A6: Security Misconfiguration

According to Open Web Application Security Project (OWASP) one of the top most critical Web Application Security risk is the Security Misconfiguration and it is in the 6th place. So the question is what is Security Misconfiguration? This threat occurs only when there is component that is open to any attack due to an unsure configuration. Security Misconfiguration is the improper or inappropriate configuration of the server or web application that might lead to different kind of flaws. Having this kind of problem may affect all the data you currently have, It can be stolen or modified slowly.

Medication

Prevention is better than cure. So the question is how can we prevent this kind of threat? Education and Training is the best way to prevent Security Misconfiguration because when you educate your staff or employee on the current security trends it will help them to make better decisions and follow best practices. Disabling defaulting accounts and changing password can also help and always keep everything updated. Running automated scans and doing inspections from time to time can help lessen the possibility to encounter this kind of threat. Always ensure that the security settings are configured correctly.

Example

If the attackers know that the directory listing of the server is not disabled, the attacker can just list all the directories and execute it. There is also a possibility that the actual code file that contains all the custom code and the attackers can find the flaws of the application.

Another example is when the server configuration allows the flaws of the app returned to the users, attackers can grab those information that the server provides. The error messages can be used by the attackers to simply penetrate those error messages.