



Retail



Web Application Penetration Testing for leading E-tailer

Company Background

Pantaloon Retail (India) Ltd, headquartered in Mumbai is India's leading retail company with their presence across fast moving consumer goods, apparel, music and education.

FutureBazaar is a one stop online shopping portal. The site has partnered with Big Bazaar and provides a vast array of merchandise in the store. A customer can purchase merchandise ranging from apparels and books to laptops, mobile phones and kitchenware. In order to purchase online, the user has to register by providing full contact information along with a secure password. Upon registering, the customer can browse through the various categories on offer and add the desired products to their shopping cart.

Business Challenge

To ascertain the impact of a security breach on their application, Pantaloon engaged AppLabs to carry out Web Application Penetration Testing (WAPT) on the servers exposed to the Internet. The objective of this exercise was to highlight the security posture of Futurebazaar.com from the Internet by identifying potential vulnerabilities that would have impacted business and the company image. The scope covered Web Application Penetration Testing for the web application hosted at FutureBazaar.com.

Solution

AppLabs adopted a phased approach to carry out the penetration testing of the FutureBazaar e-tailing site. This security testing engagement began with information gathering from various public and active probes on the application. Observations from the information gathering phase were analyzed to determine any obvious weak links. Port scans were also ran to discover environment related vulnerabilities and identify unnecessary services active on the host.

Subsequently, comprehensive application security checks were conducted to establish the applications susceptibility to hack attacks. This phase complied with Open Web Application Security Project standards and vulnerabilities identified through research by AppLabs' Security Center of Excellence. These tests were ran using a combination of automated and manual test tools.

The engagement concluded with the delivery of a comprehensive assessment report with severity ratings for the vulnerabilities, alongside detailed descriptions and recommendations on how to address them.

Key Benefits

- ▶ The intense level of security testing performed aided the client in maintaining information integrity and confidentiality of such sensitive information;
- ▶ The test results supported the client in understanding business and technical risks to help fortify the security policy;
- ▶ In working with an independent testing organization, the client's customers would be more confident that the web site is secure and online transactions are safe – providing it with a differentiator in the market;
- ▶ Implementation of the prioritized action plan which detailed the timelines to fix the different severity level vulnerabilities has enhanced the overall security posture of the application.