|  |  |  |
| --- | --- | --- |
| Term or Topic | Your Explanation | How Used in Software Security? |
| **abstract syntax tree** |  |  |
| **active scanner** |  |  |
| **Agile methodology** |  |  |
| **alpha level testing** |  |  |
| **application decomposition** |  |  |
| **application security** |  |  |
| **application-centric threat modeling** |  |  |
| **AppSec** |  |  |
| **Architecture (A2) phase** |  |  |
| **asset-centric threat modeling** |  |  |
| **authenticated scans** |  |  |
| **Benchmarks** |  |  |
| **beta level testing** |  |  |
| **black box testing** |  |  |
| **Building Security In Maturing Model (BSIMM)** |  |  |
| **code review** |  |  |
| **Common Vulnerabilities and Exposures (CVE)** |  |  |
| **Common Vulnerability Scoring System (CVSS)** |  |  |
| **construction** |  |  |
| **control flow analysis** |  |  |
| **data flow analysis** |  |  |
| **data flow diagrams** |  |  |
| **denial of service** |  |  |
| **deployment phase** |  |  |
| **Design and Development (A3) phase** |  |  |
| **Design and Development (A4) phase** |  |  |
| **design phase** |  |  |
| **design review** |  |  |
| **digital enterprise** |  |  |
| **DREAD** |  |  |
| **dynamic analysis** |  |  |
| **elevation of privilege** |  |  |
| **end of life phase** |  |  |
| **environment hardening** |  |  |
| **exploratory tests** |  |  |
| **external resources** |  |  |
| **external scans** |  |  |
| **extreme programming** |  |  |
| **functional requirements** |  |  |
| **functional testing scripts** |  |  |
| **fuzz testing** |  |  |
| **governance** |  |  |
| **gray box testing** |  |  |
| **hardware** |  |  |
| **implementation phase** |  |  |
| **information disclosure** |  |  |
| **internal resources** |  |  |
| **internal scans** |  |  |
| **intrusive target search** |  |  |
| **legacy code** |  |  |
| **maintenance phase** |  |  |
| **measurement model** |  |  |
| **merger and acquisition** |  |  |
| **metric model** |  |  |
| **National Institute of Standards and Technology (NIST)** |  |  |
| **Nmap** |  |  |
| **non-functional requirements** |  |  |
| **NVD Database** |  |  |
| **Open Software Assurance Maturity Model (OpenSAMM)** |  |  |
| **Open-Source Security Testing Methodology Manual** |  |  |
| **Open Web Application Security Project (OWASP)** |  |  |
| **open-source software license compliance** |  |  |
| **open-source software security** |  |  |
| **Operational Enablement** |  |  |
| **OWASP Zed Attack Proxy** |  |  |
| **passive scanner** |  |  |
| **PASTA** |  |  |
| **penetration testing** |  |  |
| **planning phase** |  |  |
| **policy and compliance** |  |  |
| **Post-Release Support phase** |  |  |
| **privacy impact assessment** |  |  |
| **product risk profile** |  |  |
| **Product Security Incident Response Team (PSIRT)** |  |  |
| **pull request** |  |  |
| **repudiation** |  |  |
| **requirement phase** |  |  |
| **requirement traceability matrix** |  |  |
| **risk model** |  |  |
| **scripts** |  |  |
| **Scrum** |  |  |
| **secure architecture** |  |  |
| **secure code** |  |  |
| **secure testing scripts** |  |  |
| **Security Assessment (A1) phase** |  |  |
| **security development life cycle (SDL)** |  |  |
| **security requirements** |  |  |
| **security testing** |  |  |
| **Ship (A5) phase** |  |  |
| **software development life cycle (SDLC)** |  |  |
| **Software Security Champion (SSC)** |  |  |
| **software security policy** |  |  |
| **SonarQube** |  |  |
| **spider** |  |  |
| **spoofing** |  |  |
| **SQL injection** |  |  |
| **static analysis** |  |  |
| **strategy and metrics** |  |  |
| **STRIDE** |  |  |
| **system test** |  |  |
| **tampering** |  |  |
| **target machine** |  |  |
| **testing phase** |  |  |
| **third party codes** |  |  |
| **threat assessment (TA)** |  |  |
| **threat modeling** |  |  |
| **threat profile** |  |  |
| **threat source** |  |  |
| **threat vector** |  |  |
| **Trike** |  |  |
| **verification** |  |  |
| **virtualization** |  |  |
| **V-model** |  |  |
| **vulnerability** |  |  |
| **vulnerability assessments** |  |  |
| **vulnerability management (VM)** |  |  |
| **vulnerability scan** |  |  |
| **vulnerability sites** |  |  |
| **Waterfall methodology** |  |  |
| **white box testing** |  |  |
| **Zed Attack Proxy** |  |  |