

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.

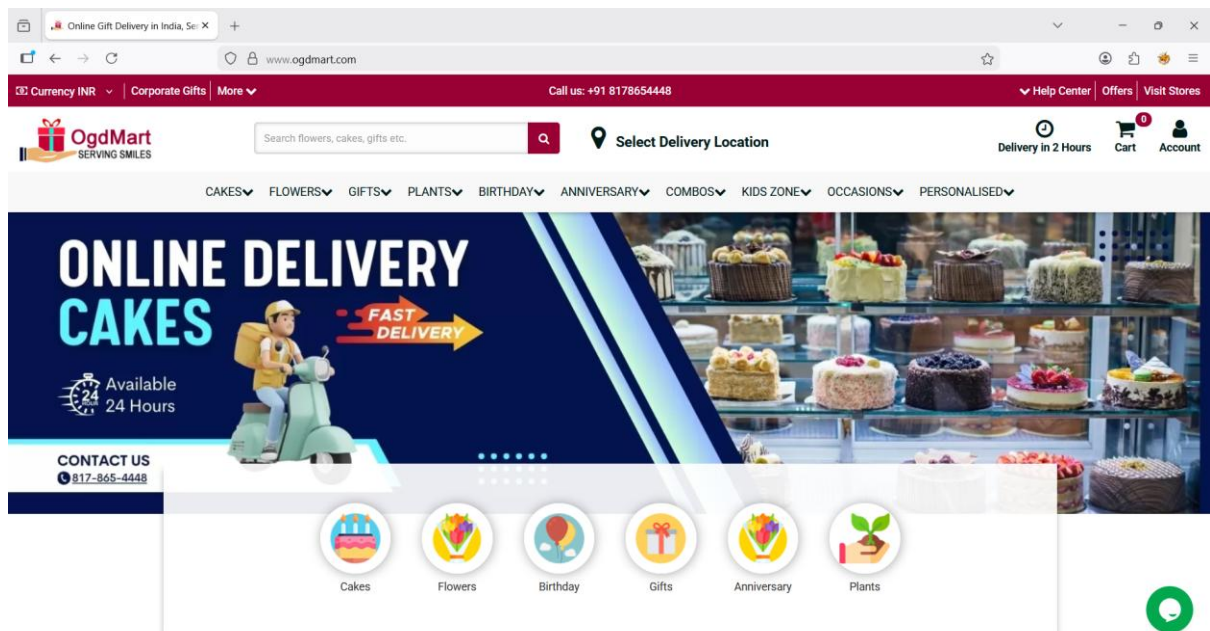
Methodology

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.

Check Out

www.ogdmart.com/checkout

Currency INR Corporate Gifts More

Call us: +91 8178654448

Help Center Offers Visit Stores

OgdMart SERVING SMILES

Search flowers, cakes, gifts etc.

Deliver To 142024

Delivery in 2 Hours Cart Account

CAKES FLOWERS GIFTS PLANTS BIRTHDAY ANNIVERSARY COMBOS KIDS ZONE OCCASIONS PERSONALISED

Home > Checkout

Billing details

First name *
Last name *

Email address *
Phone *

Company name (optional)
Address

Cart Total

Product	Subtotal
Chocolate Rolls Cake x 1	₹ 1,599.00
SubTotal	₹ 1,599.00

Promocode Apply

Payment Method

Your personal data will be used to process your order, support your experience throughout this website, and for other purposes described in our privacy policy.

☐ I have read and agree to the website

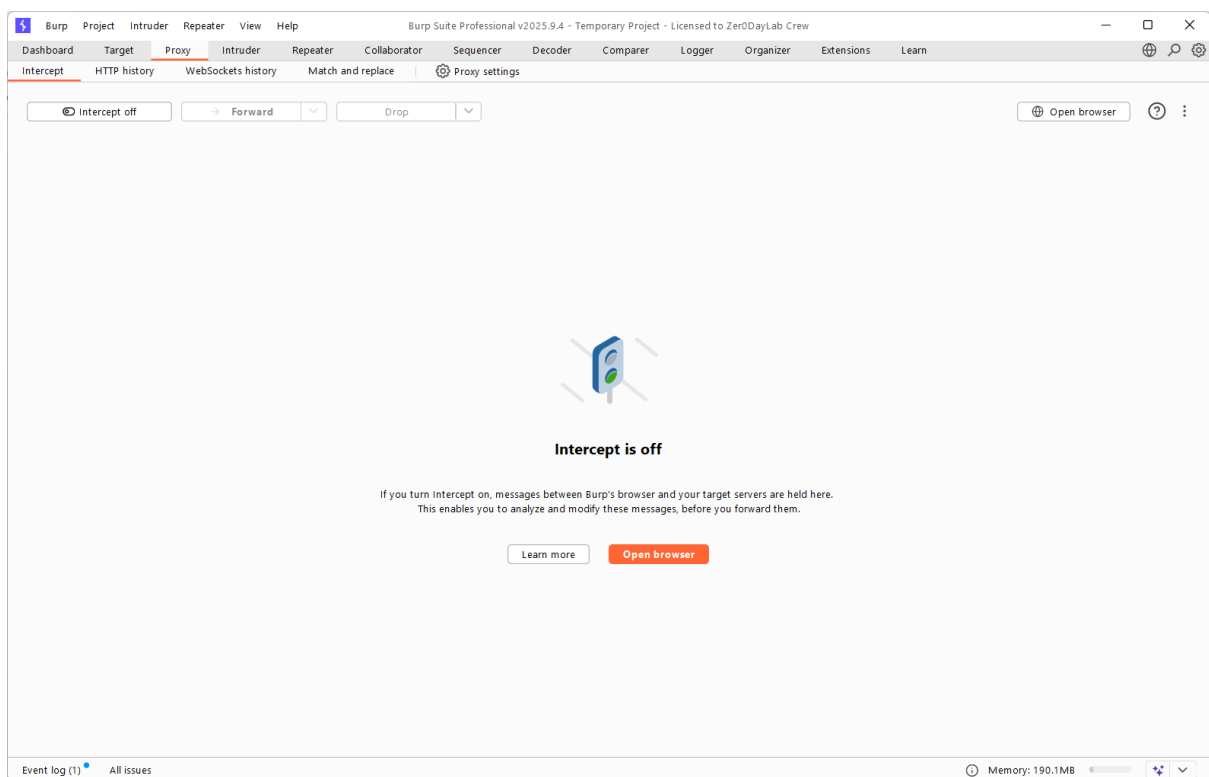
☒ Credit Card/Debit Card/Wallet/Net Banking.

