Black vs White vs Gray box

Penetration Testing Methodologies

Methodology	Key Characteristics	Advantages	Disadvantages	Real-World Scenario
White Box	Tester has full knowledge of the system's infrastructure, applications, and source code.	More focused testing, faster identification of vulnerabilities, ability to test internal systems and applications.	Requires high level of technical expertise, potential for tester bias.	Testing a newly developed internal application to identify vulnerabilities before deployment.
Black Box	Tester has no prior knowledge of the system, simulating a real-world attacker.	Realistic assessment of security posture, identifies vulnerabilities that might be missed by internal teams.	Can be time-consuming, may miss some vulnerabilities due to lack of information.	Assessing the security of a public-facing website to identify potential attack vectors.
Grey Box	Tester has partial knowledge of the system, such as network diagrams or user credentials.	Balances the benefits of white box and black box testing, provides a more realistic scenario than white box.	Requires some level of cooperation from the organization, might not be as thorough as a full black box test.	Testing a web application with limited access to internal systems and source code.