PRICE TEMPERING

Website: Ogdmart.com

Project Overview

This project focuses on identifying and mitigating **price tampering vulnerabilities** in the Odgmart.com web application through **authorized and ethical security testing**. The objective is to evaluate whether the application properly validates pricing data on the server side during the transaction process.

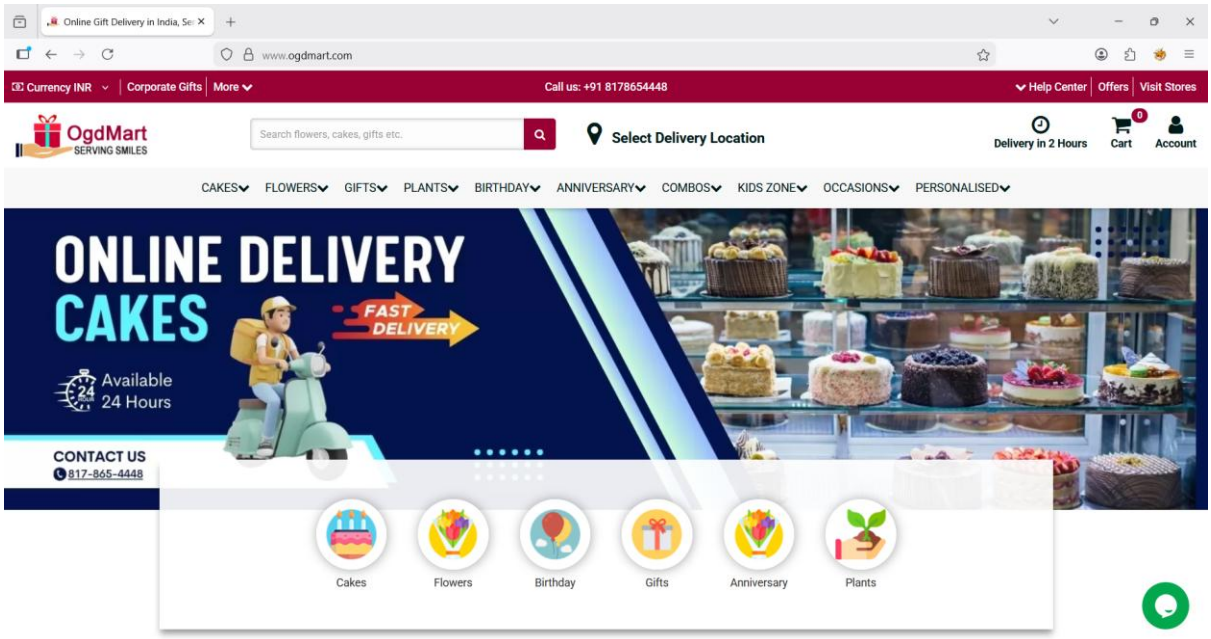
Methodology

Step 1

The website www.ogdmart.com is accessed using Google Chrome with the Burp Suite extension enabled to monitor and analyze HTTP requests.

Step 2

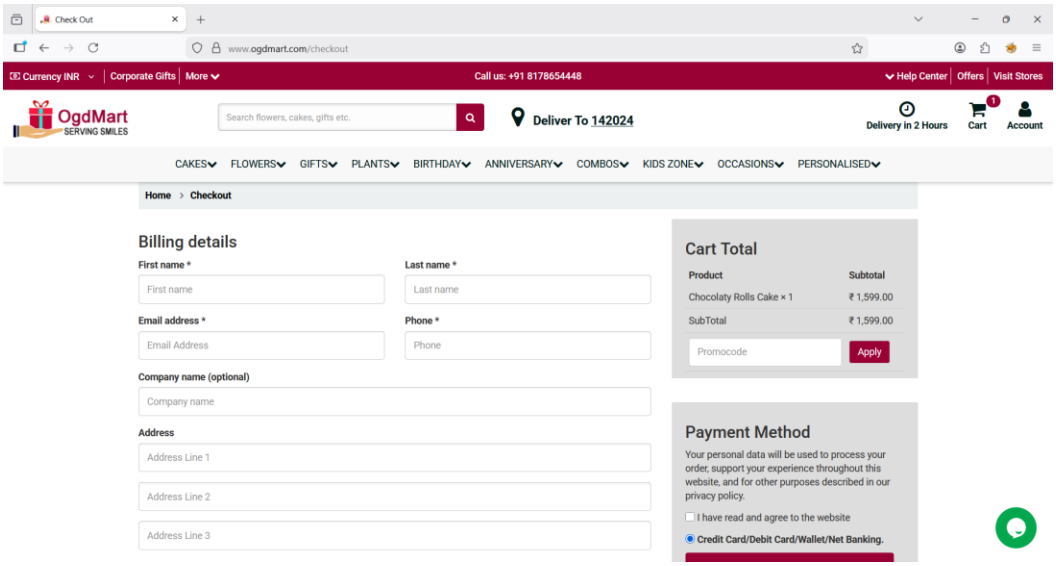
A product is selected, and the required details such as PIN code and delivery date are entered.



