**OAuth2**

Tài liệu tham khảo:

https://docs.haravan.com/blogs/authentication/1000017781-oauth

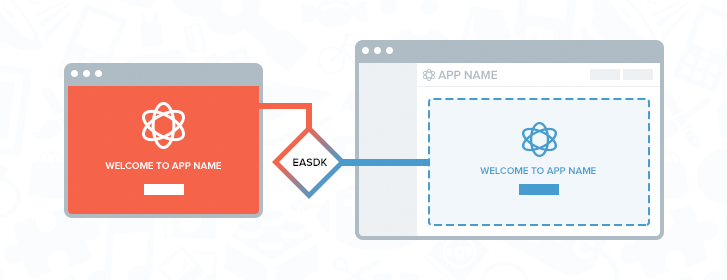
- Tạo tài khoản partner Haravan : https://app.haravan.com/services/partners/signup

- Dùng tài khoản Partner tạo DEV Shop, tạo App để làm.

- Source Haravan api ở các ngôn ngữ khác nhau: php, nodejs, C#, ....

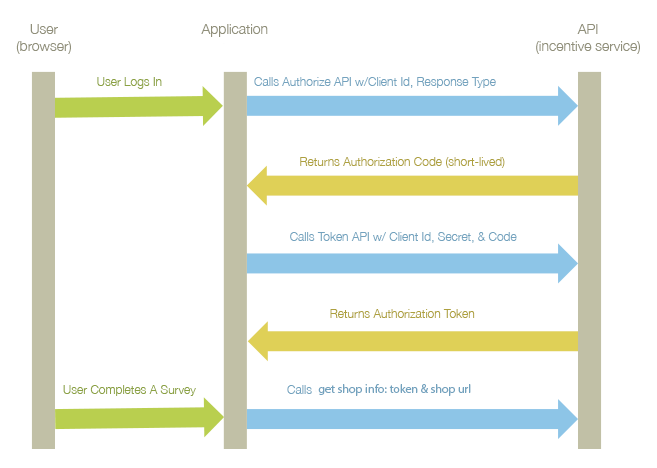
<https://github.com/Haravan>

# - App nhúng (Embedded App): đường dẫn App được đặt trong iframe.



* App không nhúng: khi click vào logo App sẽ mở ra new tab dẫn tới trang chủ App.

- OAuth 2:



* Step 1: Get the client’s credentials
* Step 2: Asking for permission
* Step 3: Confirming installation
* Step 4: Making authenticated requests
* Scopes
* Verification

**---------------------------------------------------------------------------------------------------------------------**

**OAuth2 in PHP**

Tài liệu tham khảo:

https://docs.haravan.com/blogs/authentication/1000017781-oauth

Source: https://github.com/Haravan/haravan\_php\_api/

- trong ví dụ : domain haravanapi.com dung để demo, hãy đổi nó thành domain của App.

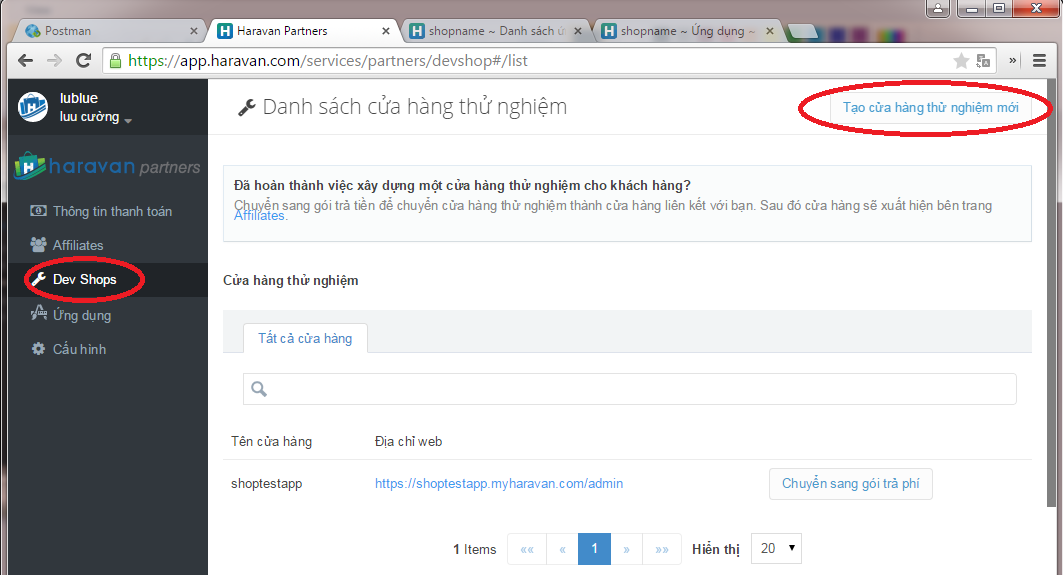
**I). Tạo tài khoản partner Haravan :**

https://app.haravan.com/services/partners/signup

( tài khoản sẽ được Haravan duyệt)

