Mindtree
A Larsen & Toubro Group Company

Mindtree helps a global consumer brand secure its ecommerce website through infrastructure security and DevSecOps

Overview

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 its ecommerce page of its other brand, that had led to 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

Solution

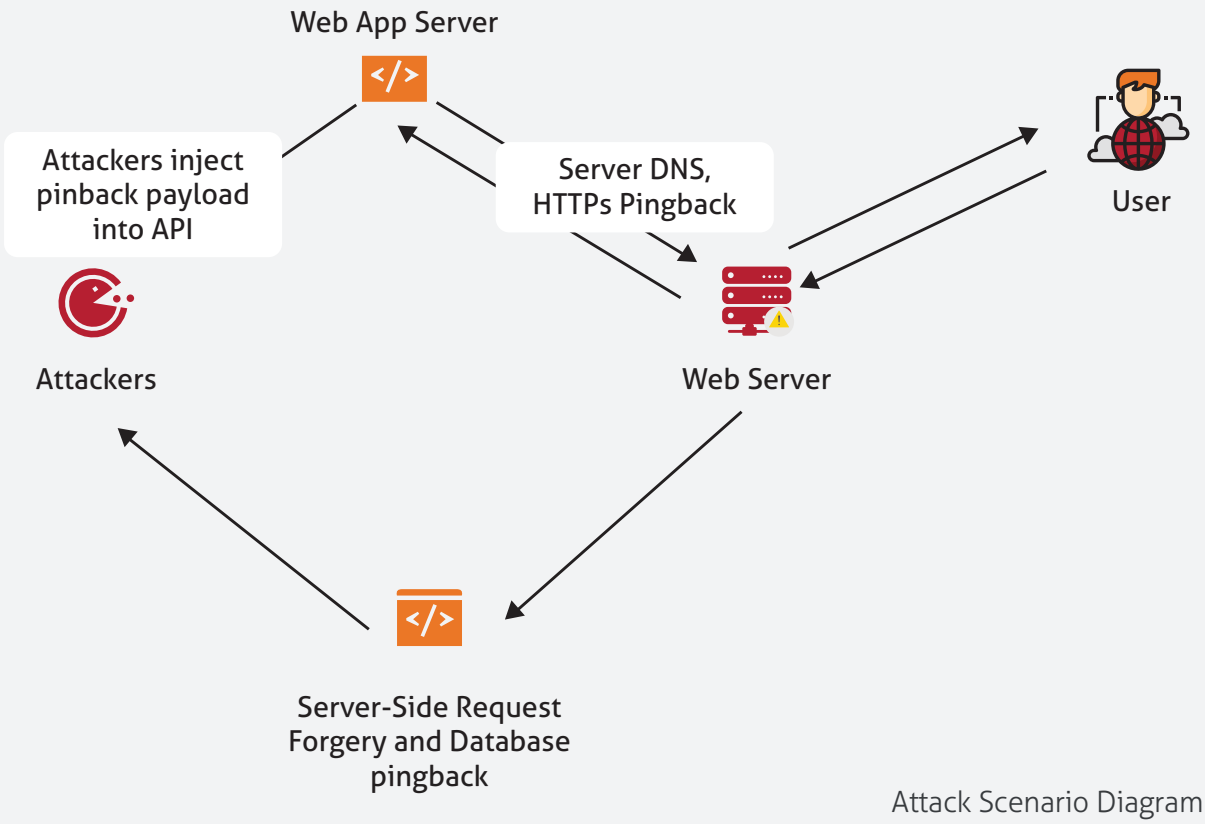
Mindtree met with the client and understood the requirement for an aggressive security plan that they wanted. The first order of business for Mindtree was to check for pre-existing flaws in the system that had caused a security breach for the other brand of the company. Based on the findings, Mindtree 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, Mindtree 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 company to undergo future threat mitigation.



Attack Scenario Diagram

ABOUT MINDTREE

Mindtree [NSE: MINDTREE] is a global technology consulting and services company, helping enterprises marry scale with agility to achieve competitive advantage. "Born digital," in 1999 and now a Larsen & Toubro Group Company, Mindtree applies its deep domain knowledge to 300+ enterprise client engagements to break down silos, make sense of digital complexity and bring new initiatives to market faster. We enable IT to move at the speed of business, leveraging emerging technologies and the efficiencies of Continuous Delivery to spur business innovation. Operating in 18 countries and over 40 offices across the world, we're consistently regarded as one of the best places to work, embodied every day by our winning culture made up of over 21,000 entrepreneurial, collaborative and dedicated "Mindtree Minds."