

# FCS Project - Security Vulnerabilities

## Group 8

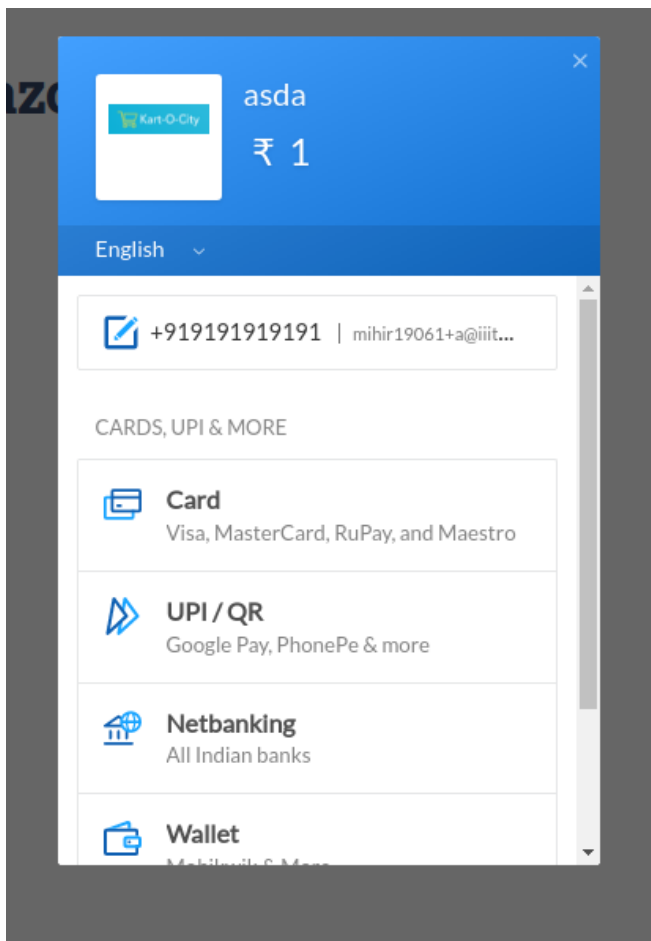
Mihir Chaturvedi - 2019061

---

### 1. Cart price can be changed by changing the value in the hidden field

- At the /otpcheckout page, we can “inspect element” and directly edit the hidden field that holds the “total\_price”. We can lower it down to “1”.

```
<input hidden type="text" name="email" value="mihir19061+a@iiitd.ac.in">  
<input hidden type="text" name="address" value="asdsa">  
<input hidden type="number" name="total_price" value="1"> == $0
```

