Owasp top 10:

It is a non-profit organization that aims to increase the level of security in software(Web, Android, System, etc….)

Owns many projects and tools that penetration testers need

It contains many projects that we can download for training on discovering vulnerabilities and penetration

Qualifies software developers to develop secure software

Every three to five years, a new version is issued that contains the latest discovered vulnerabilities

These versions are issued according to mathematical calculations based on the detected threats that have been exploited in the last three to five years

Accordingly, the results are released

Owasp API top 10 2019 :

- Broken object level authorization
- Broken authentecation
- Excessive data exposure
- Lack of resources and rate limiting
- Broken function level authorization
- Mass assignment
- Security misconfiguration
- Injection
- Improper assets management
- Insufficient logging and monitoring

Payload:

A payload is a malicious code

It is created by the hacker and injected into the target so that we can open a controlled path between the hacker and the target

This path offers us many powers:

- upload files
- System kernel control
- Access to sensitive data
- Open bind shell and reverse shell
- Etc….