Here are 10 common web server attacks:

1. Distributed Denial of Service (DDoS): In a DDoS attack, multiple compromised systems flood the target server with a massive amount of traffic, overwhelming its resources and causing it to become unavailable to legitimate users.

2. SQL Injection: This attack involves exploiting vulnerabilities in a web application's database layer. Attackers inject malicious SQL code into user input fields, tricking the server into executing unintended database commands that can reveal sensitive information or manipulate the database.

3. Cross-Site Scripting (XSS): XSS attacks occur when attackers inject malicious scripts into web pages viewed by other users. These scripts can be used to steal sensitive information, hijack user sessions, or deface websites.

4. Cross-Site Request Forgery (CSRF): In a CSRF attack, an attacker tricks a victim into unknowingly executing unwanted actions on a web application. This is done by exploiting the trust between the user's browser and the target server, leading to unauthorized actions being performed on behalf of the user.

5. Remote File Inclusion (RFI): RFI attacks involve exploiting vulnerabilities in a web application to include remote files, often from external servers controlled by the attacker. This can allow the attacker to execute arbitrary code on the server, leading to unauthorized access or system compromise.

6. Server-Side Request Forgery (SSRF): In an SSRF attack, an attacker manipulates a vulnerable web application to make requests to internal resources or external systems that the server has access to. This can be used to bypass security restrictions, scan internal networks, or exploit vulnerable services.

7. Directory Traversal: This attack aims to access files and directories outside of the intended web server directory structure. By manipulating input parameters, attackers can navigate to restricted areas and potentially retrieve sensitive information or execute arbitrary code.

8. Brute Force Attacks: In a brute force attack, an attacker systematically attempts all possible combinations of usernames and passwords to gain unauthorized access to a web server. This attack relies on weak or easily guessable credentials.

9. Server Misconfiguration: Server misconfigurations can expose sensitive information or provide unauthorized access to attackers. Examples include leaving default credentials unchanged, enabling unnecessary services, or not applying security patches.

10. Zero-Day Exploits: Zero-day exploits target vulnerabilities that are unknown to the vendor or have no official patch available. Attackers exploit these vulnerabilities before they are discovered and patched, gaining unauthorized access to web servers.

It's important for organizations to implement strong security measures, regularly update software and applications, and perform security audits to mitigate the risk of these attacks.