Injection

Injection is any attack that allows the hacker to give inputs that causes the program to interpret the command or query together with the input in a way that alters the execution of a software. These kinds of attacks can cause compromise a whole system, data loss, data theft, denial of service and even loss of data integrity and is one of the most common software vulnerability due to the fact that it is very easy to exploit, many tools for this kind of attack is free and reliable which make it an easy security risk to exploit. Also these kind of attacks can be applied to almost any programming and scripting languages. These facts are the reason why these attack scary and ranked number 1 in “OWASP Top 10 Application Security Risks - 2017”.

Common Kinds of injection

1. SQL Injection(SQLi)

An SQL injection attack is done by inserting a complete or partial SQL statement through data input of the client which is sent to the server. These attacks of such can leak sensitive data from a database, allow the hacker to modify the database and its data causing data loss, data theft or loss of data integrity, bypass authentication, and even allow the hacker to execute administrative operations which could compromise the whole system. There are 3 types of SQL injection attacks, namely, inband – straight-forward; queried data is presented in the website, out-of-band – the queried data is sent via email or other means besides from being presented in the website, inferential or Blind – no data is transferred, rather operations are sent to reconstruct the database’s information by the observation of the database server’s responses.

Prevention:

1. Use Prepared Statements and Parameterized Queries
   * Parameterized queries is when the SQL code is defined first then parameters are passed into the queries, this allows the database to differentiate code and data.
2. Use Stored Procedures
   * This option is not always safe from SQLi attacks nonetheless it has same effects like the use of prepared statements and parameterized queries.
   * The stored procedures is stored in the database then called from the application
3. Whitelisting Input Validation
   * Only allows valid input to prevent data integrity issues
4. User Input escape
   * Last resort if all choices cannot be applied
5. LDAP Injection

Hackers using LDAP Injection attacks use ways similar to SQLi and the damage to a system is also similar to a SQLi.

Prevention:

* Variable Escape
* Use available framework that counter LDAP Injection

1. OS Command injection

A type of injection wherein hackers send a system command to the operating system which could compromise the whole system.

Prevention:

* Avoid using OS commands in the code
* Escape OS commands
* Use parameters and Input Validation

General prevention

1. Input validation
2. Use appropriate API
3. Escape user input