IERG4210 Web Programming and Security (Spring 2022) Tutorial 9

TA: ZHOU Jiuqin

Alternative Security Patch

- NO:
  - Build a whitelisting wall through IPTABLES
- YES:
  - Backup the data of your websites regularly
  - SSH to your servers through certificates
  - Update the operating system of your server
  - Update dependent software such as those from Apache

Phase 5 Overview

- Build a secure checkout flow using Paypal:
    i. How to test in Paypal Sandbox Test Suite
    ii. How to integrate with Paypal Checkout Standard
    iii. How to build an Instant Payment Notification (IPN) page
    iv. How to maintain a Database about Orders (*)

Paypal Sandbox Test Suite

- Create your sandbox accounts at Sandbox accounts - PayPal Developer.

```
Merchant Account:
  Type: Bussiness
  Email ID: sb-hnszm15459856@business.example.com
  System Generated Password: -hZ/o&8D
Buyer Account:
  Type: Personal
  Email ID: sb-5qe3r15443822@personal.example.com
  System Generated Password: [<Wx7Nx?
```

Paypal Sandbox Test Suite

- View your sandbox applications at Applications - PayPal Developer.
    - Copy the Client ID for future use.

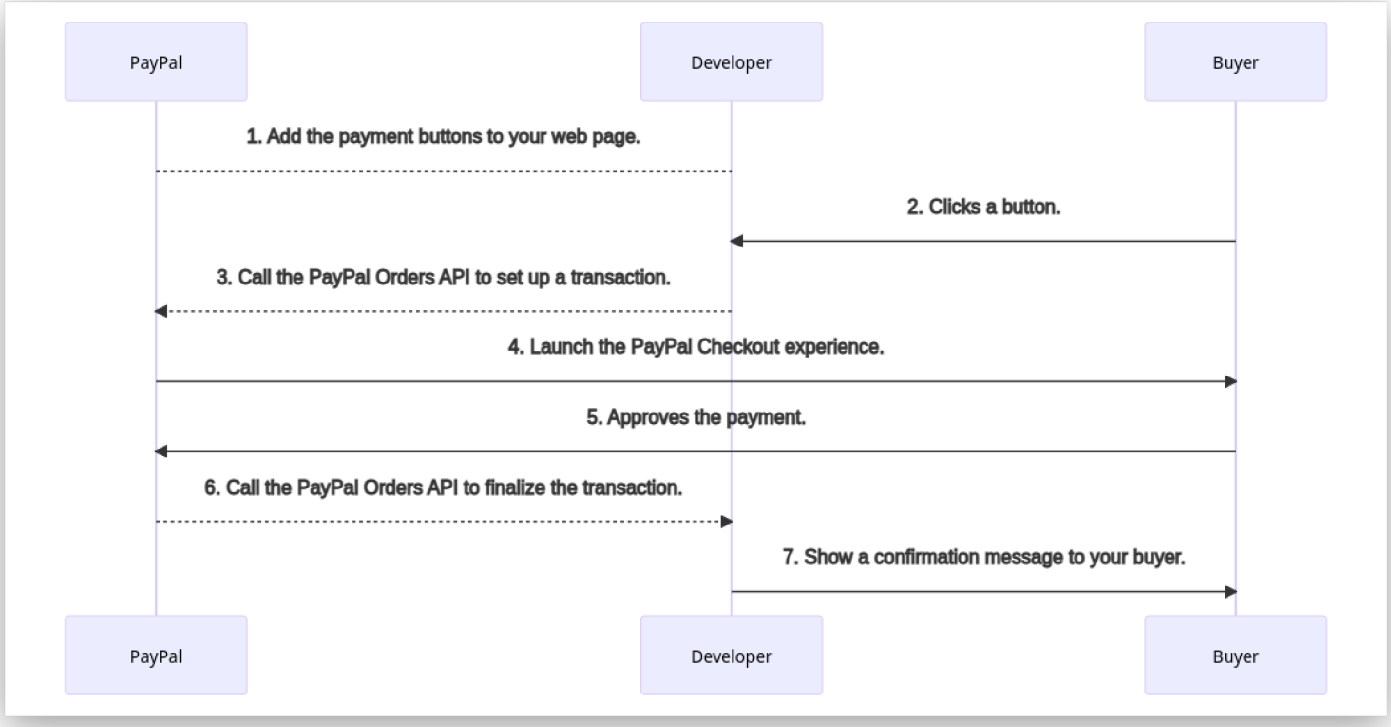
```
Default Application:
  Sandbox account: sb-hnszm15459856@business.example.com
  Client ID: Afbrqbxu4lkaCs6pl5-jWjFumMUem7j0xag5xFf1GkxI6H-qvUWDJOsbou1qP7Bu_vRrxUG-S3p0NYrc
```

Paypal Sandbox Test Suite

- Debugging Utilities:
  - Sandbox API call history - PayPal Developer
  - IPN simulator - PayPal Developer
- More Information:
  - PayPal Sandbox Testing Guide

Paypal Checkout Standard

- Integrate Paypal Checkout Standard



Paypal Checkout Standard

1. Include a Javascript SDK from Paypal for the web page.
    - Note that the value of `client-id` should be replaced by the Client ID we copied from the last section instead of `test`.

```
<script src="https://www.paypal.com/sdk/js?client-id=test&currency=USD"></script>
```

Paypal Checkout Standard

2. Set up a container element for the button.

```
<div id="paypal-button-container"></div>
```

Paypal Checkout Standard

3. Write custom scripts to render the button. Full Sample Code.

```
<script>
    paypal.Buttons({

        // Sets up the transaction when a payment button is clicked
        createOrder: ...,

        // Finalize the transaction after payer approval
        onApprove: ...
    }).render('#paypal-button-container');

</script>
```

