

【漏洞分析】METINFO 6.1.2 版本 XSS 漏洞分析

文/ icuke

0x00 漏洞概述

漏洞类型：XSS 漏洞

危险等级：中

CVE 编号：CVE-2018-18374

利用条件：该漏洞需要管理员在登录状态下访问攻击者构造的恶意链接。

漏洞位置：head.php 中的第 20 行 echo 输出语句

漏洞产生原因：echo 输出的 script 标签代码中，anyid 值由外部输入获得，且没有做很好过滤

受影响版本：全部版本

修复版本：无

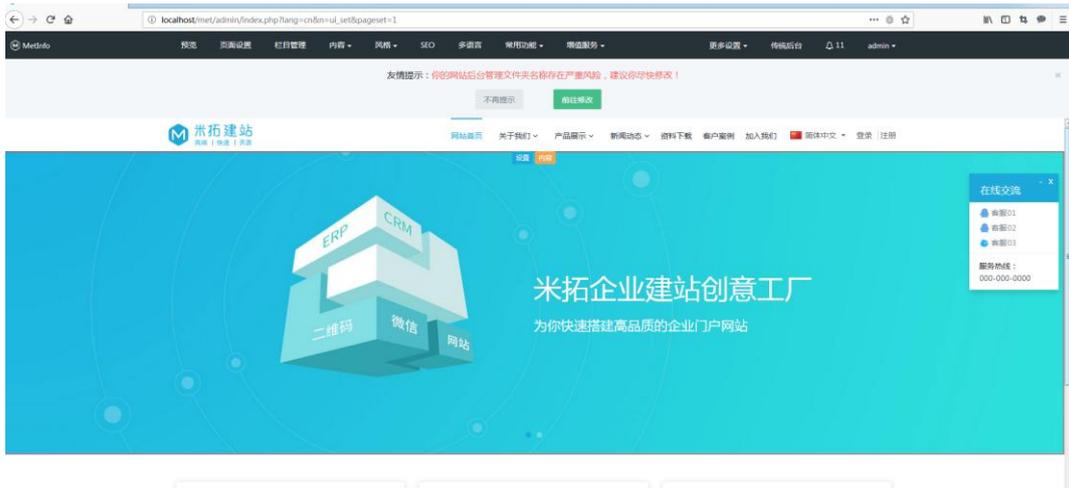
0x01 环境准备

| | |
|------------|---------------|
| IDE | PhpStorm |
| Web 环境 | phpstudy 集成环境 |
| PHP 版本 | 5.4.45 |
| MetInfo 版本 | 6.1.2 |

