Cache:
To enhance response times for subsequent requests and lessen the strain on the database, frequently accessed database query results in a web application can be cached.

Cipher:
Example: Encrypting sensitive data before putting it in a database using the Advanced Encryption Standard (AES) algorithm.

Code Injection:
An illustration of this would be taking advantage of a flaw in a web application's input field to insert malicious code, like JavaScript or SQL injection, which could allow for illegal access or actions.

Cross-Site Scripting (XSS):
Example: Inserting malicious scripts into user input on a forum website so that, when other users view the pages that are affected, the scripts will run.

Compliance:
Example: Ensuring that credit card information is protected on an e-commerce website by adhering to the Payment Card Industry Data Security Standard (PCI DSS).

Dictionary Attack:
An example would be to repeatedly try popular username/password combinations, such as "admin/admin," in an effort to obtain unauthorized access to a user's account.

Dumpster Diving:
Example: Looking through the trash cans of a company to locate sensitive documents or passwords hidden within the discarded papers.

Denial of Service (DoS) & Distributed Denial of Service (DDoS):
Example: Sending a lot of requests at once to a web server in order to overwhelm it and prevent legitimate users from accessing it (DoS). If a botnet is used to orchestrate this attack, it becomes a DDoS.

DevSecOps:
Example: Making sure that security is an essential component of the development and operations process rather than an afterthought by integrating security practices throughout the software development lifecycle.

Directory traversal:

An example of this would be taking advantage of a flaw in the way a web application handles files to access files that are not in the intended directory, thus exposing private data.

Domain Name System (DNS):
Example: Resolving the domain name "www.drcelly.com" to its corresponding IP address (e.g., 192.168.1.1) using DNS.

DNS Spoofing:
Example: Using DNS response manipulation to sway users to a malicious website so that, even when they type in a valid domain (like "bank.com"), they end up on an attacker-controlled spoof website.