Testing slide visibility

Credit card fraud

You don't want to be
the common point of purchase

Who am I?

Dan Wallis, fredden

Christchurch, NZ

@mrdanwallis, https://web.fredden.org/

I'm a sysadmin doing some web development.

Views are my own, et cetera.

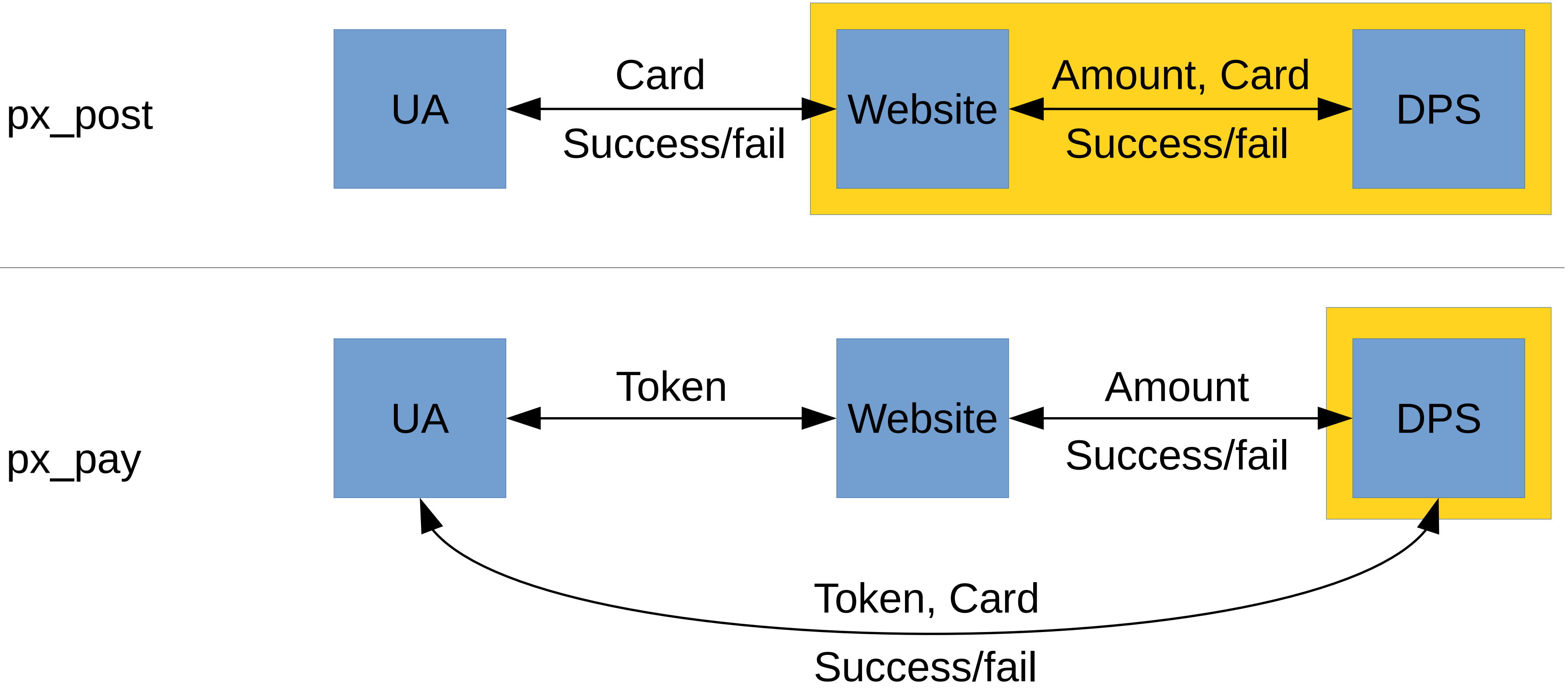
ISIG, OWASP, music, family

E2 Digital, Harvey Cameron

- Agency
- Joomla, Magento, Silverstripe
- Hosting, PCI

Payment Express (DPS)

px_post, px_pay, px_fusion



Magento

- Open-source shopping website framework
- PHP/MySQL - “standard LAMP stack”
- Very complex

- Slow.

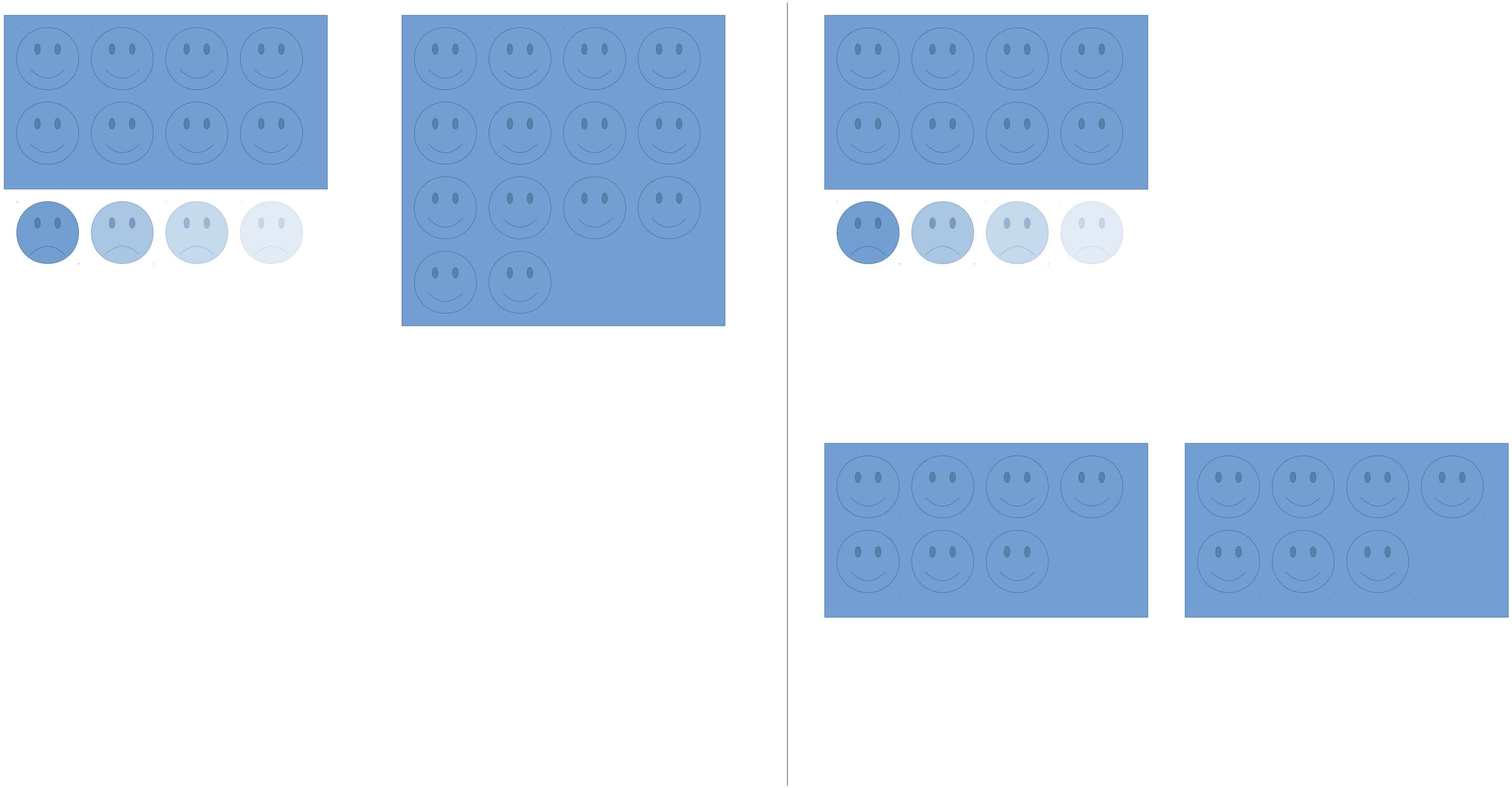
Problem: Website is slow

Problem: Website is slow

- Concurrent users
- Content Delivery Network
- Minimum page load time
- User experience

