Web Application Security Assessment Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose

The purpose of this policy is to define web application security assessments within **<ORGANIZATION>**. 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 **<ORGANIZATION>** services available both internally and externally as well as satisfy compliance with any relevant policies in place.

2.0 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 **<ORGANIZATION>**.

All web application security assessments will be performed by delegated security personnel either employed or contracted by **<ORGANIZATION>**. All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of **<ORGANIZATION>** 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.

3.0 Policy

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

- **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.

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

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

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

- **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.

3.1 Risk

Security issues that are discovered during assessments will be mitigated based upon the following risk levels. Risk rating will be based on the OWASP Risk Rating Methodology

- **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.

- **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.

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

Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

3.2 Tools

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

- <Tool/Application 1>

- <Tool/Application 2>

- …

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.

3.3 Security Assessment Level

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.

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.

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

3.4 Duration

The default duration of a web application assessment will be <X> days time for the purpose of project planning and will be modified accordingly based upon the size and scope of the application functionality.

3.5 Exemptions

Exemptions to the need for a security assessment will be made by the Chief Information Officer or delegated manager based on risk and criticality of needed application changes/functionality/architecture. Exemptions will assume the associated risk and will be documented as required by the change control policies.

4.0 Responsibilities

Security Engineering will be responsible for web application scoping, assessment, determination of discovered issue risk, and reporting to Project Management and application stakeholders.

Project Management and application stakeholders will be responsible for the appropriate assessment scheduling and remediation efforts based upon assessment findings and Security Engineering recommendations.

5.0 Enforcement

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.

6.0 Definitions

- **Web Application** – Any service that accepts and processes HTTP/HTTPS protocols.
- **Major Release** – a significant application software update/code change such as a new interface design programming platform change, etc.
- **Point Release** – An application software update/code change as part of the application lifecycle.
- **Patch Release** – An application software update/code change that addresses a bug or flaw.

7.0 References

- **OWASP Top Ten Project**: http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- **OWASP Testing Guide**: http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf
- **OWASP Risk Rating Methodology**: http://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

8.0 Revision History

- **Version 1.0 – John Hally 1/4/11**