Web Application Security Policy

Provided by ilmCon GmbH

---

1. **Overview**

   Vulnerabilities in web applications constitute the majority of attack vectors beyond malware. It is essential that every web application undergo vulnerability assessments and that any identified vulnerabilities are addressed before production deployment.

---

2. **Purpose**

   This policy aims to outline the framework for web application security assessments at ilmCon GmbH. Such assessments are conducted to uncover potential or actual weaknesses arising from inadvertent misconfigurations, inadequate authentication, poor error handling, unintentional leakage of sensitive information, and similar issues. Identifying and mitigating these concerns will reduce the attack surface of ilmCon services available internally and externally, while ensuring compliance with all pertinent policies.

---

3. **Scope**

   This policy encompasses all web application security assessments requested by any individual, group, or department to maintain the security posture, ensure compliance, manage risk, and control changes for the technologies utilized at ilmCon.

   All web application security assessments shall be carried out by designated security personnel, whether employed directly or contracted by ilmCon. All findings are deemed confidential and will be shared only with individuals who require the information. Sharing any findings externally is strictly prohibited unless authorized by the Chief Information Officer.

   Any interrelationships within multi-tiered applications identified during the scoping phase will be incorporated into the assessment unless explicitly excluded. Any exclusions along with their justifications will be documented before the assessment begins.

---

4. Policy

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

4.1.1 New or Major Application Release -- A comprehensive assessment must be completed before changing control documentation approval and/or production deployment.

4.1.2 Third Party or Acquired Web Application -- A complete assessment is required, after which the application must conform to policy requirements.

4.1.3 Point Releases -- Assessment depth will be determined by the risk level associated with changes in application functionality and/or architecture.

4.1.4 Patch Releases -- Assessment level will be based on risk evaluation of changes to application functionality and/or architecture.

4.1.5 Emergency Releases -- Under authorization from the Chief Information Officer or designated manager, emergency releases may proceed without security assessment, accepting inherent risks until proper assessment can be conducted.

4.2 Security issues discovered during assessments require mitigation according to the following risk levels, based on the OWASP Risk Rating Methodology. For medium or higher risk issues, remediation validation testing is mandatory to confirm the effectiveness of fixes and mitigation strategies.

4.2.1 High -- Immediate resolution or implementation of mitigation strategies is required for high-risk issues before deployment. Applications with high-risk issues may be suspended or blocked from production deployment.

4.2.2 Medium -- Medium-risk issues require review to determine mitigation requirements and implementation timeline. Applications may be suspended or blocked from production deployment if multiple medium-risk issues collectively present unacceptable risk levels. Issues should be addressed in

patch/point releases unless other mitigation strategies can effectively reduce exposure.

4.2.3 Low – Issues require review to determine correction requirements and implementation schedule.

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:

- Postman

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 monitor compliance through various channels, including business tool reports, internal and external audits, and policy owner feedback.

5.2 Exceptions – The Infosec team must approve any policy exceptions 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. Revision History

Date of Change	Responsible	Summary of Change
Feb 2025	ilmCon GmbH	Initial release.