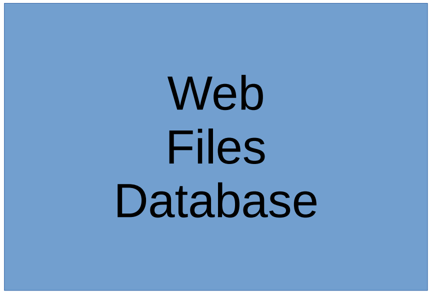
Scaling

- Vertical versus horizontal



Scaling

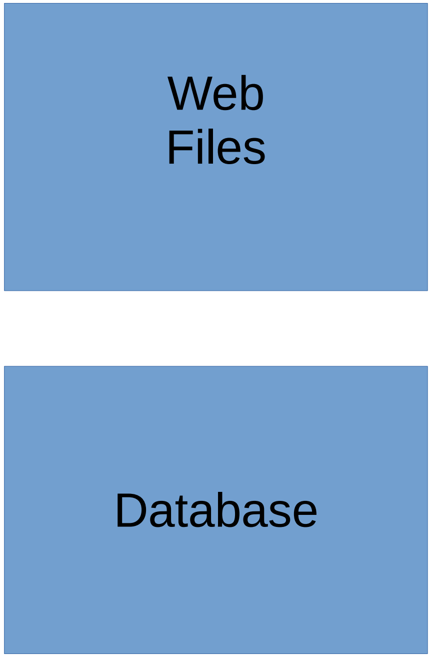
- One box



Web
Files
Database

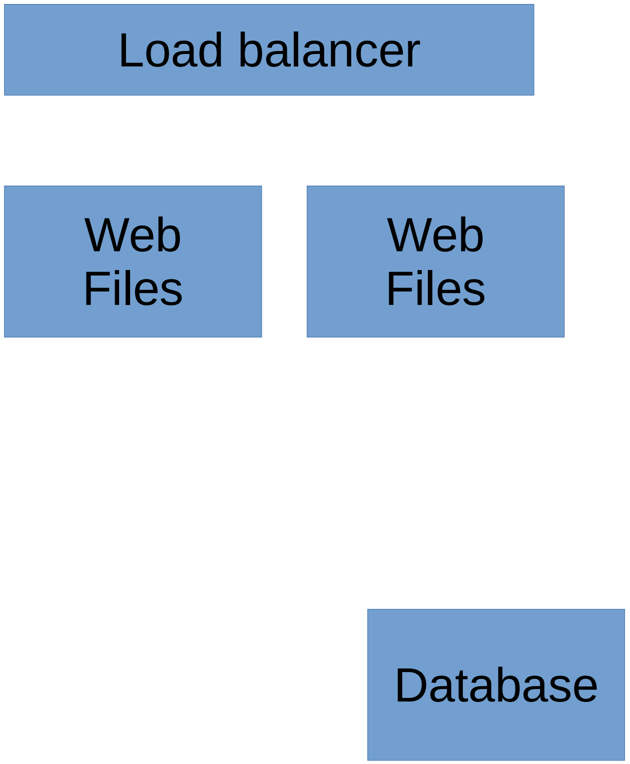
Scaling

- Two boxen



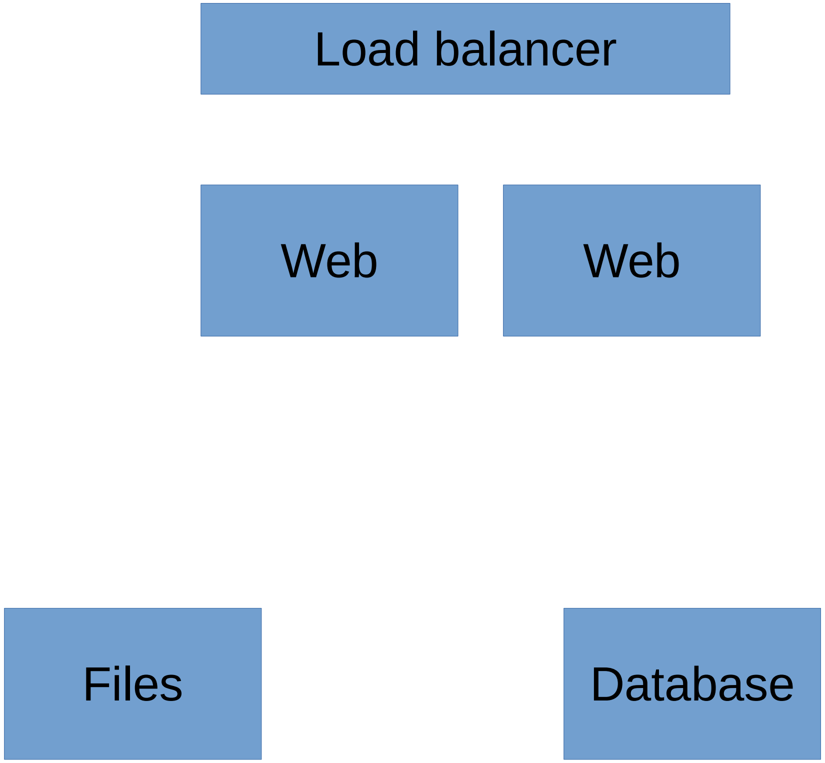
Scaling

- Small cluster
- TLS



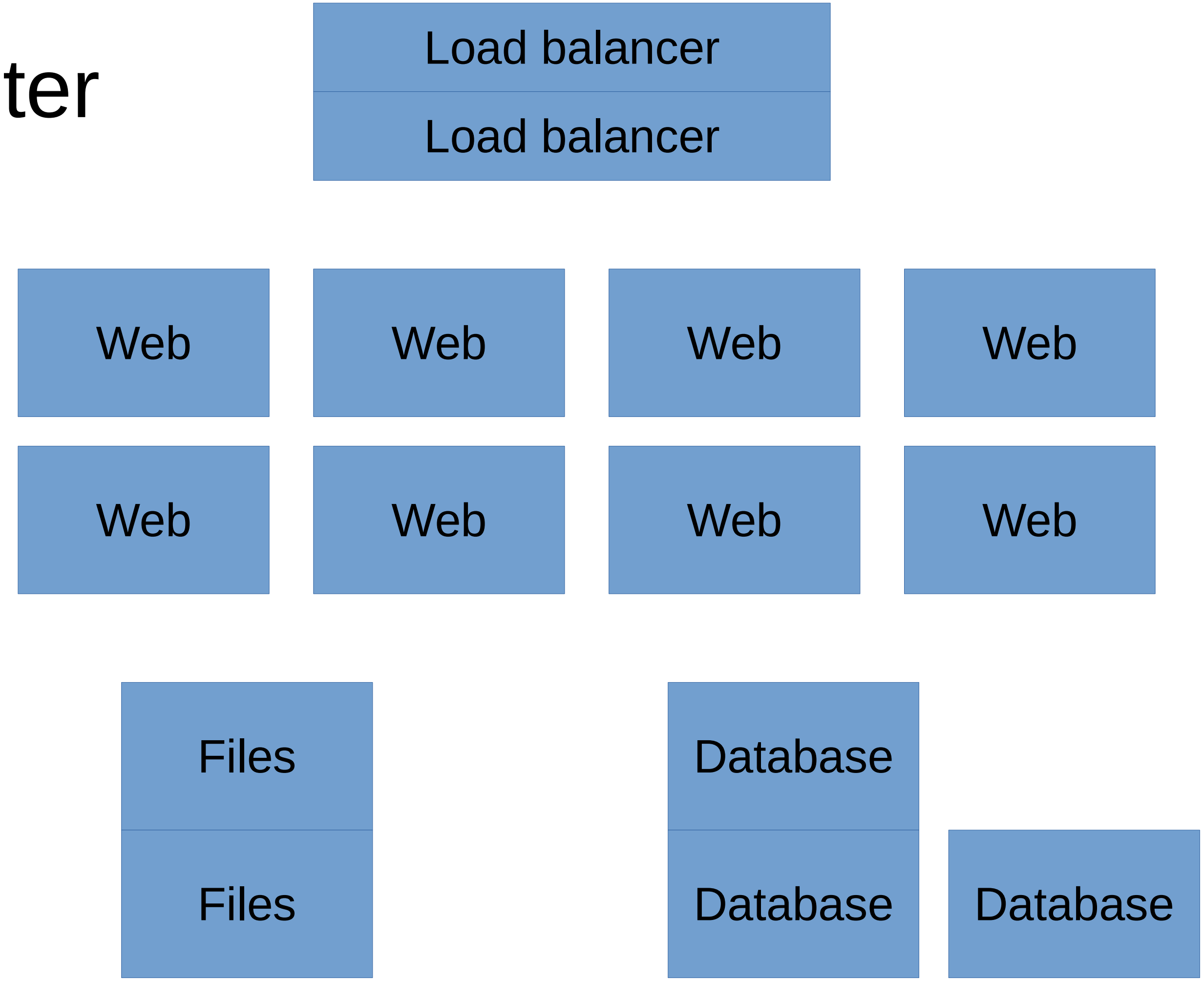
Scaling

- Small cluster
- TLS



Scaling

- Bigger cluster



Load balancer

Load balancer

Web Web Web Web

Web Web Web Web

Files

Files

Database

Database Database

Problem: Website is slow

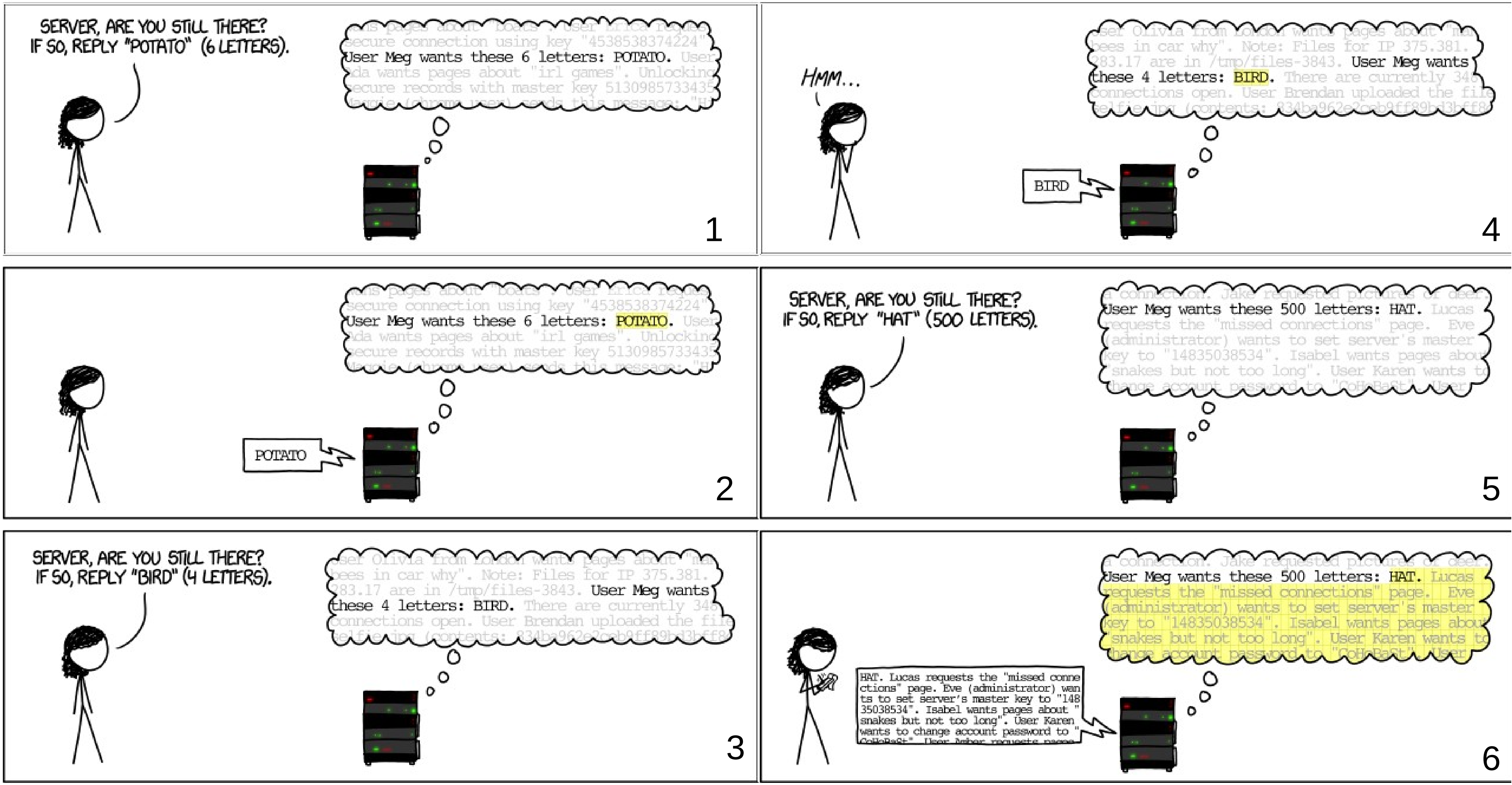
- Concurrent users
- Content Delivery Network
- Minimum page load time
- User experience

Problem: Website is slow

- ~~Concurrent users~~
- Content Delivery Network
- Minimum page load time
- User experience

Heartbleed

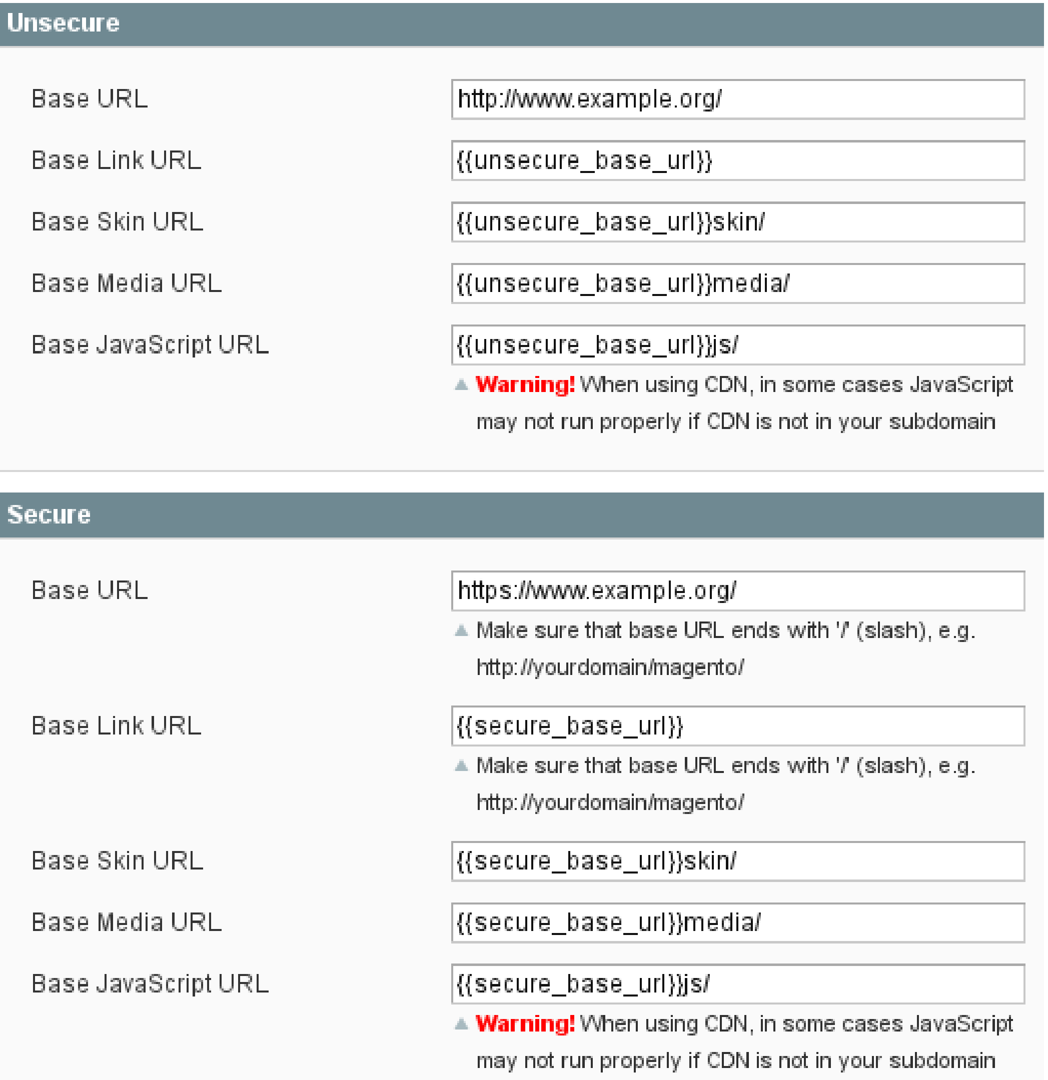
- Peek into server's memory
- https://xkcd.com/1354/


SERVER, ARE YOU STILL THERE? IF SO, REPLY "POTATO" (6 LETTERS).
ons pages about "boats". User Erica requests secure connection using key "4538538374224". User Meg wants these 6 letters: POTATO. User Ada wants pages about "irl games". Unlocking secure records with master key 5130985733435. Maggie (chrome user) sends this message: "H
1
ons pages about "boats". User Erica requests secure connection using key "4538538374224". User Meg wants these 6 letters: POTATO. User Ada wants pages about "irl games". Unlocking secure records with master key 5130985733435. Maggie (chrome user) sends this message: "H
POTATO
2
SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).
User Olivia from London wants pages about "ma bees in car why". Note: Files for IP 375.381.283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2ceb9ff89bd3bff8
3
HMM...
User Olivia from London wants pages about "ma bees in car why". Note: Files for IP 375.381.283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2ceb9ff89bd3bff8
BIRD
4
SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
5
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User Amber requests pages
6

Problem: Website is slow

- ~~Concurrent users~~
- Content Delivery Network
- Minimum page load time
- User experience

CDN

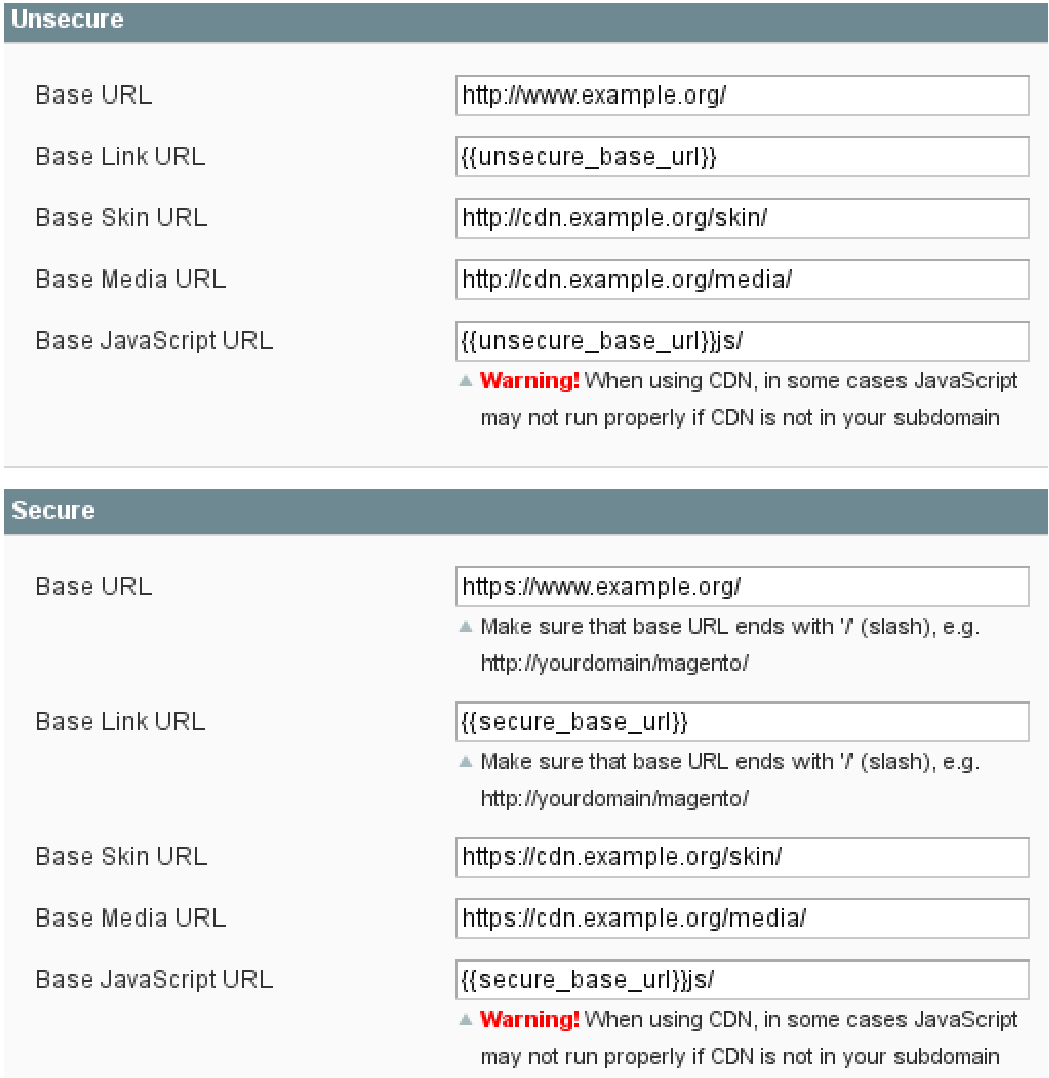


Unsecure

Base URL	http://www.example.org/
Base Link URL	{{unsecure_base_url}}
Base Skin URL	{{unsecure_base_url}}skin/
Base Media URL	{{unsecure_base_url}}media/
Base JavaScript URL	{{unsecure_base_url}}js/ ▲ **Warning!** When using CDN, in some cases JavaScript may not run properly if CDN is not in your subdomain

Secure

Base URL	https://www.example.org/ ▲ Make sure that base URL ends with '/' (slash), e.g. http://yourdomain/magento/
Base Link URL	{{secure_base_url}} ▲ Make sure that base URL ends with '/' (slash), e.g. http://yourdomain/magento/
Base Skin URL	{{secure_base_url}}skin/
Base Media URL	{{secure_base_url}}media/
Base JavaScript URL	{{secure_base_url}}js/ ▲ **Warning!** When using CDN, in some cases JavaScript may not run properly if CDN is not in your subdomain



Unsecure

Base URL	http://www.example.org/
Base Link URL	{{unsecure_base_url}}
Base Skin URL	http://cdn.example.org/skin/
Base Media URL	http://cdn.example.org/media/
Base JavaScript URL	{{unsecure_base_url}}js/ ▲ **Warning!** When using CDN, in some cases JavaScript may not run properly if CDN is not in your subdomain

Secure

Base URL	https://www.example.org/ ▲ Make sure that base URL ends with '/' (slash), e.g. http://yourdomain/magento/
Base Link URL	{{secure_base_url}} ▲ Make sure that base URL ends with '/' (slash), e.g. http://yourdomain/magento/
Base Skin URL	https://cdn.example.org/skin/
Base Media URL	https://cdn.example.org/media/
Base JavaScript URL	{{secure_base_url}}js/ ▲ **Warning!** When using CDN, in some cases JavaScript may not run properly if CDN is not in your subdomain

Problem: Website is slow

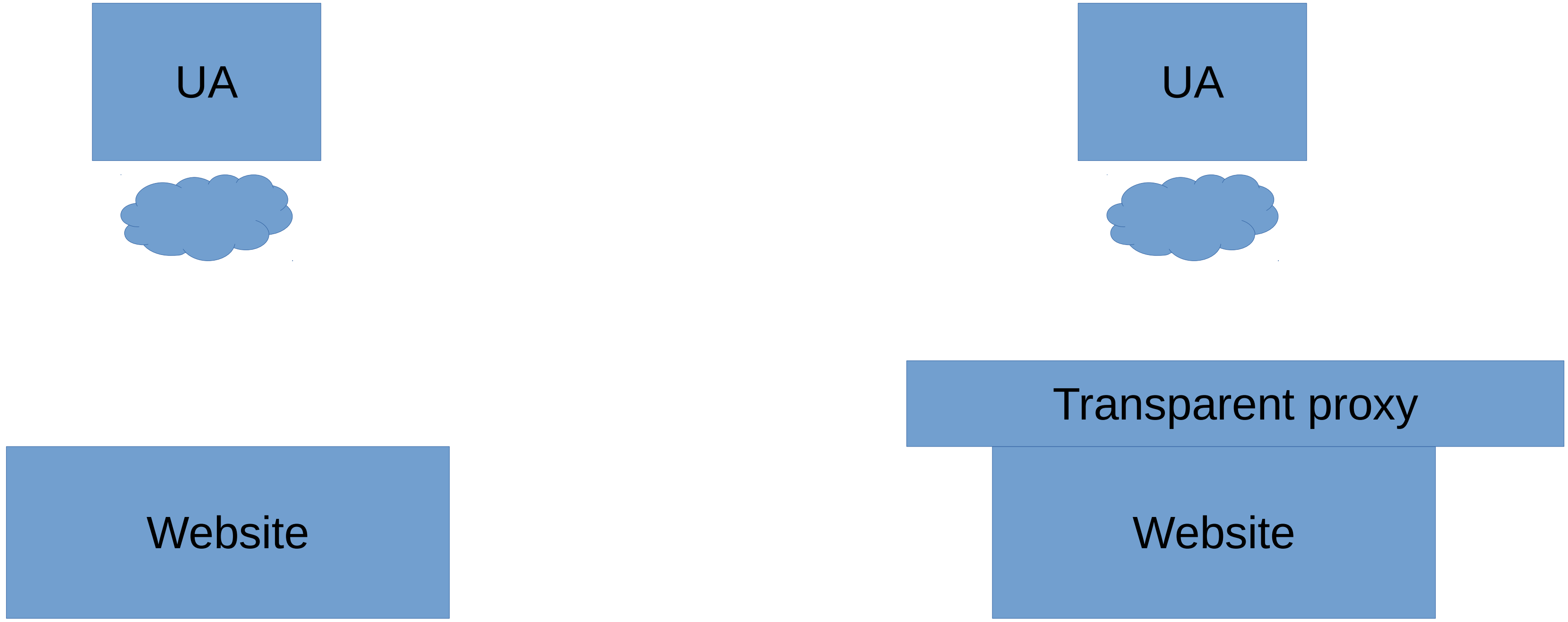
- ~~Concurrent users~~
- Content Delivery Network
- Minimum page load time
- User experience

