Transport for London

Penetration testing standard

We want our service users to enjoy a secure online experience, we carry out penetration testing to identify vulnerabilities which can be exploited to attack TfL's infrastructure and overall architecture.

We use the Common Vulnerability Scoring System (CVSS-SIG) a vulnerability scoring system to provide an open and standardised way for rating vulnerabilities.

We carry out penetration testing to evaluate the security of our systems and use the CVSS scoring system because it is an open framework that can be used, understood and improved upon by anybody, to score vulnerabilities.

Audience

- Developers
- Testing team
- Project managers

Requirements

1. You **must** test all new tfl.gov.uk websites against the scope defined below, making use of the entry and exit criteria, and scoring defects using the severity criteria.

Who	TfL nominated 3rd Party Service Provider
Scope	Ensure you carry out an application & infrastructure security scan targeted specifically for the site under test. It should aim to identify any vulnerabilities which can be exploited in order to attack the system, attack other users, bypass controls, escalate privileges or extract sensitive data
Entry criteria	• Development is complete • Exclusive access required during the penetration test • Infrastructure is stable during testing
Exit criteria	• All tests run to completion • All defects identified have been recorded, with a severity assigned
Defects	• Sev 1: security vulnerability with a CVSS score of 8.0 or higher • Sev 2: security vulnerability with a CVSS score between 7.0 and 7.9 • Sev 3: security vulnerability with a CVSS score between 4.0 and 6.9 • Sev 4: security vulnerability with a CVSS score of 3.9 or less

Approach

The elements of security testing to be considered are:

1. Application level testing
2. Public infrastructure testing
3. Internal infrastructure testing to include:

    a. Network level testing
    b. Server build and configuration reviews
    c. Database reviews
    d. Firewall rule and configuration reviews

Further reading

- Common Vulnerability Scoring System (CVSS-SIG)

Type: Standard
Owner: TfL Online Compliance
Department: TfL Online

Version History

Version	Date	Summary of changes
1.0	07/11/2013	First issue

Review History

Name	Title	Date	Comments