Step 3

The selected product is added to the cart, and user information including name and address is provided during the checkout process.

Reported By: Lakshman Kumar Das

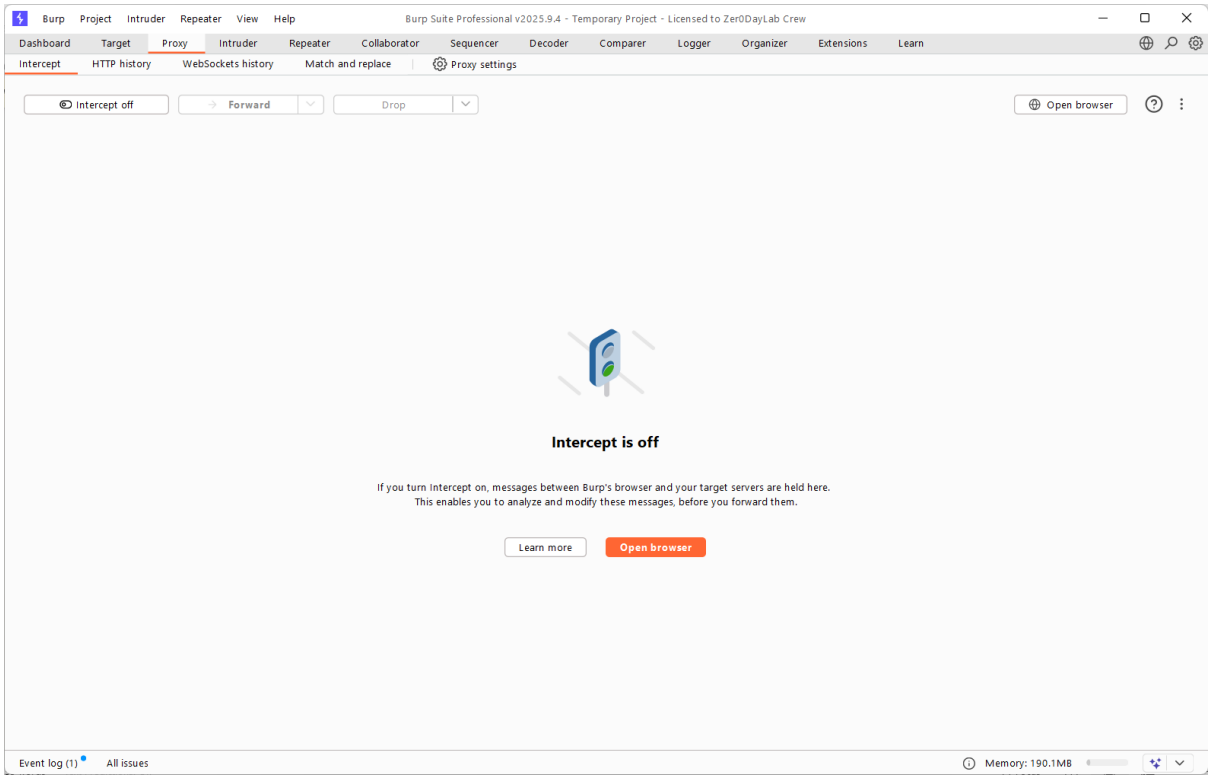


Step 4

To assess the price tampering vulnerability, Burp Suite is used as the primary testing tool to intercept and analyze client–server communication.

