Access control vulnerability in the retail industry. Cross-Site Scripting (XSS) use case

BY ELEANOR BARLOW · MARCH 13, 2025 · LAST UPDATED ON JANUARY 2, 2026

What you will learn

- **Why the retail industry is a high risk target for cyberattacks** and how broad attack surfaces, such as e commerce platforms, supply chains, and customer data systems, create opportunities for exploitation.
- **How real world web application vulnerabilities like Cross Site Scripting (XSS), information disclosure, and access control misconfigurations can be exploited** to steal data, escalate privileges, and compromise retail systems.
- **What concrete security practices can you implement to protect retail applications,** including input validation, Content Security Policy (CSP), access rights configuration, MFA, and regular security testing, to reduce the risk and impact.

Why is the retail industry being targeted?

Large-scale operations and the extensive attack surface of the retail industry render it particularly susceptible to cybercrime, on a global scale. Websites, mobile apps, and company programs create numerous entry points for malicious actors. The high volume of payment transactions and financial incentives of successful attacks present an enticing opportunity for bad actors. Customer data is also a significant lure, as this information, including addresses, credit card details, shopping history, and user preferences, can be sold to cybercriminals on the dark web for additional profit.

Supply chain vulnerabilities

A key security issue within Retail is that companies use many different systems and supply chains, which can be hard to monitor and control. If not secured properly, third-party vendors can impact the whole supply chain, leaving e-commerce platforms, customer relationship management systems, and inventory management systems vulnerable.

Neiman Marcus, a department store, reported a data breach in May 2024 where their cloud storage company, Snowflake, was targeted and customer names and contact information were released.

The threat actor tracked as UNC5537 was observed advertising data from Ticketmaster and Santander for sale in a cybercrime forum. In that same forum UNC5537 announced that they had breached the cloud data warehouse of Snowflake, and the database was sold for $150,000. UNC5537 may have accessed roughly 165 company accounts using the exploited credentials, and more than 31 million customer email addresses.

This is why companies need to check their supply chains and the cyber security in place, before utilising third-party services.

Targeted cyclical phishing campaigns

With a 'Sell! Sell! Sell!' mentality, downtime is rarely accepted in the industry, even when essential security measures are required. As a result, security is often skipped, and systems can be poorly patched or left unmonitored altogether.

Targeted threats throughout the holiday seasons and cyclical offers such as Cyber Monday or Black Friday deals provide an additional opportunity for bad actors to release targeted Social Engineering and Phishing campaigns affecting both the seller and customer.

An example of this can be observed in the latest Krispy Kreme data breach. In an article released in December 2024 by the Financial Times, the multinational doughnut company was targeted in an attack that 'came weeks after a warning that fraud and ransomware are expected to threaten retailers, hospitality and travel businesses during their busiest Christmas holiday season'.

A ransomware group by the name 'Play' claimed responsibility and announced that they had stolen Personally Identifiable Information (PII) data, including payroll, contacts, taxes, IDs and much more.

In a joint advisory, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and the Australian Cyber Security Centre (ACSC), disclosed that this specific ransomware group had breached networks of approximately 300 organisations across the globe.

Impact of 3 Common Attack Vectors

While the cause of many successful data breaches is rarely publicised, the team at Intigriti are noticing three common attack vectors across the industry.

Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) is a Web Application vulnerability whereby bad actors inject malicious scripts into a site, to execute actions on the target's browser. The aim is to steal information, change content, or redirect the user to malicious sites. The result includes information disclosure and account control issues.

Cross Site Scripting is probably the most common bug found.

> **"'In this case a hacker found a stored XSS, often the most impactful type of this bug, in a part of the website where a system of roles determined a user's privileges. Using this vulnerability by injecting a payload into the page as a low privileged user could lead to gaining more privileges after a higher privileged account visited the page and the payload was executed.' - Lennaert Oudshorn, Head of Triage, Intigriti"**

Information Disclosure

Sometimes an application discloses some information it probably shouldn't. Often this information is not super exciting, however, other times the impact can be quite severe.

> **"'For instance, an application can leak an API key inside a JavaScript file. The API key could be used to extract sensitive information about the authentication service of the application.' - Lennaert Oudshorn, Head of Triage, Intigriti"**

Access Control

Configuring the correct access rights to assets can be a tricky thing. This bug is primarily about a misconfigured S3 bucket. If the bucket served files for the interface of a production application, due to this access control misconfiguration, the attacker could gain full control of this bucket. Potentially altering what legitimate users saw on this application.

X5 mitigations to safeguard against attack vectors

1. **Train your team**. Educate employees and developers on security training and testing. Companies must maintain the right practices and regularly conduct tests like Penetration Testing and security audits to spot and prevent cyber threats.
2. **Update systems**. Systems, frameworks and libraries should be updated regularly to prevent vulnerabilities.
3. **Safeguard customers**. Ensure elements like Multifactor Authentication (MFA) are enabled to instantly provide another layer against malicious activity and unauthorised access.
4. **Attack surface reduction**. Reduce the attack surface by using external scripts and by linking them securely. Avoid using Inline JavaScript, or event handlers. Ensure that a Content Security Policy (CSP) is in place to restrict which scripts can run.
5. **Sanitize and validate data**. Check input data and ensure proper output encoding based on the content type to prevent malicious code execution.

For more information on how to spot and stop cyber threats targeting your Retail company, contact the team, to speak with an expert.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.