0x02 漏洞复现

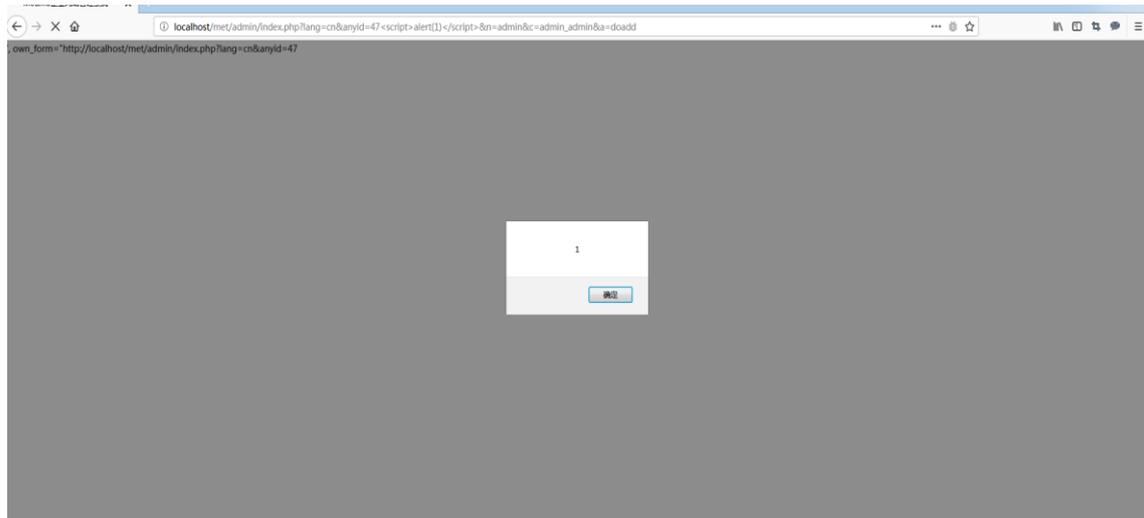
1. 管理员登录管理后台

使用 firefox 访问 localhost/met/admin/登录管理后台。



2. 管理员访问构造的恶意链接

使用 firefox 访问 [http://localhost/met/admin/index.php?lang=cn&anyid=47%3Cscript%3Ealert\(1\)%3C/script%3E&n=admin&c=admin_admin&a=doadd](http://localhost/met/admin/index.php?lang=cn&anyid=47%3Cscript%3Ealert(1)%3C/script%3E&n=admin&c=admin_admin&a=doadd) , 触发漏洞。



0x03 漏洞分析

1. 漏洞代码分析

漏洞代码在 `app/system/include/public/ui/admin/head.php` 文件 20 行的 `echo` 输出语句中：

```
69     "attention": "{$M[word][attention]}",
70     "cvall": "{$M[word][cvall]}"
71 },
72 langset="{$M['langset']}",
73 anyid="{$M['form']['anyid']}",
74 own_form="{$M['url']['own_form']}",
75 own_name="{$M['url']['own_name']}",
76 own="{$M['url']['own']}",
77 own_tem="{$M['url']['own_tem']}",
78 adminurl="{$M['url']['adminurl']}"
79 apppath="{$M['url']['api']}",
80 jsrand="{$jsrand}",
81 editorname="{$M['config']['met_editor']}",
82 met_keywords = "{$M['config']['met_keywords']}",
83 met_alt="{$M['config']['met_alt']}";
84 </script>
```

危险输出，在script标签内

阅读代码可知，anyid 的内容将直接被输出到 script 标签中，变量值来自 `$_M['form']['anyid']`，看下 `$_M['form']['anyid']` 变量值来源，在 `app/system/include/class/common.class.php` 中的 `load_form()` 方法里，可以看到 `$_COOKIE`、`$_POST`、`$_GET` 变量的 key 为 `$_M['form']` 的 key，value 需要经过 `daddslashes` 函数处理。

```
protected function load_form() {
    global $_M;
    $_M['form'] = array();
    isset($_REQUEST['GLOBALS']) && exit('Access Error');
    foreach($_COOKIE as $_key => $_value) {
        $_key[0] != '_' && $_M['form'][$_key] = addslashes($_value);
    }
    foreach($_POST as $_key => $_value) {
        $_key[0] != '_' && $_M['form'][$_key] = addslashes($_value);
    }
    foreach($_GET as $_key => $_value) {
        $_key[0] != '_' && $_M['form'][$_key] = addslashes($_value);
    }
}
```

`$_M['form']` 值来源

`daddslashes` 过滤函数：

```
function daddslashes($string, $force = 0) {
    !defined( name: 'MAGIC_QUOTES_GPC' ) && define( 'MAGIC_QUOTES_GPC', get_magic_quotes_gpc() );
    if (!MAGIC_QUOTES_GPC || $force) {
        if (is_array($string)) {
            foreach($string as $key => $val) {
                $string[$key] = daddslashes($val, $force);
            }
        } else {
            if (!defined( name: 'IN_ADMIN' )) {
                $string = trim(addslashes(sqlinsert($string)));
            } else {
                $string = trim(addslashes($string));
            }
        }
    }
    return $string;
}
```

第 59 行代码中，如果未定义 "IN_ADMIN"，会使用 `addslashes`、`sqlinsert` 函数对传入变量进行处理，如果定义 "IN_ADMIN"，只使用 `addslashes` 进行处理。全局搜索下 `IN_ADMIN` 的定义位置，在 `admin/index.php` 文件中有定义。

