Website Security

1. 2017 OWASP TOP 10

**Injection**

Sending of unauthorized data to a query which can lead to unvoluntary commands or unauthorized access of data.

**Broken Authentication**

This threat leads to the compromising of passwords or encryption keys which can also lead to unauthorized access of data.

**Sensitive Data Exposure**

Sensitive data encompasses information such as healthcare or financial information being used for their benefit.

**XML External Entities**

XML external entities hold information that may expose data such as ports which could lead to remote attacks or denial of service attacks.

**Broken Access Control**

Flawed user authorization can be used by attackers to view hidden files or change user restrictions.

**Security Misconfiguration**

This involves security measures done but are misconfigured or flawed.

**Cross-site Scripting(XSS)**

Untrusted data is embedded into a new or existing web page which could lead to redirection to malicious sites or hijacking of user sessions.

**Insecure Deserialization**

This is done remotely most of the time and leads to injection attacks.

**Using Components with Known Vulnerabilities**

A vulnerable API or framework which attackers can use to get inside a system.

**Insufficient Logging and Monitoring**

Lenient monitoring of who accesses the system will lead to a breach.

1. Preventive Measures

**Software updates**

Hackers found a way of infiltrating older versions of softwares so it is best to keep them updated.

**User permissions**

Proper analyzing what your users can do to the system is vital and it is best not to be too trusting.

**SSH**

A secure shell encrypts communication between two machines.

**Validation**

Validation is done between the server and client to prevent unknown entities from breaching the website.

**Complex Passwords**

Passwords should be something other people would be able to guess but don’t make it too complex that you will forget it.

**HTTPS**

This will provide security over the internet.