Continuous Dynamic OWASP Top 10 Coverage

Continuous Dynamic

Black Duck® Continuous Dynamic is a software-as-a-service (SaaS) production safe, continuous assessment dynamic application security testing (DAST) solution that allows your business to quickly deploy a scalable web security program. No matter how many websites you have or how often they change, Continuous Dynamic can scale to meet any demand. It provides security and development teams with fast, accurate, and continuous vulnerability assessments of applications in QA and production, applying the same techniques hackers use to find weaknesses, so you can remediate them before the bad guys exploit them.

This table outlines the OWASP Top 10 categories and the corresponding CWEs covered by our service levels.

		PE	SE	BE
A01:2021 – Broken Access Control				
Directory Indexing	CWE-548	Yes	Yes	Yes
Insecure Indexing	CWE-548	Yes	No	No
Insufficient Authorization	CWE-287	Yes	No	No
Insufficient Process Validation	CWE-424, CWE-425	Yes	No	No
Path Traversal	CWE-35	Yes	Yes	Yes
Predictable Resource Location	CWE-425	Yes	Yes	Yes
URL Redirector Abuse	CWE-601	Yes	Yes	Yes
Cross-Site Request Forgery	CWE-352	Yes	Yes	Yes
A02:2021 – Cryptographic Failures				
Insufficient Transport Layer Protection	CWE-319, CWE-311	Yes	Yes	Yes
Session Prediction	CWE-330	Yes	No	No

		PE	SE	BE
A03:2021 – Injection				
Application Code Execution	CWE-94	Yes	Yes	Yes
Cross-Site Scripting	CWE-79	Yes	Yes	Yes
HTTP Response Splitting	CWE-113	Yes	Yes	Yes
Improper Input Handling	CWE-20	Yes	Yes	Yes
LDAP Injection	CWE-90	Yes	No	No
Mail Command Injection	CWE-77	Yes	Yes	Yes
OS Command Injection	CWE-78	Yes	Yes	Yes
Query Language Injection	CWE-943	Yes	No	No
SQL Injection	CWE-89	Yes	Yes	Yes
SSI Injection	CWE-97	Yes	Yes	Yes
XML Injection	CWE-91	Yes	Yes	Yes
XPath Injection	CWE-643	Yes	Yes	Yes
XQuery Injection	CWE-652	Yes	Yes	Yes
OS Commanding	CWE-78	Yes	Yes	Yes
Routing Detour	CWE-610	Yes	No	No
A04:2021 – Insecure Design				
Cacheable Sensitive Response	CWE-525	Yes	No	No
Frameable Resource	CWE-1021	Yes	No	No
Abuse of Functionality	CWE-840	Yes	Yes	Yes
Brute Force	CWE-799	Yes	Yes	Yes
Clickjacking	CWE-1021	Yes	No	No
Insufficient Antiautomation	CWE-799	Yes	No	No

		PE	SE	BE
A05:2021 – Security Misconfiguration				
Application Misconfiguration	CWE-16	Yes	Yes	Yes
Autocomplete Attribute	CWE-16, CWE-525, CWE-200	Yes	No	No
Fingerprinting	CWE-497	Yes	Yes	Yes
Information Leakage	CWE-200, CWE-202, CWE-544, CWE-550, CWE-209, CWE-703	Yes	Yes	Yes
Non-HttpOnly Session Cookie	CWE-1004	Yes	No	No
Server Misconfiguration	CWE-16	Yes	Yes	Yes
Unsecured Session Cookie	CWE-614	Yes	No	No
XML External Entities	CWE-611	Yes	Yes	Yes
Missing Secure Headers	CWE-693	Yes	Yes	Yes
A06:2021 – Vulnerable and Outdated Components				
Unpatched Software	CWE-1104	Yes	No	No
A07:2021 – Identification and Authentication Failures				
Insufficient Authentication	CWE-285	Yes	No	No
Insufficient Password Policy Implementation	CWE-521	Yes	No	No
Insufficient Password Recovery	CWE-640	Yes	No	No
Insufficient Session Expiration	CWE-613	Yes	No	No
Session Fixation	CWE-384	Yes	No	No
A08:2021 – Software and Data Integrity Failures				
Content Spoofing	CWE-451, CWE-345, CWE-148	Yes	Yes	Yes
Remote File Inclusion	CWE-829	Yes	Yes	Yes
A10:2021 - Server-Side Request Forgery				
Server-Side Request Forgery	CWE-918	Yes	No	No
A11:2021 - Denial of Service				
Denial of Service	CWE-400	Yes	Yes	Yes
A11:2021 - Memory Management Errors				
Buffer Overflow	CWE-788	Yes	No	No

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.

©2024 Black Duck Software, Inc. All rights reserved. Black Duck is a trademark of Black Duck Software, Inc. in the United States and other countries. All other names mentioned herein are trademarks or registered trademarks of their respective owners. October 2024