**CTF Challenge: Hacking Web Servers**

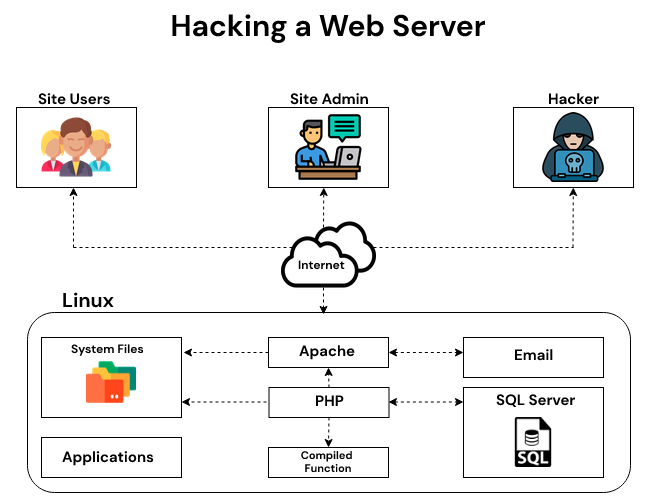
****

**Hacking Web Servers?**

****

"Hacking web servers" involves exploiting vulnerabilities in web servers, web applications, or associated services to gain unauthorized access, manipulate data, or disrupt services. Here are some key points about hacking web servers:

### **Common Techniques for Hacking Web Servers**



1. **SQL Injection (SQLi)**: Injecting malicious SQL queries through input fields to manipulate the database.
2. **Cross-Site Scripting (XSS)**: Injecting malicious scripts into web pages that are then executed by the user's browser.
3. **Remote File Inclusion (RFI)**: Including a remote file, typically through a URL, to execute malicious code on the server.
4. **Local File Inclusion (LFI)**: Including local files on the server through vulnerable scripts to execute malicious code or access sensitive data.
5. **Directory Traversal**: Accessing files and directories outside the intended web directory by manipulating URL paths.
6. **Command Injection**: Injecting and executing arbitrary commands on the server through vulnerable applications.
7. **Brute Force Attacks**: Using automated tools to guess login credentials through repeated attempts.
8. **Server Misconfigurations**: Exploiting poorly configured servers, such as default credentials, exposed services, and unnecessary open ports.

### **Tools for Hacking Web Servers**

* **SQLMap**: An automated tool for SQL injection and database takeover.
* **Burp Suite**: A comprehensive platform for testing web application security, including web server attacks.
* **Nikto**: A web server scanner that detects vulnerabilities and misconfigurations.
* **Metasploit**: A penetration testing framework that includes modules for exploiting web server vulnerabilities.
* **OWASP ZAP (Zed Attack Proxy)**: A popular tool for finding security vulnerabilities in web applications.

# **Capture the Flag (CTF) Challenges**

**Flag 1. Which technique involves injecting malicious SQL queries to manipulate a database?**

Answer: SQL Injection

**Flag 2. What is the name of the automated tool used for SQL injection and database takeover?**

Answer: SQLMap

**Flag 3. Which method includes remote files to execute malicious code on the server?**

Answer: Remote File Inclusion (RFI)

**Flag 4. What technique involves injecting and executing arbitrary commands on the server?**

Answer: Command Injection

**Flag 5. Which tool is a comprehensive platform for testing web application security, including web server attacks?**

Answer: Burp Suite