nixu cybersecurity.

Imaginary Online Shopping System

Threat modeling example target

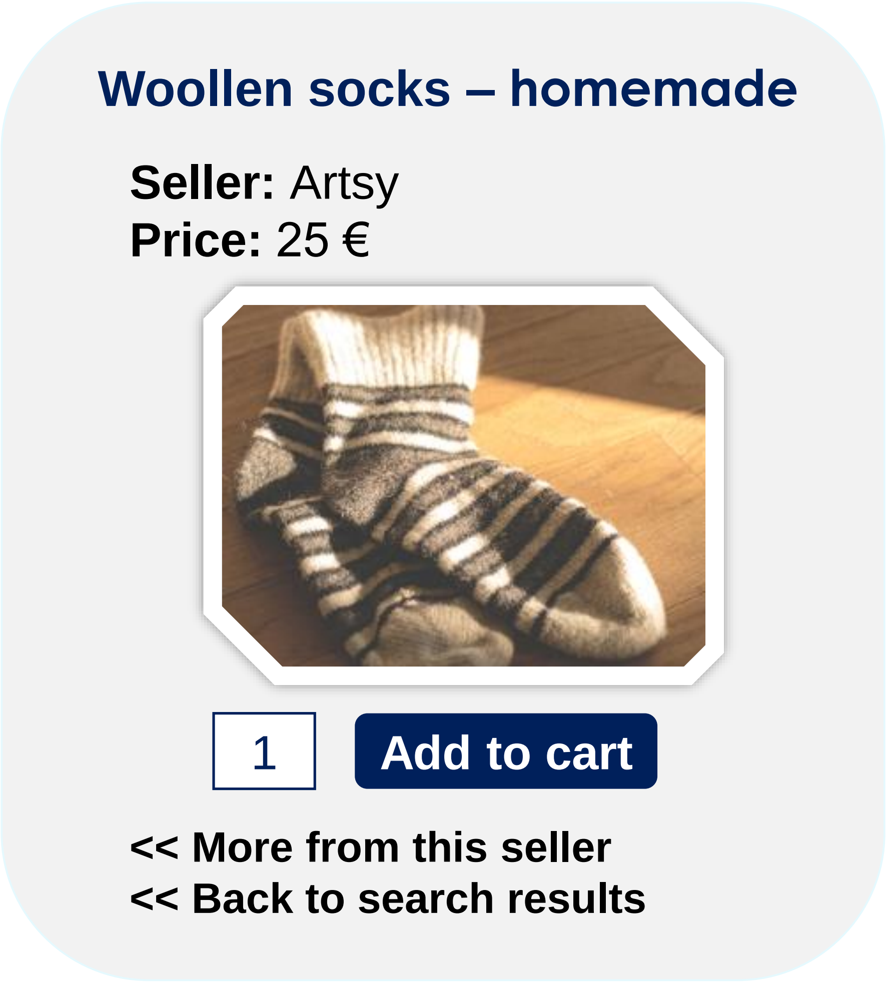
EasyShoppe Platform

Online shopping platform connecting sellers and buyers

- **Our motto: We take care of the whole online shopping experience**
- Anyone can register as a seller
- Sellers will just create their products and ship them to buyers

Note: EasyShoppe is an imaginary online shopping platform and its design contains some weaknesses on purpose. So use this for threat modeling purposes only :)