Problem: Website is slow

- ~~Concurrent users~~
- ~~Content Delivery Network~~
- Minimum page load time
- User experience

Varnish & Turpentine

- TLS

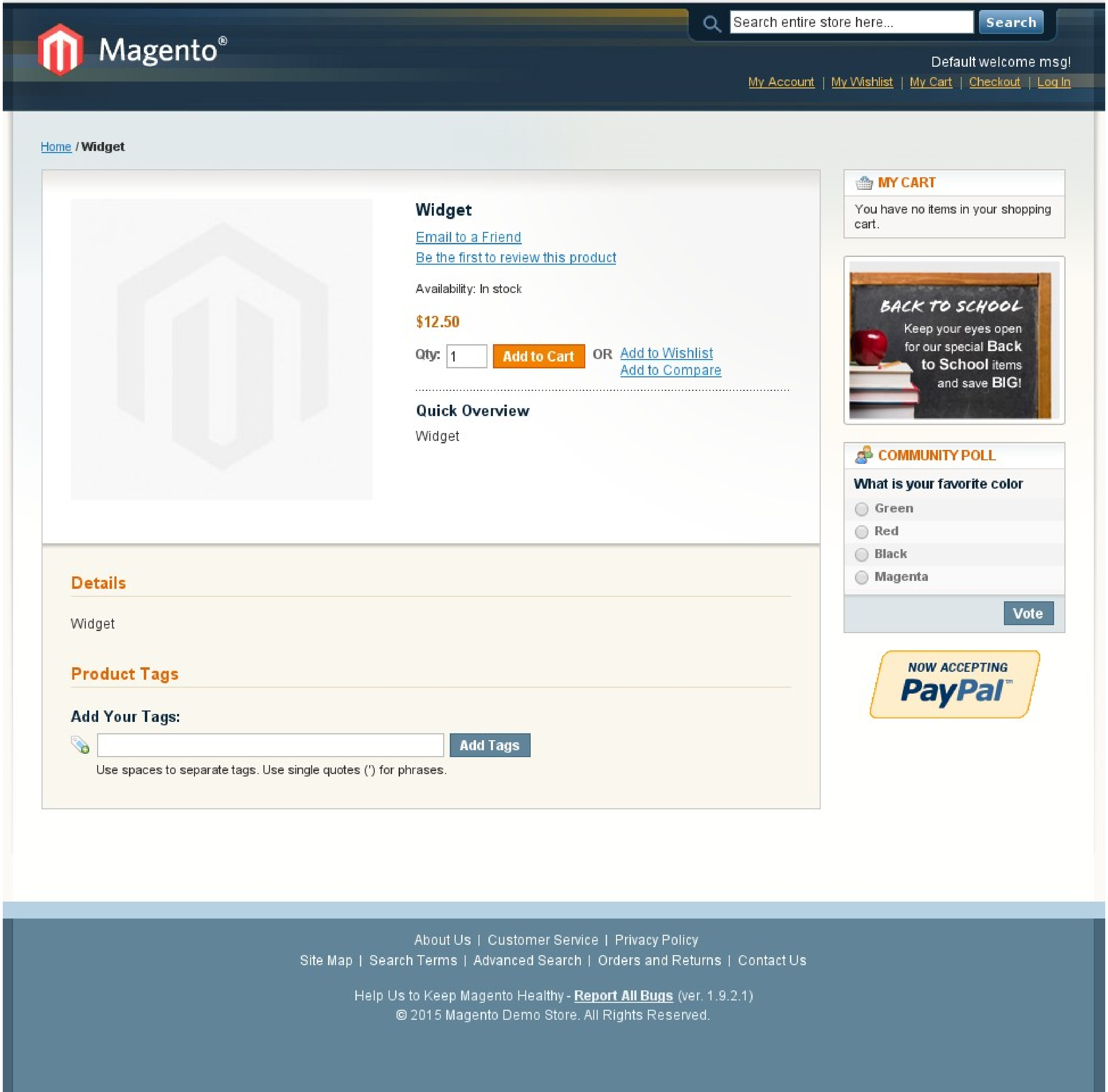


Problem: Website is slow

- ~~Concurrent users~~
- ~~Content Delivery Network~~
- Minimum page load time
- User experience

Problem: Website is slow

- ~~Concurrent users~~
- ~~Content Delivery Network~~
- ~~Minimum page load time~~
- User experience



Default welcome msg!

Widget

Availability: In stock

$12.50

Quick Overview

Widget

Details

Widget

Product Tags

Add Your Tags:

Use spaces to separate tags. Use single quotes (') for phrases.

You have no items in your shopping cart.

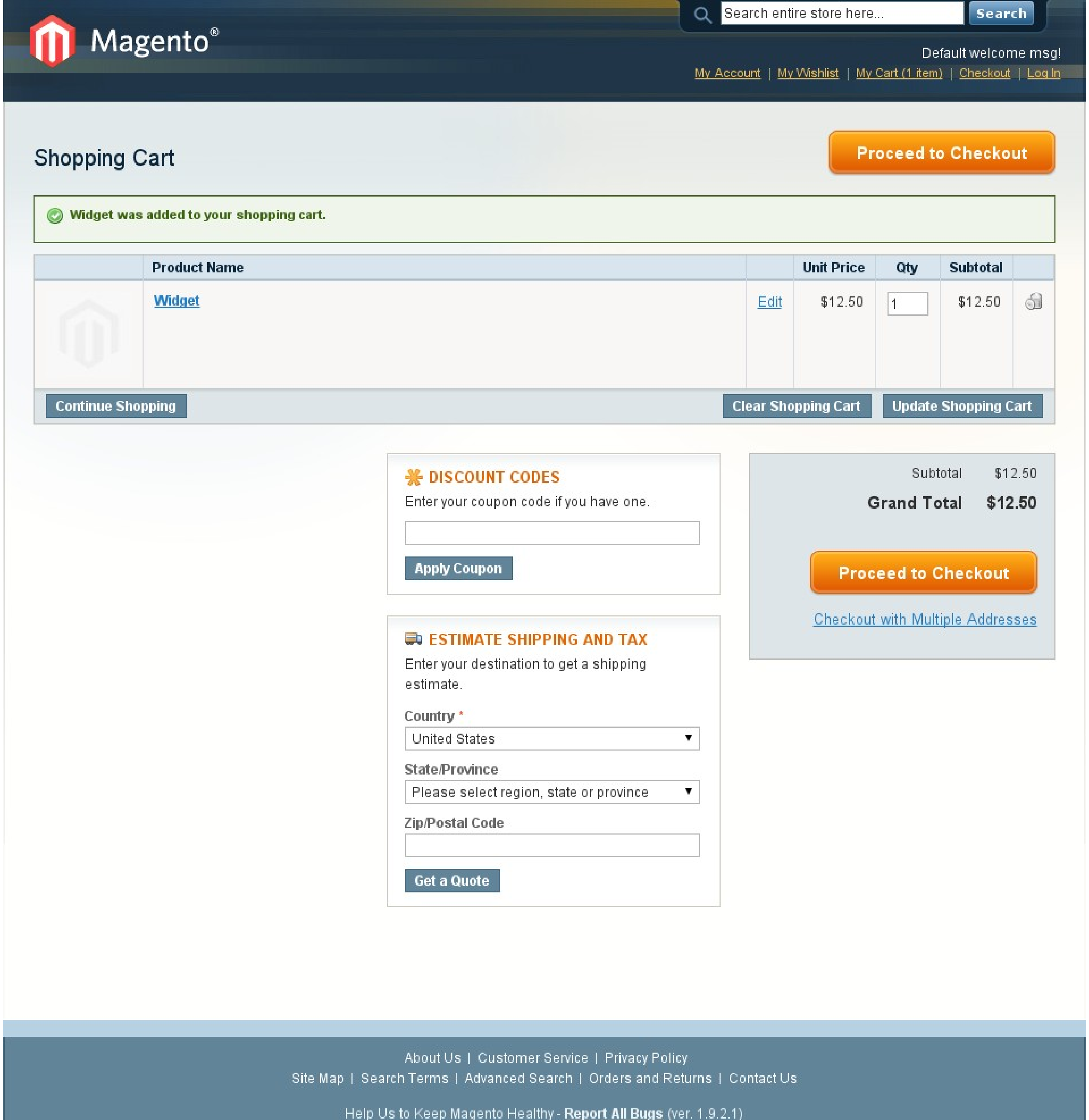
BACK TO SCHOOL
Keep your eyes open for our special Back to School items and save BIG!

What is your favorite color

○ Green
○ Red
○ Black
○ Magenta

About Us | Customer Service | Privacy Policy
Site Map | Search Terms | Advanced Search | Orders and Returns | Contact Us

Help Us to Keep Magento Healthy - Report All Bugs (ver. 1.9.2.1)
© 2015 Magento Demo Store. All Rights Reserved.


Magento®
Search entire store here...
Search
My Account | My Wishlist | My Cart (1 item) | Checkout | Log In
Proceed to Checkout
Continue Shopping
Clear Shopping Cart
Update Shopping Cart
Apply Coupon
Proceed to Checkout
Checkout with Multiple Addresses
Get a Quote
About Us | Customer Service | Privacy Policy
Site Map | Search Terms | Advanced Search | Orders and Returns | Contact Us

Default welcome msg!

Shopping Cart

Widget was added to your shopping cart.

	Product Name		Unit Price	Qty	Subtotal	
	Widget	Edit	$12.50	1	$12.50	

DISCOUNT CODES

Enter your coupon code if you have one.

ESTIMATE SHIPPING AND TAX

Enter your destination to get a shipping estimate.

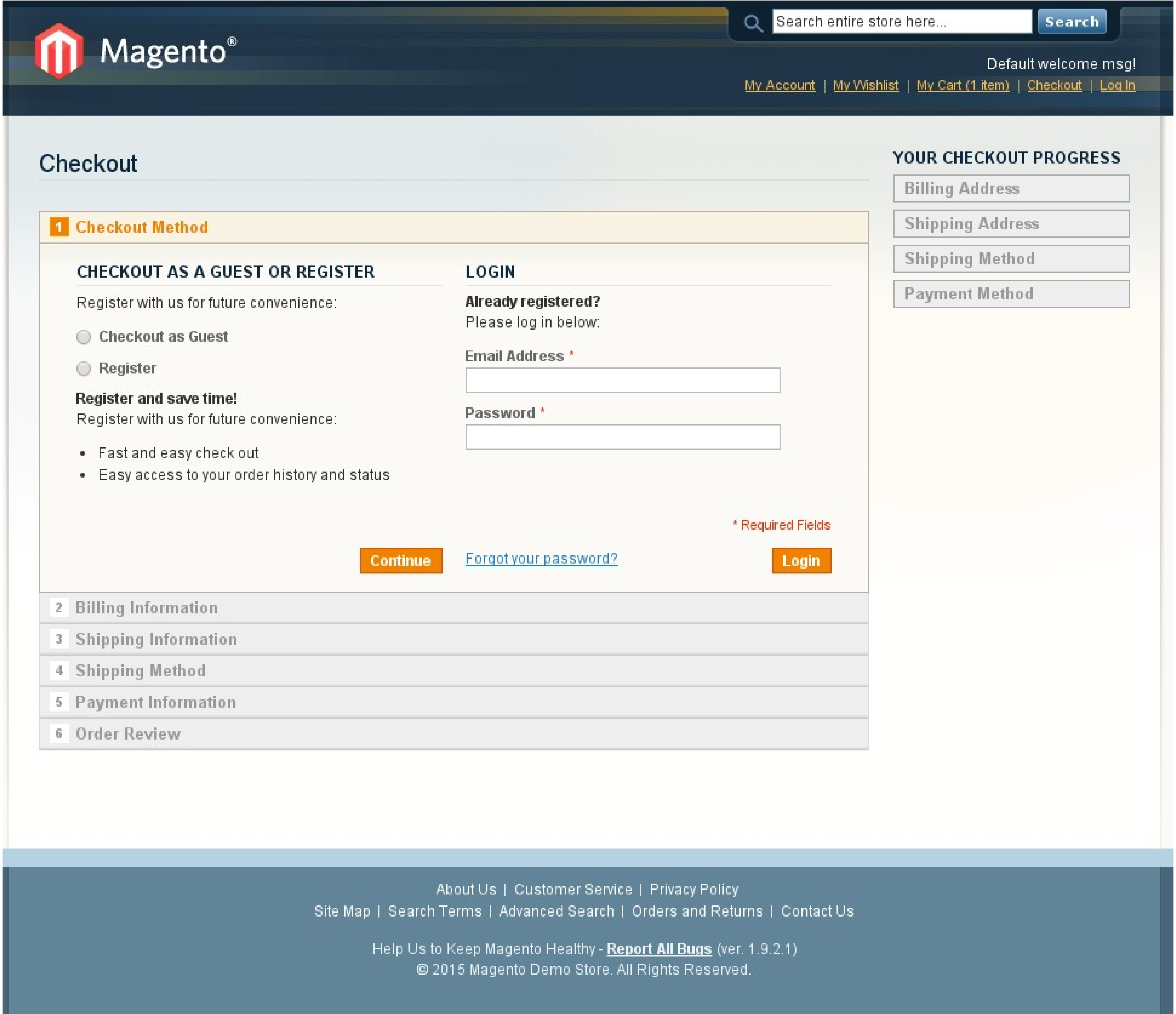
Country *
United States

State/Province
Please select region, state or province

Zip/Postal Code

Subtotal	$12.50
Grand Total	**$12.50**

Help Us to Keep Magento Healthy - **Report All Bugs** (ver. 1.9.2.1)


Magento®
Search entire store here...
Search
Default welcome msg!
My Account | My Wishlist | My Cart (1 item) | Checkout | Log In

Checkout

YOUR CHECKOUT PROGRESS

- Billing Address
- Shipping Address
- Shipping Method
- Payment Method

1 Checkout Method

CHECKOUT AS A GUEST OR REGISTER

Register with us for future convenience:

○ Checkout as Guest

○ Register

Register and save time!
Register with us for future convenience:

- Fast and easy check out
- Easy access to your order history and status

LOGIN

Already registered?
Please log in below:

Email Address *

Password *

* Required Fields

2 Billing Information

3 Shipping Information

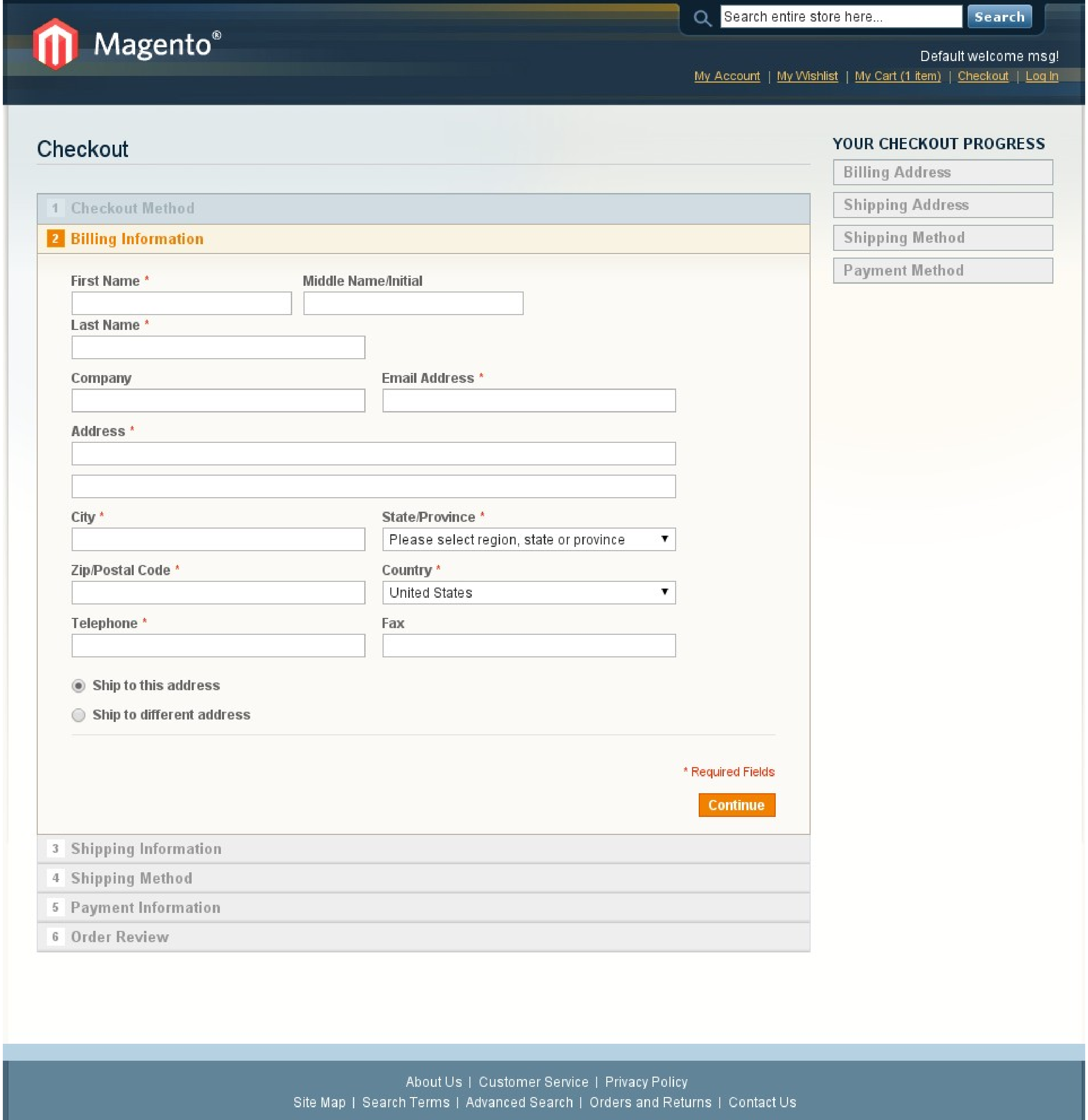
4 Shipping Method

5 Payment Information

6 Order Review

About Us | Customer Service | Privacy Policy
Site Map | Search Terms | Advanced Search | Orders and Returns | Contact Us

Help Us to Keep Magento Healthy - **Report All Bugs** (ver. 1.9.2.1)
© 2015 Magento Demo Store. All Rights Reserved.



