Black Friday and Cyber Monday price distortion identification

BY ELEANOR BARLOW · NOVEMBER 19, 2025 · LAST UPDATED ON DECEMBER 24, 2025

What you will learn

- **How price manipulation works during big sales:** Learn the common ways discounts, coupon systems, and pricing logic can be exploited by threat actors in high-traffic e-commerce events.
- **Key vulnerability types to watch for:** Understand issues like insecure coupon validation, currency confusion, and integer overflow that can lead to financial loss and fraud.
- **Why secure validation and testing matter:** See how robust validation and cybersecurity approaches help prevent price distortion and protect revenue.

Brick-and-click sales leaving no dollar behind

The evolution of the internet and, with it, international levels of e-commerce, meant that Black Friday soon became the unofficial start of winter purchases ahead of holiday festivities across the globe. In the early 2000s, Cyber Monday, held on the Monday after Thanksgiving, materialized to encourage people to shop online following the black-Friday in-store rushes.

Together, digital e-commerce and traditional retail push for holiday shopping frenzies on a universal level.

According to DHL:

- 75% of global shoppers purchase during Black Friday and Cyber Monday.
- 71% say discounts and savings motivate them to spend.
- Electronics are the most purchased item, with 37% of shoppers buying these during sales.
- Gen Z and Millennials are the most active Black Friday Shoppers, with only 8% not buying at all.

And we're not talking small purchases. In the US, the average consumer is expected to spend $340 on Black Friday and another $300 on Cyber Monday.

This presents an attractive opportunity for threat actors, and with numerous offers featured on every website, price manipulation attempts are on the rise.

Intigriti observations: Price manipulation attempts

There are many ways prices can be manipulated. In this blog, we explore three types of price manipulation, each illustrating a shared underlying theme: insufficient validation, which threat actors increasingly exploit at this time of year. Vulnerabilities that allow price manipulation can lead to financial losses, fraud, and damage to a brand's reputation, which is why secure checkouts are essential.

"An Intigriti researcher found a critical bug in our eCommerce site a few months before. We were very grateful that we could patch and fix that bug so that we didn't lose sales over the Christmas period."- MuuseLabs

1. Discount disasters in coupon validation systems

Coupon scams come in all shapes and sizes. From fraudulent QR codes, bogus coupon sites mimicking legitimate providers, to counterfeit printable coupons, there are many ways false coupons can be created from scratch.

But what happens when legitimate coupons, on legitimate sites, are hacked and altered?

When a coupon is not set up correctly by the provider, it leaves the user and the company vulnerable. For instance, when coupons are implemented insecurely, it can potentially allow malicious actors to redeem expired codes, apply the same code multiple times, or even generate new codes by abusing incorrect application logic.

A threat actor can also take advantage of a lack of validation elements by bypassing insecure payment walls and even altering the price of a product via logic errors (more on this later).

What is the impact of vulnerable validation systems?

A large-scale threat or high-value coupons can lead to significant financial loss. But it's not just the financial impact; the marketing metrics will also be distorted, meaning that teams will be optimizing based on inaccurate data.

Reputation can equally be damaged if coupons have to be retracted or cancelled altogether. Users may also view any retraction as a direct lack of cybersecurity measures and, therefore, have concerns for the company's storage/use of personal data.

Incorrect record keeping and inability to validate birthdays could also cause legal risks and regulatory fines in terms of staying GDPR compliant.

What are long and short-term fixes?

Actions can be put in place to enhance validation.

For quick fixes:

- Enable edit cooldown. Ensure the user has to provide a reason for any requested changes to personal details and set a time, such as 30 days, until another edit can be made.
- Change settings so that one coupon is provided per account ID per year, rather than via date of birth or based on any other personal information.
- Identify exploitation taking place right now by searching for new accounts or accounts with new purchase history, clusters of accounts sharing payment methods, or multiple changes from the same IP.

For long-term support, bug bounty programs mean that researchers can hunt for any areas that lack validation to identify any entry points, not just across your coupons and promotions, but across the company's entire digital environment.

2. Lost in translation: currency confusion

Exchange rate functions are used by e-commerce companies to cater to global audiences. They are a necessary part of business. But what makes organizations vulnerable to currency confusion is, again, a lack of validation.

When there is a lack of validation, a threat actor takes advantage of the exchange rate function, with the goal of manipulating the transaction to pay a small amount in one currency, while being charged for a much larger value item priced in a different currency.

'Whenever inspecting an HTTP request, check if you can alter the currency from USD to, for example, INR or JPY while leaving the price or amount parameter untouched. If your ordered item is priced at 100 USD, you'd eventually pay 100 INR, the equivalent of 1.10 USD, instead.' – Blackbird-EU

Not only can currency be edited, but if a formula injection is used to change the parameter for the amount, equally so can the quantity of the item be edited. This vulnerability can be exploited at any point in the year. But the impact during Black Friday or Cyber Monday can be amplified as bargain-hunting shopping leads to quick cross-border transactions.

A lack of expiration date can also mean that seasonal coupons issued a year or two years ago, specifically for black Friday or Cyber Monday, can be stored and reused this year.

How to identify currency confusion?

If included in the scope, a bug bounty program can spot currency and exchange-rate validation issues. Researchers are able to provide integrity checks, identify logic issues and race conditions, view API endpoints, as well as any tampering with exchange rates or tokens, and much more.

3. Unsafe arithmetic: What are Integer overflow vulnerabilities?

Machines can store up to a specific number of both positive and negative numbers. This reach depends on the machine. If a threat actor were to set a number that exceeded the highest number on the backend system, and if the correct validation was not in place, the number would be converted to a negative number or reset back to zero, allowing the user to bypass the process.

‘When testing checkout systems, try altering the price or quantity of your ordered items and set them to an excessively high number. If no validation is present, it may reset your quantity or price to a negative number or simply set it to 0, allowing you to bypass the checkout system altogether.’ – *Price manipulation vulnerabilities in e-commerce*

Integer overflows are a significant risk for e-commerce and financial systems during high-traffic sales periods like Black Friday or Cyber Monday. On top of the financial impact, they can also lead to system crashes, which can further impact brand reputation, customer loyalty, and marketing efforts.

There are no immediate warnings for this type of vulnerability. The best way to find these bugs is to examine all operations before release and use a bug bounty platform for continuous monitoring.

How does a layered cybersecurity approach support process validation?

For most businesses, Black Friday and Cyber Monday prove to be one of the most profitable times of the year. Targeted and continuous testing from a global community of security experts can highlight any gaps in your environment that could leave you, your customers, employees, and systems vulnerable.

PTaaS is especially useful before big events, like Black Friday and Cyber Monday, when new products are shipped, to test for any bugs before going live with campaigns or new offers. A Vulnerability Disclosure Program (VDP) delivers a secure and legal framework for ethical hackers to submit vulnerabilities that internal teams might miss. And bug bounty programs drive high-skill, continuous real-world testing for your business’s critical systems.

For more information, take a look at how we support organizations in Retail, view vulnerabilities impacting sales this Black Friday and Cyber Monday, or, for more information on any of the points discussed in this article, contact the team today.

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.

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com