DASSAULT SYSTEMES

SECURING THE **3DEXPERIENCE®** PLATFORM

OWASP AND APPLICATION SECURITY

WHITE PAPER

EXECUTIVE SUMMARY

As part of Dassault Systèmes efforts to counter threats of hacking, particularly in cloud deployments, security countermeasures are at the heart of our development process for the **3D**EXPERIENCE® platform. The Open Web Application Security Project standard (OWASP[1]) is used as a baseline as part of our security efforts.

WHAT IS OWASP?

The Open Web Application Security Project (OWASP) is a web security community dedicated to enabling organizations to develop, purchase, and maintain applications with the highest levels of security. The OWASP organization and community provides:

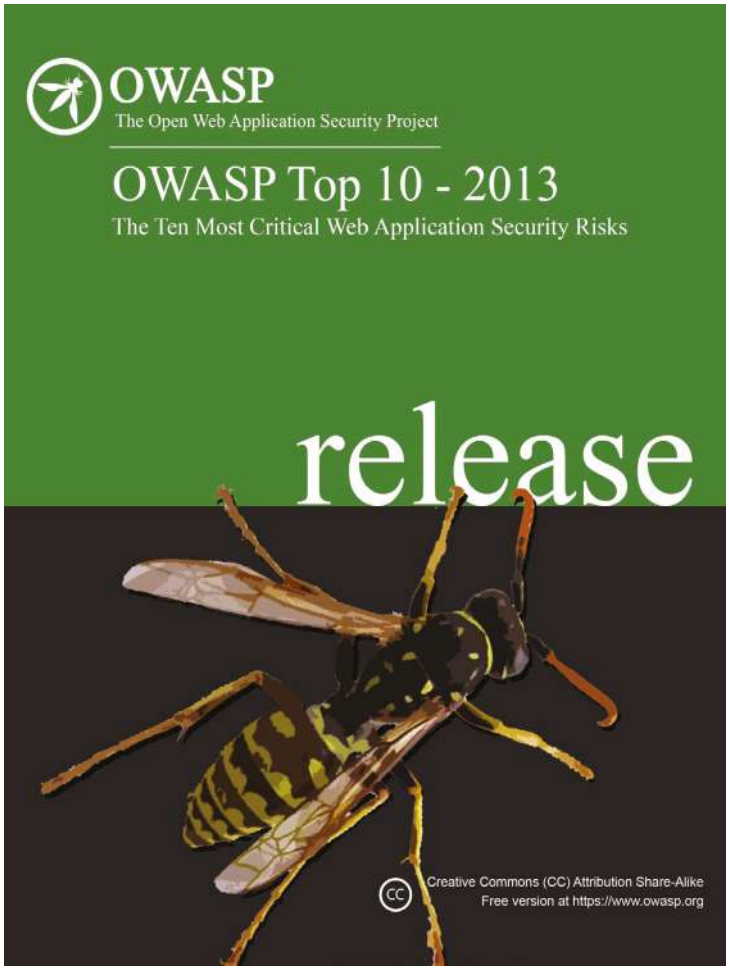
- Application security tools and standards
- Complete books on application security testing, secure code development, and secure code reviews
- OWASP methodologies
- Standard security controls and libraries

The OWASP organization has local chapters worldwide that provide cutting edge research, a range of conferences, and mailing lists for members. Their major publications include:

- OWASP Top 10
- Secure Coding Practices Quick Reference Guide
- OWASP Code Review Guide
- OWASP Application Security Verification
- OWASP Testing Guide

OWASP TOP 10 LIST

Of particular interest to Dassault Systèmes is the OWASP Top 10 list of threats against internet security. Published on a regular basis for educating developers, designers, architects, managers, and organizations, it documents the most important web application vulnerabilities and their consequences. It represents a broad consensus concerning the most critical security flaws, with the Top 10 list items selected and prioritized in combination with consensus estimates of exploitability, detectability, and impact on application security.



The standard is based on eight datasets from seven firms specializing in application security. It uses over half a million vulnerabilities detected across hundreds of organizations and thousands of applications. Included in the report are techniques to protect against these high risk problem areas and where to go for more information. This Top 10 list is referenced by a wide array of standards, books, tools, and organizations.