Magento®

Search entire store here... Search

Default welcome msg!

My Account | My Wishlist | My Cart (1 item) | Checkout | Log In

Checkout

1 Checkout Method

2 Billing Information

First Name *

Middle Name/Initial

Last Name *

Company

Email Address *

Address *

City *

State/Province *

Please select region, state or province ▾

Zip/Postal Code *

Country *

United States ▾

Telephone *

Fax

● Ship to this address

○ Ship to different address

* Required Fields

Continue

3 Shipping Information

4 Shipping Method

5 Payment Information

6 Order Review

YOUR CHECKOUT PROGRESS

Billing Address

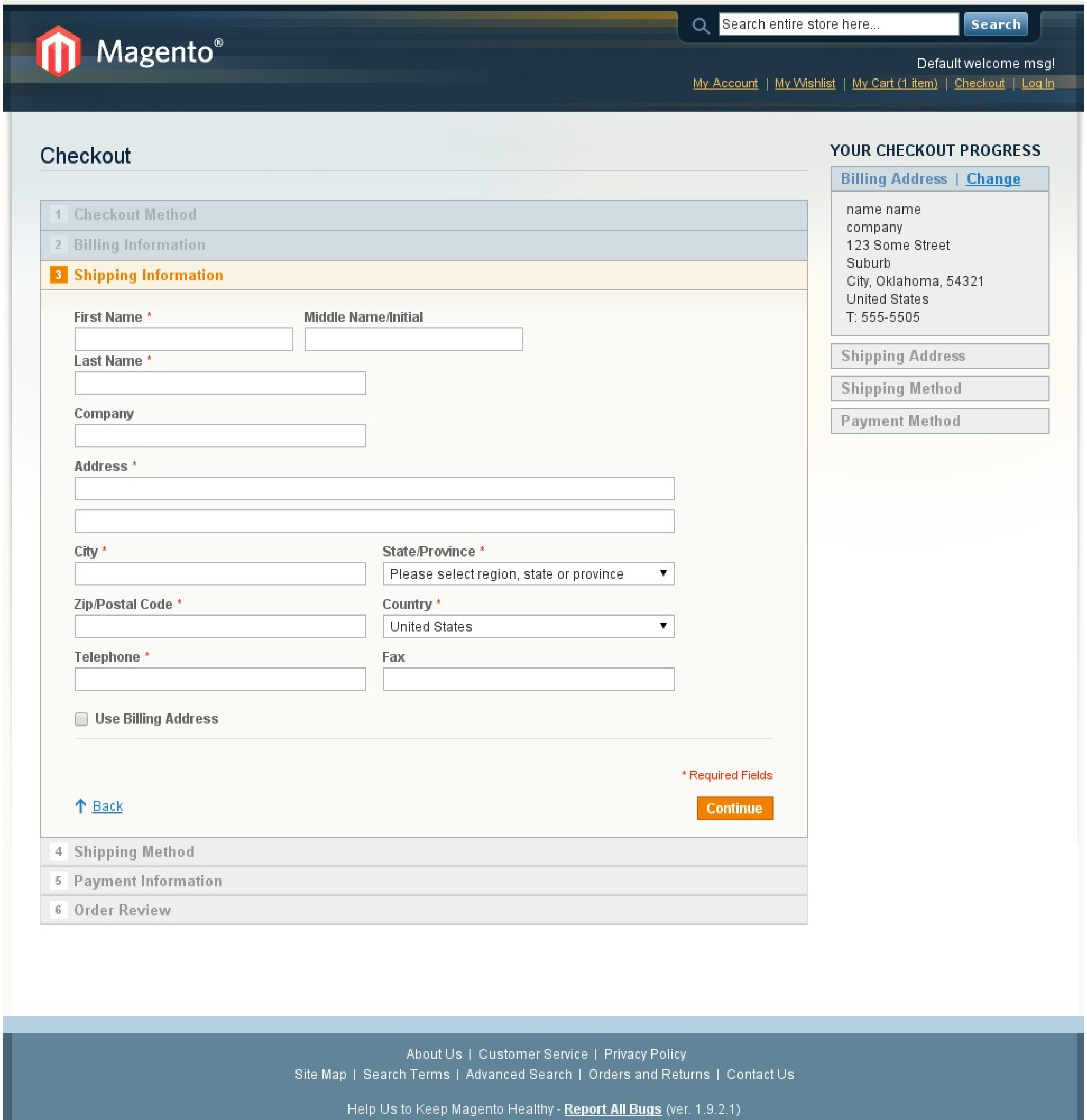
Shipping Address

Shipping Method

Payment Method

About Us | Customer Service | Privacy Policy

Site Map | Search Terms | Advanced Search | Orders and Returns | Contact Us



Magento®

Search entire store here... Search

Default welcome msg!

My Account | My Wishlist | My Cart (1 item) | Checkout | Log In

Checkout

1 Checkout Method

2 Billing Information

3 Shipping Information

First Name *

Middle Name/Initial

Last Name *

Company

Address *

City *

State/Province * Please select region, state or province ▾

Zip/Postal Code *

Country * United States ▾

Telephone *

Fax

□ Use Billing Address

* Required Fields

↑ Back

Continue

4 Shipping Method

5 Payment Information

6 Order Review

YOUR CHECKOUT PROGRESS

Billing Address | Change

name name
company
123 Some Street
Suburb
City, Oklahoma, 54321
United States
T: 555-5505

Shipping Address

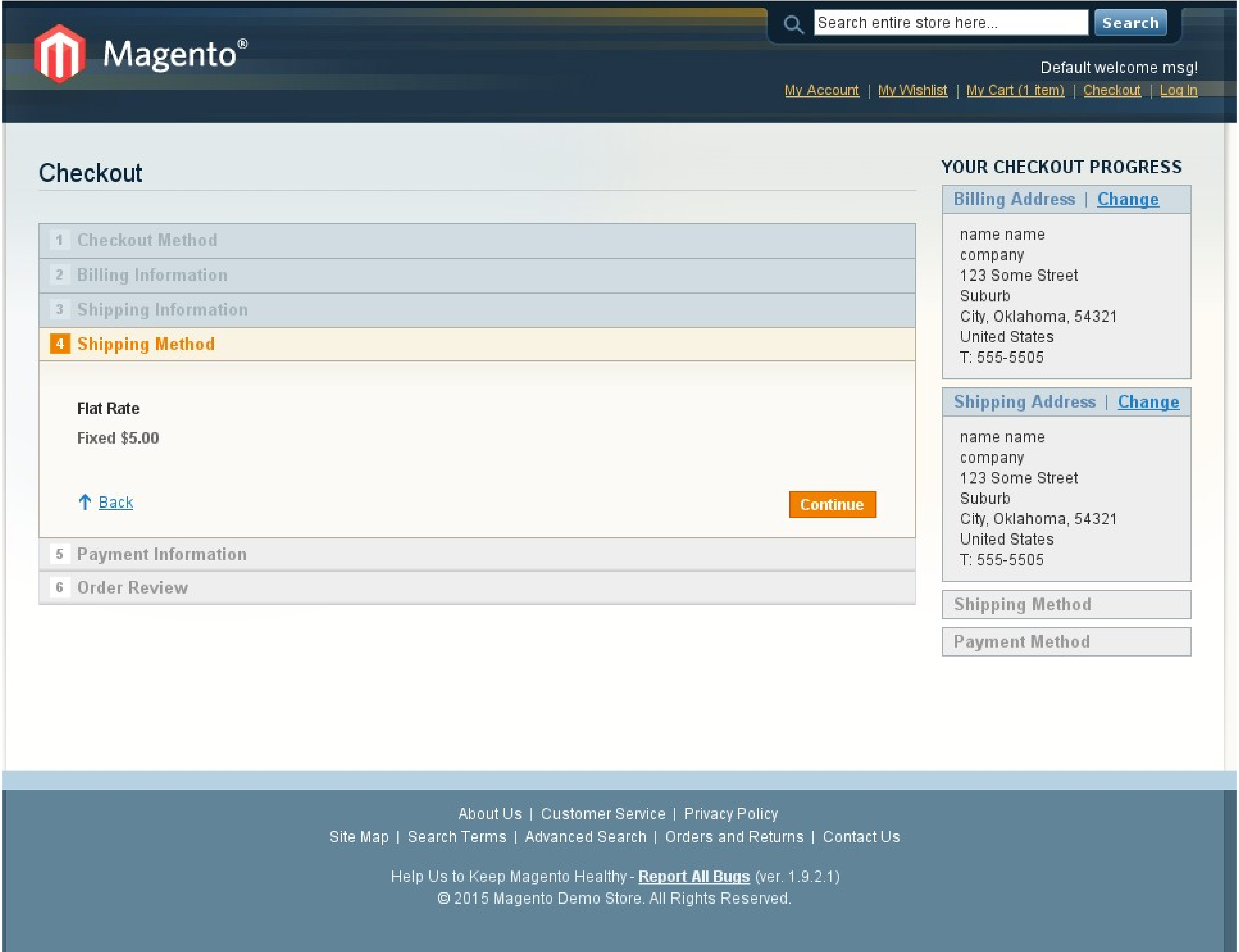
Shipping Method

Payment Method

About Us | Customer Service | Privacy Policy

Site Map | Search Terms | Advanced Search | Orders and Returns | Contact Us

Help Us to Keep Magento Healthy - **Report All Bugs** (ver. 1.9.2.1)


Magento®
Search entire store here...
Search
Default welcome msg!
My Account | My Wishlist | My Cart (1 item) | Checkout | Log In

Checkout

1 Checkout Method

2 Billing Information

3 Shipping Information

4 Shipping Method

Flat Rate

Fixed $5.00

↑ Back

Continue

5 Payment Information

6 Order Review

YOUR CHECKOUT PROGRESS

Billing Address | Change

name name
company
123 Some Street
Suburb
City, Oklahoma, 54321
United States
T: 555-5505

Shipping Address | Change

name name
company
123 Some Street
Suburb
City, Oklahoma, 54321
United States
T: 555-5505

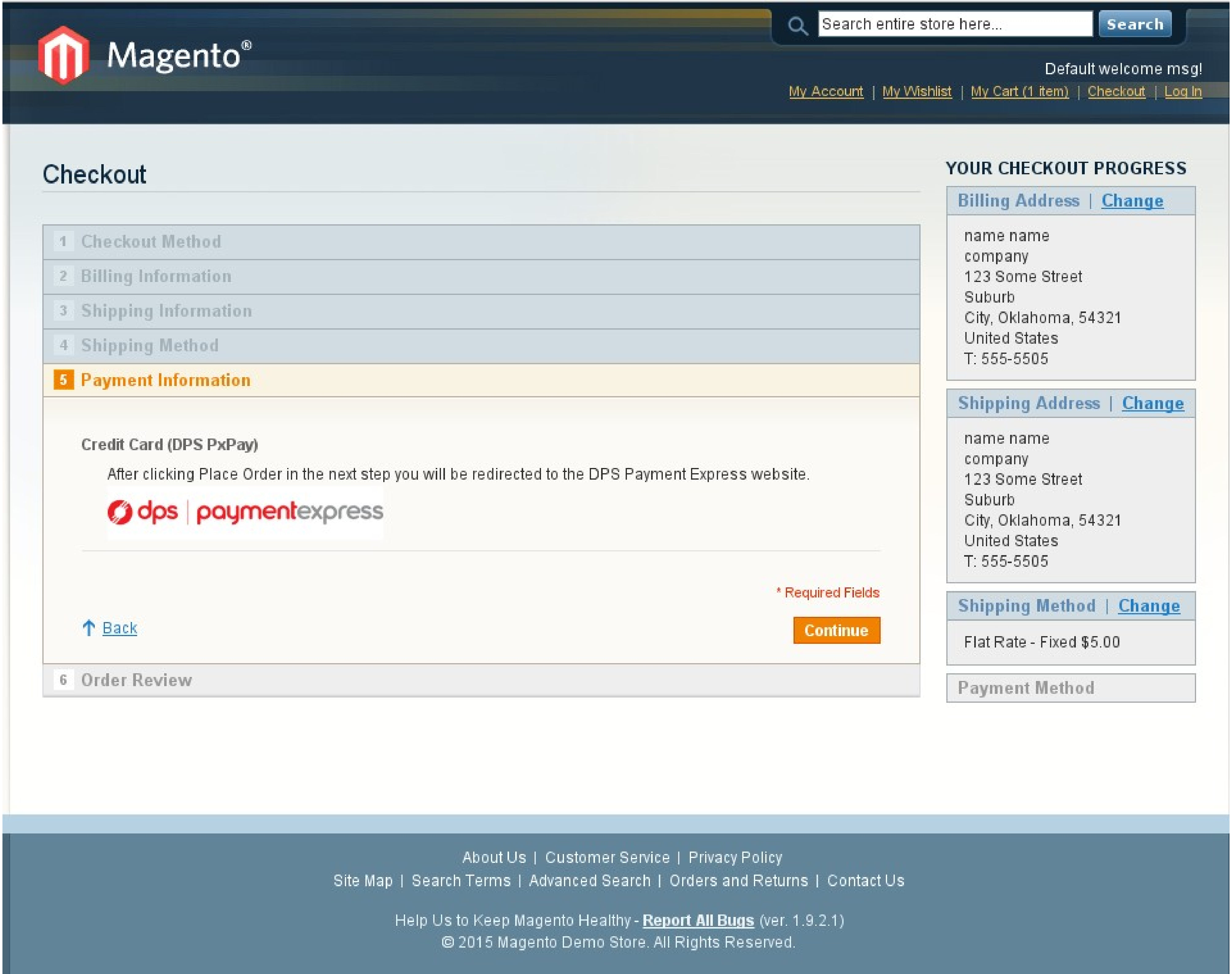
Shipping Method

Payment Method

About Us | Customer Service | Privacy Policy
Site Map | Search Terms | Advanced Search | Orders and Returns | Contact Us

Help Us to Keep Magento Healthy - **Report All Bugs** (ver. 1.9.2.1)

© 2015 Magento Demo Store. All Rights Reserved.


Magento®
Search entire store here...
Search
Default welcome msg!
My Account | My Wishlist | My Cart (1 item) | Checkout | Log In

Checkout

1 Checkout Method

2 Billing Information

3 Shipping Information

4 Shipping Method

5 Payment Information

Credit Card (DPS PxPay)

After clicking Place Order in the next step you will be redirected to the DPS Payment Express website.

