

buuctf-upload

原创

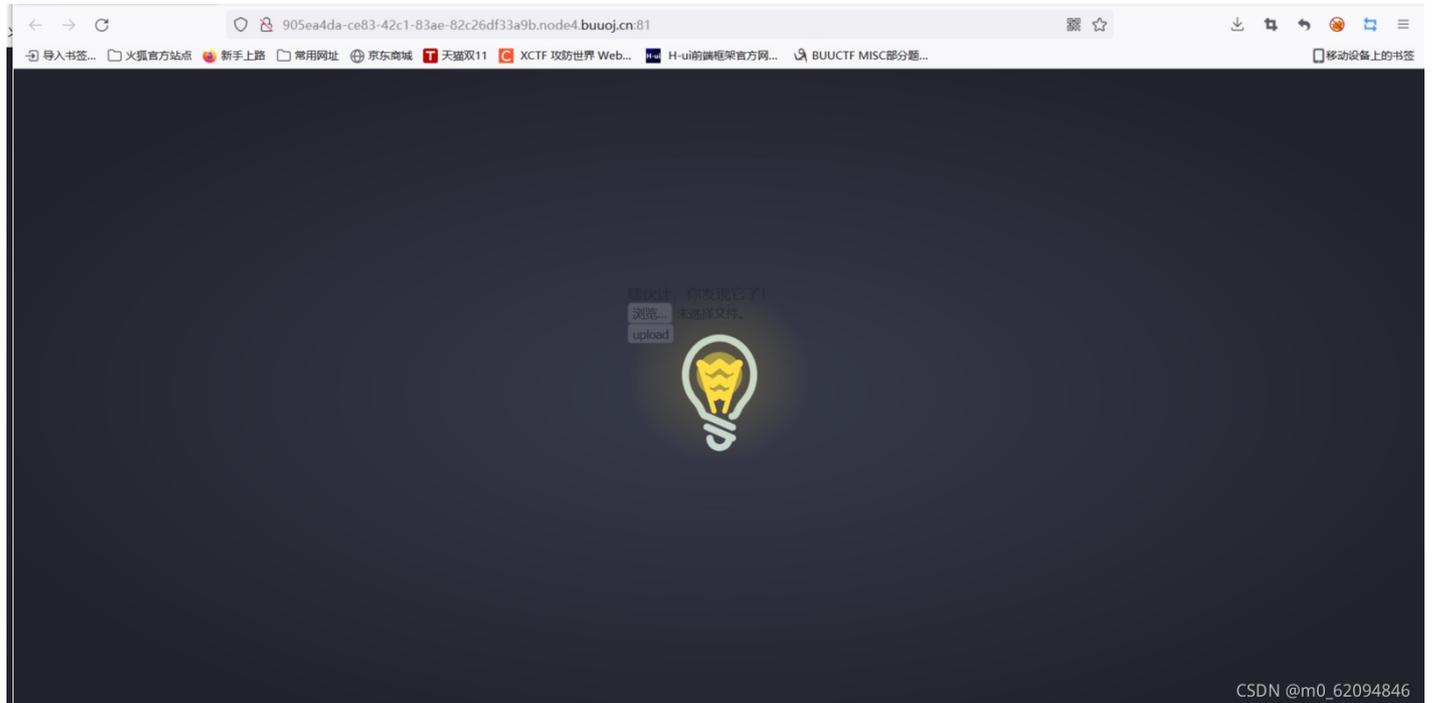
[m0_62094846](#) 于 2021-10-31 15:05:22 发布 409 收藏

文章标签：[安全](#)

