

Policy and Guidance for Web Application Penetration Testing



EAST RIDING
OF YORKSHIRE COUNCIL

Lead Directorate and Service:	Corporate Resources - Digital Change and Technology
Effective Date:	*
Contact Officer/Number:	David Cox - ICT Security Manager
Approved By:	Cabinet

Contents

Policy and Guidance for Web Application Penetration Testing

1. Introduction.....	1
2. Scope.....	1
3. Corporate Requirements	1
4. Policy Development Including Consultation	1
5. Links with Other Policies	1
6. Policy Guidelines and Procedures	2
7. Policy Implications	2
8. Policy Compliance.....	Error! Bookmark not defined.
9. Financial Implications	3
10. Review	3

Policy and Guidelines for Web Application Penetration Testing

1. Introduction

East Riding of Yorkshire Council (ERYC) are making ever increasing use of Information and Communication Technology (ICT) and customer information held by the council and other public sector organisations. The information that ERYC holds, processes, maintains and shares with other public sector organisations is an important asset that, like other important business assets, needs to be suitably protected.

Penetration testing simulates a real-world attack to achieve an objective, or objectives, in a target environment. It attempts to exploit vulnerabilities by discovering coding bugs, configuration errors, weak authentication. This is done to identify and remove vulnerabilities before they are discovered and exploited. The identification and removing vulnerabilities protects the confidentiality, integrity and availability of the council's IT systems and data.

2. Scope

A discussion with the IT Security Team will help identify when an full independent Penetration Test is required, or when utilising the available web application scanning tools currently at the ICT security teams disposal are appropriate.

This requirement is a key Security Principle within the IT Security Policy Framework, supporting the Principle that "IT Security will not be compromised (physically, virtually, Quality and Cost)".

3. Corporate Requirements

Penetration testing (or vulnerability testing) must be undertaken:

- Against new web sites, applications and modules or existing sites and modules which have undergone an upgrade of infrastructure, functionality, or major release upgrade.
- Annually to ensure that no new vulnerabilities have been discovered (this will generally be undertaken as a part of the council's Public Services Network and Cyber Essentials Plus accreditation).

4. Policy Development Including Consultation

This Policy has been developed in consultation with:

- Corporate Management Team.
- Senior Management Team.
- Information Governance Management Board.
- Portfolio Holder.
- Head of Digital, Change & Technology
- Head of Legal and Democratic Services and Senior Information Risk Owner (SIRO).
- Head of Human Resources.
- Data Protection Team.
- ICT Management Team
- ICT Security Manager.

5. Links with Other Policies

The following East Riding of Yorkshire Council Policy documents are directly relevant to this Policy and are referenced within this document:

- Information Management Strategy
- ICT Strategy and Technical Framework
- ICT Security Policy.

6. Policy Guidelines and Procedures

The Pen testing is undertaken to discover, amongst other things, vulnerabilities in web applications and weak or out of date security ciphers that protect them. The objectives of the penetration test will need to be scoped and agreed before any testing is undertaken.

As we are talking about testing an on-site application being accessed from the Internet, the testing will be undertaken remotely.

Prior to a test being carried out the following must be completed:

- The application is built to the level as it will go live. Any changes that take place after testing may introduce new vulnerabilities that are then unknown. It is acceptable to make cosmetic changes afterwards but not, for example, the addition of new modules or functionality.
- The application has been made available or 'presented out' via the council's reverse proxy servers by the Server Team and there is a URL link to the application.
- Test accounts have been created for each level of access and each has been tested by the Administrator internally.
- The Application Specialist and/or System Administrator is on site for the duration of the testing to resolve any unexpected issues which occur relating to the testing itself or

action any CRITICAL findings at the point of discovery.

- Following the return of the Pen Test report the Security Team will provide details and advise on which of the actions must be completed before the web site/service can be made live. As a rule all findings with a CVSS / Risk score of 6.8 or categorised as CRITICAL or HIGH must be removed or mitigated before the system can be published. It may be required for certain findings to be retested after the remediation actions have been undertaken. An external DNS entry will only be added once the agreed mitigations are completed and the site is in its final state and is ready to be made live.

7. Policy Implications

Following the return of the Pen Test report the Security Team will provide details and advise on which of the actions must be completed before the web site/service can be made live. As a rule, all findings with a CVSS / Risk score of 6.8 or categorised as CRITICAL or HIGH must be removed or mitigated before the system can be published. It may be required for certain findings to be retested after the remediation actions have been undertaken. An external DNS entry will only be added once the agreed mitigations are completed and the site is in its final state and is ready to be made live.

8. Policy Compliance

If you do not understand the implications of this Policy or how it may apply to you, seek advice from the IT Service Desk or ICT Security Team.

9. Financial Implications

The requirement to ensure appropriate protection of the council's corporate infrastructure is one that can be managed within existing budgets.

10. Review

This policy will be reviewed on an annual basis unless there is a major changes or security-event, then the policy will be reviewed after the event has been resolved.