* Required Fields

6 Order Review

YOUR CHECKOUT PROGRESS

Billing Address | Change

name name
company
123 Some Street
Suburb
City, Oklahoma, 54321
United States
T: 555-5505

Shipping Address | Change

name name
company
123 Some Street
Suburb
City, Oklahoma, 54321
United States
T: 555-5505

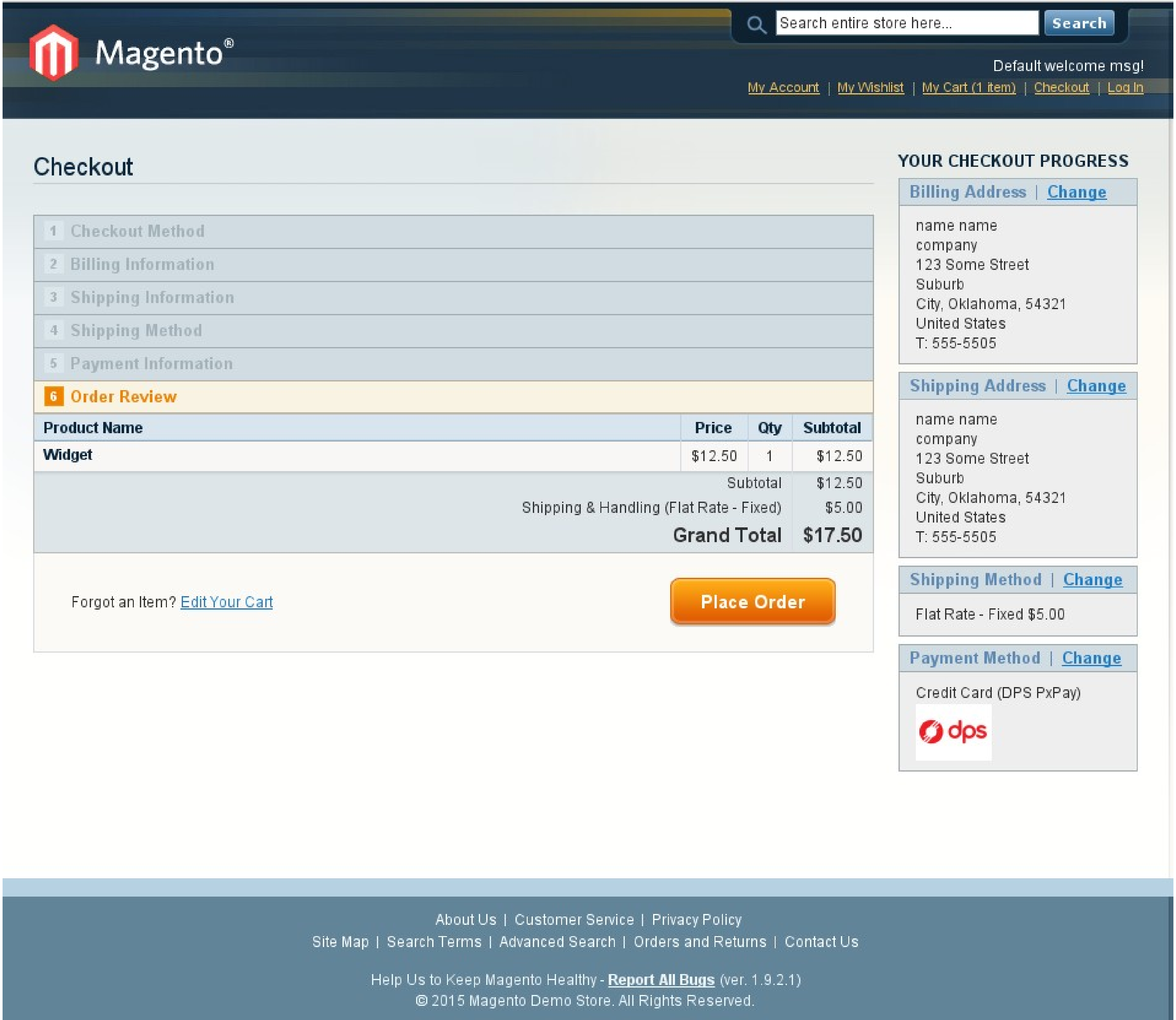
Shipping Method | Change

Flat Rate - Fixed $5.00

Payment Method

About Us | Customer Service | Privacy Policy
Site Map | Search Terms | Advanced Search | Orders and Returns | Contact Us

Help Us to Keep Magento Healthy - **Report All Bugs** (ver. 1.9.2.1)
© 2015 Magento Demo Store. All Rights Reserved.



Default welcome msg!

My Account | My Wishlist | My Cart (1 item) | Checkout | Log In

Checkout

1 Checkout Method

2 Billing Information

3 Shipping Information

4 Shipping Method

5 Payment Information

6 Order Review

Product Name	Price	Qty	Subtotal
Widget	$12.50	1	$12.50
		Subtotal	$12.50
		Shipping & Handling (Flat Rate - Fixed)	$5.00
		Grand Total	**$17.50**

Forgot an Item? Edit Your Cart

YOUR CHECKOUT PROGRESS

Billing Address | Change

name name
company
123 Some Street
Suburb
City, Oklahoma, 54321
United States
T: 555-5505

Shipping Address | Change

name name
company
123 Some Street
Suburb
City, Oklahoma, 54321
United States
T: 555-5505

Shipping Method | Change

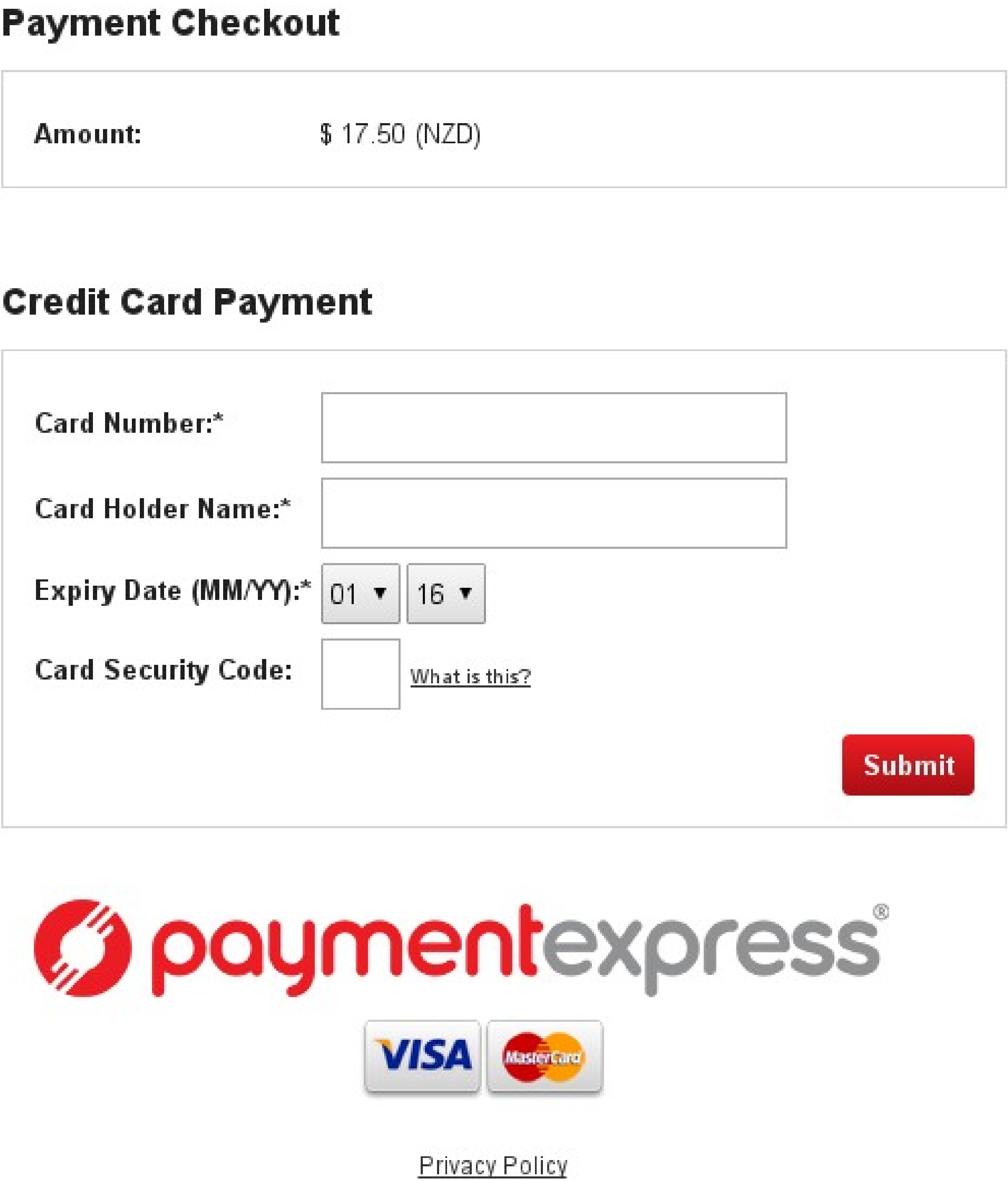
Flat Rate - Fixed $5.00

Payment Method | Change

Credit Card (DPS PxPay)

About Us | Customer Service | Privacy Policy
Site Map | Search Terms | Advanced Search | Orders and Returns | Contact Us

Help Us to Keep Magento Healthy - **Report All Bugs** (ver. 1.9.2.1)
© 2015 Magento Demo Store. All Rights Reserved.



Payment Checkout

Amount: $ 17.50 (NZD)

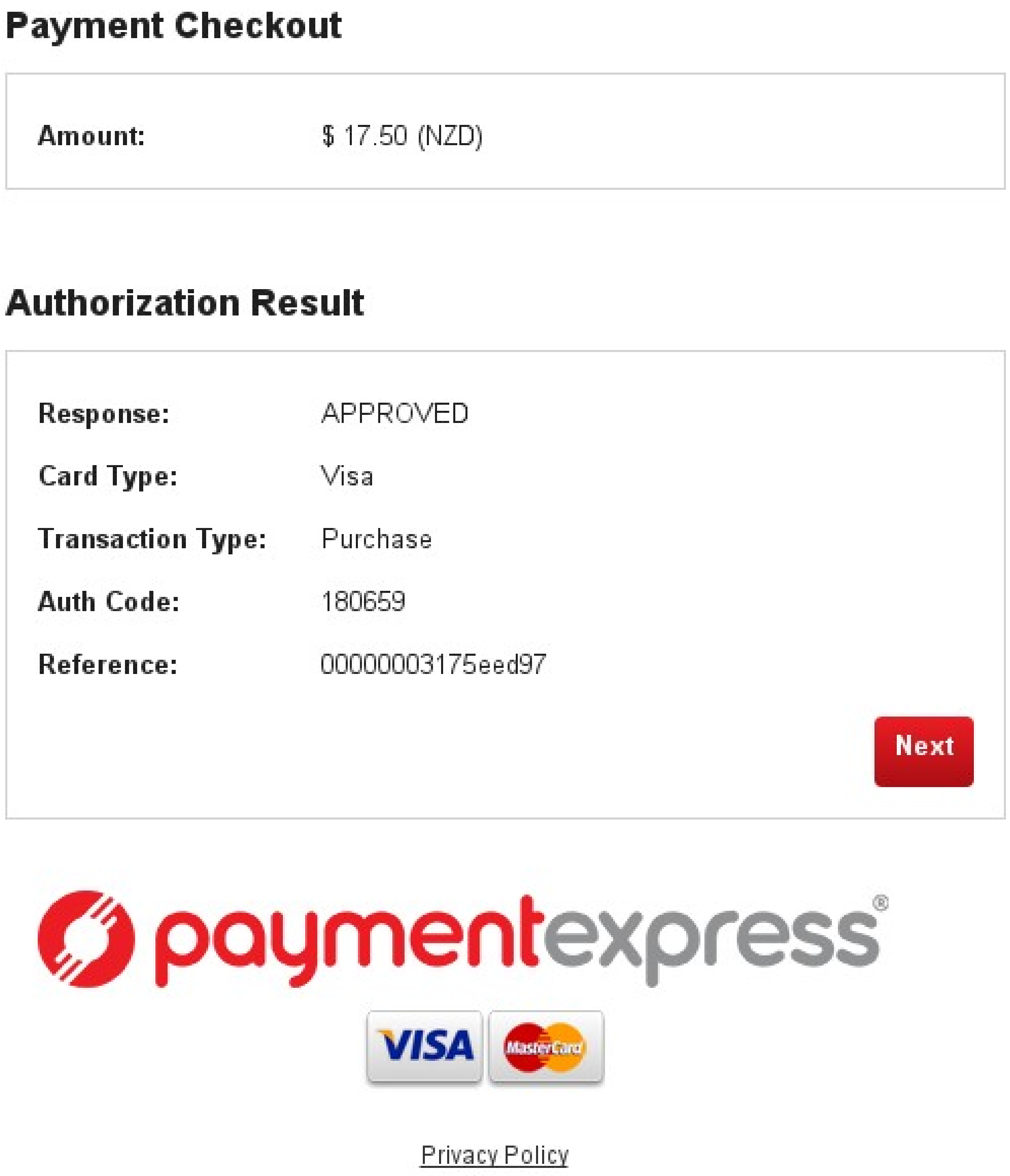
Credit Card Payment

Card Number:*

Card Holder Name:*

Expiry Date (MM/YY):* 01 ▼ 16 ▼

Card Security Code:

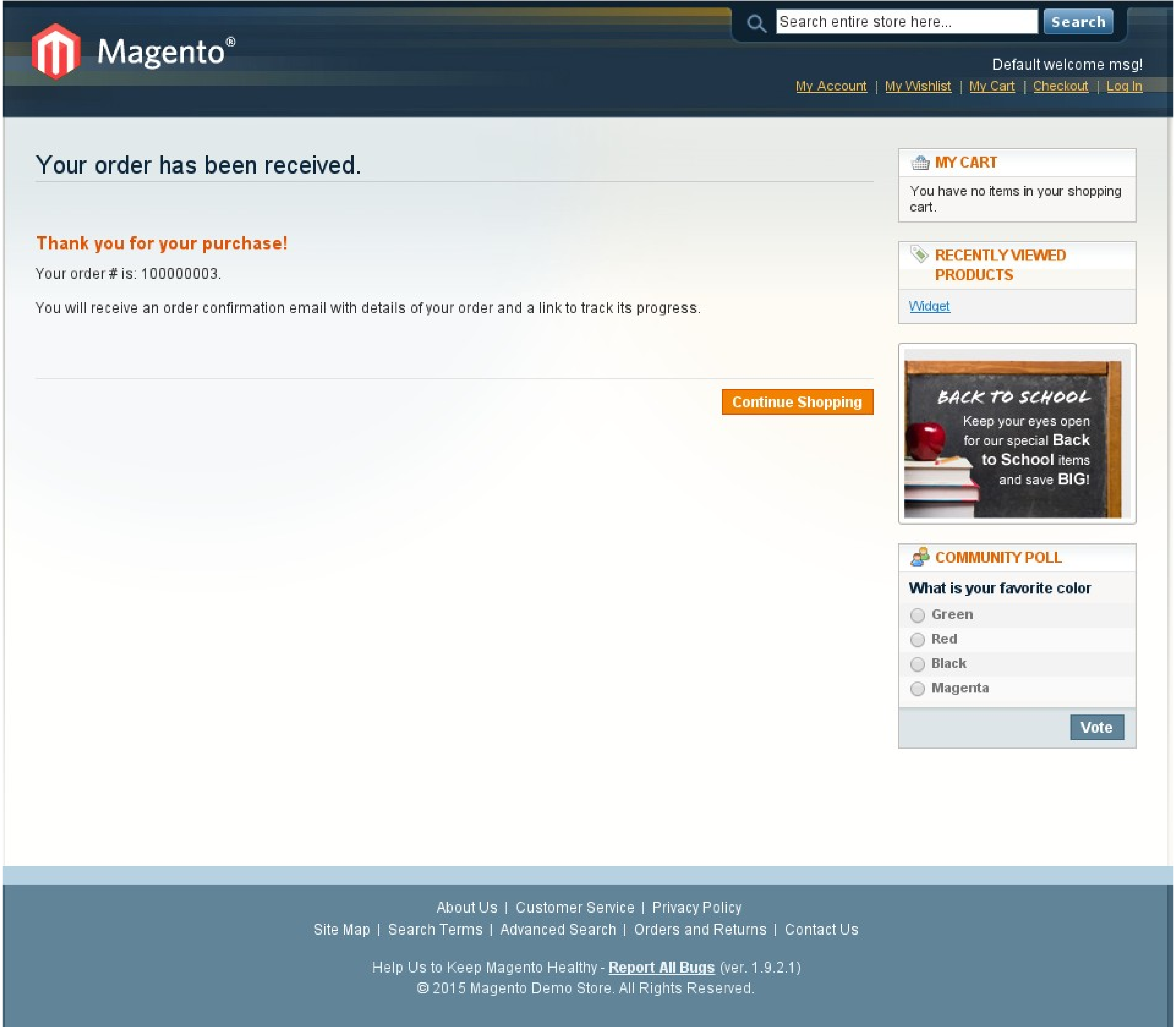


Payment Checkout

Amount:	$ 17.50 (NZD)

Authorization Result

Response:	APPROVED
Card Type:	Visa
Transaction Type:	Purchase
Auth Code:	180659
Reference:	00000003175eed97


Magento®
Search entire store here...
Search
My Account | My Wishlist | My Cart | Checkout | Log In
Continue Shopping
MY CART
RECENTLY VIEWED PRODUCTS
Widget
BACK TO SCHOOL
Keep your eyes open for our special Back to School items and save BIG!
COMMUNITY POLL
Vote
About Us | Customer Service | Privacy Policy
Site Map | Search Terms | Advanced Search | Orders and Returns | Contact Us

Default welcome msg!

Your order has been received.

Thank you for your purchase!

Your order # is: 100000003.