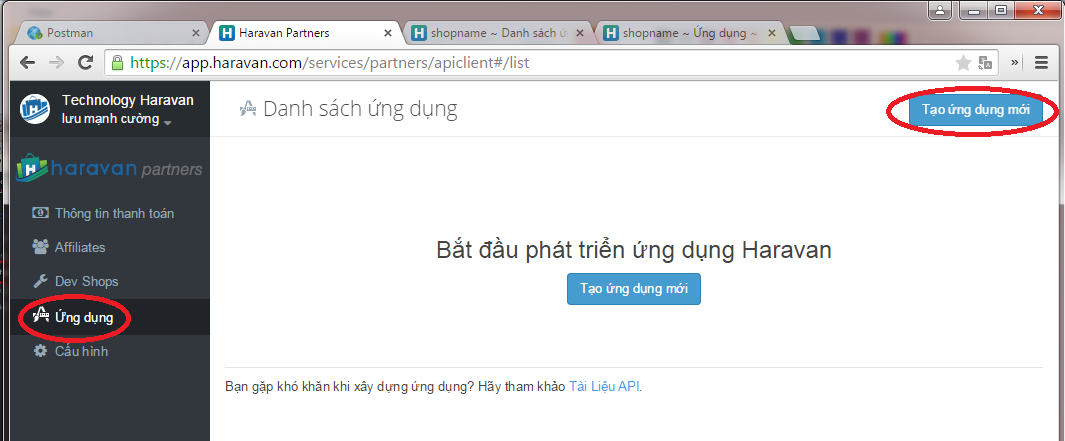
Link Đăng nhập : https://app.haravan.com/services/partners

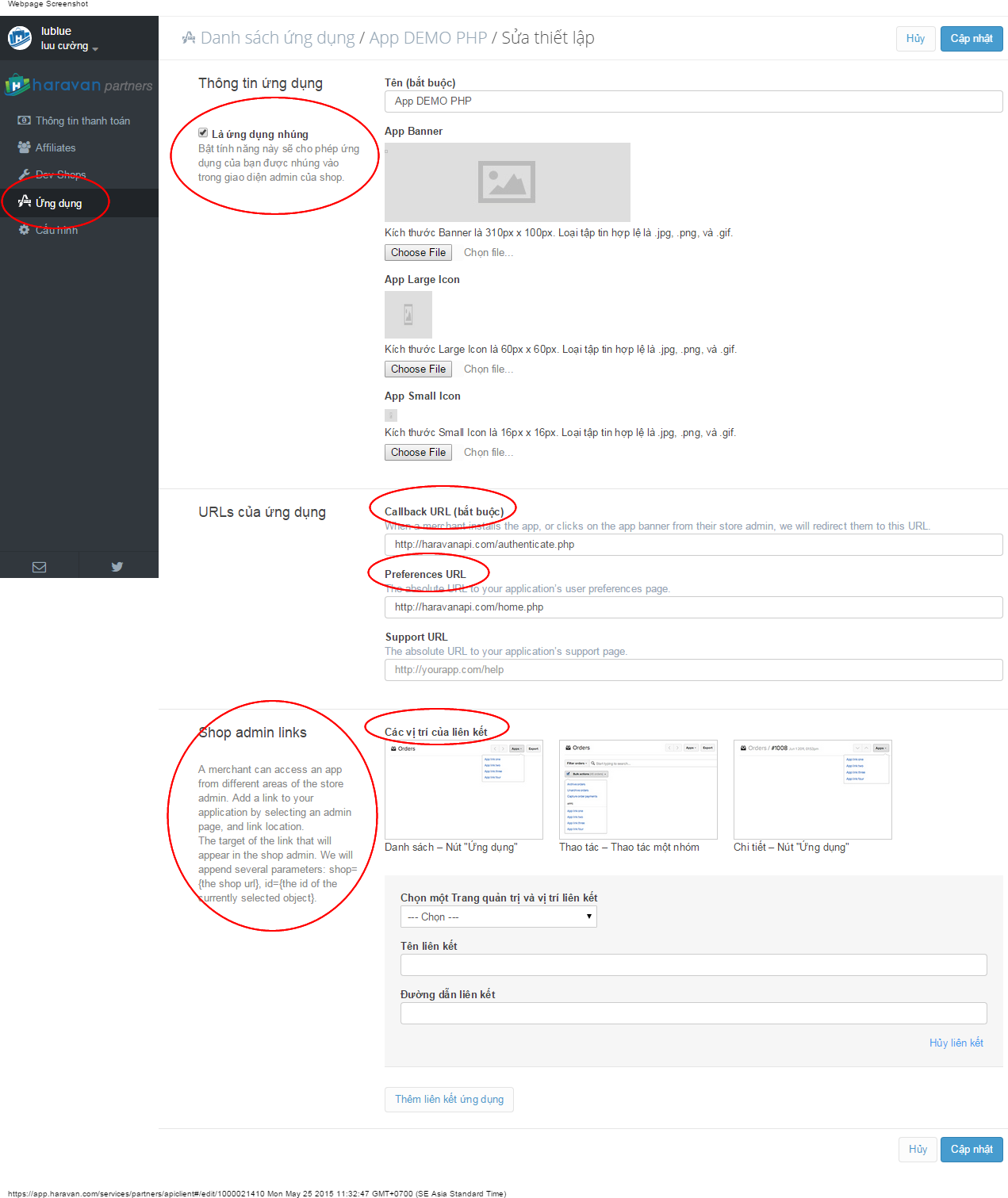
**II). Dùng tài khoản Partner tạo DEV Shop.**



**III). Dùng tài khoản Partner tạo App.**

1. Tạo App





- Ứng dụng nhúng (Embed App): Bật tính năng này sẽ cho phép ứng dụng của bạn được nhúng vào trong giao diện admin của shop ( bằng iframe ). Nếu không thì sẽ mở ra tab mới.