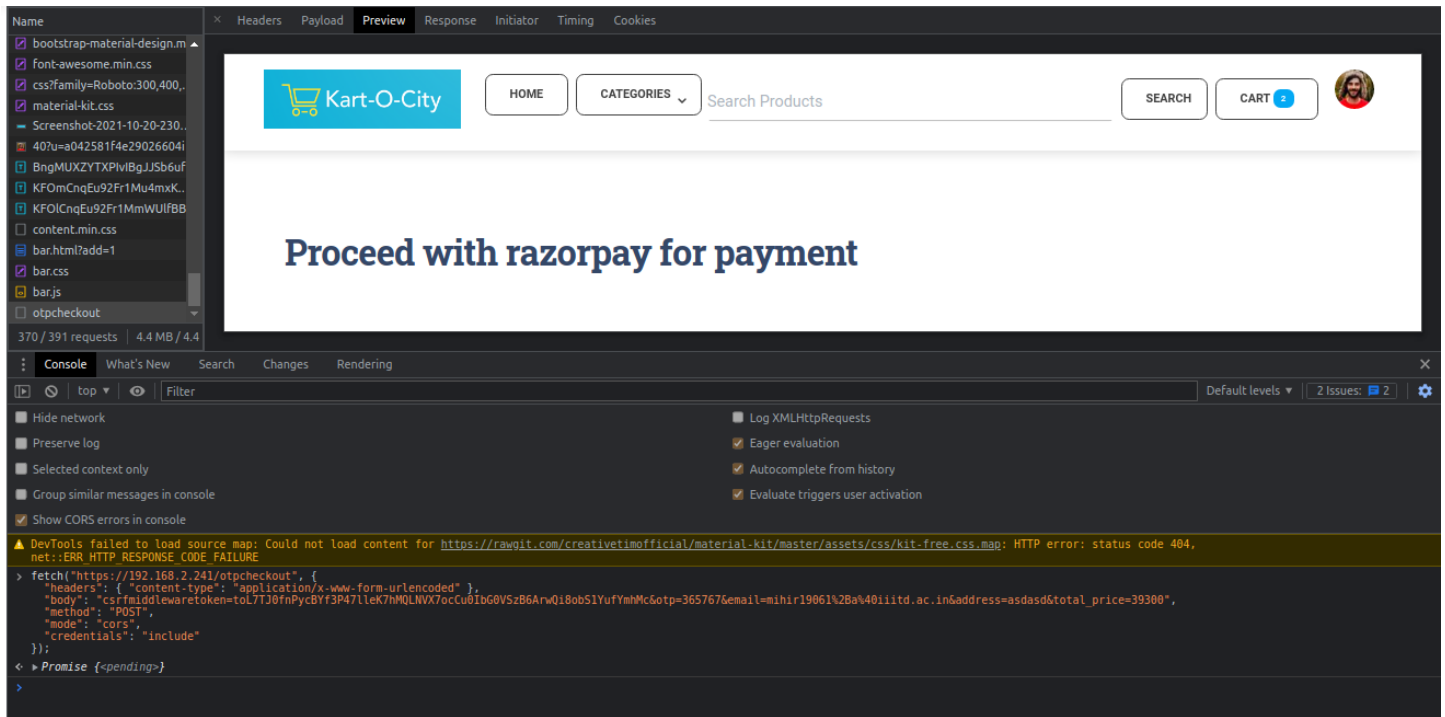


### 2. OTP verification can be brute-forced on login

Since the CSRF tokens can be re-used as they are not setup properly, one can copy the same request and send it through again, by incrementally changing the request.

The website does not have an OTP expiry nor max login attempts.

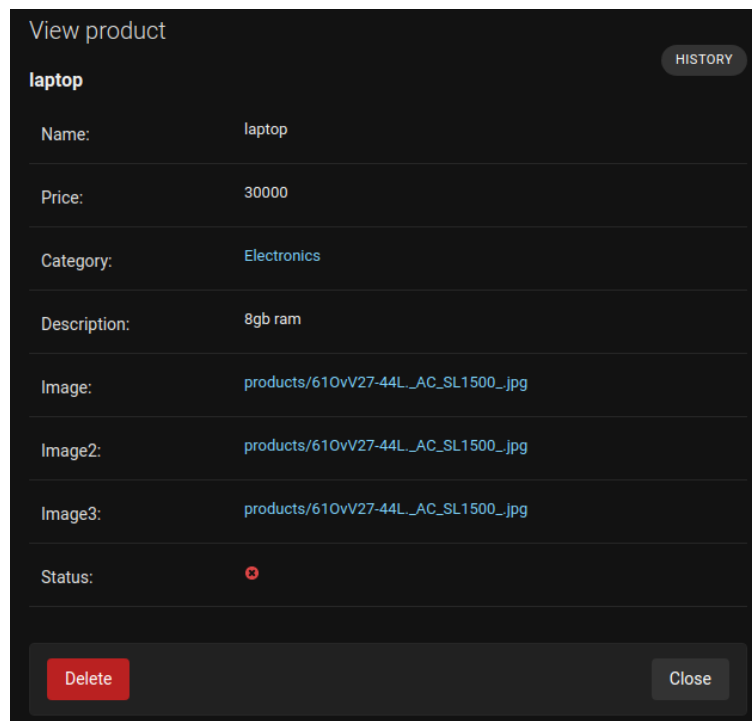
The following screenshot shows a successful OTP sent through a `fetch` request from the browser console.



### 3. CSRF tokens' verification not setup correctly

As shown above, including the screenshot, the same CSRF middleware token that is present to authenticate the request, can be sent multiple times to multiple requests to bypass CSRF protection.

### 4. Admin view does not have ability to edit products, so we can't verify them and view them on the site



5. Products with negative prices can be added through the Admin view, and can be checked out

### Add product

**Name:**

**Price:**

**Category:**

**Description:**




**Image:**  G8jtY0P.png

**Image2:**  G8jtY0P.png

**Image3:**  G8jtY0P.png

☒ **Status**

### Your Cart

Sno.	Image	Product	Price	Quantity	Total
1		SERA Women's Georgette A-Line Mini Dress	₹ 767	3	₹ 2301
2		OnePlus 9R 5G(Lake Blue, 8GB, 128GB )-Phone	₹ 36999	1	₹ 36999
3		asd	₹ -10	1	₹ -10
				<b>Total</b>	<b>₹ 39290</b>

[Checkout](#) 