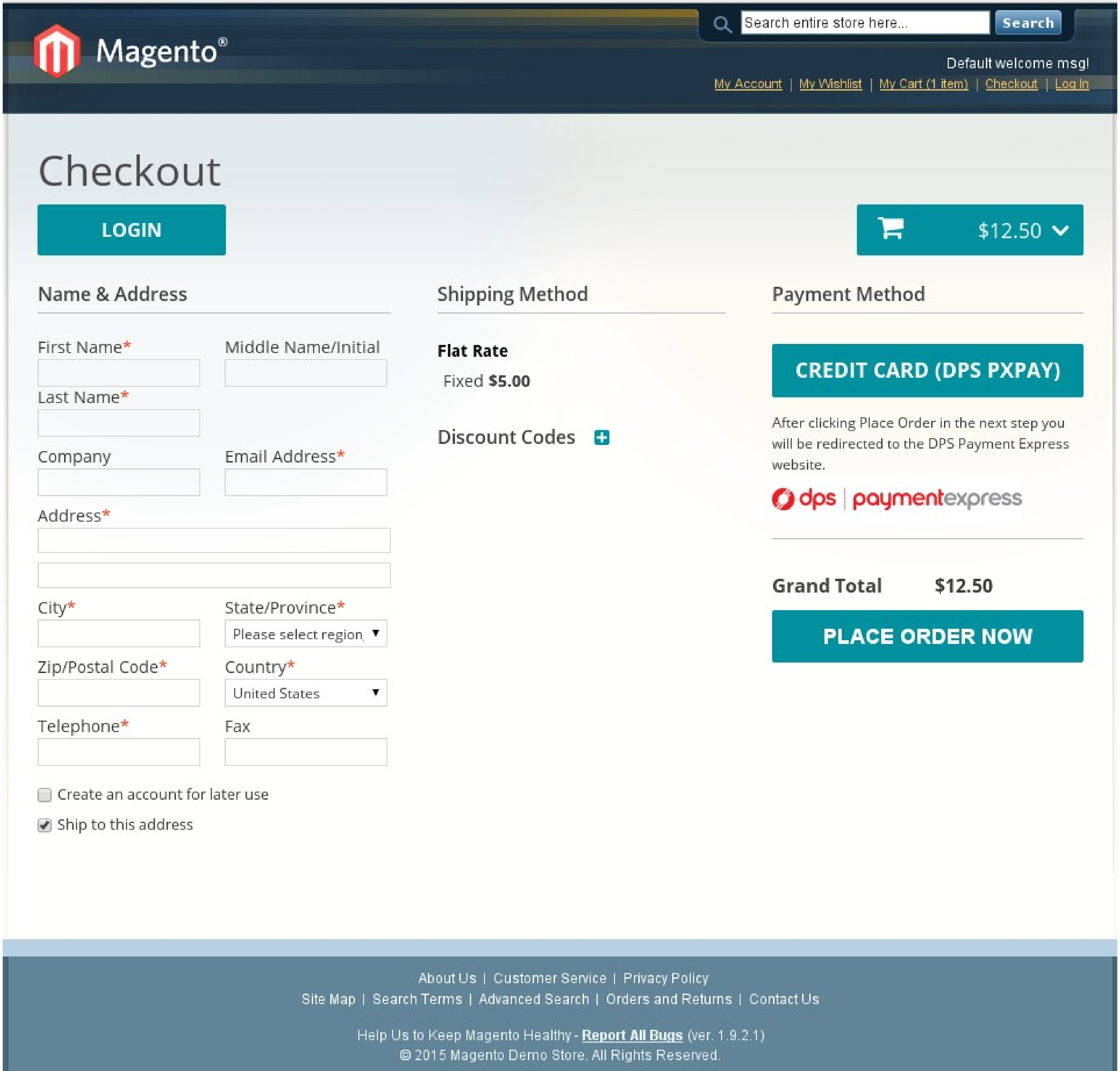
You will receive an order confirmation email with details of your order and a link to track its progress.

You have no items in your shopping cart.

What is your favorite color

○ Green
○ Red
○ Black
○ Magenta

Help Us to Keep Magento Healthy - **Report All Bugs** (ver. 1.9.2.1)
© 2015 Magento Demo Store. All Rights Reserved.



Magento®

Search entire store here... Search

Default welcome msg!

My Account | My Wishlist | My Cart (1 item) | Checkout | Log In

Checkout

LOGIN

$12.50

Name & Address

First Name*

Middle Name/Initial

Last Name*

Company

Email Address*

Address*

City*

State/Province* Please select region, ▾

Zip/Postal Code*

Country* United States ▾

Telephone*

Fax

☐ Create an account for later use

☑ Ship to this address

Shipping Method

Flat Rate

Fixed **$5.00**

Discount Codes ⊞

Payment Method

CREDIT CARD (DPS PXPAY)

After clicking Place Order in the next step you will be redirected to the DPS Payment Express website.

dps | paymentexpress

Grand Total $12.50

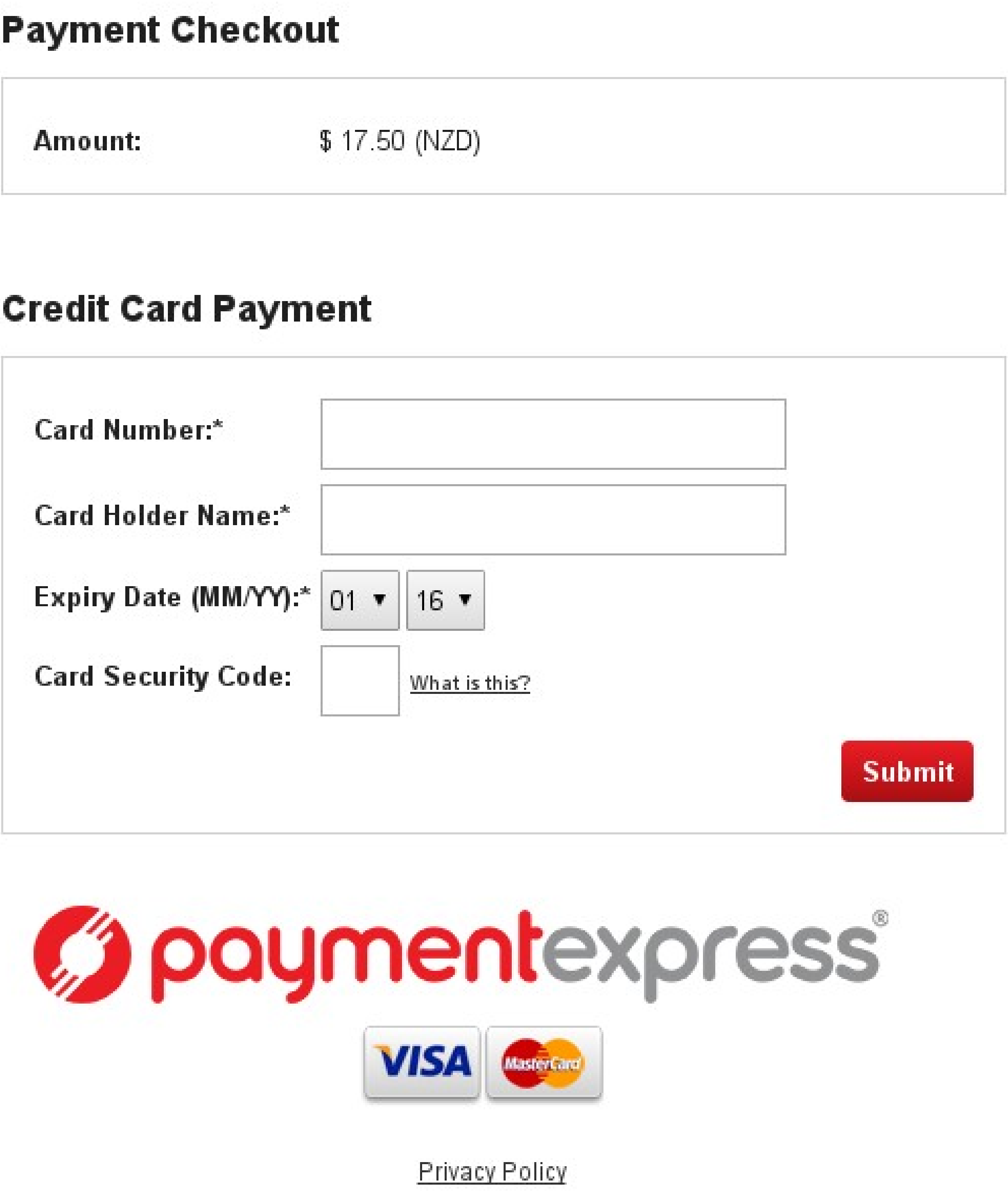
PLACE ORDER NOW

About Us | Customer Service | Privacy Policy

Site Map | Search Terms | Advanced Search | Orders and Returns | Contact Us

Help Us to Keep Magento Healthy - **Report All Bugs** (ver. 1.9.2.1)

© 2015 Magento Demo Store. All Rights Reserved.

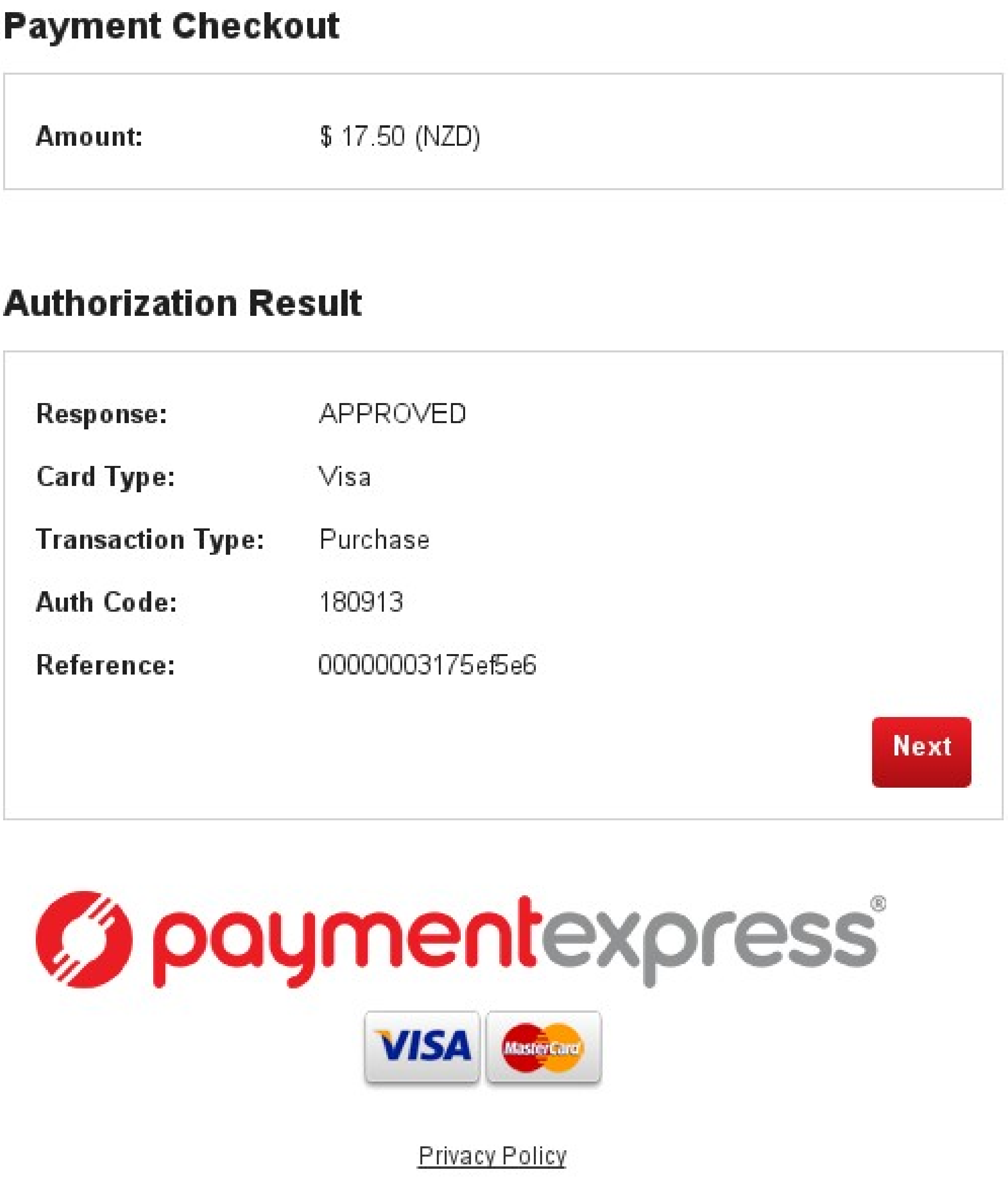


Payment Checkout

Amount:	$ 17.50 (NZD)

Credit Card Payment

Card Number:*	
Card Holder Name:*	
Expiry Date (MM/YY):*	01 ▾ 16 ▾
Card Security Code:	What is this?



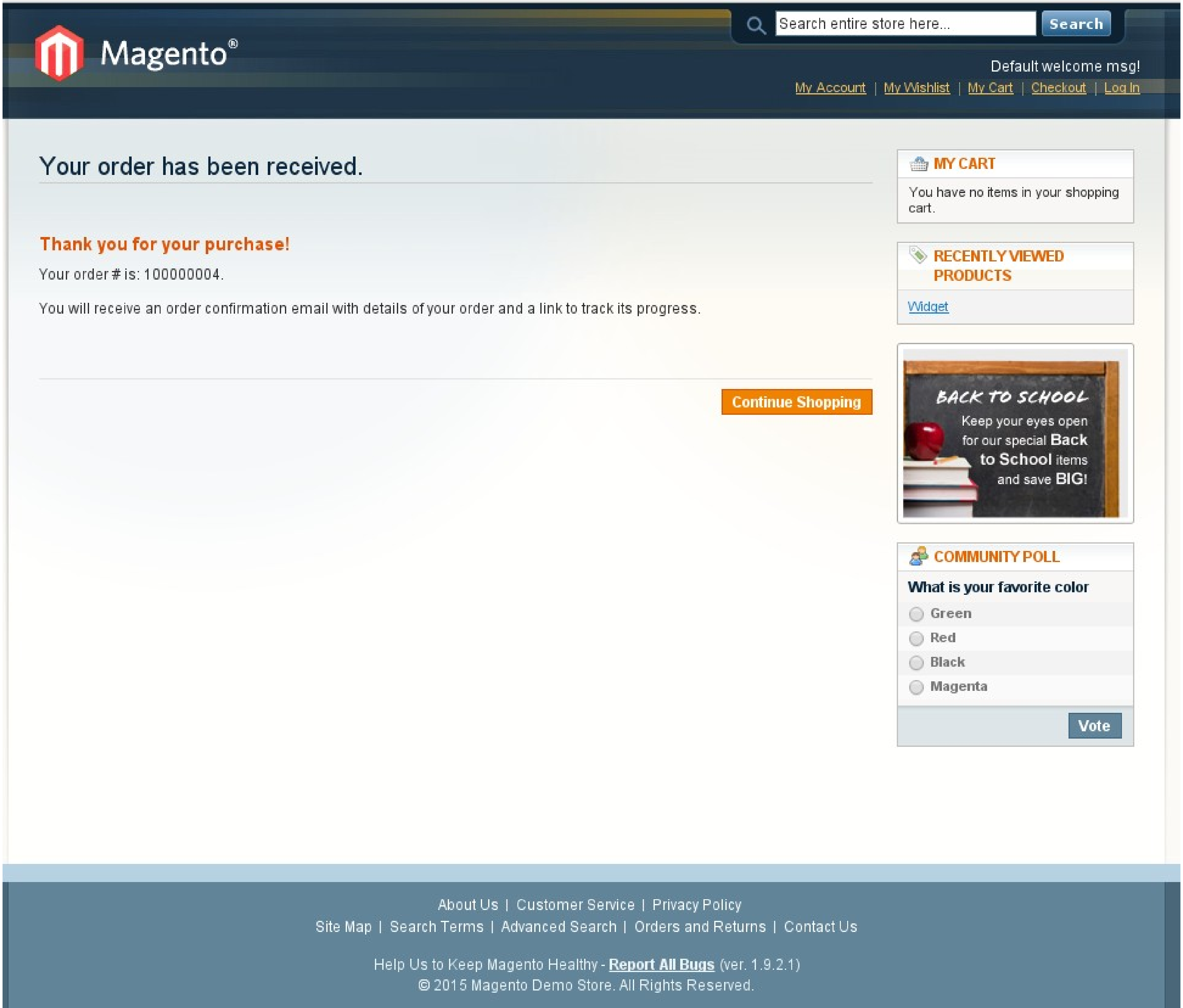
Payment Checkout

Amount:	$ 17.50 (NZD)

Authorization Result

Response:	APPROVED
Card Type:	Visa
Transaction Type:	Purchase
Auth Code:	180913
Reference:	00000003175ef5e6

Privacy Policy


Magento®
Search entire store here...
Search
Default welcome msg!
My Account | My Wishlist | My Cart | Checkout | Log In

Your order has been received.

Thank you for your purchase!

Your order # is: 100000004.

You will receive an order confirmation email with details of your order and a link to track its progress.

MY CART

You have no items in your shopping cart.

RECENTLY VIEWED PRODUCTS

Widget

BACK TO SCHOOL
Keep your eyes open for our special Back to School items and save BIG!