- Khi Shop cài App cần lưu lại Shop name và Access\_token.

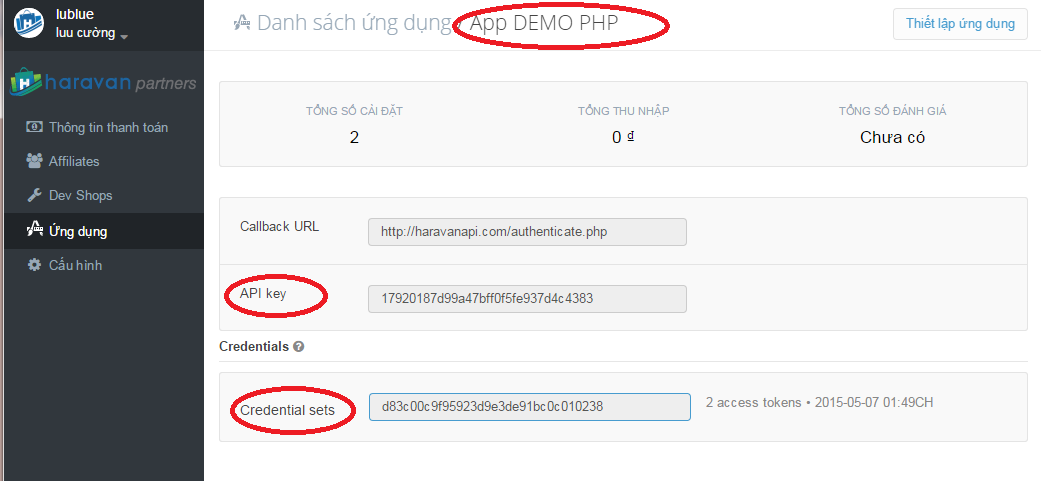
token có thời hạn mãi mãi ko hết hạn. Tuy nhên khi thêm quyền vào scope thì cần tháo app cài lại.

#### - URLs của ứng dụng

Callback URL (bắt buộc) : When a merchant installs the app, we will redirect them to this URL. ( khi cài App thì link này được sử dụng).

Preferences URL: When a merchant clicks on the app banner from their store admin, we will redirect them to this URL. The absolute URL to your application’s user preferences page. ( sau khi App đã cài xong thì link này được dùng. nếu link này để trống thì sẽ dùng Callback URL)

#### - Shop admin links : cho phép chèn các liên kết trong các page admin đến App kèm theo ID.



- App tạo xong sẽ cung cấp 2 tham số dùng trong chứng thực: "API key" và "Credential sets" (Credential sets : còn gọi là api secret hay secret key).

2. Config App Demo PHP

- Source: https://github.com/Haravan/haravan\_php\_api/

- Add hosts domain App local:

127.0.0.1 haravanapi.com

- Tạo vhost trỏ tớ source

- File /config.php

điền các tham số tưng ứng với App vừa tạo: API\_KEY, SECRET key

- REDIRECT\_URI: link trả về biến "code", đặt tên thế nào thì tùy App nhưng lưu ý bến này có dùng trong chứng thực. Hiện tại App này đặt giống "Callback URL".

## - Scopes: Quyền truy xuất dữ liệu ( cách nhau bằng khoảng trắng).

<https://docs.haravan.com/blogs/authentication/1000017781-oauth#scopes>

Part of the authorization process requires specifying which parts of a shop’s data the client would like access to (see the “Getting permission” part of this guide). A client can ask for any of the following scopes:

* read\_content, write\_content  
  Access to [Article](https://docs.shopify.com/api/article), [Blog](https://docs.shopify.com/api/blog), [Comment](https://docs.shopify.com/api/comment), [Page](https://docs.shopify.com/api/page), and [Redirect](https://docs.shopify.com/api/redirect).
* read\_themes, write\_themes  
  Access to [Asset](https://docs.shopify.com/api/asset) and [Theme](https://docs.shopify.com/api/theme).
* read\_products, write\_products  
  Access to [Product](https://docs.shopify.com/api/product), [Product Variant](https://docs.shopify.com/api/product_variant), [Product Image](https://docs.shopify.com/api/product_image), [Collect](https://docs.shopify.com/api/collect), [Custom Collection](https://docs.shopify.com/api/customcollection), and [Smart Collection](https://docs.shopify.com/api/smartcollection).
* read\_customers, write\_customers  
  Access to [Customer](https://docs.shopify.com/api/customer) and [Customer Group](https://docs.shopify.com/api/customergroup).
* read\_orders, write\_orders  
  Access to [Order](https://docs.shopify.com/api/order), [Transaction](https://docs.shopify.com/api/transaction) and [Fulfillment](https://docs.shopify.com/api/fulfillment).
* read\_script\_tags, write\_script\_tags  
  Access to [Script Tag](https://docs.shopify.com/api/scripttag).
* read\_fulfillments, write\_fulfillments  
  Access to [Fulfillment Service](https://docs.shopify.com/api/fulfillmentservice).
* read\_shipping, write\_shipping  
  Access to [Carrier Service](https://docs.shopify.com/api/carrierservice).