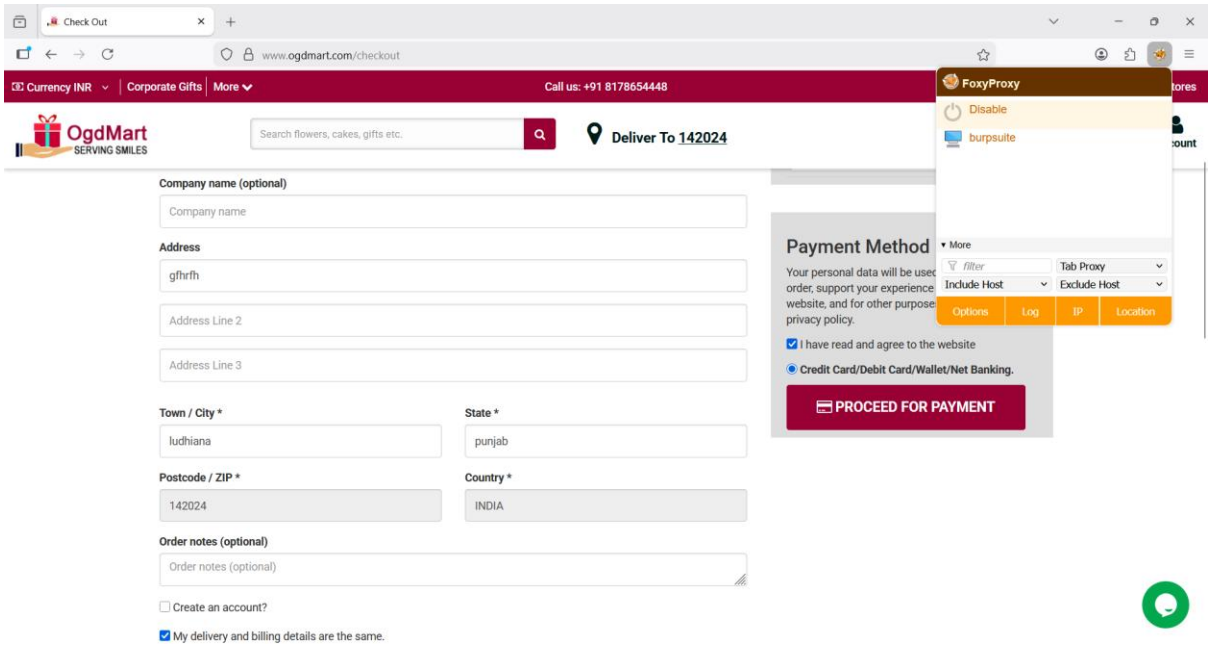
Step 5

Burp Suite is opened, and the Proxy → Intercept feature is enabled to capture the HTTP requests generated during the checkout process.