Find in Path Match case Words Regex ? File mask: *.php

Q: IN_ADMIN 14 matches in 9 files

| In Project | Module | Directory | Scope |
|------------|--------|-----------------------|-----------------------|
| | | | mysqlold.class 101 |
| | | | mysql.class 85 |
| | | | mysql.class 115 |
| | | | mysql.class 135 |
| | | | ui_compile.class 207 |
| | | | ui_compile.class 212 |
| | | | power.func 18 |
| | | | power.func 63 |
| | | | common.func 59 |
| | | | parameter_op.class 20 |
| | | admin\index | 5 |
| | | admin\...\mysql_class | 275 |

```

admin/index.php
1 <?php
2 # MetInfo Enterprise Content Management System
3 # Copyright (C) MetInfo Co., Ltd (http://www.metinfo.cn). All rights reserved.
4
5 define('IN_ADMIN', true);
6 //❖❖❖
7 $M_MODULE='admin';
8 if (@$_GET['m'])$M_MODULE=$_GET['m'];
9 if (@$_GET['n'])$_GET['n']="index";
10 if (@$_GET['c'])$_GET['c']="index";
11 if (@$_GET['a'])$_GET['a']="doindex";
12 @define('M_NAME', $_GET['n']);
  
```

IN_ADMIN定义

我们就是从 admin/index.php 文件入口进行利用的，所以对于 \$_GET、\$_POST、\$_COOKIE 传入的变量值只会进行 addslashes 处理。