- Vì App chưa lên store nên khi cài App thì dùng link sau :

https://{{shopname}}.myharavan.com/admin/api/auth/?api\_key={{API key}}

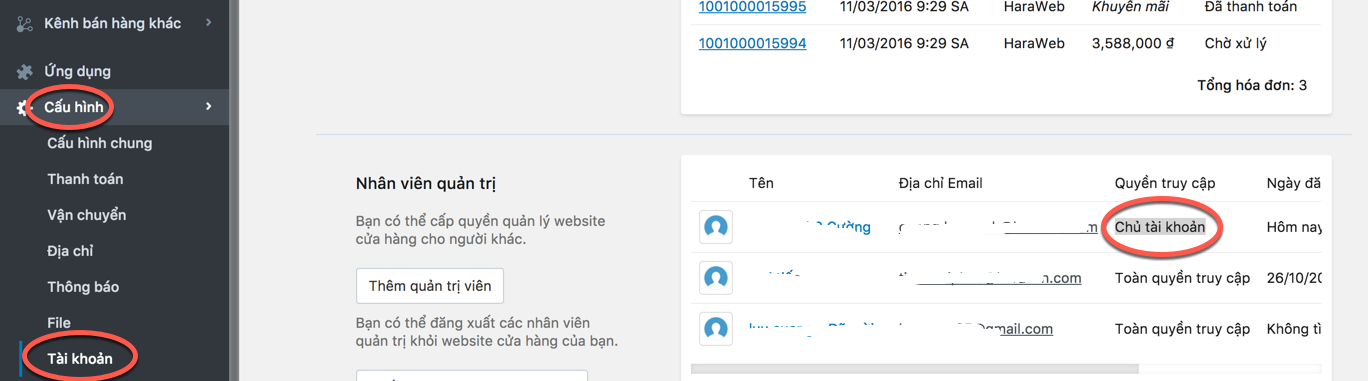
VD: https://shopname.myharavan.com/admin/api/auth/?api\_key=17920187d99a47bff0f5fe937d4c4383

- Sau khi cài App, Shop có thể vào App bằng cách click vào Banner App trong phần Ứng dụng hoặc vào trực tiếp bằng link sau:

https://{{shopname}}.myharavan.com/admin/app#/embed/{{API key}}

VD: <https://shopname.myharavan.com/admin/app#/embed/17920187d99a47bff0f5fe937d4c4383>

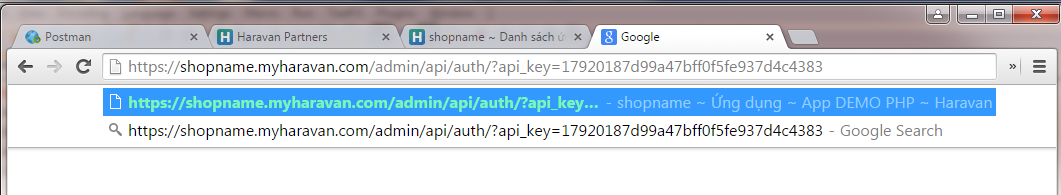
Lưu ý: cần đăng nhập bằng tài khoản chủ shop mới cài được app.



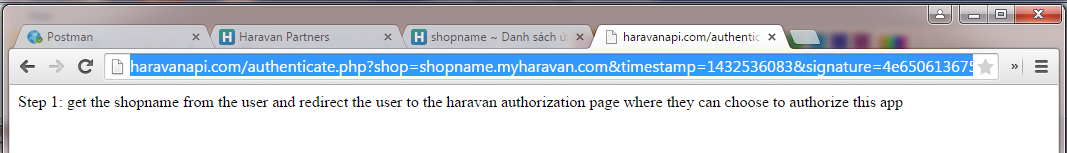
3. Thao tác cài App lấy Access\_token

- Step 1: chạy link cài App

https://shopname.myharavan.com/admin/api/auth/?api\_key=17920187d99a47bff0f5fe937d4c4383