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.

The screenshot shows the OgdMart checkout page. The page has a header with navigation links, a search bar, and a delivery location set to 142024. The main form contains fields for company name, address, town/city, state, postcode, and country. A payment method section is on the right, and a FoxyProxy extension overlay is visible in the top right corner.

Company name (optional)

Company name

Address

gfhfrh

Address Line 2

Address Line 3

Town / City *

ludhiana

State *

punjab

Postcode / ZIP *

142024

Country *

INDIA

Order notes (optional)

Order notes (optional)

☐ Create an account?

☒ My delivery and billing details are the same.

Payment Method

Your personal data will be used to complete your order, support your experience, and for other purposes. See our privacy policy.

☒ I have read and agree to the website

☒ Credit Card/Debit Card/Wallet/Net Banking.

PROCEED FOR PAYMENT

FoxyProxy

Disable

burpsuite

More

filter

Include Host

Exclude Host

Options

Log

IP

Location

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.

The screenshot shows the Burp Suite Professional interface. The 'Intercept' tab is active, displaying a list of intercepted requests. The first request is a POST to https://www.ogdmart.com/submitcheckout. The 'Request' tab is selected, showing the raw HTTP request. The 'Inspector' tab is also visible, showing the request attributes, query parameters, body parameters, cookies, and headers.

Request

Pretty Raw Hex

```

12 Upgrade-Insecure-Requests : 1
13 Sec-Fetch-Dest : document
14 Sec-Fetch-Mode : navigate
15 Sec-Fetch-Site : same-origin
16 Sec-Fetch-User : ?1
17 Priority : u=0, i
18 Te: trailers
19 Connection : keep-alive
20
21 txtBillingAddressFname =Lakshman+ &txtBillingAddressLname =Kumar &txtBillingAddressEmailAddress =hjhkjkk440gmail.com &
txtBillingAddressPhone =2554158744 &txtBillingAddressCompany = &txtBillingAddressLine1 =gfhfrh &txtBillingAddressLine2 = &
txtBillingAddressLine3 = &txtBillingTown =ludhiana &txtBillingState =punjab &txtBillingPostcode =142024 &txtBillingCountry =INDIA &
txtOrderNotes = &password = &txtShippingAddressFname =Lakshman+ &txtShippingAddressLname =Kumar &txtShippingAddressEmailAddress =
hjhkjkk440gmail.com &txtShippingAddressPhone =2554158744 &txtShippingAddressLine1 =gfhfrh &txtShippingAddressLine2 = &
txtShippingAddressLine3 = &txtShippingTown =ludhiana &txtShippingState =punjab &txtShippingPostcode =142024 &txtShippingCountry =INDIA &
coupon_code = &cart_subt =1599 &cart_disc =0 &cart_total =1599 &paymenttype =2