Features for buyers



Woollen socks – homemade

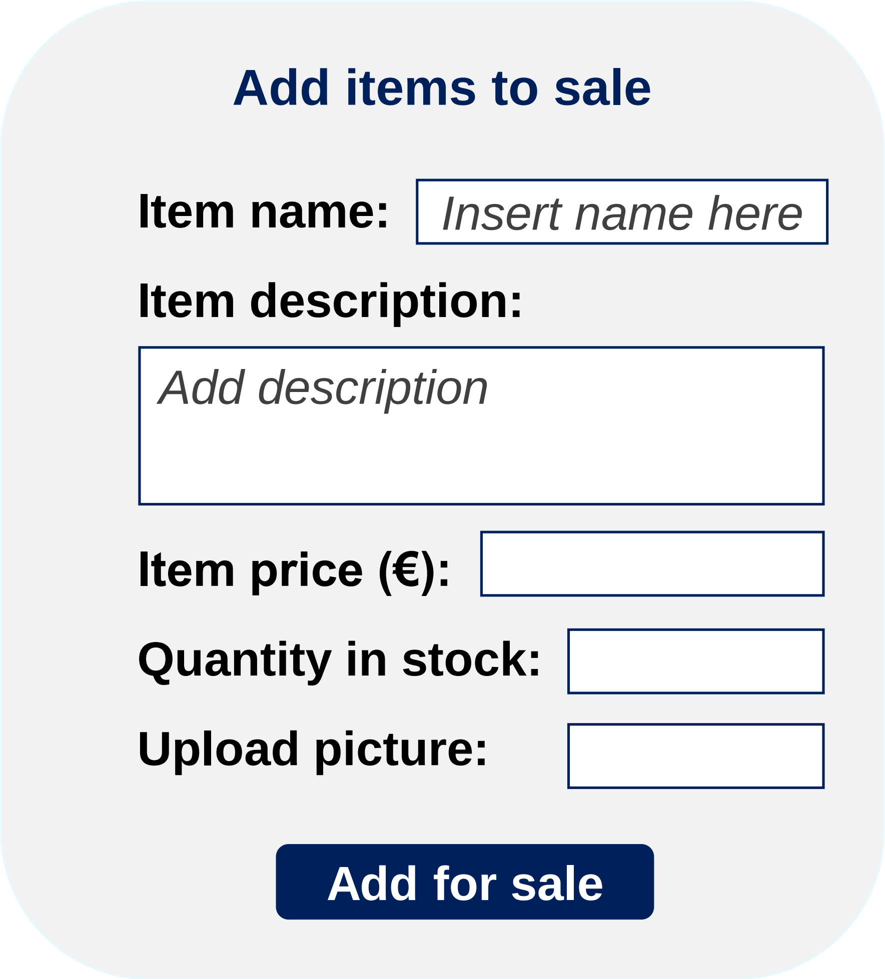
Seller: Artsy
Price: 25 €

1 **Add to cart**

<< More from this seller
<< Back to search results

- Buyers can
  - Create an account
  - Login with username and password or Facebook
  - Search products
  - Buy products
  - Give ratings for sellers ★★★
  - Give ratings for products ★★★
  - Share their purchases on Facebook and Twitter
  - See their purchase history

Features for Sellers



Add items to sale

Item name: *Insert name here*

Item description:

Add description

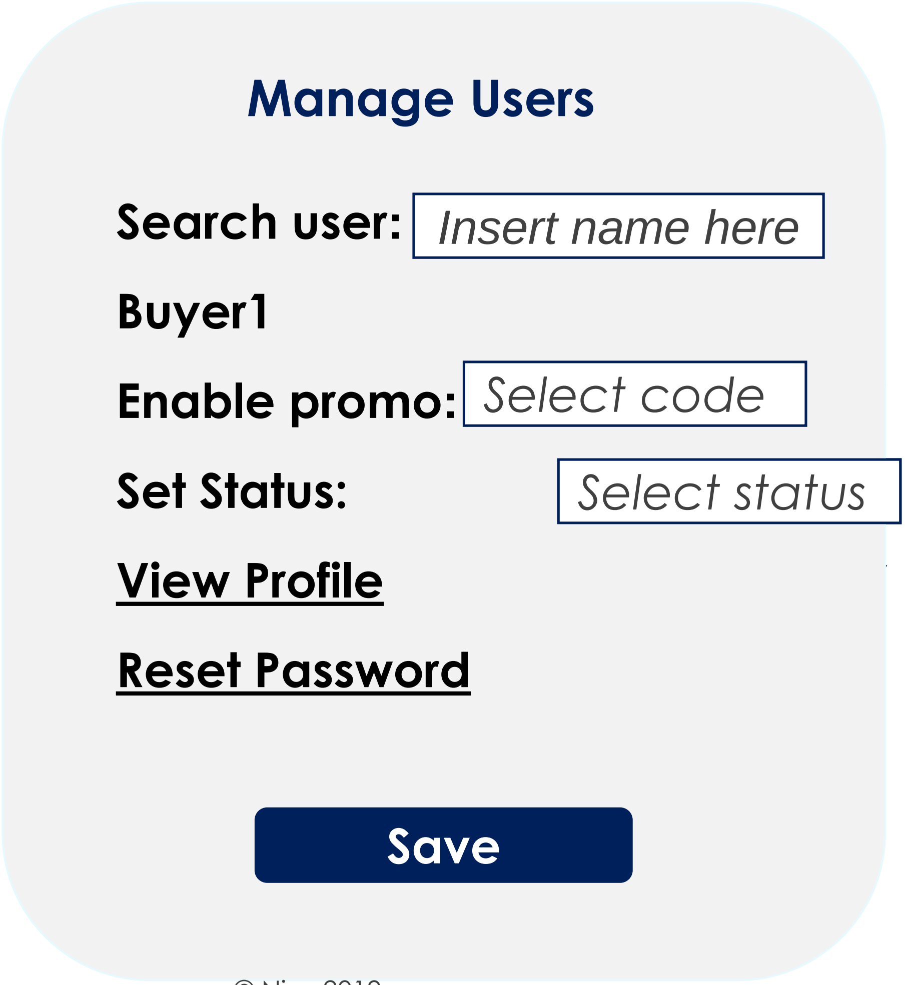
Item price (€):

