**Top 10 OWASP Application Security Risks in the Year 2017**

**The first application is Injection.** The application Injection happens when the suspicious data is being sent to an interpreter in a macro/command or query. It basically makes the hacker attack with a suspicious data and deceives the interpreter in making unintentional commands or accesses the data without permission.

**The second application is Broken Authentication.** The application lets the user accounts compromised by hackers and to exploit usernames, passwords, keys and other personal information. The session management is the foundation of all authentication and access controls, so hackers can identify the application – Broken Authentication with tools that have an index of all password lists and dictionary.

**The third application is Sensitive Data Exposure.** Hackers target protected data in many credit cards, identity theft and many more other crimes. The sensitive data for users could be penetrated without additional security. For example: In a browser, a hacker decides to attack a user in its credentials with retrieved previous passwords in a database using Graphics Processing Units (GPUs).

**The fourth application is XML External Entities(XXE).** The application allows hackers to utilize the vulnerability of XML processors to upload XML that comprises of suspicious content in an XML document. The types of attacks by hackers in this case comprises of internal file sharing, internal port scanning, URI handling and denial of service attacks.

**The fifth application is Broken Access Control.** The application lets the hackers detect the deficiency of access controls without the verification if the function is present. The reason for vulnerability is because the restrictions that provided for authenticated users are not properly implemented. The attacks include exploitations such as the access of unauthorized data, access to user accounts, privilege to view sensitive files, modification of authorized data, and remove the credibility of the user.

**The sixth application is Security Misconfiguration.** The application is a common issue because of the default configuration that hackers could attack easily. The default user accounts that includes passwords and all the configuration without updating regularly all the ad hoc, open cloud storage, HTTP headers, and other sensitive containing information would definitely make an easy target for hackers.

**The seventh application is Cross-Site Scripting (XSS).** The hacker uses suspicious data with a HTML snippet – an automated tool that could exploit all the Cross-Site Scripting that works as a framework, to hack the credentials of authenticated users. The application is the second most common issue in the top 10 OWASP application security risk. In addition, the automated tools could detect automatically the problems of XSS which are PHP, J2EE/JSP, and ASP.NET.

**The eight application is Insecure deserialization.** The application is all about remote code execution which is the most dangerous attacks made by hackers. Moreover, the type of attack includes, replay attacks, injection attacks, and privilege escalation attacks.

**The ninth application is Using Components with Known Vulnerabilities.** The attack can be initiated and can be overpowered if only the components of the applications that includes the libraries, frameworks, and software modules are exploited, then the attack would allow serious data loss or server control. In addition, applications and APIS that are common for hackers to penetrate, would compromise the security for application defense and other various-enabled attacks.

**The tenth application is Insufficient Logging and Monitoring.** Hackers attack through the system with tampering, extraction or collapse of data by the patience in timely for the monitoring and finishing the goal without getting caught. A successful attack by a hacker is determined with vulnerability searching by which it allows searching to continue to raise likelihood of successful exploits.