[1] OWASP and all related references to the OWASP Top 10 are copyrighted content and/or trademarks of the OWASP Foundation. Copyrighted contents are covered under the Creative Commons Attribution ShareAlike 3.0 License. This Top 10 list is referenced by a wide array of standards, books, tools, and organizations.

For an example, see the illustration below detailing the Top 10 risks from 2013:

A1 –INJECTION	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2 – BROKEN AUTHETICATION ADN SESSION MANAGEMENT	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys or session tokens, or to exploit other implemantation flaws to assume other users' identities.
A3 – CROSS-SITE SCRIPTING (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A4 – INSECURE DIRECT OBJECT REFERENCES	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
A5 – SECURITY MISCONFIGURATION	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
A6 – SENSITIVE DATA EXPOSURE	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected such as encryption at rest or in transit, as well as special precautions when exchanged with teh brower.
A7 – MISSING FUNCTION LEVEL ACCESS CONTROL	Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.
A8 – CROSS-SITE REQUEST FORGERY (CSRF)	A CSRF attack forces a logged_on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
A9 – USING COMPONENTS WITH KNOWN VULNERABILITIES	Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such as attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.
A10 – UNVALIDATED REDIRECTS AND FORWARDS	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

OWASP AND 3DEXPERIENCE PLATFORM APPLICATION SECURITY PROGRAM

The **3D**EXPERIENCE® platform puts particular and specific emphasis on platform security during R&D processes. This includes in-house training for developers and quality groups with particular emphasis on relevant OWASP topics and includes countermeasures against other vulnerabilities. Taking security even further, our SaaS (Software as a Service) platform is released on the cloud after we perform an external test against the entire **3D**EXPERIENCE® platform to help ensure that known vulnerabilities from the OWASP Top 10 are covered and secured in our code. Note that specific fixes are not documented externally, so as to limit information to would-be hackers while providing the guidance necessary to use the platform.

APPLICATIONS AND DATA PROTECTION

Protecting your data is important to us. The **3D**EXPERIENCE® platform is built and deployed with extensive protections against critical Web Applications security risks and vulnerabilities.
The **3D**EXPERIENCE® platform uses strong universal best practices for authentication, access control, encryption, injection detection and prevention, auditing and server hardening, as part of the effort to protect the confidentiality, integrity, and availability of data.

The **3D**EXPERIENCE® platform closely follows several industry standards, such as, MITRE CWE (Common Weakness Enumeration) and many of the OWASP best practices, most notably:

AUTHENTICATION	• OWASP Authentication • OWASP Password Storage • OWASP Access Control
CONFIDENTIALITY & INTEGRITY	• OWASP Session Management • OWASP Access Control
ENCRYPTION	• OWASP Transport Layer Protection
INJECTION, SCRIPTING, HARDENING	• OWASP Input Validation • OWASP XSS • OWASP SQL Injection
MONITORING & AUDIT	• OWASP Logging

AUTHENTICATION

A Secure Authentication mechanism supports SSO capabilities within **3D**EXPERIENCE® platform services. Users should be fully authenticated to be able to access data, and assigned specific licenses and policies, while events and actions remain traceable. Certificates are managed by a certificate authority and key stores. There is a strong password policy and strong user policy for access control lists in order to protect the **3D**EXPERIENCE® platform against brute force, privilege escalations, and session hijacking.

CONFIDENTIALITY AND INTEGRITY

Access to data stored in the **3D**EXPERIENCE® platform is restricted via access lists to only the roles, organizations, and/or collaborative spaces that have been authorized for access. The mechanisms are implemented in the business logic and the database to help ensure data integrity and strict confidentiality throughout the lifecycle of the data.

ENCRYPTION

Primary defenses are implemented to keep out attackers and control access.The **3D**EXPERIENCE® platform deploys strong encryption to protect data from being accessed by attackers while in transport, and strong access controls, when the data is stored (see the above paragraph about Confidentiality). File transfers on the cloud are secured via HTTPS/TLS encryption and use a strong key cypher for data access.

INJECTION, SCRIPTING, AND PARSER HARDENING

The **3D**EXPERIENCE® platform was designed to be resilient to injection flaws and attacks, like SQL, Parameter, Commands, and OS Injections. Methods and pages employ several layers to protect against cross-site scripting (XSS). XML Parsers are hardened using best practices to protect against XML External Entity attacks. The software architecture embeds input validation, and the use of parameterized interface is encouraged and monitored for compliancy.