Quantity in stock:

Upload picture:

- Anyone can register as a seller
- Sellers can
  - Add items for sale
  - Add and modify their bank account number for payments
  - Get a list or ordered items for delivery
  - Give discounts (per person or seasonal)
  - Get their products listed first by paying an extra fee

Features for Admins



Manage Users

Search user: *Insert name here*

Buyer1

Enable promo: *Select code*

Set Status: *Select status*

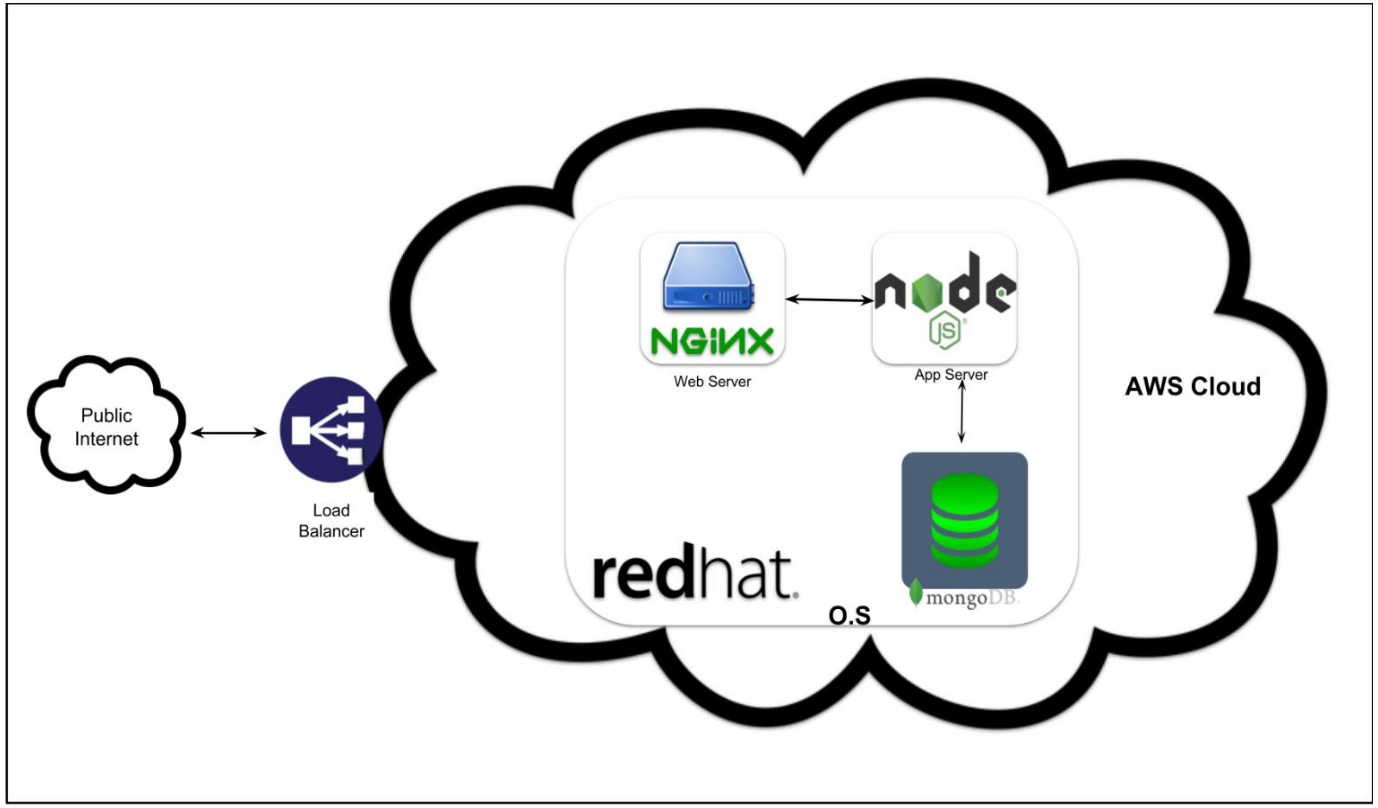
View Profile

Reset Password

- Admins can
  - Manage users
    - Enable promotional codes
    - Enable / lock users
    - View user's profile
    - Reset Password
  - Cancel or modify orders
- **Admin has privileged access to the platform and all user information**

