Protecting Against the 10 Most Critical Web Security Risks

1. Injection
   - Security Risk: Attackers inject malicious code into a web application's input fields, leading to a variety of的危害s.
   - Sitefinity CMS Protects: Uses parameterized query execution and provides an entirely parameterized interface, ensuring no single method can be executed without privileges.

2. Broken Authentication
   - Security Risk: Users can be impersonated or accounts hijacked.
   - Sitefinity CMS Protects: Uses the default authentication based on OAuth 2.0 and OpenID Connect, and provides an easy infrastructure for deploying and applying security standards such as FIPS.

3. Sensitive Data Exposure
   - Security Risk: Sensitive data can be accessed or exposed.
   - Sitefinity CMS Protects: Stores the minimal set of sensitive data that is required and provides a logging mechanism that is extensible and can be customized.

4. XML External Entities (XXE)
   - Security Risk: Attackers can use malicious XML documents to reveal sensitive information.
   - Sitefinity CMS Protects: With the number of standard and security breaches in processing web applications, Sitefinity provides an easy infrastructure for deploying and applying security standards such as FIPS to prevent broken authentication.

5. Broken Access Control
   - Security Risk: Users can access unauthorized resources or actions.
   - Sitefinity CMS Protects: Use of the serializers securely.

6. Security Misconfiguration
   - Security Risk: Configuration settings are not correctly implemented, resulting in access to admin interfaces, error messages in the clear, and other vulnerabilities.
   - Sitefinity CMS Protects: Sitefinity provides a mechanism that is extensible and can be customized.

7. Cross-Site Scripting (XSS)
   - Security Risk: Attackers inject malicious scripts into web applications or websites.
   - Sitefinity CMS Protects: Sitefinity uses three authentication models that comply with industry standards such as FIPS and runs on the latest .NET Framework.

8. Using Components with Known Vulnerabilities
   - Security Risk: Components with vulnerabilities can be used to attack applications.
   - Sitefinity CMS Protects: Sitefinity uses components with the number of standard and security breaches in processing web applications, Sitefinity provides an easy infrastructure for deploying and applying security standards such as FIPS to prevent broken authentication.

9. Insecure Deserialization
   - Security Risk: Deserialization attacks can lead to remote code execution.
   - Sitefinity CMS Protects: Sitefinity does both; it calls the underlying provider that manages the data access through Data Access ORM.

10. Insufficient Logging and Monitoring
    - Security Risk: Attackers can exploit vulnerabilities without detection.
    - Sitefinity CMS Protects: Without sufficient logging and monitoring measures, it may take enterprises even longer to detect attacks and breaches, which could lead to an even greater financial impact.