



Basics of Web Security Testing

Last Updated: 7th May, 2007



Executive Summary

Exposing systems to the internet increases the risk that security weaknesses in those systems will be leveraged to compromise the system or the underlying data. It is therefore necessary to examine the actual business risks this brings, understand the basic difficulties in implementing “secure systems”, and adequately test internet applications for security, as well as functionality and load performance, before they are exposed to the net.

Introduction

Most organizations now have some of their corporate IT infrastructure connected to the internet. This may vary from allowing users to surf the web and receive email, to fully functional internet banking systems. For some organizations, compromise or failure of these systems would have significant business impact.

Software testing is becoming an accepted part of the development and maintenance cycle. Internet solutions are often required to be implemented extremely quickly. Functional, usability and load testing are all as appropriate for internet as conventional client-server solutions, however the requirement to test security is more emphatic for the internet, due to the much wider connectivity – to the incompetent, nosy or malicious – the internet brings.

The Risks

Why should an organization care about compromise of their systems?

Direct Financial Loss

If a payment's system is being operated, the contracts with the banks and the credit card organizations will specify significant financial penalties and charges that will be levied in cases of continuing fraud. In addition, the cost of shipped goods for which payment will not be recovered needs to be taken into account.

Loss of Reputation

Many hackers do it for the public recognition and therefore will publicize the compromise of a site. Security news sites are also very quick to learn of compromises. The UK consumer is still nervous about transmitting payments



information across the web – gaining a reputation as an insecure site will affect internet business growth.

Legal Repercussions

The Data Protection Act places a legal responsibility on organizations to keep person-identifiable data secure. The Data Protection Registrar may take legal action against organizations that breach this obligation, in addition to civil damages suits from affected individuals. Also, exposure of commercially sensitive data acquired under contract or privilege may lead to damages suits from affected parties.

Testing as Part of a Solution

Security testing of internet solutions provides two fundamental services:

- ▶ It allows cost-effective selection of security controls at all stages of the project cycle, allowing proper integration of security measures (procedural and technical) into the final solution;
- ▶ Management are given firm evidence of the level of security provided, showing that, in the event of a security breach, “due diligence” was exercised, which may limit damages claims or criminal liability.

Testing a system will involve a number of separate checks:

- ▶ All software involved should be examined for known security flaws;

- ▶ The infrastructure design should be implemented to allow secure operation;
- ▶ Site functionality should be examined to ensure that access to sensitive information and administrative functions is protected appropriately. This applies to operating system and server level functions, as well as application level;
- ▶ Only services necessary for the business process should be running on web-facing servers (the more different systems, the greater the likelihood of a serious flaw);
- ▶ Network traffic should be monitored to check for plain text transmission of user names and passwords (whether related to site users or to back-office functions such as databases).

If flaws are found, detailed analysis should follow, which will attempt to identify software patches, replacement service daemons or applications, or additional technical issues.

Summary

Since web-facing systems provide numerous opportunities for unauthorized access to areas of a computer network, security testing is a critical activity. This paper highlights the need to 'design in' and 'test out' security from the beginning of a project lifecycle.

Taking this approach, costs are reduced by:

- ▶ Undertaking the work as an integral part of the design, development and testing, thereby reducing the need for additional staff to undertake separate sub-projects;
- ▶ Reducing rework on security design so often highlighted by extensive penetration testing at the later stages of a project.

AppLabs has considerable experience of security testing in web-facing systems and can increase the success of your project through early involvement in the planning process, and a rigorous implementation of these methods.