2. 回溯触发路径

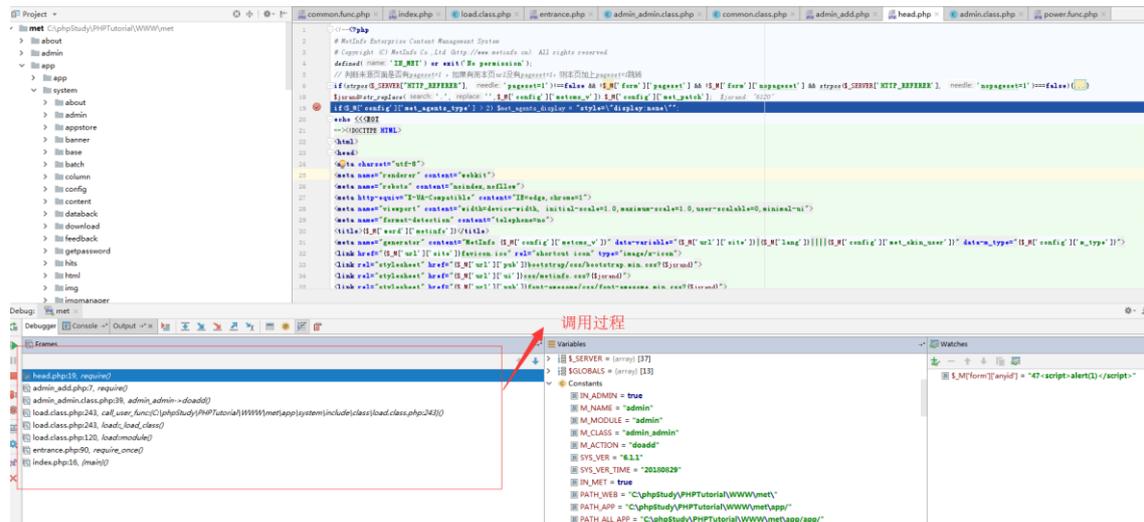
此处使用 PhpStorm xdebug 调试方式进行动态调试。在 app/system/include/public/ui/admin/head.php 的 19 行设置断点

```

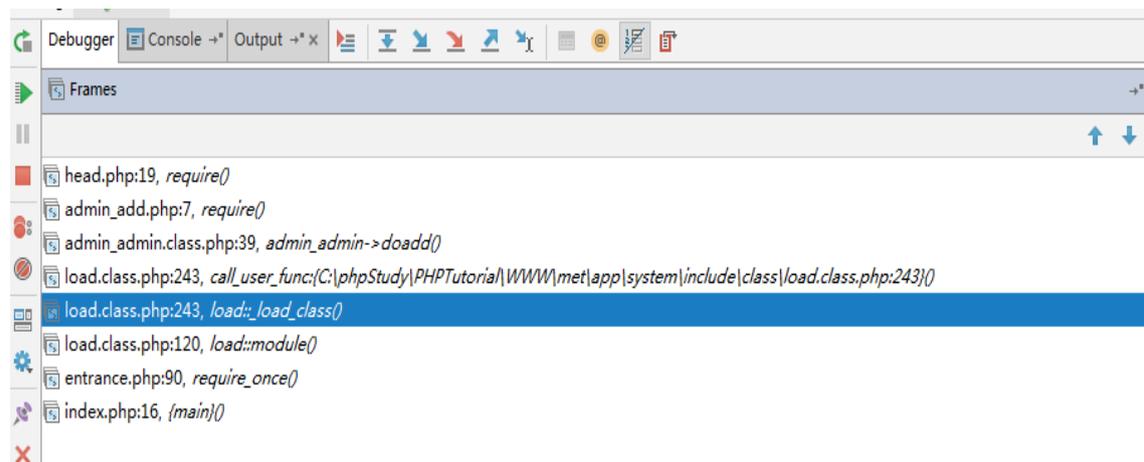
<!--<?php
# MetInfo Enterprise Content Management System
# Copyright (C) MetInfo Co., Ltd (http://www.metinfo.cn). All rights reserved.
defined( 'name: 'IN_ADMIN' ) or exit( 'No permission' );
// 判断来源页面是否有 pageset=1，如果有而本页没有 pageset=1，则本页加上 pageset=1 跳转
if (strpos($_SERVER['HTTP_REFERER'], 'needle: 'pageset=1')!==false && !$_M['form']['pageset'] && !$_M['form']['nopageset'] && strpos($_SERVER['HTTP_REFERER'], 'needle:
$jsrand=str_replace( 'search: ', 'replace: ', $_M['config']['metcms_v']); $_M['config']['met_patch']; $jsrand: '6120"
if ($_M['config']['met_agents_type'] > 2) $met_agents_display = "style='display:none'";
echo <<<ROT
--><!DOCTYPE HTML>
<html>
<head>
<meta charset="utf-8">
<meta name="renderer" content="webkit">
<meta name="robots" content="noindex, nofollow">
<meta http-equiv="I-UA-Compatible" content="IE=edge, chrome=1">
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=0, minimal-ui">
<meta name="format-detection" content="telephone=no">
<title>$_M['word']['metinfo']</title>
<meta name="generator" content="MetInfo ($_M['config']['metcms_v'])" data-variable="($_M['url']['site'])|($_M['lang'])|($_M['config']['met_skin_user'])" data-
link href="($_M['url']['site'])favicon.ico" rel="shortcut icon" type="image/x-icon">
  
```

断点位置

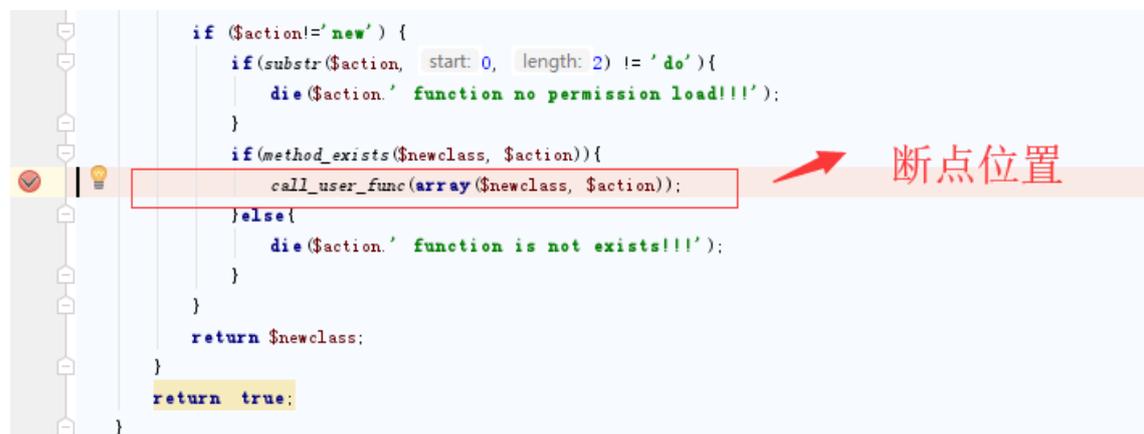
管理员登录后台后访问 [http://localhost/met/admin/index.php?lang=cn&anyid=47%3Cscript%3Ealert\(1\)%3C/script%3E&n=admin&c=admin_admin&a=doadd](http://localhost/met/admin/index.php?lang=cn&anyid=47%3Cscript%3Ealert(1)%3C/script%3E&n=admin&c=admin_admin&a=doadd)，触发断点。