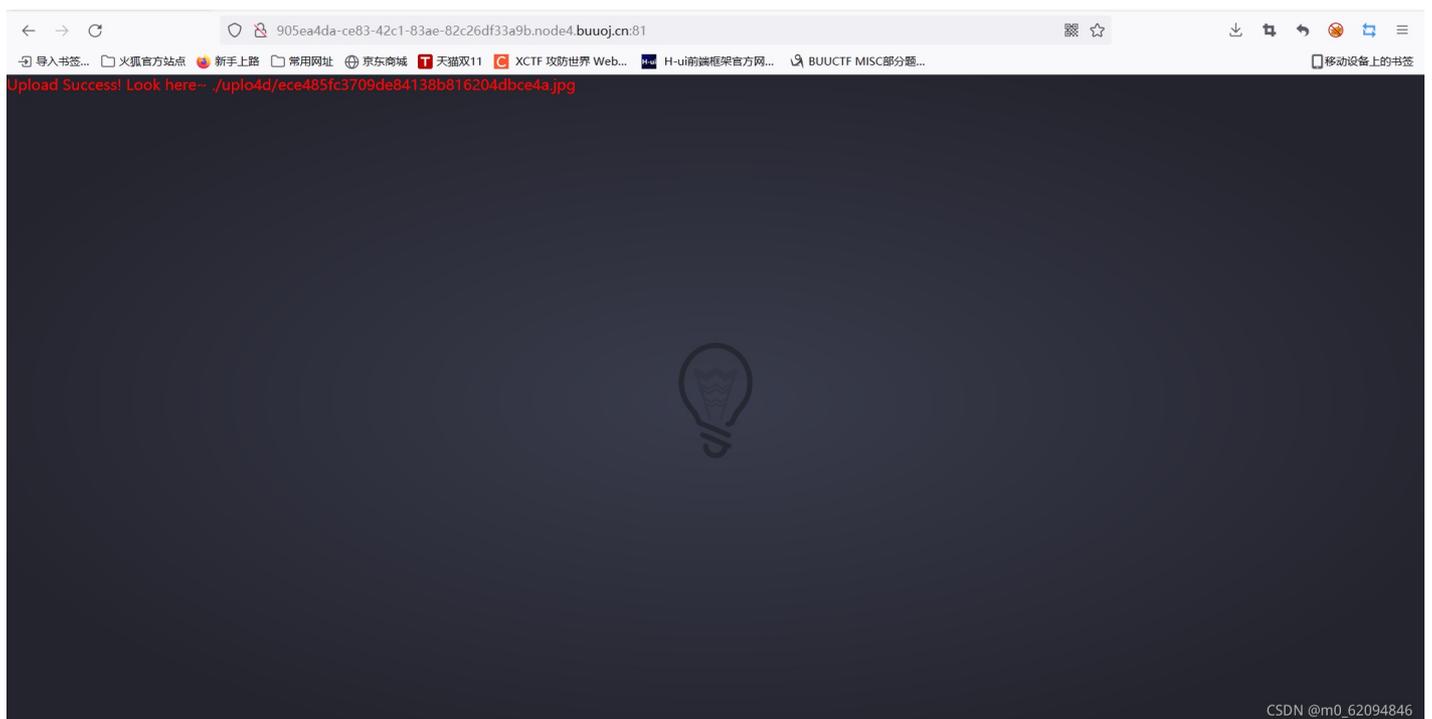
版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/m0_62094846/article/details/121063766

版权



按照指示上传文件



用burp抓取

直接看到flag，我以为就这么做完了，但是交不上去，再看页面，Look here，可能还是需要木马，

但用上次的方法，改文件格式为php，就不会显示上传成功了

The screenshot shows the Burp Suite interface with the Repeater tab selected. The target is `http://905ea4da-ce83-42c1-83ae-82c26df33a9b.node4.buuoj.cn:81`. The request is a POST to `/HTTP/1.1` with a multipart form-data body. The file part is named `upload_file` and has a filename of `1.php`. The response is a 200 OK with a body containing a message: `nonono- Bad file!`. The response body is rendered in HTML, showing a form with an input field for the file name and a submit button.

查找发现，也可以上传，phtml文件名

就可以得到成功的返还了

The screenshot shows the Burp Suite interface with the Repeater tab selected. The target is `http://905ea4da-ce83-42c1-83ae-82c26df33a9b.node4.buuoj.cn:81`. The request is a POST to `/HTTP/1.1` with a multipart form-data body. The file part is named `upload` and has a filename of `1.phtml`. The response is a 200 OK with a body containing a message: `Upload Success! Look here -> /upload/4d3b284530b9d236c664e6f32315ccac3.phtml`. The response body is rendered in HTML, showing a message and a link to the uploaded file.

接下来按照原来的方法做，用蚁剑，最后可以在根目录下得到flag