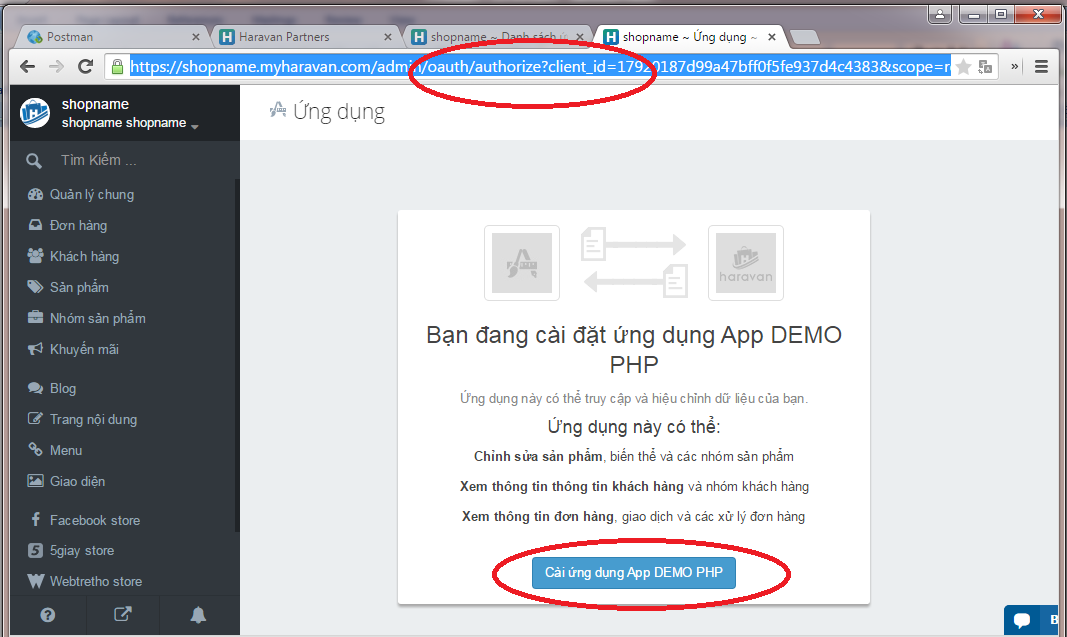


-> haravan sẽ gọi vào App bằng Callback URL cùng với các tham số (shop, timestamp, signature) : http://haravanapi.com/authenticate.php?shop=shopname.myharavan.com&timestamp=1432535727&signature=1c977bb5add823056ae72ac43ab77bd3659087574bf569c3bef42fa3b9703bed



-> App tạo link authorize và gọi lại Shop với các tham số (client\_id, scope, redirect\_uri, response\_type):

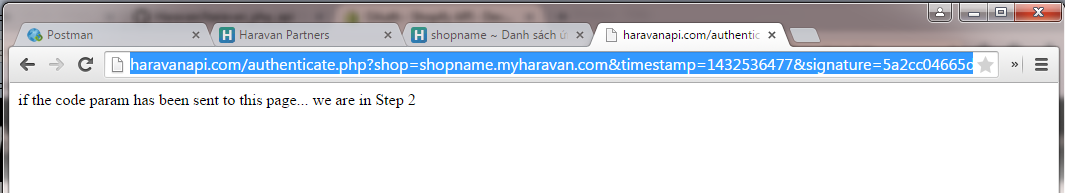
https://shopname.myharavan.com/admin/oauth/authorize?client\_id=17920187d99a47bff0f5fe937d4c4383&scope=read\_products,write\_products,read\_orders,read\_customers&redirect\_uri=http%3A%2F%2Fharavanapi.com%2Fauthenticate.php&response\_type=code



-> Chủ Shop Click "Cài ứng dụng App DEMO PHP"

-> haravan gọi lại App bằng link redirect\_uri với các tham số (shop, timestamp, signature, code)

http://haravanapi.com/authenticate.php?shop=shopname.myharavan.com&timestamp=1432536477&signature=5a2cc04665d149a906114ce99eb2d61e147aa15966cd507e52908a7990c156c5&code=434fee80d39f4b9cb4dbbd42c2793e4ec747494818a54cc3b6a78cd43ed6920a



- Step 2: lấy Access\_token

dùng biến "code" (Authorization Code) để đổi lấy access token bằng cách POST lại vào Shop.

Lưu ý post dùng x-www-form-urlencoded

public function getAccessToken($code, $redirect\_url='') {

// POST to https://SHOP\_NAME.myharavan.com/admin/oauth/access\_token

$url = "https://{$this->shop\_domain}/admin/oauth/access\_token";

$payload = "client\_id={$this->api\_key}&client\_secret={$this->secret}&code=$code";

$payload .= "&redirect\_uri=" . urlencode($redirect\_url);

$payload .= '&grant\_type=authorization\_code';

