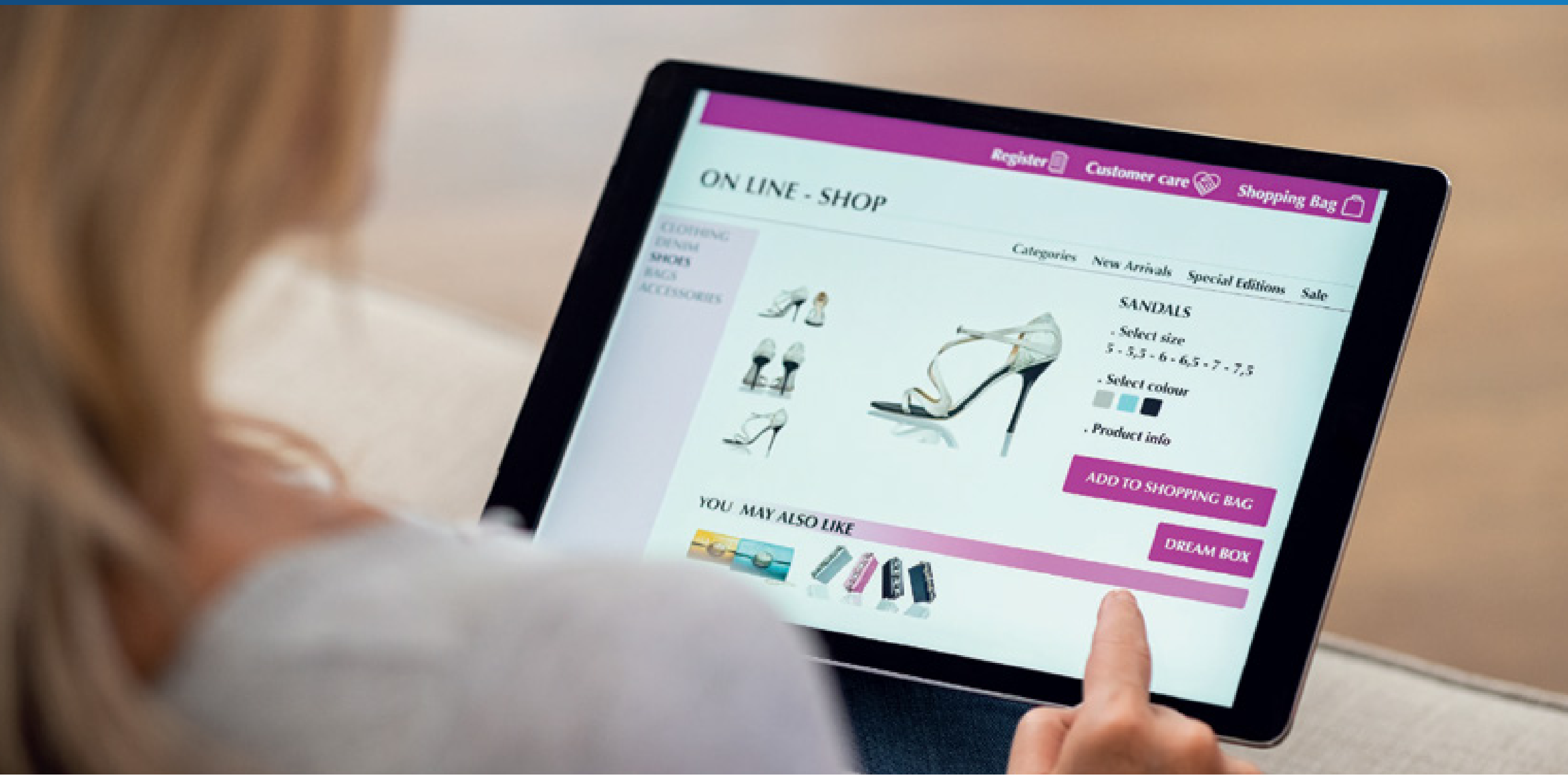
LTIMindtree

Case study

LTIMindtree Helps a Global Consumer Brand Secure Its Ecommerce Website through Infrastructure Security and DevSecOps



Client

One of the cornerstones of the digital economy is the ecommerce marketplace. The ecommerce market is slated to surpass $4.6 trillion globally and is the source of a rich and diversified database which can be used in all sectors to understand consumer preferences and patterns. When a global consumer conglomerate wanted to launch a revamped website for one of its brands, it had to make sure the data it handled was secure.

