Code Security

An important variant of black box testing is an analysis technique called taint analysis. A significant portion of today's security vulnerability are string-based code injection vulnerability. SQL security—an SQL injection training platform that allows for customization of white and black listed characters and sequences focused on a challenge-based platform to train the basic skills necessary to test and defeat SQL security measures.

* It can be prevented by Validate and sanitize inputs: Scan for escape characters and other special symbols for the application language and operating system, such as comment marks, line termination characters and command delimiters. If your application only expects a limited set of values, accept only those values, for example by whitelisting or conditionally switching on them, also by Scan your applications: Use a [**dynamic web vulnerability scanner**](https://www.netsparker.com/web-vulnerability-scanner/) to ensure your applications are safe from various types of attacks, including code injection.

Reference:- https://www.sciencedirect.com/topics/computer-science/code-injection

Data Security

TO prevent your data to get public or to use it securely there are several ways as following:

1. Be Alert to Impersonators. ...
2. Safely Dispose of Personal Information. ...
3. Encrypt Your **Data**. ...
4. Keep Passwords Private. ...
5. Don't Overshare on Social Networking Sites. ...
6. Use Security Software. ...
7. Avoid Phishing Emails. ...
8. Be Wise About Wi-Fi.