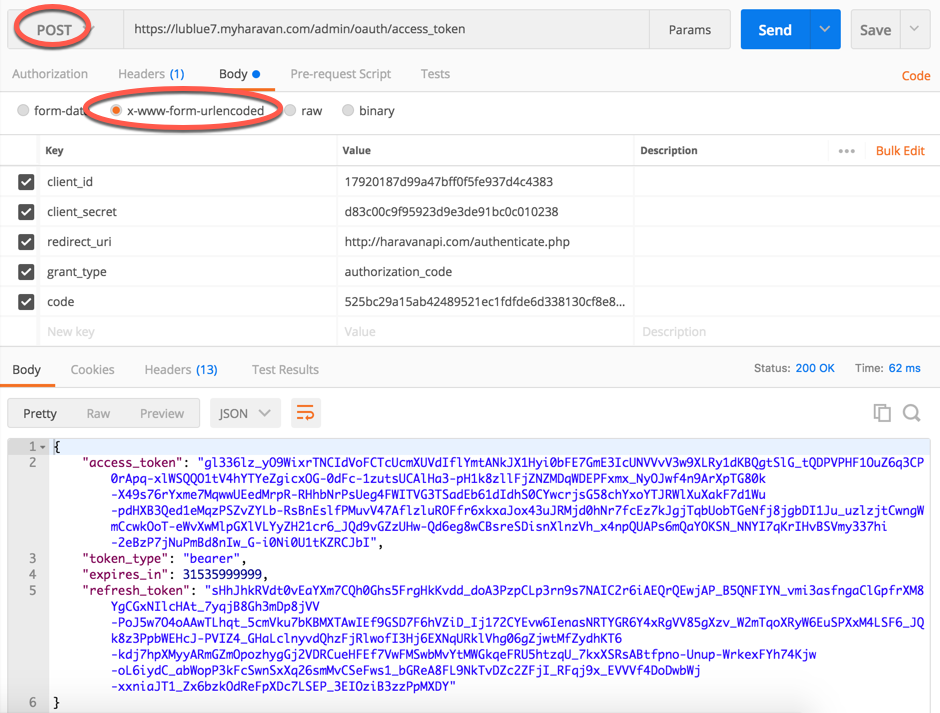
$response = $this->curlHttpApiRequest('POST', $url, '', $payload, array());

$response = json\_decode($response, true);

if (isset($response['access\_token'])) return $response['access\_token'];

return '';

}



Khi lấy được token rồi thì lưu lại token và shopname vào Database để sử dụng.

(lưu ý : redirect\_uri phải trùng với redirect\_uri đã dùng ở bước trước đó )

- Nếu app nhúng thì cài app xong chuyển trang qua link Shop Admin, nếu không phải nhúng thì qua link App.

if(IS\_EMBED\_APP){

//https://shopname.myharavan.com/admin/app#/embed/17920187d99a47bff0f5fe937d4c4383

header("Location: " . 'https://' . $\_SESSION['shop'] . '/admin/app#/embed/' . HARAVAN\_API\_KEY);

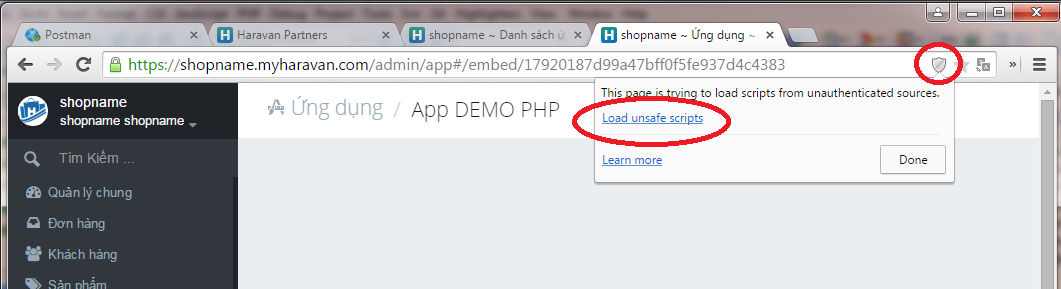
}else{

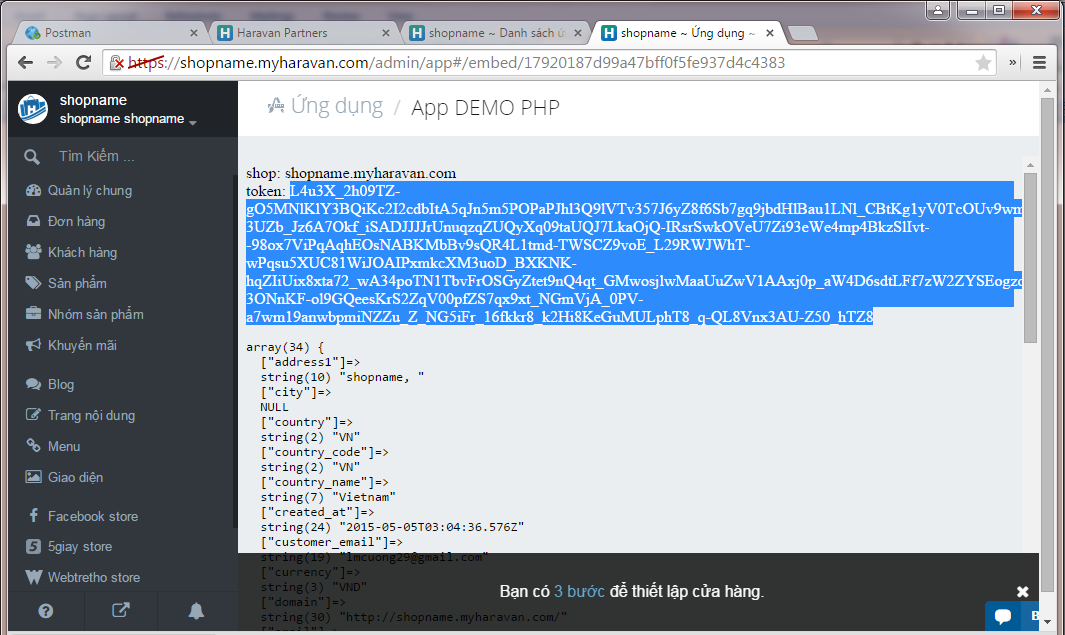
header("Location: home.php");

}

- Để iframe App được load trong admin Shop thì ta cần cài đặt domain App dùng "https://".

nếu link App là "http://" thì cần click chọn allow unsafe scripts ( Chrome) .