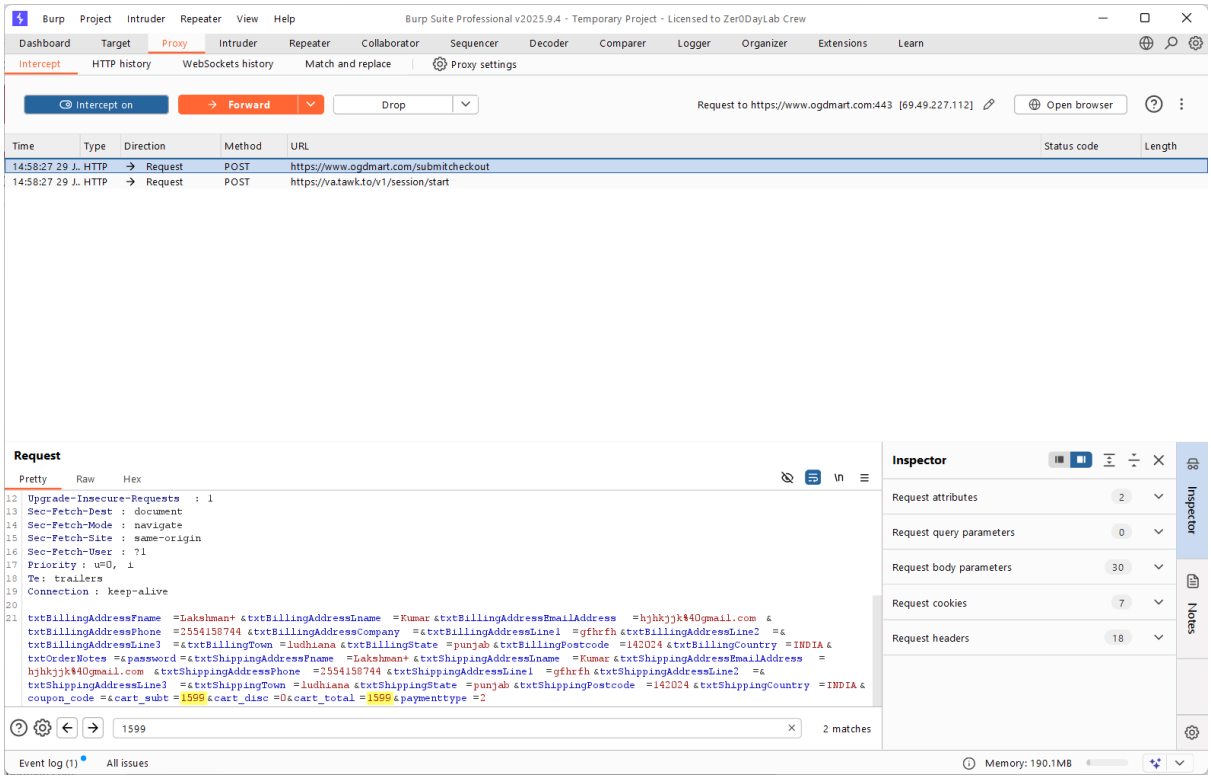
Step 6

The FoxyProxy extension is activated in the browser to route traffic through Burp Suite.