左下方为调用过程：



在 app/system/include/class/load.class.php 的 243 行代码下断点，重新调试。



`$newclass` 是一个类对象，我们 F7 跟踪 `call_user_func` 函数调用，进入 `admin_admin` 的 `doadd` 方法，类 `admin_admin` 存在构造函数，会调用父类的构造方法，父类为 `admin`。

```
class admin_admin extends admin {
    public $moduleclass;
    public $module;
    public $database;
    /**
     * 初始化
     */
    function __construct() {
        global $_M;
        parent::__construct();
        $this->database = load::mod_class( classname: 'admin/admin_database', action: 'new');
    }
    /**
     * 新增内容
     */
    public function doadd() {
        global $_M;
        $a = 'doaddsave';
        $list['admin_group'] = '3';
        $list['lang'] = load::mod_class( classname: 'language/language_op', action: 'new')->get_lang();
        foreach ($list['lang'] as $key => $val) {
            $list['lang_check'][$key] = $val['mark'];
        }
        $list['lang_check'] .= '#metinfo#';
        $list['admin_issueok'] = 1;
        $list['op_check'] = "metinfo|add|editor|del";
        $list['pop_check'] = 'all';
        $metinfocolumn = $this->admin_list();
    }
}
```

继承admin类

```
load::sys_class( classname: 'common');
load::sys_class( classname: 'nav');
load::sys_func( funcname: 'admin');

class admin extends common {
    public function __construct() {
        global $_M;
        met_cookie_start();
        $this->load_language();
        $this->check();
        $this->lang_switch();
        load::plugin( plugin: 'doadmin');
        $_M['url']['help_tutorials_url'] = "http://help.metinfo.cn/help/show.php?langset={$_M['langset']}&helpid=";
        if($_M['user']['cookie'] && $_M['form']['sysui_pack']){
            require PATH_WEB.'public/ui/v2/static/library.php';
            die;
        }
        $_M['config']['m_type'] = M_TYPE;
    }
}
```

admin类继承common类

类 admin 继承 common 类，查看 common 类，构造函数调用 load_form 方法，完成对 \$_M['form'] 的赋值过程。

```

class common {
    /**
     * 初始化
     */
    public function __construct() {
        global $_M; //全局数组$_M
        ob_start(); //开启缓存
        $this->load_mysql(); //数据库连接
        $this->load_form(); //表单过滤
        $this->load_lang(); //加载语言配置
        $this->load_config_global(); //加载全站配置数据
        $this->load_url_site();
        $this->load_config_lang(); //加载当前语言配置数据
        $this->load_url(); //加载url数据
    }

    /**
     * 链接数据库
     */
    protected function load_mysql() {
        global $_M;
        $db_settings = array();
        $db_settings = parse_ini_file( filename: PATH_CONFIG . 'config_db.php' );
        @extract($db_settings);
        DB::dbconn($con_db_host, $con_db_id, $con_db_pass, $con_db_name, $con_db_port);
        $_M['config']['tablepre'] = $tablepre;
        return true;
    }
}

