

# Cenzic Products

## Common Weakness Enumeration (CWE) Compatibility

Cenzic Enterprise, Cenzic Desktop, Cenzic Cloud and Cenzic Mobile products are compatible with the CWE standard or Common Weakness Enumeration as maintained by Mitre Corporation. Application security assessment results from the Cenzic product suite are mapped to the relevant CWE IDs providing users with additional information to classify and describe common weaknesses found in applications.

For additional details on CWE, please visit: <http://cwe.mitre.org/index.html>

Following is a mapping between Cenzic's SmartAttacks® and CWE IDs.

Cenzic SmartAttack Name	CWE ID/s
Application Exception	CWE-388: Error Handling
Application Exception (WS)	CWE-388: Error Handling
Application Path Disclosure	CWE-200: Information Leak (rough match)
Authentication Bypass	CWE-89: Failure to Sanitize Data into SQL Queries (aka 'SQL Injection') (rough match)
Authorization Boundary	CWE-285: Missing or Inconsistent Access Control, CWE-425: Direct Request ('Forced Browsing')
Blind SQL Injection	CWE-89: Failure to Sanitize Data into SQL Queries (aka 'SQL Injection')
Blind SQL Injection (WS)	CWE-89: Failure to Sanitize Data into SQL Queries (aka 'SQL Injection')
Browse HTTP from HTTPS List	CWE-200: Information Leak
Brute Force Login	CWE-521: Weak Password Requirements
Buffer Overflow	CWE-120: Unbounded Transfer ('Classic Buffer Overflow')
Buffer Overflow (WS)	CWE-120: Unbounded Transfer ('Classic Buffer Overflow')
Check Basic Auth over HTTP	CWE-200: Information Leak
Check HTTP Methods	CWE-650: Trusting HTTP Permission Methods on the Server Side
Cookie Vulnerabilities	CWE-539: Information Leak Through Persistent Cookies, CWE-614: Sensitive Cookie in HTTPS Session Without "Secure" Attribute
Credit Card Disclosure	CWE-359: Privacy Violation
Cross-Frame Scripting	CWE-293: Using Referrer Field for Authentication



Cross-Site Scripting	CWE-79: Failure to Sanitize Directives in a Web Page (aka 'Cross-site scripting' (XSS))
Database Server Version Checks	CWE-200: Information Leak
Detect Off-Site Images	CWE-673: External Influence of Sphere Definition
Directory Browsing	CWE-548: Information Leak Through Directory Listing
Document Caching	CWE-525: Information Leak Through Browser Caching
External Applet, Script, or Object	CWE-673: External Influence of Sphere Definition
File & Directory Discovery	CWE-552: Files or Directories Accessible to External Parties
Form Caching	CWE-525: Information Leak Through Browser Caching
Format String	CWE-134: Uncontrolled Format String
Format String (WS)	CWE-134: Uncontrolled Format String
GET for POST	CWE-20: Insufficient Input Validation
HTML & JavaScript Comments	CWE-615: Information Leak Through Comments
HTTP Response Splitting	CWE-113: Failure to Sanitize CRLF Sequences in HTTP Headers (aka 'HTTP Response Splitting')
Ineffective Session Termination	CWE-613: Insufficient Session Expiration
Integer Overflow	CWE-190: Integer Overflow (Wrap or Wraparound), CWE-680: Integer Overflow to Buffer Overflow
J2EE Session ID Length	CWE-6: J2EE Misconfiguration: Insufficient Session-ID Length
LDAP Injection	CWE-90: Failure to Sanitize Data into LDAP Queries (aka 'LDAP Injection')
LDAP Exception	CWE-90: Failure to Sanitize Data into LDAP Queries (aka 'LDAP Injection'), CWE-388: Error Handling
Lockout	CWE-521: Weak Password Requirements
Login Redirect	CWE-525: Information Leak Through Browser Caching
Non-masked Password	CWE-549: Missing Password Field Masking
Non-SSL Form	CWE-201: Information Leak Through Sent Data
Non-SSL Password	CWE-201: Information Leak Through Sent Data CWE 261: Weak Cryptography for Passwords
Open Redirect	CWE-601: URL Redirection to Untrusted Site
Parameter Addition	CWE-20: Insufficient Input Validation



