Security testing for eCommerce websites and retailers

BY ANNA HAMMOND · FEBRUARY 19, 2024 · LAST UPDATED ON JUNE 13, 2025

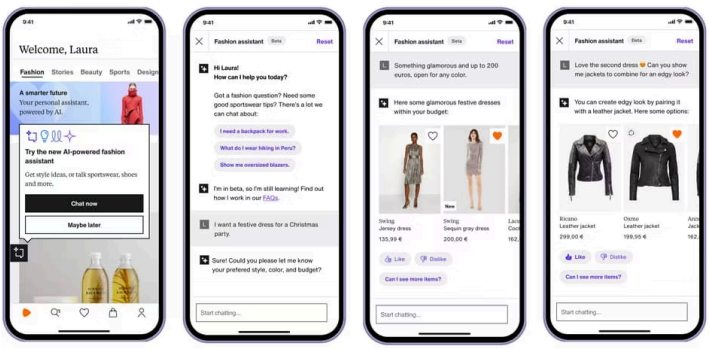
Security testing for eCommerce websites has become indispensable for online retailers, as it plays a vital role in safeguarding customer data, financial information, and brand reputation. The process involves evaluating and testing the security measures implemented by retailers, aiming to identify vulnerabilities and potential threats that cyber attackers may exploit.

In this article, we cover what security testing means for retailers and why it's important.

Retail in 2024: The age of online dominance

It was estimated that 2.71 billion people worldwide are expected to shop online in 2024 to purchase goods and services, according to eMarkerter and Oberlo. This represents a significant leap from the 1.66 billion online shoppers recorded in 2016. The exponential growth in online shopping comes as no surprise, considering the widespread availability of internet connectivity and the increasing convenience it offers.

As competition in the retail industry intensifies, retailers are compelled to enhance their strategies to attract and retain customers. Gone are the days when exclusive discounts, such as those seen during Black Friday and Cyber Monday, were solely associated with retail giants like Amazon. Retailers are now exploring various avenues, including the integration of AI-powered shopping assistants, to elevate the online shopping experience.



Zalando's ChatGPT-powered fashion assistant [Source: FashionUnited]

Yet as the online shopping experience evolves, so does the opportunities for threat actors to capitalize on for financial gain. In the retail world, web applications commonly take the form of an eCommerce website or app, as well as third-party sites, plugins, vendors and supply chains. These assets and platforms often

store a wealth of sensitive information, including payment details, personal data, and proprietary information.

So, what steps can retailers take to mitigate these risks and ensure a secure online shopping environment?

Security testing must be a priority for retailers

It's critical for retailers to prioritize security testing throughout the development lifecycle. Adopting a proactive approach allows for timely detection and resolution of vulnerabilities, mitigating the potential for costly breaches and reputational harm. Further, security testing plays a vital role in ensuring retailers remain PCI compliant.

To assist you in your efforts, we have compiled our top tips for effective security testing:

1. Test early and often

Initiating **security testing early in the development process** allows ample time to address vulnerabilities before they escalate into major issues. This approach reduces the risk of costly rework and potential downtime, ensuring a smoother development process and timely product delivery. Conversely, delaying security testing until the end of the development cycle can be both time-consuming and expensive, as modifications at this stage are more complex and resource-intensive.

By integrating security testing as a fundamental component of the development process, businesses can guarantee the ongoing protection of their systems and customer data

2. Involve developers throughout the process

Involving developers throughout the security testing process is crucial for the overall success of your security testing efforts. It is not just the responsibility of the security team to test for vulnerabilities, but also the developers who are writing the code and fixing any issues that are found.

By involving developers from the beginning, you can ensure that they are aware of the security risks and can take steps to mitigate them as they build the application. This proactive approach can significantly reduce the number of vulnerabilities that make it into production, saving time, money, and reputation in the long run.

Additionally, involving developers in security testing helps to build a culture of security awareness within the development team. When developers are actively involved in the testing process, they gain a better understanding of the importance of security and are more likely to consider security implications as they write code. This can lead to a significant improvement in the overall security posture of the organization.

3. Continuously test to uncover new hidden vulnerabilities

New vulnerabilities are constantly emerging in the digital landscape and cybercriminals are always looking for creative ways to exploit them. By continuously testing your website, you can stay ahead of the curve and protect your customers' data and your business from costly security breaches.

In addition to regular security testing, it is also important to test your website after any major changes, such as adding new product lines, features, or upgrading your software. This will help you ensure that the changes have not introduced any new vulnerabilities.

4. Prioritize the right vulnerabilities

To prioritize vulnerabilities, consider the potential impact of a vulnerability, the likelihood of it being exploited, and the ease of exploitation. Retailers can use vulnerability scoring systems and risk assessment frameworks to help prioritize vulnerabilities or create their own. Either way, by considering these factors, businesses can focus their security testing efforts on the most critical areas. This will help to minimize the risk of costly breaches and reputational damage.

Common types of security testing techniques for retailers

Penetration testing

Penetration testing, or pentesting, is a simulated cyberattack that helps retailers identify and fix security vulnerabilities in their systems. By conducting regular pentests, retailers can:

- Protect themselves from data breaches and other security incidents
- Build trust with their customers
- Comply with industry regulations and standards.

The scope of a pentest can vary depending on the retailer's needs and budget. Some pentests may only focus on a specific part of the retailer's network or application, while others may cover the entire infrastructure.

The results of a pentest are typically documented in a report that identifies the vulnerabilities that were found and provides recommendations for how to fix them. Retailers should take the findings of a pentest seriously and swiftly initiate steps to remediate the vulnerabilities that were found.

Bug bounty programs

Bug bounty programs provide an ideal solution for conducting continuous security testing on platforms and software to identify vulnerabilities. These programs effectively assist development and security teams in accelerating the process of building, testing, and releasing application features.

By implementing a bug bounty program, your software undergoes meticulous examination by numerous (or even thousands of) dedicated and highly motivated expert hackers. These individuals meticulously replicate the methods employed by malicious hackers, continuously testing for as long as the program remains active.

In addition to these benefits, the generation of vulnerability reports contributes to an elevated level of security awareness within organizations. The comprehensive nature of these reports, coupled with the accompanying support provided, serves as exceptional learning resources.

Vulnerability Disclosure Policies (VDPs)

While VDPs may not be as proactive as bug bounty programs and pentests, they play a crucial role in maintaining a strong set of security standards. The primary objective of a VDP is to provide ethical hackers with clear guidelines for reporting vulnerabilities to an organization. In addition to reducing the risk of undetected security issues, having a VDP offers several benefits for businesses, including:

- Streamlining the process of vulnerability reporting
- Demonstrating a commitment to information security and data protection
- Building trust among stakeholders and customers
- A framework of rules for hackers to follow when testing your services.

A disclosure policy applies to any researcher who reports a vulnerability. However, it also presents an opportunity for organizations to showcase their willingness to collaborate with external actors who are acting in good faith.

Continuous security testing for ecommerce websites is a must

Gone are the days when retailers could exist without a digital approach. If your retail business operates online, it's essential to recognize the importance of rigorous security testing. By following our tips, you can help protect your eCommerce website and your customers' data from cybercrime.

To learn more about security testing for ecommerce websites, check out our ebook: Reducing Risk for Retailers.