```

类common构造函数调用load_form

再看下类 admin 的构造过程，其中有一步会调用 check() 方法，在此处下一断点，重新调试，并使用 F7 跟进该调用过程。

```

protected function check() {
    global $_M;
    $http = isset($_SERVER['REQUEST_SCHEME']) ? $_SERVER['REQUEST_SCHEME'] : 'http';
    $current_url = $http . '://' . $_SERVER['HTTP_HOST'] . $_SERVER['REQUEST_URI'];
    $login_url = $_M['url']['site_admin'] . "index.php?n=login&c=login&a=doindex";
    if (strstr($current_url, $login_url)) {
        $admin_index = 1;
    } else {
        $admin_index = 0;
    }
    $met_adminfile = $_M['config']['met_adminfile'];
    $met_admin_table = $_M['table']['admin_table'];
    $metinfo_admin_name = get_net_cookie('metinfo_admin_name');
    $metinfo_admin_pass = get_net_cookie('metinfo_admin_pass');

    if (($metinfo_admin_name || $metinfo_admin_pass) {
        if ($admin_index) {
            net_cookie_unset();
            net_setcookie("re_url", $re_url, time() - 3600);
            Header (string: "Location: " . $login_url);
        } else {
            if ($re_url) {
                $re_url = $_SERVER['HTTP_REFERER'];
                $HTTP_REFERERs = explode( delimiter: '?', $_SERVER['HTTP_REFERER'] );
                $admin_file_len1 = strlen( string: "/" . $met_adminfile . "/" );
                $admin_file_len2 = strlen( string: "/" . $met_adminfile . "/index.php" );
                if (strstr(substr($HTTP_REFERERs[0], start: 0, $admin_file_len1)) == "/" . $met_adminfile . "/" || strstr(substr($HTTP_REFERERs[0], start: 0, $admin_file_len2)) == "/" . $met_adminfile . "/index.php") {
                    $re_url = ($http . "://" . $_SERVER['SERVER_NAME'] . $_SERVER['REQUEST_URI']);
                }
            }
            if ($COOKIE[$re_url] && strstr($re_url, $re_url)) net_setcookie("re_url", $re_url, time() + 3600);
            net_cookie_unset();
            Header (string: "Location: " . $login_url);
        }
        exit;
    } else {
        $query = "SELECT * FROM {$_M['table']['admin_table']} WHERE admin_id = '{$_metinfo_admin_name}' AND admin_pass = '{$_metinfo_admin_pass}' AND usertype = '3'";
    }
}

```

登录判断

阅读代码可知，会从 cookie 中取 metinfo_admin_name ,met_info_admin_pass 进行判断，若判断未通过，则重定向到登录页面。

F8 回到 admin_admin.class.php 的 doadd 方法调用

```
26 public function doadd() {
27     global $_M;
28     $a = 'doaddsave';
29     $list['admin_group'] = '3';
30     $list['lang'] = load::mod_class( classname: 'language/language_op', action: 'new' )->get_lang();
31     foreach ($list['lang'] as $key => $val) {
32         $list['lang_check'] .= $val['mark'] . ' ';
33     }
34     $list['lang_check'] .= '#metinfo#';
35     $list['admin_issueok'] = 1;
36     $list['op_check'] = "metinfo|add|editor|del";
37     $list['pop_check'] = 'all';
38     $metinfocolumn = $this->admin_list();
39     require $this->template( path: 'own/admin_add' );
40 }
41
```

调用template

运行到 39 行 F7 步入：

```
protected function template($path){
    global $_M;
    // 前缀、路径转换优化（新模板框架v2）
    $dir = explode( delimiter: '/', $path);
    $postion = $dir[0];
    $file = substr( strstr($path, needle: '/'), start: 1);

    if ($postion == 'own') {
        return PATH_OWN_FILE . "templates/{file}.php";
    }

    if ($postion == 'ui') {
        if (M_MODULE == 'admin') {
            $ui = 'admin';
        } else {
            $ui = 'web';
        }
        return PATH_SYS . "include/public/ui/{ui}/{file}.php";
    }
}
```