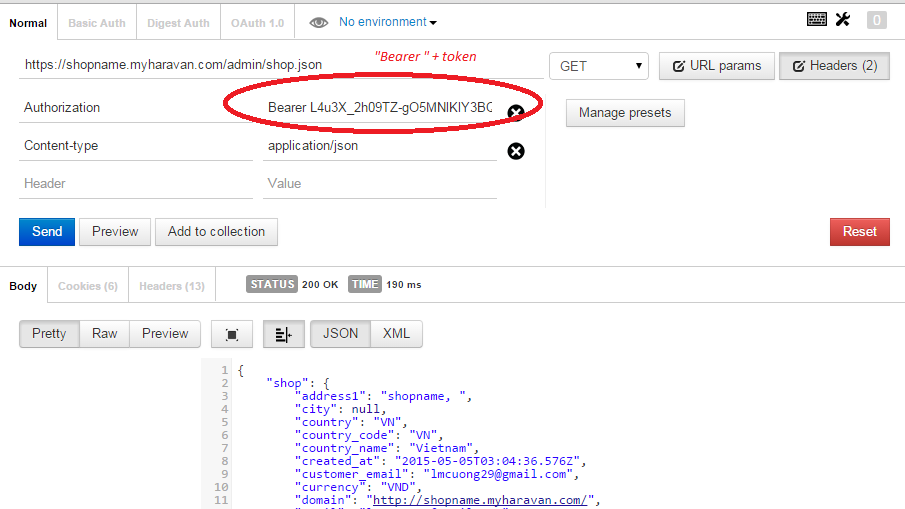


- Step 3: dùng token lấy Data từ Shop, dữ liệu json giống BasicAuthenticate.

$sc = new HaravanClient($\_SESSION['shop'], $\_SESSION['token'], HARAVAN\_API\_KEY, HARAVAN\_SECRET);

$shopjson = $sc->call('GET', '/admin/shop.json?page=1', array());

Hoặc dùng POSTMAN để test lại :



## - Verification: chứng thực request là hợp lệ, được gọi từ Haravan ( với một shop tại một thời điểm cụ thể):

if(!$haravanClient->validateSignature($\_GET)) die('Error: invalid signature.');

public function validateSignature($query)

{

if(!is\_array($query) || empty($query['signature']) || !is\_string($query['signature'])) return false;

$calculated\_signature = "";

if($query['code']) $calculated\_signature .= 'code=' . $query['code'];

$calculated\_signature .= 'shop=' . $query['shop'] . 'timestamp=' . $query['timestamp'];

$signature = bin2hex(hash\_hmac('sha256', $calculated\_signature, $this->secret, true));

return $query['signature'] == $signature;

}

IV). Webhook:

- webhook dùng để đăng kí các sự kiện. ví dụ : sự kiện tháo App, đặt hàng, tạo mới product,....

- Tham khảo:

<https://docs.haravan.com/blogs/webhooks/1000017841-introduction>

<https://docs.haravan.com/blogs/api-reference/1000017858-webhook>

- Step1: Tạo webHook

$data = array(

"webhook" => array(

"topic" => "orders/create",

"address" => "http://haravanapi.com/webhook.php",

"format" => "json"

)

);

$sc = new HaravanClient($\_SESSION['shop'], $\_SESSION['token'], HARAVAN\_API\_KEY, HARAVAN\_SECRET);

$registerhook = $sc->call('POST', '/admin/webhooks.json', $data);

Get webhook:

$gethook = $sc->call('GET', '/admin/webhooks.json?topic=orders/create&address=http://haravanapi.com/webhook.php', array());

Lưu ý : nếu topic đã tạo rồi thì khi tạo lại sẽ bị báo lỗi trùng. khi Shop tháo app thì các webhook cũng bị tháo.

## - Step 2 : Receive and Verify a webhook

## Khi nhận webhook cần Verify chứng thực xem có đúng hook của shop haravan gọi vô.

Cần trả lại status **200 OK** response cho hook. nếu không thấy status 200 thì hook sẽ retry bắn lại.

