General
McAfee secures websites by testing for software security using industry standards like the Open Web Application Security Project (OWASP) Top 10. OWASP is an open source organization dedicated to securing software. The organization a top 10 list of the most prevalent and most damaging software security vulnerabilities. McAfee information security specialists on the Vulnerability Management team conduct automated and manual web application security testing against these vulnerabilities. We also test and secure our own websites—internal and external—both with credentials and without credentials. Testing includes logic, session management, and authentication and authorization. Many active OWASP members—current and former chapter and project leads—work at McAfee and are involved with testing and securing McAfee websites.

The latest OWASP Top 10 are derived from these software security vulnerability categories:

1. Injection
2. Broken authentication
3. Sensitive data exposure
4. XML external entities (XXE)
5. Broken access control
6. Security misconfiguration
7. Cross-site scripting (XSS)
8. Insecure serialization
9. Using components with known vulnerabilities
10. Insufficient logging and monitoring
11. Cross-site request forgery

https://www.owasp.org/index.php/Main_Page

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2020 McAfee, LLC. 4403_0120
JANUARY 2020