MONITORING & AUDIT

Monitoring capabilities are deployed to critical operations, providing vital functional, performance, and secure operational data in real-time. Events, actions, and activities are logged and retained, to allow investigative actions and audit trail.

INFRASTRUCTURE SECURITY AND THE 3DEXPERIENCE PLATFORM

Security must start with a strong foundation. The on cloud **3D**EXPERIENCE® platform is hosted in a secure data center where the operating systems, servers, and software are all hardened, patched, and kept up-to-date. The communications with the platform are filtered and segmented by firewalls, and the network is monitored 24/7/365. See the white paper entitled "Cloud Security", also available from Dassault Systèmes.

CONCLUSION

Security is paramount for any application exposed to the internet today. With the **3D**EXPERIENCE® platform, Dassault Systèmes uses OWASP as a baseline as part of our efforts to provide a high level of protection with our solutions for our customers and their data. Immediate implementation of countermeasures for the OWASP Top 10 list as well as any other vulnerability is one of the highest priorities for our R&D organization. We also go beyond OWASP when it is seen as a business priority. You can feel assured when using the **3D**EXPERIENCE® platform that it is deployed using these countermeasures as part of our efforts to help protect your data.

GENERAL THREAT GLOSSARY AND PREVENTIVE APPROACHES

• Spoofing

To spoof is to impersonate a user or process in an unauthorized way. A malicious user might change the contents of a cookie to pretend that he is a different user or that the cookie comes from a different server. In general, you can help prevent spoofing by using stringent authentication and keeping credential information safe.

• Tampering

Changing or deleting a resource without authorization. One example is defacing a web page, where a malicious user gets into your site and changes files. An indirect way to tamper is by using a script exploit where a malicious user manages to get code (script) to execute on your website by masking it as user input from a page or as a link.

• Repudiation

A repudiation threat involves making a transaction in such a way that there is no proof after the fact of the principals involved. In a web application, this can mean impersonating an innocent user's credentials. You can help guard against repudiation by using stringent authentication and auditing legs.

• Information Disclosure

Information disclosure simply means stealing or revealing information that is supposed to be private. A typical example is stealing passwords, but information disclosure can involve access to any file or resource on the server. The best defenses are encryptions, hashing, and authentication.

• Denial of Service

A denial of service attack is to deliberately cause an application to be less available than it should be. A typical example is to overload a web application so that it cannot serve ordinary users. Alternatively, malicious users might try to simply crash your server. Defenses include limiting the number of requests that will be served, blocking IPs, and using a white list or black list.

• Elevation of Privilege

An elevation-of-privilege attack is to use malicious means to get more access to the underlying machine than normally assigned. For example, in a successful elevation-of-privilege attack, a malicious user manages to get administrative privileges to your web server for access to any data on the server as well as control over server capabilities. To help protect against elevation of privilege, you can run the application in a low-privilege context, if practical.

• **Cross-Site Scripting**

Cross-Site Scripting (XSS) attacks are a type of injection problem in which malicious scripts are injected into otherwise benign and trusted web sites. XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites. Main countermeasures are XSS Input validation and XSS Output escaping.

• **XML External Entities**

XML External Entities (XXE) is an attack technique that takes advantage of a feature of XML to build documents dynamically at the time of processing. An XML message can either provide data explicitly or by pointing to a URL where the data exists. In the attack technique, external entities may replace the entity value with malicious data, alternate referrals, or may compromise the security of the data the server/XML application can access. The main countermeasure is XML parser hardening, mainly disabling external entities.

DASSAULT SYSTEMES | The **3D**EXPERIENCE® Company

Americas
Dassault Systèmes
175 Wyman Street
Waltham, Massachusetts
02451-1223
USA

Europe/Middle East/Africa
Dassault Systèmes
10, rue Marcel Dassault
CS 40501
78946 Vélizy-Villacoublay Cedex
France

Asia-Pacific
Dassault Systèmes K.K.
ThinkPark Tower
2-1-1 Osaki, Shinagawa-ku,
Tokyo 141-6020
Japan