COMMUNITY POLL

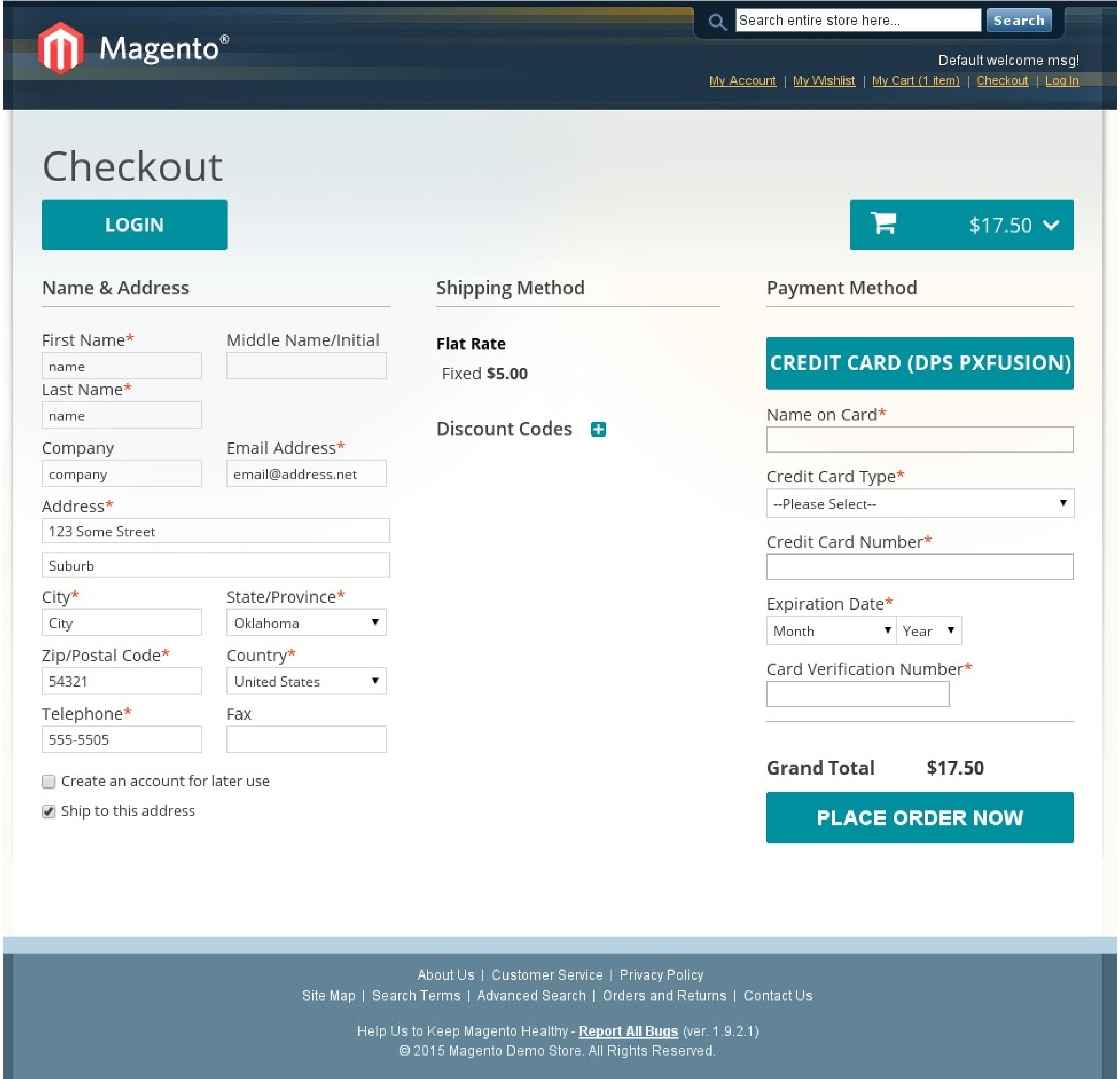
What is your favorite color

○ Green
○ Red
○ Black
○ Magenta

About Us | Customer Service | Privacy Policy
Site Map | Search Terms | Advanced Search | Orders and Returns | Contact Us

Help Us to Keep Magento Healthy - **Report All Bugs** (ver. 1.9.2.1)

© 2015 Magento Demo Store. All Rights Reserved.


Magento®
Search entire store here...
Search
Default welcome msg!
My Account | My Wishlist | My Cart (1 item) | Checkout | Log In

Checkout

Name & Address

First Name* name

Middle Name/Initial

Last Name* name

Company company

Email Address* email@address.net

Address* 123 Some Street

Suburb

City* City

State/Province* Oklahoma

Zip/Postal Code* 54321

Country* United States

Telephone* 555-5505

Fax

☐ Create an account for later use

☑ Ship to this address

Shipping Method

Flat Rate

Fixed **$5.00**

Discount Codes ⊞

Payment Method

Name on Card*

Credit Card Type* --Please Select--

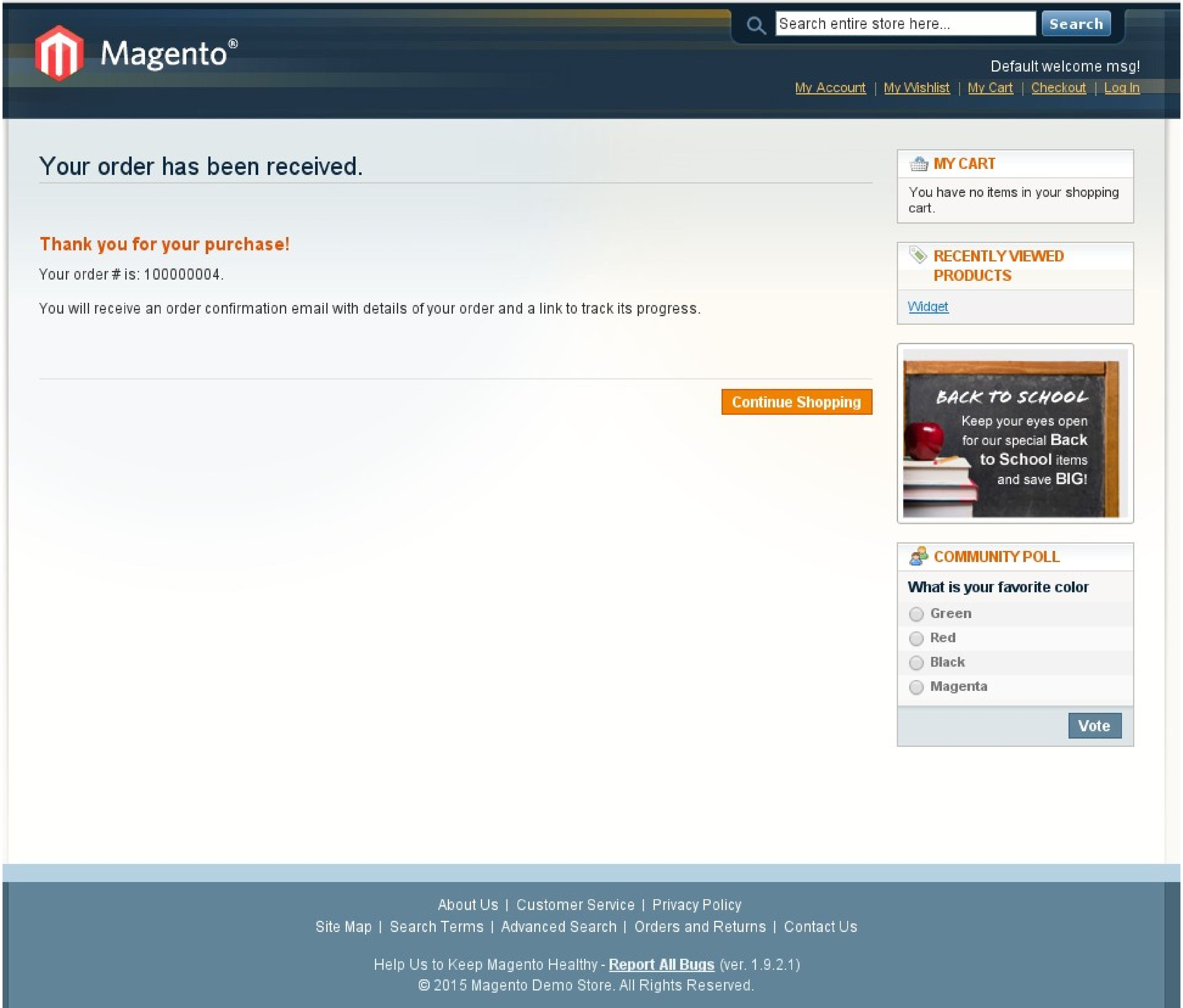
Credit Card Number*

Expiration Date* Month Year

Card Verification Number*

Grand Total **$17.50**

About Us | Customer Service | Privacy Policy
Site Map | Search Terms | Advanced Search | Orders and Returns | Contact Us
Help Us to Keep Magento Healthy - Report All Bugs (ver. 1.9.2.1)
© 2015 Magento Demo Store. All Rights Reserved.



Magento®
Search entire store here...
Search

Default welcome msg!

My Account | My Wishlist | My Cart | Checkout | Log In

Your order has been received.

Thank you for your purchase!

Your order # is: 100000004.

You will receive an order confirmation email with details of your order and a link to track its progress.

MY CART

You have no items in your shopping cart.

RECENTLY VIEWED PRODUCTS

Widget

BACK TO SCHOOL
Keep your eyes open for our special Back to School items and save BIG!

COMMUNITY POLL

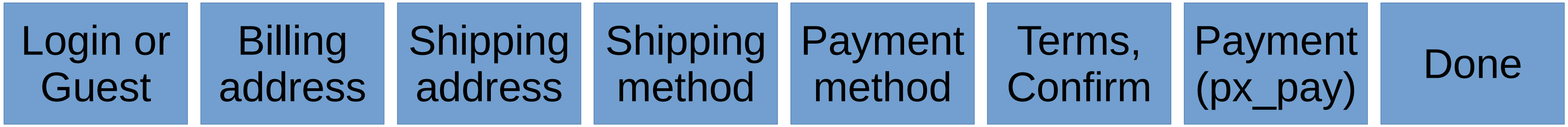
What is your favorite color

○ Green
○ Red
○ Black
○ Magenta

About Us | Customer Service | Privacy Policy
Site Map | Search Terms | Advanced Search | Orders and Returns | Contact Us

Help Us to Keep Magento Healthy - **Report All Bugs** (ver. 1.9.2.1)
© 2015 Magento Demo Store. All Rights Reserved.

Checkout experience



Login or Guest

Billing address

Shipping address

Shipping method

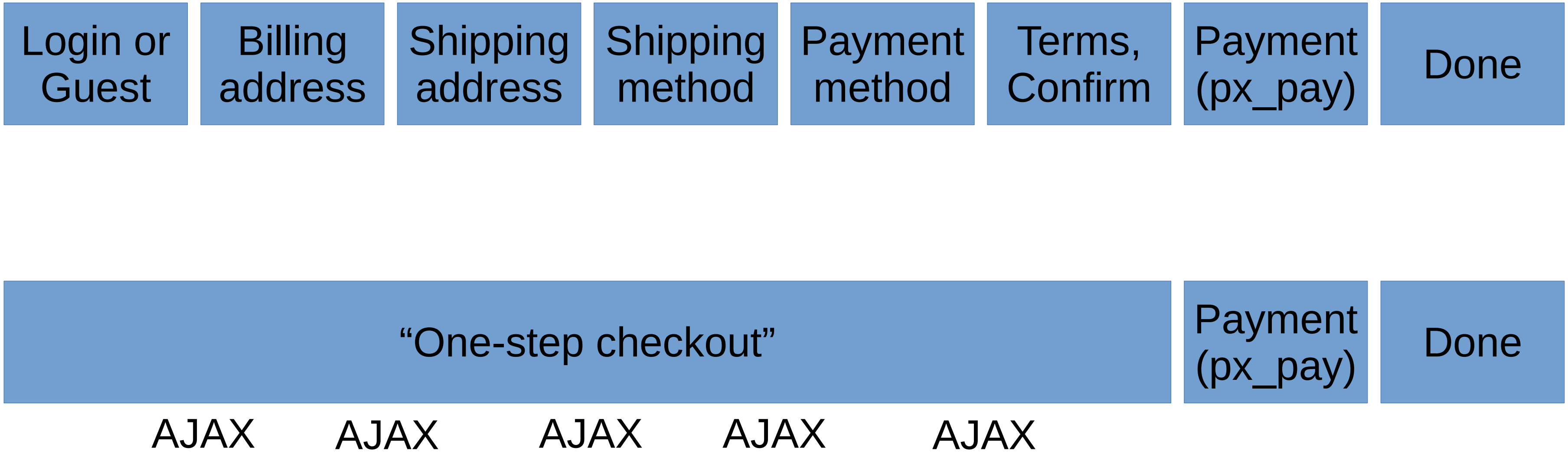
Payment method

Terms, Confirm

Payment (px_pay)

Done

Checkout experience



Login or Guest

Billing address

Shipping address

Shipping method

Payment method

Terms, Confirm

Payment (px_pay)

Done

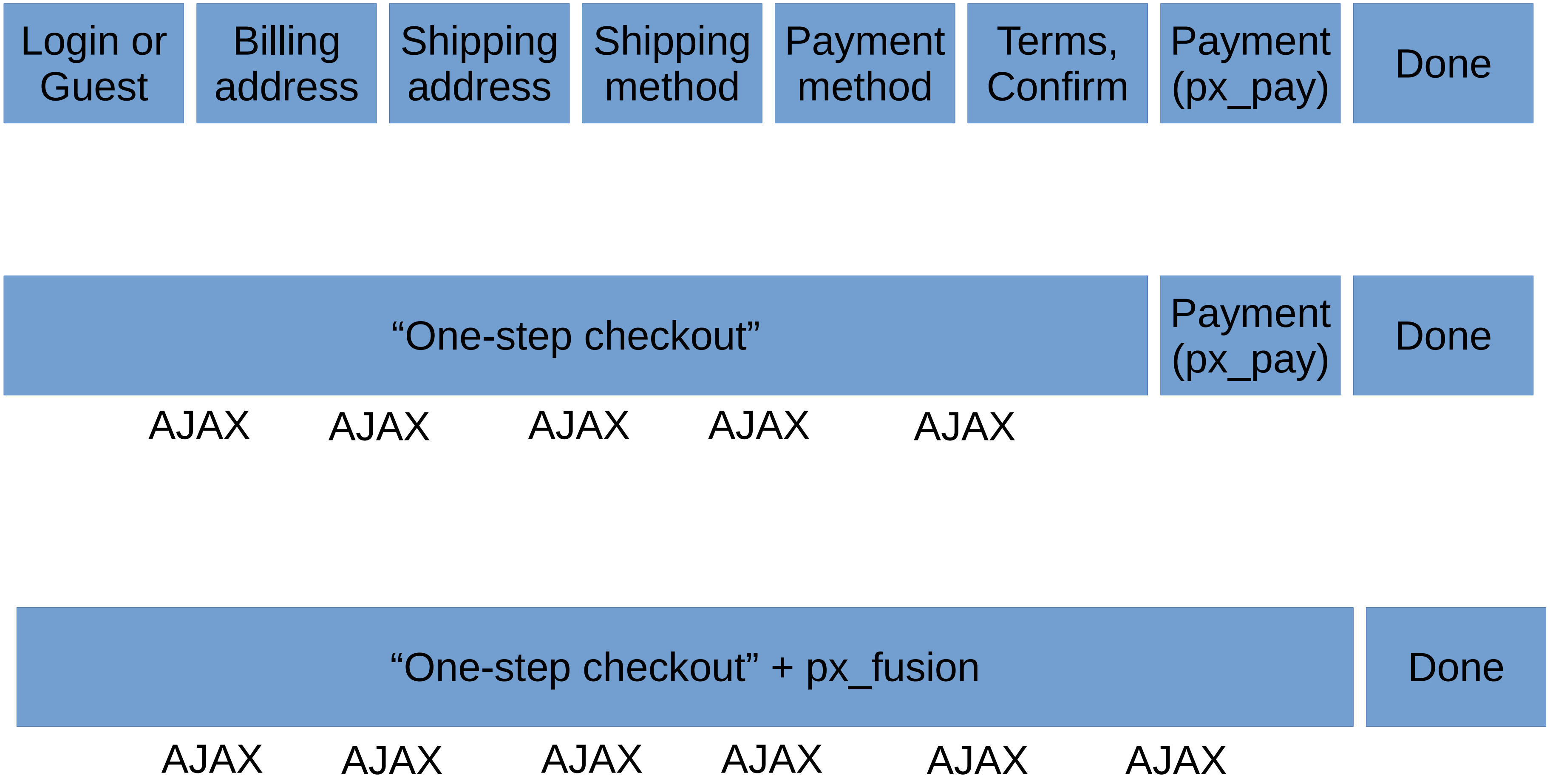
“One-step checkout”

Payment (px_pay)

Done

AJAX AJAX AJAX AJAX AJAX

Checkout experience



Login or Guest

Billing address

Shipping address

Shipping method

Payment method

Terms, Confirm

Payment (px_pay)

Done

“One-step checkout”

Payment (px_pay)

