data including account information, operating system type and version, server names, and information about the database layout. The attacker uses various tools to gather information about the server.
Enumeration	During the enumeration steps, the attacker uses various commands and tools, such as nmap, to enumerate information about the target.
Mirroring	During the mirroring step, the attacker uses mirroring tools to create a duplicate of the website, including the directory structure, the external links, and the file structure. The attacker will then analyze and carefully scour the source code for useful information.
Vulnerability scanning	The attacker runs vulnerability scanners to find possible weaknesses in a network. These tools test the web server for outdated content, configuration errors, and other vulnerabilities.
Session hijacking	Attackers sniff for valid session IDs in an attempt to get access to a web server. They use session hijacking methods to capture session cookies and IDs.
Hacking web passwords	An attacker uses brute force attacks, dictionary attacks, and guessing to crack the passwords to web servers.

Web Server Attack Tools

The following is a list of commonly used tools.

Tool	Description
Metasploit	Metasploit is a penetration testing toolkit that contains remote exploits for various platforms. It provides fully automated web server attacks that target known vulnerabilities in web servers.
Wfetch	Using Wfetch, an attacker can create an HTTP request. This tool targets web sites that have Active Server Pages (ASP) or wireless protocols.
TCH-Hydra	TCH-Hydra is a password cracking tool that supports several different protocols.
Brutus	Brutus is a password cracking tool that can make over 50 simultaneous target connections. It supports various scenarios, including no user name, multiple user names, password list, and multiple usernames.