Thuật toán **Verify:**

function verify\_webhook($data, $hmac\_header)

{

$calculated\_hmac = base64\_encode(hash\_hmac('sha256', $data, HARAVAN\_SECRET, true));

return ($hmac\_header == $calculated\_hmac);

}

if($\_SERVER['HTTP\_X\_HARAVAN\_HMAC\_SHA256']) $hmac\_header = $\_SERVER['HTTP\_X\_HARAVAN\_HMAC\_SHA256'];

if($\_SERVER['HTTP\_HARAVAN\_SHOP\_DOMAIN']) $shopdomain = $\_SERVER['HTTP\_HARAVAN\_SHOP\_DOMAIN'];

if($\_SERVER['HTTP\_X\_HARAVAN\_TOPIC']) $topic = $\_SERVER['HTTP\_X\_HARAVAN\_TOPIC'];

$data = file\_get\_contents('php://input');

$verified = verify\_webhook($data, $hmac\_header);

if($verified){ echo "OK";

}else{ echo "Unauthorized"; }

header("Status: 200 OK");

V). Lưu ý:

1. Với App nhúng: cần kiểm tra xem app có đang nằm trong iframe hay không, nếu không thì redirect lại link shop ( link sẽ yêu cầu login nếu shop chưa đăng nhập ), link như sau:

"{shopname}/admin/app#/embed/{api\_key }"

- Script Ví dụ : ( thay các tham số cho phù hợp)

<script>

function isNoIframeOrIframeInMyHost() {

var myresult = true;

var app\_domain = "onapp.haravan.com";

try {

var tophref = top.location.href;

var tophostname = top.location.hostname.toString();

var myhref = location.href;

if (tophref === myhref) {

myresult = true;

} else if (tophostname !== app\_domain) {

//tophostname !== "www.your\_app\_domain.com"

myresult = false;

}

} catch (error) {

myresult = false;

}

return myresult;

}

if(isNoIframeOrIframeInMyHost()){

//web

var app\_key = "7dee65023f7f5b087eb75dd882135aff";

var url = "https://lublue.myharavan.com/admin/app#/embed/" + app\_key;

window.location = url;

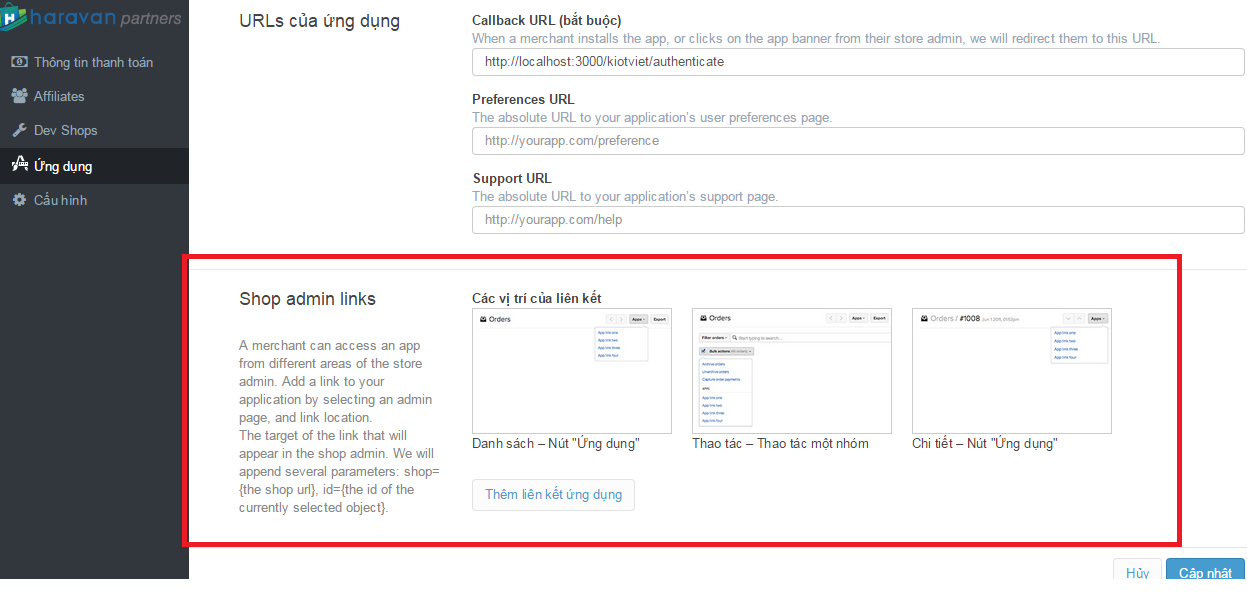
}

</script>

#### 2. Shop admin links:

A merchant can access an app from different areas of the store admin. Add a link to your application by selecting an admin page, and link location. The target of the link that will appear in the shop admin. We will append several parameters: shop={the shop url}, id={the id of the currently selected object}.

- gắn link App ở các vị trí khác nhau trong admin



- shop tìm kiếm và click chọn nhiều object ( như product, customer ...) sau đó click vào link App thì sẽ mở một new tab đến link đó kèm theo danh sách id. -> App sử lý xong thì đóng tab lại để shop về màn hình ban đầu.

3. Api limit

Api gọi nhiều sẽ bị chạm giới hạn cho phép, 1 app gọi vào 1 shop, sẽ cho phép 40 request/s, và 1200 request/5min, vượt qua giới hạn này, haravan trả về 429, và buộc app phải chờ 5 phút sau mới dc gọi tiếp .

rule app dụng cho từng IP, từng shop, nếu 1 shop bị, shop khác không bị ảnh hưởng gì.

* để tránh lỗi này khi 1 IP gọi nhiều vô 1 shop thì có thể gọi tuần tự, sleep 301 millisecond cho mỗi request.
* Hoặc khi gặp 429 thì ngưng gọi API trong 5 phút.