Done

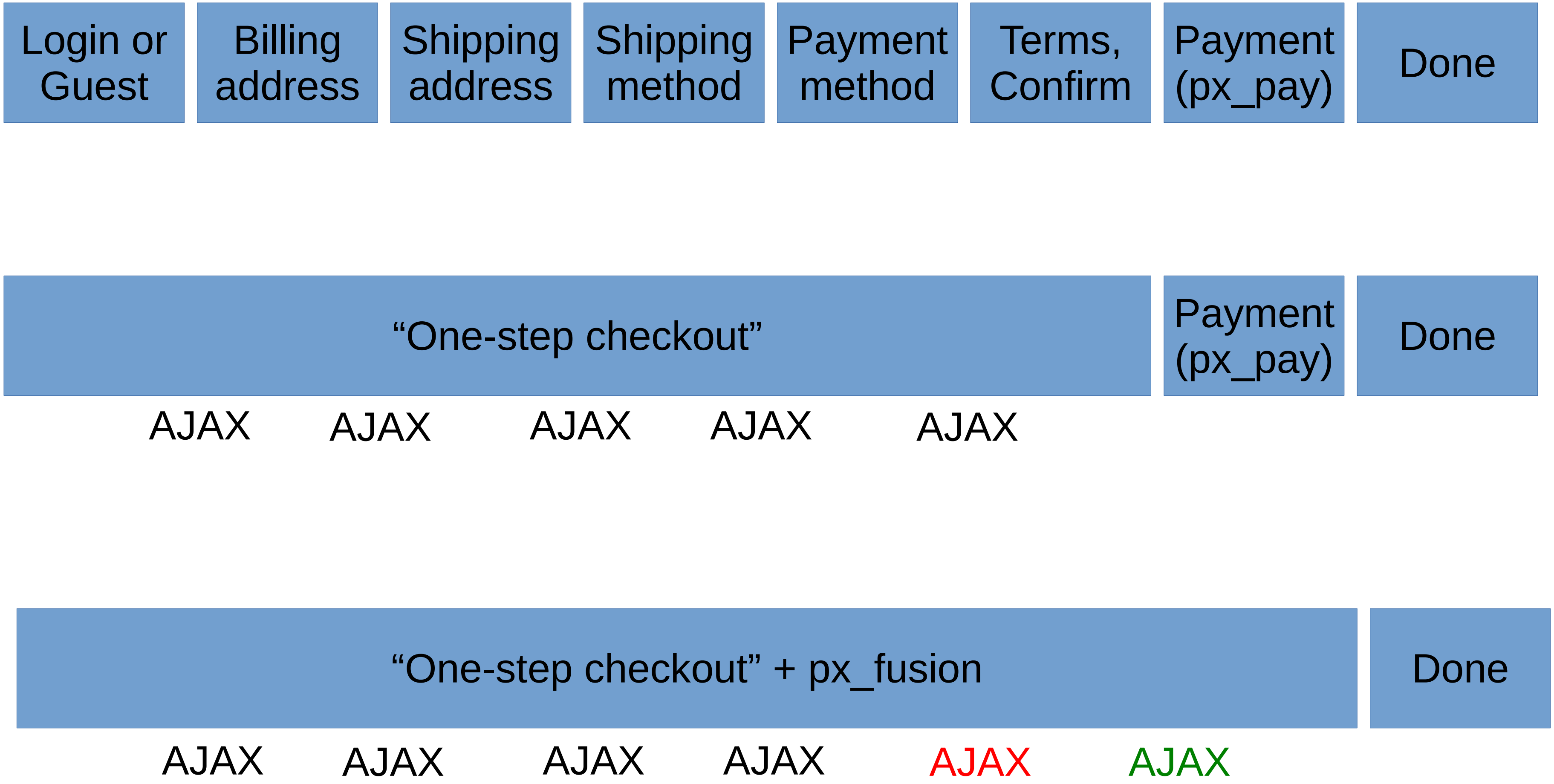
AJAX AJAX AJAX AJAX AJAX

“One-step checkout” + px_fusion

Done

AJAX AJAX AJAX AJAX AJAX AJAX

Checkout experience



Login or Guest | Billing address | Shipping address | Shipping method | Payment method | Terms, Confirm | Payment (px_pay) | Done

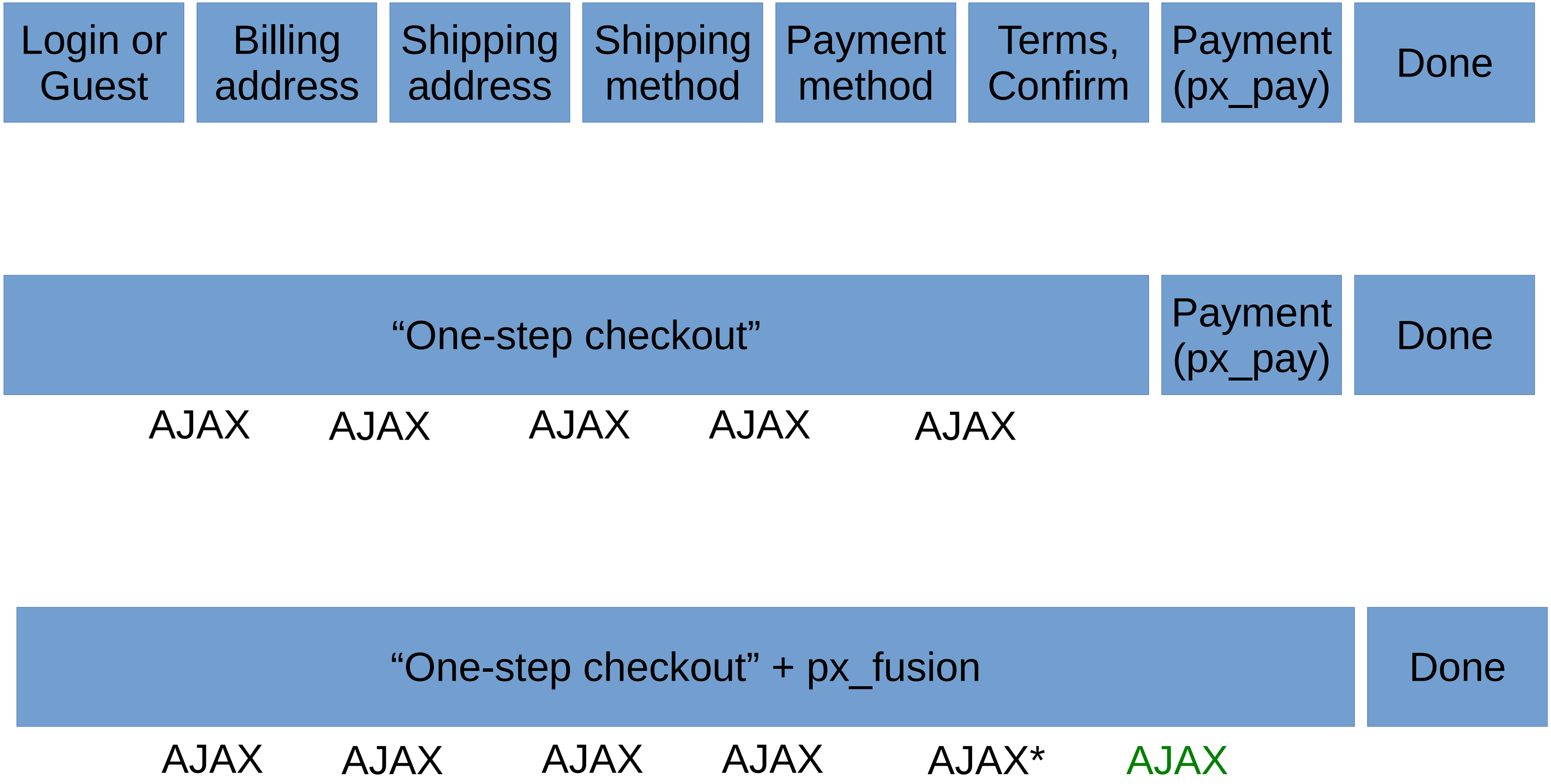
"One-step checkout" | Payment (px_pay) | Done

AJAX AJAX AJAX AJAX AJAX

"One-step checkout" + px_fusion | Done

AJAX AJAX AJAX AJAX AJAX AJAX

Checkout experience



Login or Guest | Billing address | Shipping address | Shipping method | Payment method | Terms, Confirm | Payment (px_pay) | Done

“One-step checkout” | Payment (px_pay) | Done

AJAX AJAX AJAX AJAX AJAX

“One-step checkout” + px_fusion | Done

AJAX AJAX AJAX AJAX AJAX* AJAX

Problem: Website is slow

- ~~Concurrent users~~
- ~~Content Delivery Network~~
- ~~Minimum page load time~~
- User experience

Problem: Website is slow

- ~~Concurrent users~~
- ~~Content Delivery Network~~
- ~~Minimum page load time~~
- ~~User experience~~

Success

- Website no longer “slow.”
- Win!

- The end.

It's never the end

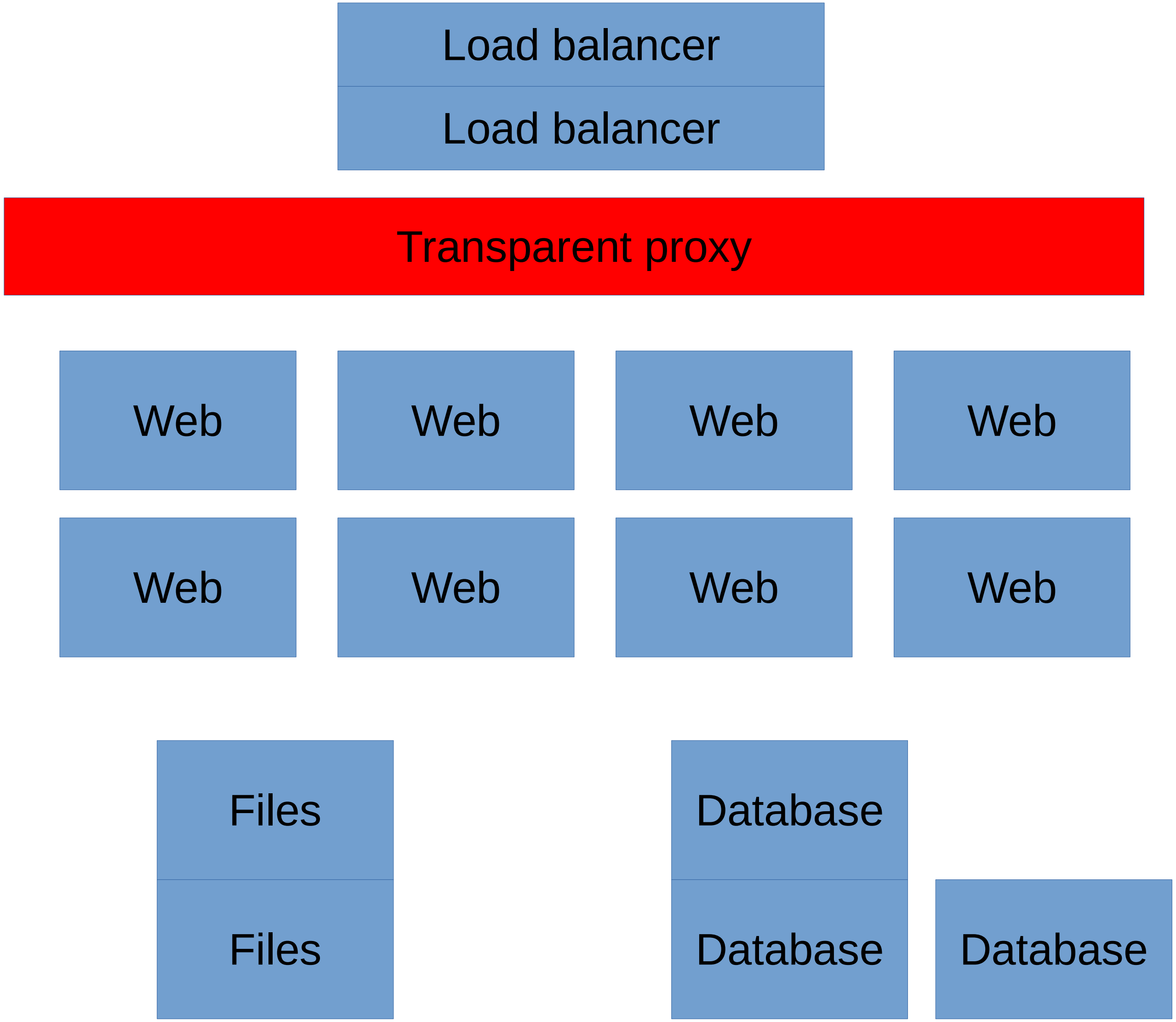
Problem: “website hacked”

- Incident response

- SVN
- DB in staging & dev

Credit card fraud

- Common point of purchase



Load balancer

Load balancer

Transparent proxy

Web

Web

Web

Web

Web

Web

Web

Web

Files

Files

Database

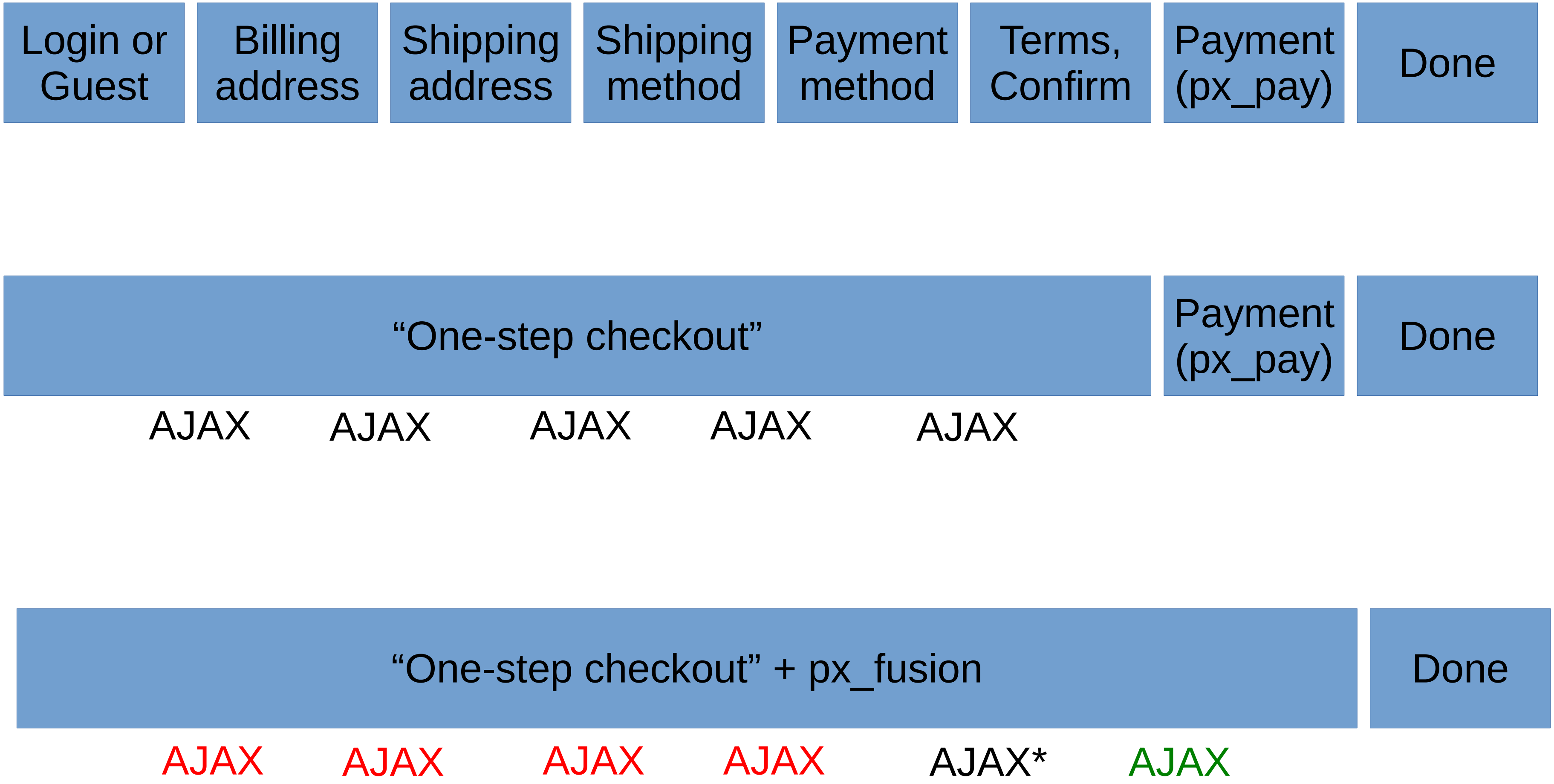
Database

Database

Credit card fraud

- Common point of purchase
- Single-use card

Checkout experience



Login or Guest

Billing address

Shipping address

Shipping method

Payment method

Terms, Confirm

Payment (px_pay)

Done

“One-step checkout”

Payment (px_pay)

Done

AJAX AJAX AJAX AJAX AJAX

“One-step checkout” + px_fusion

Done

AJAX AJAX AJAX AJAX AJAX* AJAX

Multi-factor

- Credit card details sent to web server
- Heartbleed to read these out of memory

Lessons learnt

- Patch CVEs. Whose responsibility.
- Expect the unexpected from users.
- Staff attrition. Hand-overs important.
- Documentation of policy, process.
- Incident team, process.

Thanks