

1. Overview

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment.

2. Purpose

The purpose of this policy is to define web application security assessments within TSD. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of TSD services available both internally and externally as well as satisfy compliance with any relevant policies in place.

3. Scope

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at TSD.

All web application security assessments will be performed by delegated security personnel either employed or contracted by TSD. All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of TSD is strictly prohibited unless approved by the Chief Information Officer.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

4. Policy

4.1 Web applications are subject to security assessments based on the following criteria:

4.1.1 New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.

4.1.2 Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.

4.1.3 Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.

4.1.4 Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

4.1.5 Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

4.1.6 Annual Review – all applications will be subject to a full annual review in its entirety to review potential risks of functionality and/or architecture.

4.2 All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

4.2.1 High – Any high-risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.

4.2.2 Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.

4.2.3 Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

4.3 The following security assessment levels shall be established by the InfoSec organization or other designated organization that will be performing the assessments.

4.3.1 Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.

4.3.2 Quick – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.

4.3.3 Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

4.4 The current approved web application security assessment tools in use which will be used for testing are:

- Veracode
- Checkmarx SAST
- Burp Suite Professional
- InsightAppSec
- Codacy
- GitLab
- Web Application Scanning (WAS)
- SonarQube
- GitHub Enterprise

Other tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All application releases must pass through the change control process. Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Information Officer.

6. Related Standards, Policies and Processes

[OWASP Top Ten Project](#)

[OWASP Testing Guide](#)

[OWASP Risk Rating Methodology](#)

7. Definitions and Terms

None

8. Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.
Oct 2022	SANS Policy Team	Converted to new format.