Challenge

The conglomerate had earlier faced security issues in one of its 20 odd acquired brands. Therefore, they understood the importance of implementing security from the early stages of website development. The website for the brand in case had APIs for retailers and connections to the parent company site. In an earlier instance, the company had uncovered malicious codes in the ecommerce page of its other brand, which led to the exposure of payment information.

Therefore, the company wanted to make sure that the same incident was not repeated. They needed a best-in-class website, API and WAF security measures

LTIMindtree Solution

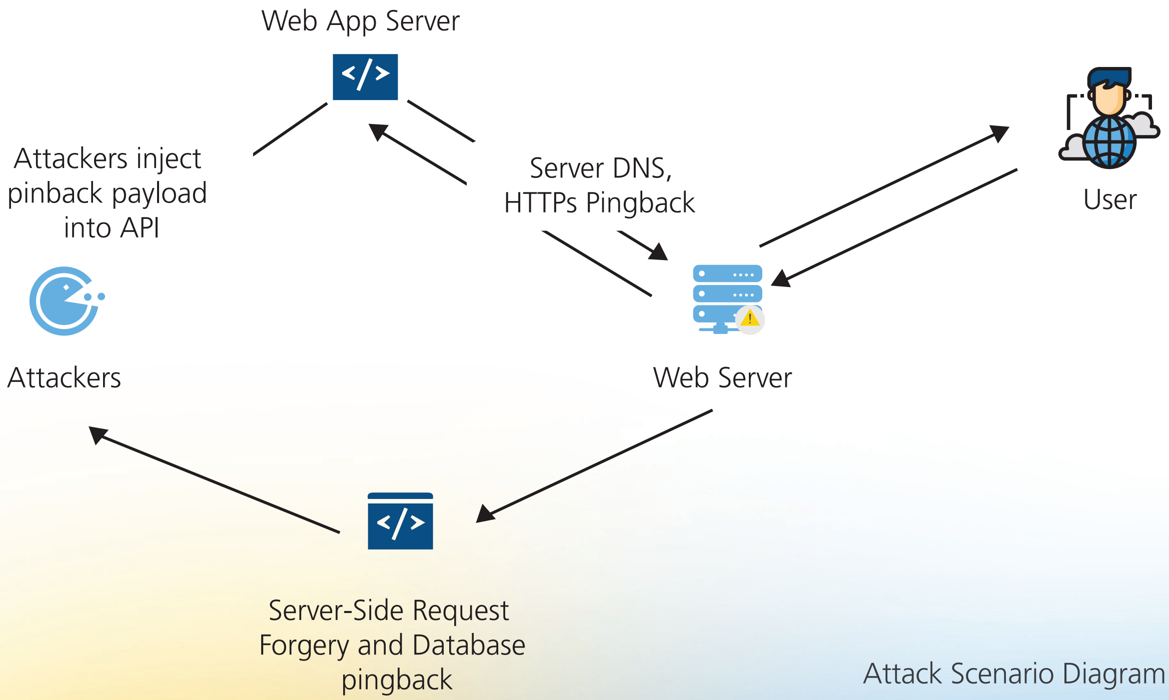
LTIMindtree met with the client and understood the requirement for an aggressive security plan that they wanted. The first order of business for LTIMindtree was to check for pre-existing flaws in the system that had caused a security breach for the other brand of the company. Based on the findings, LTIMindtree provided Hacking-as-a-Service and Managed Security Services to meet client security requirements.

Penetration testing was conducted to find any issues that could pose to be future threats. The vulnerability assessment revealed the presence of misconfigurations in the retailer side APIs and blind Server Side Request Forgery (SSRF) vulnerabilities. This posed a threat of data exploitation, not only to the brand, but also to the parent company site.

Over 10 critical vulnerabilities were found, which were patched to secure the data of the client as well as the financial transactions. The misconfigured APIs were fixed to avoid siphoning of data from the website.

Next, LTIMindtree created a Continuous Implementation and Continuous Development (CI/CD) pipeline and secure coding rules to automate the security tests.

Finally a checklist and step-by-step guideline was created for the company to undergo future threat mitigation.


Web App Server
Attackers inject pinback payload into API
Server DNS, HTTPs Pingback
User
Attackers
Web Server
Server-Side Request Forgery and Database pingback

Attack Scenario Diagram