Paypal Checkout Standard

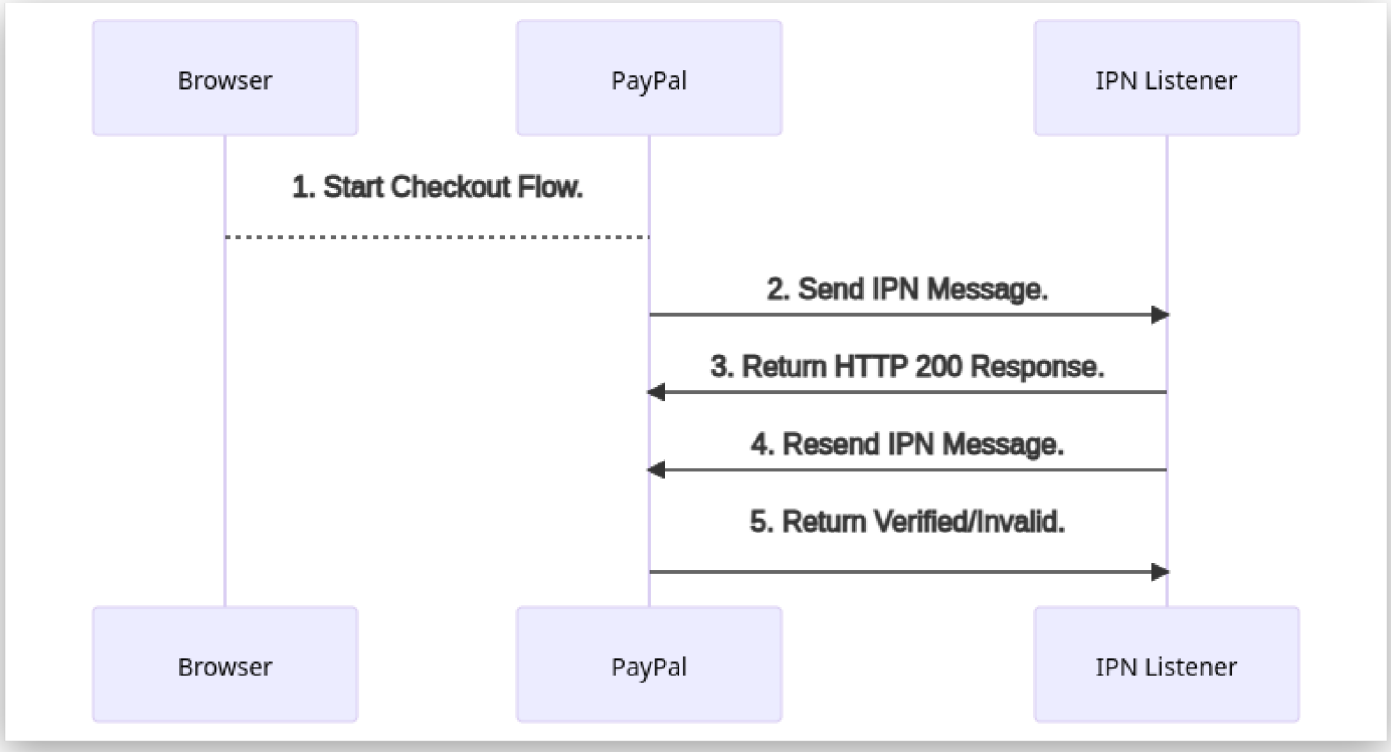
- Further debugging:
  - Sandbox API call history - PayPal Developer
- Customization:
  - Customize your buyers' experience
  - JavaScript SDK reference.

Paypal Checkout Standard

- Legacy Button:
  - Sample Code
  - PayPal PHP Website Integration Tutorial | Think Tank
  - How to Create a Simple Shopping Cart With PayPal
  - Button Manager API

Paypal Instant Payment Notification

- Introducing IPN



Paypal Instant Payment Notification

- Duties of a IPN Listener:
  - Returns an empty HTTP 200 response
  - Send unaltered message back to PayPal:
    - `https://ipnpb.paypal.com/cgi-bin/webscr?cmd=_notify-validate&` + `IPN-MESSAGE`
    - Wait for `VERIFIED` or `INVALID`

Paypal Instant Payment Notification

- A Sample IPN Message:
  - Format: `variable=value` with a delimiter `&`

```
mc_gross=19.95&...&txn_id=61E67681CH3238416&...&test_ipn=1&...
```

Paypal Instant Payment Notification

- Several Important variables:
  - `receiver_email`: who the IPN is supposed to be sent to
  - `test_ipn`: whether it is testing in a sandbox
  - `txn_id`: the unique id of the transaction
  - `payment_status`: whether the transaction is completed
  - `mc_fee` `mc_currency`: the amount of money received

Paypal Instant Payment Notification

- Other Logic to be implemented:
    i. Check that the `payment_status` is `Completed`.
    ii. If the `payment_status` is `Completed`, check the `txn_id` against the previous PayPal transaction that you processed to ensure the IPN message is not a duplicate.
    iii. Check that the `receiver_email` is an email address registered in your PayPal account.
    iv. Check that the price (carried in `mc_gross`) and the currency (carried in `mc_currency`) are correct for the item (carried in `item_name` or `item_number`).

Paypal Instant Payment Notification

- The same Sample Code from last section.
- Further Debugging:
  - IPN simulator - PayPal Developer
- More Information:
  - IPN testing

Micellaneous

- Deadline: April 11, 2022
- My Email: zj021@ie.cuhk.edu.hk
- No tutorial next week due to Ching Ming Festival. Happy Holiday!