**Gray Box testing:**

Gray box testing (a.k.a grey box testing) is a method you can use to debug software and evaluate vulnerabilities. In this method, the tester has limited knowledge of the workings of the component being tested. This is in contrast to [black box testing](https://www.imperva.com/learn/application-security/black-box-testing/), where the tester has no internal knowledge, and [white box testing](https://www.imperva.com/learn/application-security/white-box-testing/), where the tester has full internal knowledge.

**Gray box testing techniques:**

**Matrix Testing:**

Matrix testing is a technique that examines all variables in an application. In this technique, **technical and business risks** are defined by the **developers** and a list of all application variables are provided. Each variable is then assessed according to the risks it presents. You can use this technique to identify unused or un-optimized variables.

**Pattern Testing:**

Pattern testing is a technique that evaluates past defects to identify patterns that lead to defects. Ideally, these evaluations can highlight which details contributed to defects, how the defects were found, and how effective fixes were. You can then apply this information to identifying and **preventing similar defects in new versions of an application or new applications with similar structures.**

**Orthogonal Array Testing:**

Orthogonal array testing is a technique you can use when your application has only a few inputs that are too complex or large for extensive testing. This technique enables you to perform test case optimization, where the quality and number of tests performed balance test coverage with effort. This technique is systematic and uses statistics to test pair-based interactions.