**西瓜视频存在云储存桶泄露**

漏洞url：<https://studio.ixigua.com/upload?from=post_article>

漏洞类型：云储存桶泄露

漏洞危害：高危

1. 访问域名来到西瓜视频主页，点击发布视频



1. 这里进行点击上传封面进行burp抓包，将其发送到Repeat模块处



1. 这里发送到Repeat模块后，进行Send，发现回显泄露了云储存的密钥信息

"AccessKeyId":"AKTPMjgxODkwOTgwN2MzNDliY2FlYzFkMzgzOGNjMjYyYmE","SecretAccessKey":"ruaNfxRtfpaE0pQH3wKYAABGBP2Hmx5ldd3NTNIbd1R/C7YZ9Uc9036Cxv5xhTH+C/63qg2lrmNZbhD3dR6aiQ=="}



下面附上burp数据包：

GET /api/upload/getAuthKey/?params=%7B%22type%22%3A%22video%22%2C%22isLandscape%22%3Afalse%2C%22isSecret%22%3Afalse%7D HTTP/2

Host: studio.ixigua.com

Cookie: passport\_csrf\_token=654291f6c6731c263edfac074a62b043; passport\_csrf\_token\_default=654291f6c6731c263edfac074a62b043; MONITOR\_WEB\_ID=259113057001075; studio\_web\_id=7111665387901158920; \_tea\_utm\_cache\_2562=undefined; gftoken=NDM1MjE3OTA4fDE2NTU4MTM5MTkyNHx8MAcHBwcHBwc; \_ga=GA1.2.413719316.1656244531; odin\_tt=0f124ff101d1d179e69e60205ca9ee93a6859138e898a758581c72ecf7519e6dd48799f193eb059a7611f99e00605f70bc584d0c5c7dc511d2ed6d51ca770c43; passport\_auth\_status=5a919320e11a1be406ce81f90a3dadb3%2Cd5c7124e405a8096049929bf83d39cab; passport\_auth\_status\_ss=5a919320e11a1be406ce81f90a3dadb3%2Cd5c7124e405a8096049929bf83d39cab; sid\_guard=436d0deded38d8473ce10d6c5983b7c1%7C1656244620%7C5184000%7CThu%2C+25-Aug-2022+11%3A57%3A00+GMT; uid\_tt=057f7b267a08f2c411e17565d788157a; uid\_tt\_ss=057f7b267a08f2c411e17565d788157a; sid\_tt=436d0deded38d8473ce10d6c5983b7c1; sessionid=436d0deded38d8473ce10d6c5983b7c1; sessionid\_ss=436d0deded38d8473ce10d6c5983b7c1; sid\_ucp\_v1=1.0.0-KDg1ZjFmMmMxOTBiYzllOGJmZDIwMmJiYmVjNDdhMjRlNjkyZTQ5NTcKGAjzvOCtl\_U6EIyT4ZUGGJcMIAw4AkDxBxoCaGwiIDQzNmQwZGVkZWQzOGQ4NDczY2UxMGQ2YzU5ODNiN2Mx; ssid\_ucp\_v1=1.0.0-KDg1ZjFmMmMxOTBiYzllOGJmZDIwMmJiYmVjNDdhMjRlNjkyZTQ5NTcKGAjzvOCtl\_U6EIyT4ZUGGJcMIAw4AkDxBxoCaGwiIDQzNmQwZGVkZWQzOGQ4NDczY2UxMGQ2YzU5ODNiN2Mx; Hm\_lvt\_5ef88140a857780eb79a65f7d563f9ef=1655813633,1656376792; s\_v\_web\_id=verify\_l4xfz4gs\_m156Ghfi\_uU75\_4IAF\_8GsH\_Zs9lQicJfKqs; ttwid=1%7ClHddBBFTv1qEKGaeLxBtyAHM8u4QgckGL2uTHeDvIQI%7C1656376816%7C22bc50efdde8af73300e692ab683be317c85a02c1b119e73581a2ebd05066a8a; Hm\_lpvt\_5ef88140a857780eb79a65f7d563f9ef=1656379478; tt\_scid=Q3s2SeOu2g35qgbuZXIiiI7rRL1G9fug0EWeFKjDqaVXs8gYd-fmqayGtczdPQSI4e5c

Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="102", "Google Chrome";v="102"

Sec-Ch-Ua-Mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36

Sec-Ch-Ua-Platform: "Windows"

Accept: \*/\*

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: empty

Referer: https://studio.ixigua.com/upload?from=post\_article

Accept-Encoding: gzip, deflate

Accept-Language: zh,zh-CN;q=0.9

漏洞危害：如果此处云储存桶泄露造成传播，造成云储存的接管操作，将严重影响业务，故评高危

漏洞修复：进行云储存桶后端限制加固，防止信息泄露