```

Inspector

Request attributes

Request query parameters

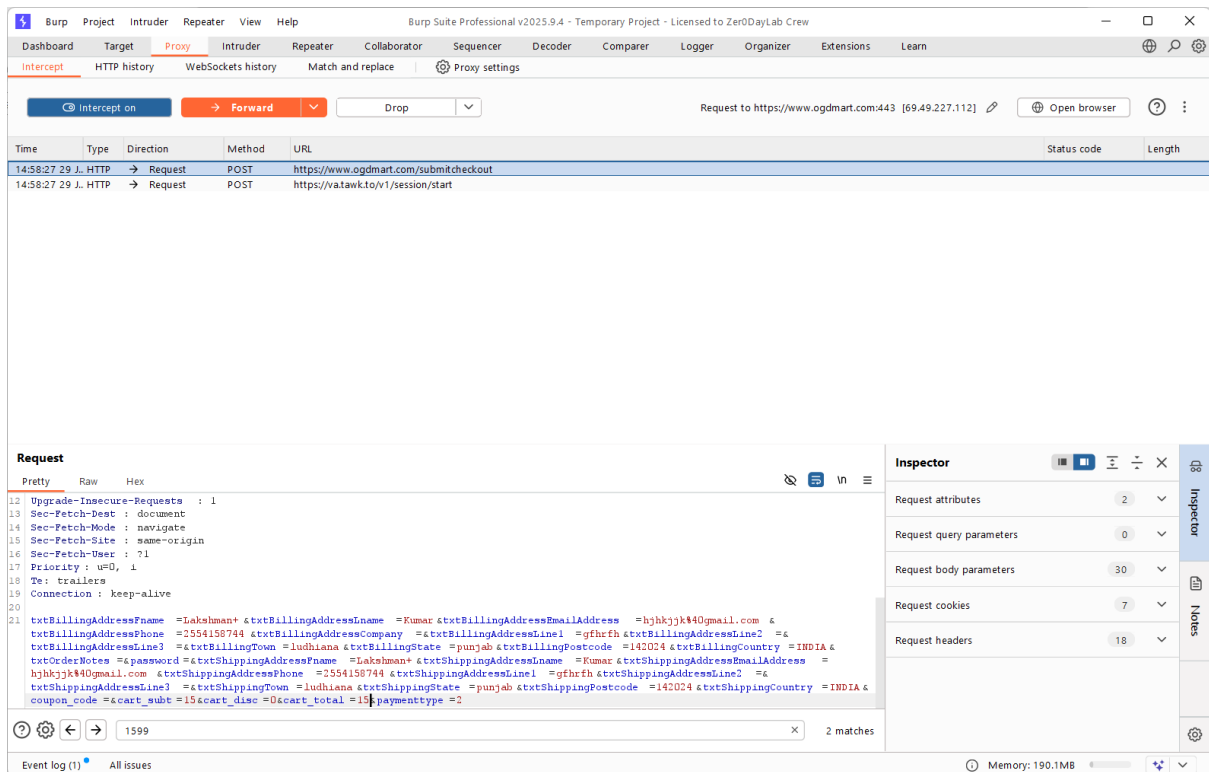
Request body parameters

Request cookies

Request headers

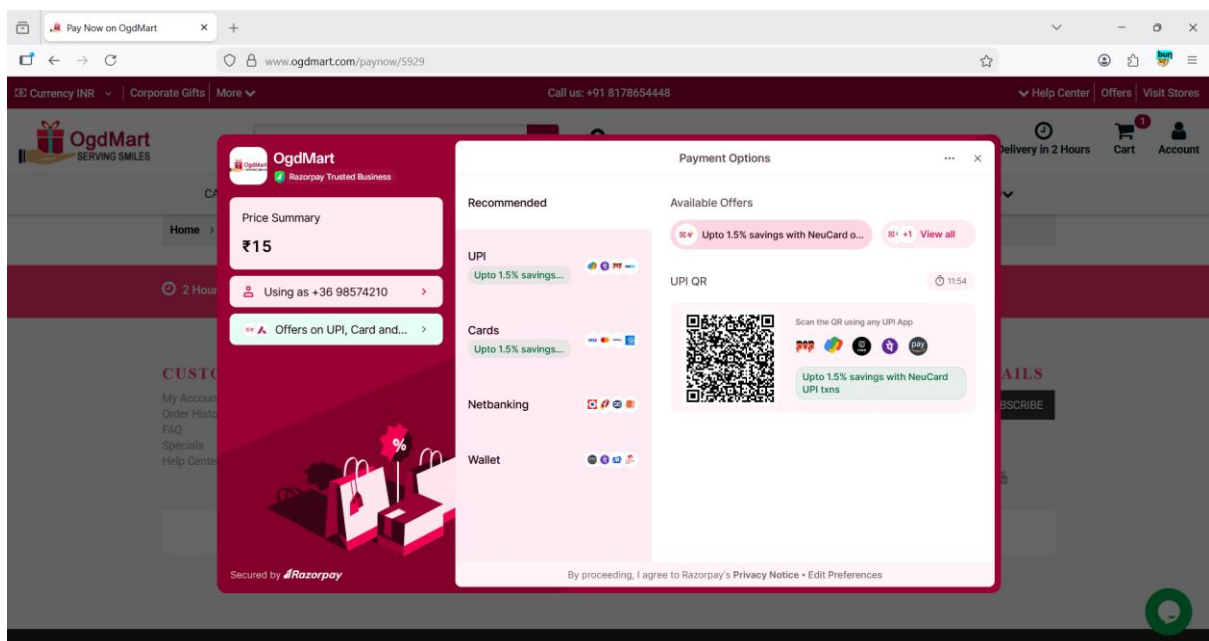
Event log (1) All issues

Memory: 190.1MB



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.