

OWASP CLASP

Security Development Lifecycle (SDL), developed by Microsoft to answer the issues faced by them during various development projects and hence, mostly caters to the need of their development methodology only. The lifecycle of Microsoft SDL includes Training, Requirements, Design, Implementation, Verification, Release, Response while Owasp has a similar lineup with Requirements & Analysis, Design, Implementation, Testing & Verification, Maintenance in the life cycle model

CLASP — Comprehensive, Lightweight Application Security Process — is an activity driven, role-based set of process components whose core contains formalized best practices for building security into your existing or new-start software development lifecycles in a structured, repeatable, and measurable way.

CLASP is the outgrowth of years of extensive field work in which system resources of many development life cycles were methodically decomposed in order to create a comprehensive set of security requirements. These resulting requirements form the basis of CLASP's best practices which allow organizations to systematically address vulnerabilities that, if exploited, can result in the failure of basic security services — e.g., confidentiality, authentication, and access control.

CLASP process is composed of

- 1)CLASP Views
- 2)CLASP Resources

CLASP Views

These views are broken down into activities which in turn broken into components to provide a brief understanding of the CLASP process.

Activities defined under it explain how they can be easily embedded into software development lifecycle. Views contains following perspectives:

- 1)Concept view
- 2)Role-Based view
- 3)Activity –Assessment view
- 4)Activity –Implementation view
- 5)**VulnerabilityView**

Concept view:provides high-level introduction of CLASP views, best practices, security policies, process components.

Role-Based view: explains how roles could be associated with each best practice.

Activity-Assessment view: provides assistance to managers to assess the accuracy of the CLASP activities into their project.

Activity-Implementation view:It contains the 24 CLASP activities that can be integrated with the software development process.

VulnerabilityView:CLASP identified 104 problem types that may form as a basis of security vulnerabilities which helps to identify what are the possible conditions in which threat can occur.

Vulnerability Use Cases assist project manager to identify attack surface and the associated vulnerabilities security services

CLASP Resources

CLASP provides list of resources which are being required to put in focus while planning implementing and performing activities

Following is the abstracted list of resources which are further categories into organization specific architecture and processes.

Basic principles of application security

Descriptions of core security principles

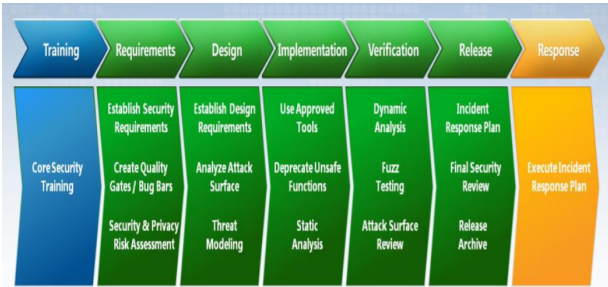
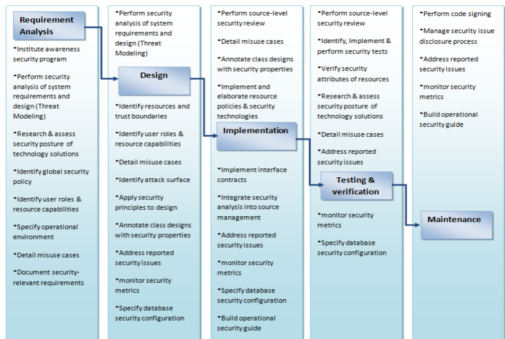
System assessment worksheet

Network resources

System resources

File system and registry

Sample road maps

FACTORS	MICROSOFT SDL	OWASP CLASP
STAGES IN THE LIFE CYCLE	1) Microsoft SDL(Security Development lifecycle): Training,Requirements,Design,Implementation ,Verification,Release,Response	1) Owasp CLASP(Comprehensive, Lightweight Application Security Process): Requirements & Analysis, Design ,Implementation, Testing & Verification, Maintenance
DIAGRAM	2) 	2) 
APPLICABILITY	3)Software development life cycle phases only (SDLC)	3)Any software development process
NATURE	4)Heavy weight	4)Light weight
CODE INTEGRITY CHECK	5)No	5)Yes
SUITABILITY	6)Large organization	6)Small and large sized organization
NATURE OF ACTIVITIES	7)Constructive	7)Constructive
ASSESSMENTS	8)SDL can only identify risk assessment cannot able to identify vulnerability assessment	8)CLASP can identify vulnerability assessment
SEPARATE PRIVACY REQUIREMENT EVALUATION	9)Yes	9)No
APPLICATION TESTING AND ASSESSMENT	10)Extensively	10)Through Threat Modeling,Code Level Review, Security Tests, but No Verification of security attributes of resources