Web Application Security

Document Classification:	**Public**
Document Ref.	**ISMS-DOC-A14-6**
Version:	**1.0.4**
Dated:	**06 November 2017**
Document Author:	**John Moylan**
Document Owner:	

Revision History

Version	Date	Revision Author	Summary of Changes
1	7/4/2016	John Moylan	Initial Draft
1.0.2	11/4/2016	John Moylan	Additional section 5.1, 'Ownership'
1.0.3	13/4/2016	John Moylan	Additions from Technology Security team & reclassified Public
1.1.0	6/11/2017	John Moylan	Reviewed and Published in New template

Distribution

Name	Title

Approval

Name	Position	Signature	Date

Contents

1 Introduction

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 by remediated prior to production deployment.

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

This policy covers all web application security assessments and responsibilities for a group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at RTÉ.

All web application security assessments will be performed by delegated security personnel either employed or contracted by RTÉ. All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of RTÉ is strictly prohibited unless approved by the Chief Technology Officer (CTO), or his/her delegate.

2 Web Application Security Policy

All Web applications, both internal and external are subject to security assessments based on the following criteria:

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.
2. Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.
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. Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
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 Technology Security team or an appropriate manager who has been delegated this authority by the CTO.
6. Externally facing applications - will be required to undergo regular monthly scans which may at the discretion of the Information Security team replace the scans at 3,4,5 above.

2.2 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.

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.
2. Medium – Any 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.
3. Low – Any low risk Issues should be reviewed to determine what is required to correct the issue and scheduled accordingly.

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

• Edgescan
• Nessus

Application owners may be required to whitelist the IP addresses used for authorised testing.

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 Information team.

3 Policy Compliance

3.1 Ownership

Every web application must have a documented owner. The owner is a necessary point of contact in case any issues are detected, for ensuring that risks are mitigated and for budgeting for security scans based on estimates that will be provided by the Information security team.

3.2 Compliance Measurement

The Information security team will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

3.3 Exceptions

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

3.4 Non-Compliance

Any application found to be in violation of this policy may be removed at the discretion of the CTO or his/her delegate. 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 Infosec team or an appropriate manager who has been delegated this authority by the CTO.

4 Related Standards, Policies and Processes

OWASP Top Ten Project
OWASP Testing Guide
OWASP Risk Rating Methodology
http://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

5 Definitions and Terms

None.