



# Incomplete Mediation - The Shopping Cart Attack

order=(#2956,10,9,90)





Server Trusted  
Domain

Client Trusted Domain

amazon.com

Hello. [Sign in](#) to get personalized recommendations. New customer? [Start here.](#)[Your Amazon.com](#)[Today's Deals](#)[Gifts & Wish Lists](#)[Gift Cards](#)[Your Account](#)[Help](#)[Shop All Departments](#)Search: [Cart](#)[Wish List](#)

Earn **\$50 Cash Back** after your first card purchase,  
And get **5% Cash Back** in bonus categories with Chase Freedom®.

[Learn more](#)

**Shopping Cart** Already a customer?  
[Sign in](#)

[See more items like these in your cart](#)subtotal = **\$5.49**Make any changes below? [Update](#)

## Shopping Cart Items—To Buy Now

Price:

Qty:

Item added on  
November 20,  
2009

[Live Free or Die Hard \(Unrated Edition\)](#) - Bruce Willis, DVD

Condition: New

Includes Video On Demand 24 hour  
rental as a gift with purchase

[Live Free or Die](#)

In Stock

[Details](#)

Eligible for FREE Super Saver Shipping

**\$5.49**

You Save:  
**\$9.49 (63%)**

**READY TO ORDER?**  
Add **\$19.99** of eligible  
items to your order to  
qualify for **FREE Super  
Saver Shipping**.

[See details](#)[Proceed to Checkout](#)

[Sign in](#) to turn on 1-Click  
ordering.

☐ This will be a Gift [Learn more](#)

Express Checkout with PayPal

[Inductive Sense](#) [Watch this](#) | [Create Playlist](#)

## Recently Viewed Items



[Live Free or Die  
Hard \(Unrated  
Edition\) DVD](#) - Bruce  
Willis

\*Notice that Annaz is not able to do this attack





Thank you for your order!



amazon.com



The total is calculated by  
a script on the client

The order is generated  
based on the request

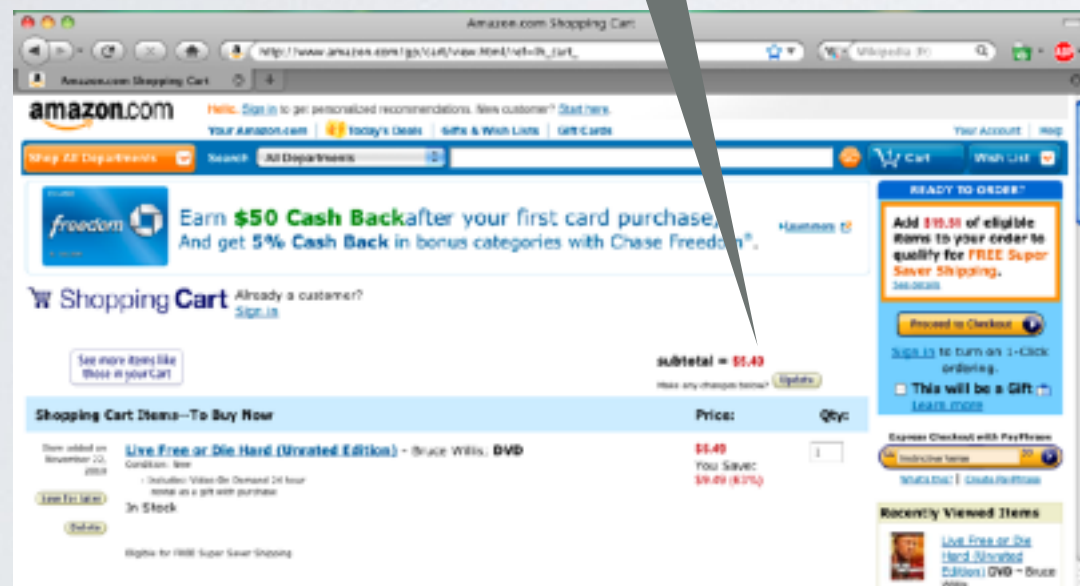
1

10

# Incomplete Mediation - The Shopping Cart Attack

The total is calculated by a script on the client

The order is generated based on the request



Client Trusted Domain

\*

order=(#2956, 10, 1, 10)

Thank you for your order!

amazon.com



Server Trusted Domain

\* Notice that Amazon is **not** vulnerable to this attack

The backend is the **only trusted domain**

- Data coming from the frontend cannot be trusted
- ✓ Sensitive operations must be done on the backend