Chapter 4 - Key Terms

Term	Page	Description
SQL Injection	588	An attack whereby an attacker *injects* a SQL query via the input data from a client to the application or database.
CSRF	579	Cross-site request forgery. Forces an end user to execute malicious steps typically after the authentication process has occurred by abusing the trust between client and application. Target state changing requests, attackers cannot steal data because they cannot see response. Attacks usually carried out via social engineering.
XSS	590	A type of web app attack where malicious scripts are injected into trusted websites. Typically delivered via browser-side scripts.
Buffer Overflow	578	A situation where a program writes more data to the buffer than it can hold overwriting adjacent memory space. Can cause memory corruption, DoS, or code execution conditions.
War Driving	589	An attacker can drive around and locate wireless access points.
Rainbow Tables	586	A lookup table into which an attacker computes possible passwords and their hashes and puts the results. Allows attackers to simply search based on hashes derived from victim system. Mitigate, disable LM hashes & use complex passwords.
DNS Tunneling	581	Method in which attackers can encapsulate chunks of data into DNS packets to exfiltrate data.
Botnet	578	A collection of compromised machines an attacker can manipulate with a C2 or CNC system to participate in DoS, spam, etc.
Backdoors	578	A piece of malware or config change that allows an attacker to control the system remotely. Used for exfiltration or future access.