Password Autocomplete	CWE-525: Information Leak Through Browser Caching
Password Change	CWE-521: Weak Password Requirements
Phishing Referrer Trust	CWE-293: Using Referrer Field for Authentication
PHP & Perl Code Injection	CWE-94: Code Injection
Platform Path Disclosure	CWE-209: Error Message Information Leaks
Privacy Notification	CWE-359: Privacy Violation
Privilege Escalation	CWE-264: Permissions, Privileges, and Access Controls
Register Password	CWE-521: Weak Password Requirements
Remote File Inclusion	CWE-98: Insufficient Control of Filename for Include/Require Statement in PHP Program
Session Fixation	CWE-384: Session Fixation
Session Hijacking	CWE-264: Permissions, Privileges, and Access Controls
Session ID Randomness	CWE-334: Small Space of Random Values
Social Insurance Disclosure	CWE-359: Privacy Violation
Social Security Disclosure	CWE-359: Privacy Violation
SQL Disclosure	CWE-566: Access Control Bypass Through User-Controlled SQL Primary Key
SQL Disclosure (WS)	CWE-566: Access Control Bypass Through User-Controlled SQL Primary Key
SQL Error Message	CWE -209: Error Message Information Leaks
SQL Error Message (WS)	CWE -209: Error Message Information Leaks
SSI Injection	CWE-97: Failure to Sanitize Server-Side Includes (SSI) Within a Web Page
Unix Command Injection	CWE-78: Failure to Sanitize Data into an OS Command (aka 'OS Command Injection')
Unix Command Injection (WS)	CWE-78: Failure to Sanitize Data into an OS Command (aka 'OS Command Injection')
Unix Relative Path	CWE-22: Path Traversal
Unix Relative Path (WS)	CWE-22: Path Traversal
URL In Query	CWE-598: Information Leak Through Query Strings in GET Request
Username or Password in HTTP Request	CWE-200: Information Leak
	CWE 261: Weak Cryptography for Passwords



Weak Password	CWE-521: Weak Password Requirements
Web Server Configuration Vulnerabilities	CWE-529: Information Leak Through Access Control List Files CWE-552: Files or Directories Accessible to External Parties
Web Server Miscellaneous Vulnerabilities	CWE-200: Information Leak
Web Server Version Vulnerabilities	CWE-200: Information Leak
Web Server Vulnerabilities	CWE-200: Information Leak
Windows Command Injection	CWE-78: Failure to Sanitize Data into an OS Command (aka 'OS Command Injection')
Windows Command Injection (WS)	CWE-78: Failure to Sanitize Data into an OS Command (aka 'OS Command Injection')
Windows Relative Path	CWE-22: Path Traversal
Windows Relative Path (WS)	CWE-22: Path Traversal

## Cenzic Products

Cenzic Enterprise	Cenzic Enterprise is a software solution that assesses the security of Cloud and Web applications and supports security risk management throughout the software development lifecycle. Cenzic Enterprise provides a company-wide view of security vulnerabilities and status to executives as well as customized views for other users from a Web-based dashboard.
Cenzic Desktop	Cenzic Desktop is a single-user version of Cenzic Enterprise. It is designed for the power user that wants to run their security assessments on Cloud and Web applications from a single system.
Cenzic Managed Cloud	With Cenzic Managed Cloud, Cenzic's security experts remotely perform full vulnerability testing on Cloud, Mobile and Web applications. From a Web-based dashboard, users can request assessments, view results, run reports, analyze trends and re-test applications to verify remediation efforts.
Cenzic Cloud	Cenzic Cloud allows users to test their own Cloud and Web applications for basic attacks and receive actionable results all within their own Web portal – no security experts needed.
Cenzic Hybrid – Software + Cloud	Cenzic Hybrid provides access to both Cenzic Enterprise software and Cenzic Managed Cloud services. Vulnerability testing can be done either by using the software on premise or by leveraging Cenzic's expert security services team.
Cenzic Mobile	Cenzic Mobile service is delivered as a managed service. Cenzic's security experts remotely perform full vulnerability testing on mobile applications. All testing is managed from a Web-based dashboard where users can request assessments, view results, run reports, analyze trends and re-test applications to verify remediation efforts.
Cenzic Services	Cenzic services and training help those responsible for Cloud, Mobile and Web application security to implement best practices and procedures to protect data from hacker attacks.

## About Cenzic

Cenzic provides an application security intelligence platform to continuously assess Cloud, Mobile and Web vulnerabilities. This helps brands of all sizes protect their reputation and manage security risk in the face of malicious attacks. Today, Cenzic secures more than half a million online applications and trillions of dollars of commerce for Fortune 1000 companies, all major security companies, government agencies, universities and SMBs.