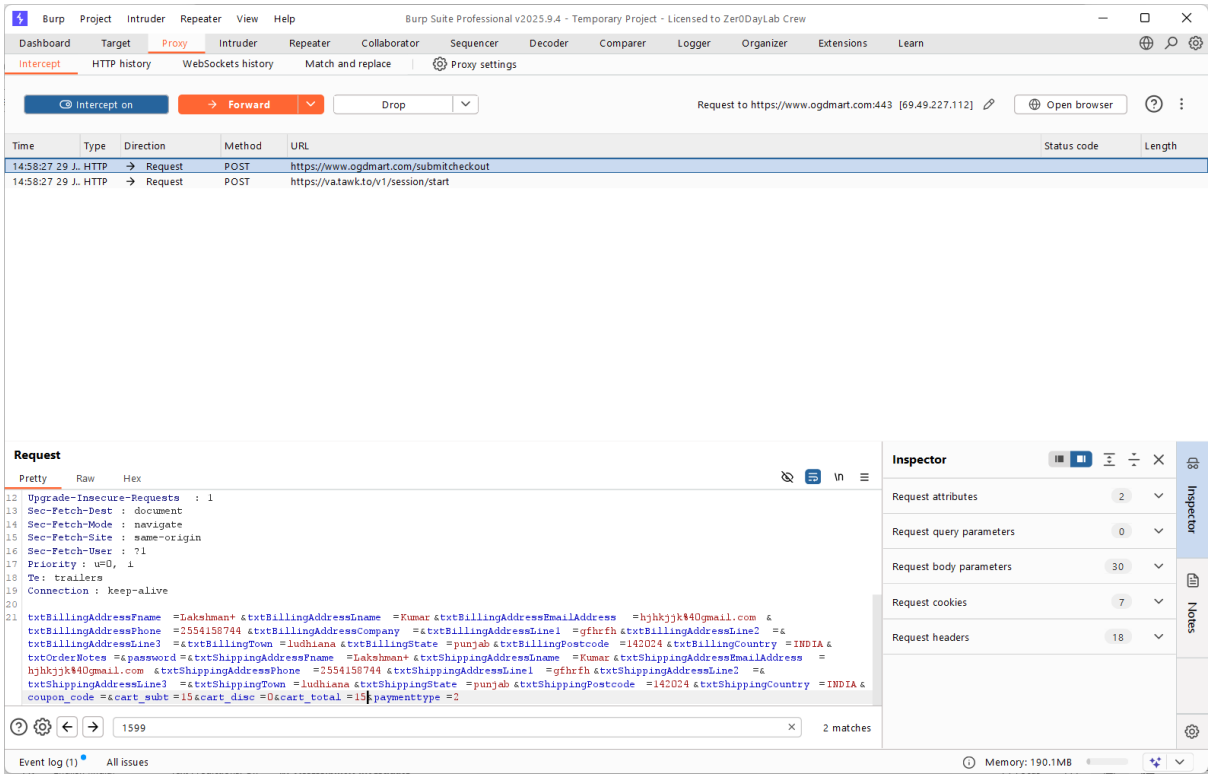


Step 7

The intercepted POST request is analyzed, and the product price value is modified (for example, changing ₹1599 to ₹15) to test whether the application accepts manipulated pricing data.

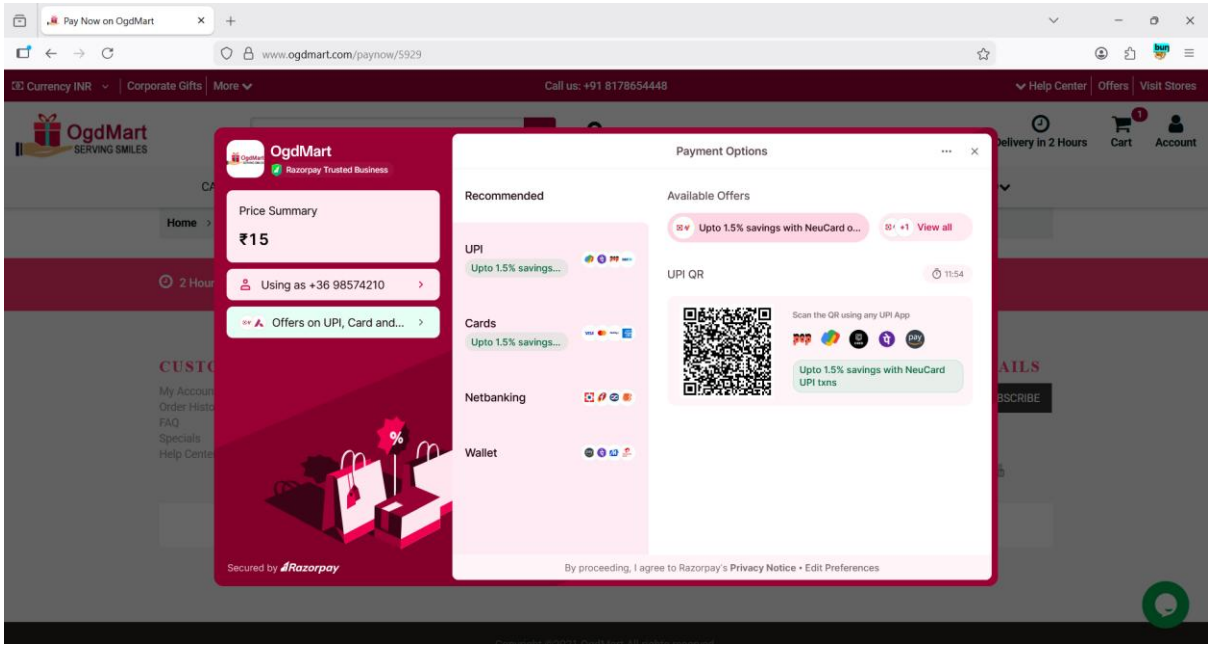


Reported By: Lakshman Kumar Das



Step 8

After modifying the value, interception is disabled, and the request is forwarded to the server. The application response is observed to determine whether the manipulated price is processed successfully.



Conclusion

Price tampering is a high-severity security vulnerability that allows attackers to manipulate product prices, potentially resulting in significant financial losses. This issue arises when applications rely on client-side price values without proper server-

side validation. To prevent such attacks, it is essential to implement strict server-side price verification, secure transaction handling, and integrity checks throughout the payment workflow.