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

px_post

px_pay
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

- Web Files

- Database
Scaling

- Small cluster
- TLS

- Load balancer
- Web Files
- Web Files
- Database
Scaling

- Small cluster
- TLS
Scaling

- Bigger cluster
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/](https://xkcd.com/1354/)
Problem: Website is slow

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

<table>
<thead>
<tr>
<th>Unsecure</th>
<th>Secure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base URL</strong></td>
<td><strong>Base URL</strong></td>
</tr>
<tr>
<td><img src="http://www.example.org/" alt="Image" /></td>
<td><img src="https://www.example.org/" alt="Image" /></td>
</tr>
<tr>
<td><strong>Base Link URL</strong></td>
<td><strong>Base Link URL</strong></td>
</tr>
<tr>
<td>{{unsecure_base_url}}</td>
<td>{{secure_base_url}}</td>
</tr>
<tr>
<td><strong>Base Skin URL</strong></td>
<td><strong>Base Skin URL</strong></td>
</tr>
<tr>
<td>{{unsecure_base_url}}skin/</td>
<td><a href="https://cdn.example.org/skin/">https://cdn.example.org/skin/</a></td>
</tr>
<tr>
<td><strong>Base Media URL</strong></td>
<td><strong>Base Media URL</strong></td>
</tr>
<tr>
<td>{{unsecure_base_url}}media/</td>
<td><a href="https://cdn.example.org/media/">https://cdn.example.org/media/</a></td>
</tr>
<tr>
<td><strong>Base JavaScript URL</strong></td>
<td><strong>Base JavaScript URL</strong></td>
</tr>
<tr>
<td>{{unsecure_base_url}}js/</td>
<td>{{secure_base_url}}js/</td>
</tr>
</tbody>
</table>

**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

![Diagram showing UA, Website, and Transparent proxy connections]
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
Widget

Email to a Friend
Be the first to review this product

Availability: In stock

$12.50

Qty: 1 [Add to Cart] OR Add to Wishlist
Add to Compare

Quick Overview
Widget

Details
Widget

Product Tags

Add Your Tags:

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

Add Tags
### Shopping Cart

**Widget**

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Unit Price</th>
<th>Qty</th>
<th>Subtotal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Widget</td>
<td>$12.50</td>
<td>1</td>
<td>$12.50</td>
</tr>
</tbody>
</table>

**Discount Codes**

Enter your coupon code if you have one.

[Apply Coupon]

**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**: 

[Get a Quote]

---

**Subtotal**: $12.50

**Grand Total**: $12.50

[Proceed to Checkout]
Checkout

2 Billing Information

First Name
Last Name
Company
Address
City
State/Province
Zip/Postal Code
Country
Telephone
Fax

Ship to this address
Ship to different address

* Required Fields

Continue
Checkout

1. Checkout Method
2. Billing Information
3. Shipping Information
4. Shipping Method

Flat Rate
Fixed $5.00

Continue

5. Payment Information
6. Order Review
Credit Card (DPS PxPay)

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

*d Required Fields

Continue
### Order Review

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Price</th>
<th>Qty</th>
<th>Subtotal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Widget</td>
<td>$12.50</td>
<td>1</td>
<td>$12.50</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Subtotal</strong></td>
<td></td>
<td></td>
<td>$12.50</td>
</tr>
<tr>
<td><strong>Shipping &amp; Handling</strong></td>
<td></td>
<td></td>
<td>$5.00</td>
</tr>
<tr>
<td><strong>Grand Total</strong></td>
<td></td>
<td></td>
<td><strong>$17.50</strong></td>
</tr>
</tbody>
</table>

Forgot an item? [Edit Your Cart](#)
Payment Checkout

Amount: $17.50 (NZD)

Credit Card Payment

Card Number:*  
Card Holder Name:*  
Expiry Date (MM/YY):* 01 16  
Card Security Code:  

Submit

Privacy Policy
Payment Checkout

Amount: $ 17.50 (NZD)

Authorization Result

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

Privacy Policy
Your order has been received.

Thank you for your purchase!
Your order # is: 10000003.
You will receive an order confirmation email with details of your order and a link to track its progress.

Continue Shopping
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?

Submit

paymentexpress®

Privacy Policy
Payment Checkout

Amount: $ 17.50 (NZD)

Authorization Result

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

Next

paymentexpress

Privacy Policy
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.
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.

Continue Shopping
Checkout experience

- Login or Guest
- Billing address
- Shipping address
- Shipping method
- Payment method
- Terms, Confirm
- Payment (px_pay)
- Done
Checkout experience

1. Login or Guest
2. Billing address
3. Shipping address
4. Shipping method
5. Payment method
6. Terms, Confirm
7. Payment (px_pay)
8. Done

---

“One-step checkout”

AJAX AJAX AJAX AJAX AJAX

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  Done

“One-step checkout” + px_fusion  Done

AJAX  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”
AJAX AJAX AJAX AJAX AJAX
Payment (px_pay)
Done

“One-step checkout” + px_fusion
AJAX AJAX AJAX AJAX AJAX AJAX
Done
Checkout experience

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

“One-step checkout”
AJAX AJAX AJAX AJAX AJAX

“One-step checkout” + px_fusion
AJAX AJAX AJAX AJAX AJAX* AJAX

Done
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
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”

AJAX AJAX AJAX AJAX AJAX

“One-step checkout” + px_fusion

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