Julian Rodriguez

Common Web Server Vulnerabilities

1. Buffer Overflow

The way a buffer overflow work is that some one gives more information than a server expect to receive for a specific task, causing it to send data to another section of a process and causing it to be accessible and readable by the users.

Buffer overflows require, for the most part, for the user trying to attack the server to know exactly what software you are using and know what version you are using to be able to know were to attack to get specific data. Simple solution to that is to keep that information unknown to all users. Another solution to an overflow is to simply validate any information before submitting to the server.

1. Authentication and Session Management

Authentication and session management simply means that a session from a server is not properly validated or terminated after a cretin period of time and there fore is left vulnerable to exploitation for an attack. By not validating a session you leave data to be read and allow access to be tampered with.

A simple and common solution to this is to problem is to make sure unique password and user names are implemented. That said it is not enough, SSL encryption is a good place to start to assure that some one as well authentication and access control modules should be integrated into a single modules or system and applied globally, allowing global updates and corrections.

1. SQL Injection

An SQL injection is a method of attacking a data-driven application, such as billing information inputs or search inputs, by causing the application to incorrectly process data for special characters within the SQL inputs. Note that these inputs are stored in a variable and the attack relies on poor validation from the server’s part for the attack to succeed.

Again a simple solution is, for critical validation from the server’s part to make sure that any information that is not expected in the proper manner is not received or processed alt all. Ways to facilitate this is to add character limitation and to tell the server what kind of character to expect or not expect.