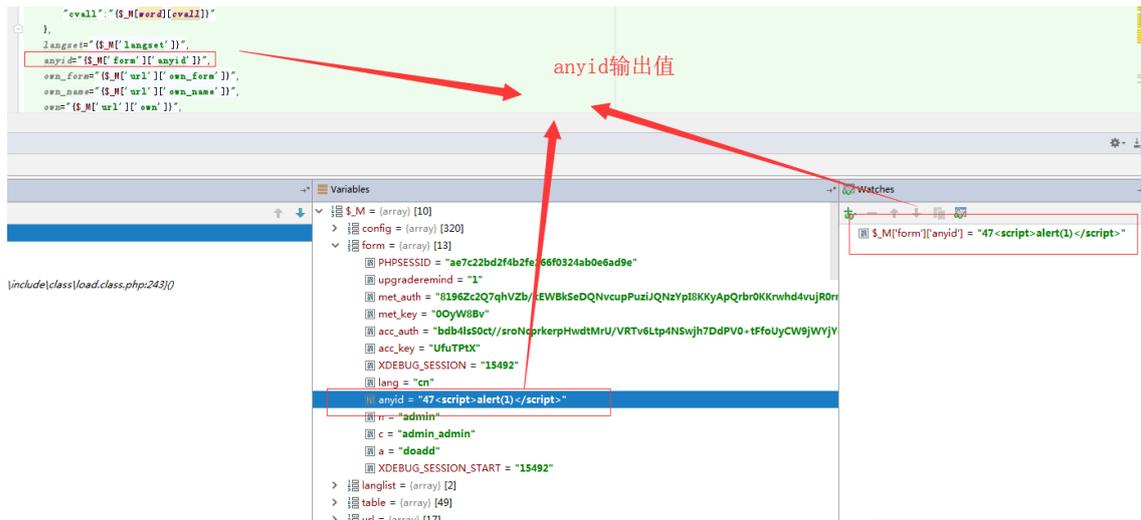
此处传入的\$path值为own/admin_add

发现 template 方法是用于模板寻址，此处我们寻址地址为 template/admin_add.php。F8 跳出，进入 admin_add.php 文件。

```
5 defined( name: 'IN_MBT' ) or exit( 'No permission' );
6
7 require $this->template( 'ui/head' );
8 echo <<<EOT
9 -->
10
11 <link rel="stylesheet" href="{$_M[url][own_tem]}css/metinfo.css?{$jsrand}" />
12 <form method="POST" class="ui-form" name="myform" action="{$_M[url][own_form]}a={$a}" target="_self">
13     <input type="hidden" name="id" value="{$_M['form']['id']}" />
14     <div class="v52fmbx">
15         <h3 class="v52fmbx_hr">{$_M['word']['admininfo']}</h3>
16         <dl>
17             <dt>{$_M['word']['adminusername']}</dt>
18             <dd class="ftype_input">
19                 <div class="fbox">
20                     <input type="text" name="admin_id" value="{list['admin_id']}" data-required="1">
21                 </div>
22             </dd>
23         </dl>
24     </form>
25     <dt>{$_M['word']['adminpassword']}</dt>
```

调用template传入/ui/head

第 7 行调用后进入 head.php 文件，触发漏洞执行。



0x04 总结

当管理员登录后台后，通过 url 传递的参数值 anyid 不会经过 sqlinsert 函数过滤，只经过 addslashes 处理后就返回到前台页面 script 标签中。

提供另一个触发链接：

[http://localhost/met/admin/index.php?lang=cn&n=system&c=news&a=doindex&anyid=12%3Cscript%3Ealert\(1\)%3C/script%3E](http://localhost/met/admin/index.php?lang=cn&n=system&c=news&a=doindex&anyid=12%3Cscript%3Ealert(1)%3C/script%3E)

0x05 修复方法

修改 app/system/include/function/common.func.php 的 daddslashes 方法，当 IN_ADMIN 为 true 时，对\$string 进行标签过滤。