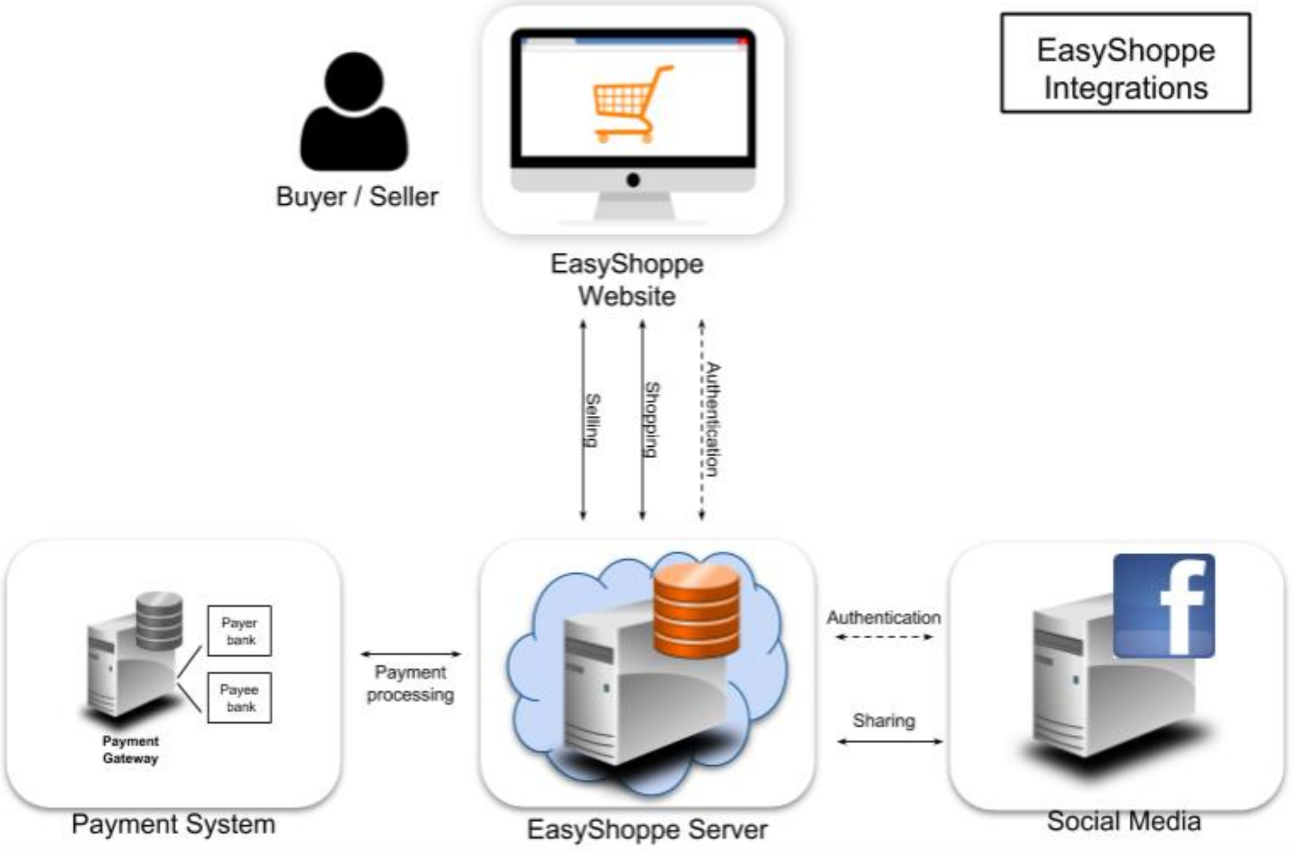
Architecture

Proof-of-concept architecture



- Deployed in AWS
- Red Hat server
- NodeJS application running on nginx
- MongoDB database
- Single server instances, no redundancy
- Backup default: 7 days
- No monitoring
- No log server

Integrations



- Username and password - based authentication
- Alternatively, uses Facebook API for authentication
- Uses Facebook and Twitter API for sharing
- External payment processing