**What is Web Application Security?**

Web application security is the idea of building websites that function as expected, even under an attack. It includes a collection of security controls that are engineered into a web application for protecting its assets from potential threats.

Like any other software, web applications can also have errors. Some of these issues can be actual vulnerabilities that can be exploited. These can pose serious risks to the organization. Web application security can defend your organization against such vulnerabilities. It involves the implementation of security measures during the entire Software Development Life Cycle. Hence, it ensures that you address all implementation-level bugs and design-level flaws.

**Why is Web Application Security Important?**

Web application security testing primarily targets the application layer to see what runs on the HTTP. A pentester sends different inputs to provoke errors, and tries to see the behaviour of the system. These tests intend to check if the system is showing any unusual behaviour, or doing something that it is not designed to do.

Another important thing to consider is that web security testing is not just about testing security features such as authorisation and authentication. It is also important to test that you have implemented all other features securely. For instance, using correct input validation and output encoding. The ultimate goal is to test that all exposed features in the web application are secure.

**How Does Web Application Security Testing Reduce Risks for my Organization?**

Majority of web application attacks include cross site scripting, SQL injections, path traversal or remote command execution. These attacks can result in compromised user accounts, access to restricted content, lost sales revenue, loss of customer trust, installation of malicious code, and much more.

If you know the different attacks your application can face along with their outcomes, you can proactively address these vulnerabilities and conduct your tests accurately. By determining the root cause of vulnerabilities, you can implement mitigation controls during early stages of your SDLC. Furthermore, have knowledge of how the attacks work can help you target known interest points during a web app security test.

Another key to managing risk is to recognize the impact of attack. By identifying issues during a web security test, your organisation can prioritise its remediation efforts. Before identifying an issue, evaluate potential impact against each application. With a list of high-profile applications, you can schedule web application security testing to target the critical applications first with targeted testing. Hence, it will help lower the risk of threats against your organisation.