



Chapter 8

The Digital Discount: Price Tampering Techniques

In today's digital world, where e-commerce thrives, price tampering is one of the most fascinating yet dangerous vulnerabilities that we, as cybersecurity experts, must understand. It's not just about performing price tampering but also about preventing it and safeguarding online platforms.

UNDERSTANDING PRICE TAMPERING WITH AN EXAMPLE

To simplify, price tampering can be compared to someone sneaking into a shop and secretly changing the price tags on items to make them cheaper. However, in the digital world, this manipulation happens online, where people can alter prices during transactions.

For instance, imagine an online course priced at ₹2000. Using price tampering, someone could manipulate the transaction and purchase the course for just ₹1. This demonstrates the potential financial damage such

vulnerabilities can cause to businesses. As cybersecurity professionals, our goal is to understand how price tampering works, ethically test for it, and develop strategies to prevent it from happening.

TOOLS AND TECHNIQUES FOR PRICE TAMPERING

To test price tampering, we will use **Burp Suite**, a powerful cybersecurity tool. Burp Suite is widely known for its ability to test web application vulnerabilities. Its features include tools like Proxy, Repeater, Scanner, and Intruder, which work together to assess and exploit security flaws.

Intruder Tool

Automates the process of testing multiple parameters or values to identify weaknesses in server-side validation.

Repeater Tool

Enables you to manually resend and modify captured requests. You can experiment with different values for the price parameter to test the website's response.

Proxy Tool

Captures the communication between the user's browser and the website server, allowing you to view and modify the data being transmitted.

Example: Intercepting a price parameter (*price=2000*) and modifying it to *price=1*.

Identify the Weak URL Parameter

After scanning, SQL Map will list the vulnerable URLs with parameters. Choose one of the links.

STEPS TO PERFORM PRICE TAMPERING (FOR LEARNING PURPOSES)

Here are the steps to perform Price Tampering:

Step 1: Intercept the Request

Using Burp Suite's Proxy tab, intercept the HTTP request sent when adding an item to the cart or proceeding to checkout. Look for parameters like *price*, *amount*, or *total* in the request.

Step 2: Modify the Price

Edit the intercepted request and replace the original price with a significantly lower amount (e.g., ₹2000 to ₹1). Forward the modified request to the server and observe the response.

Step 3: Test for Server-Side Validation

If the server accepts the modified price and processes the transaction, the website is vulnerable to price tampering.

WHY PRICE TAMPERING HAPPENS

The primary reason behind price tampering vulnerabilities is the reliance on client-side validation. This means the price is stored or validated on the user's browser instead of the server. When attackers intercept the communication, they can manipulate the data before it reaches the server.

Example in Action

Imagine shopping for a course online. The original URL might look like this:

```
https://example.com/checkout?product_id=123&price=2000
```

By intercepting this request using Burp Suite, an attacker could change it to:

```
https://example.com/checkout?product_id=123&price=1
```

If the server does not validate the price on its side, the transaction will be processed for ₹1 instead of ₹2000.

PREVENTION TIPS FOR DEVELOPERS

Implement Server-Side Validation

Ensure all prices and critical data are validated on the server side. Do not trust client-side inputs.

Hash and Validate Parameters

Use secure hash algorithms (like SHA-256) to encrypt sensitive data (e.g., prices) before sending it to the client. Verify the hash on the server during checkout.

Encrypt Communication

Always use HTTPS to encrypt data in transit, making it harder for attackers to intercept and modify requests.

Limit Client Privileges

Restrict users from directly modifying critical fields (like price) in requests. Use backend-controlled data wherever possible.

MASTERING BURP SUITE

To fully utilize Burp Suite, you should:

- ❖ Learn the basics of HTTP/HTTPS protocols and how web servers handle requests.
- ❖ Experiment with tools like Proxy, Repeater, and Intruder in controlled environments.
- ❖ Stay updated with the latest features and vulnerabilities by following ethical hacking communities.

CONCLUSION

Price tampering is a critical vulnerability that highlights the importance of secure coding practices and ethical testing. By understanding how

attackers exploit these weaknesses and using tools like Burp Suite responsibly, we can strengthen the security of online platforms.

By [ScripterJee](#)