[ACTF2020 新生赛]Upload

原创

Wuuconix 于 2021-03-11 10:39:52 发布 154 收藏

文章标签： web 安全漏洞 upload

Wuuconix wanna a girlfriend!

[ACTF2020 新生赛]Upload

考点 `前端后缀名绕过的方式` `php可执行文件后缀名的种类`

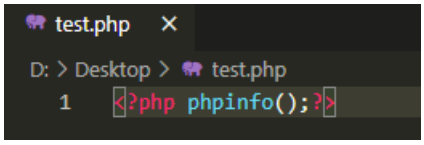
主界面 有一个灯泡，提示你上传文件，前端有验证，只能上传 `jpg|png|gif`

这个时候我们有两种方式绕过前端验证

直接在`源码`里把验证函数删掉

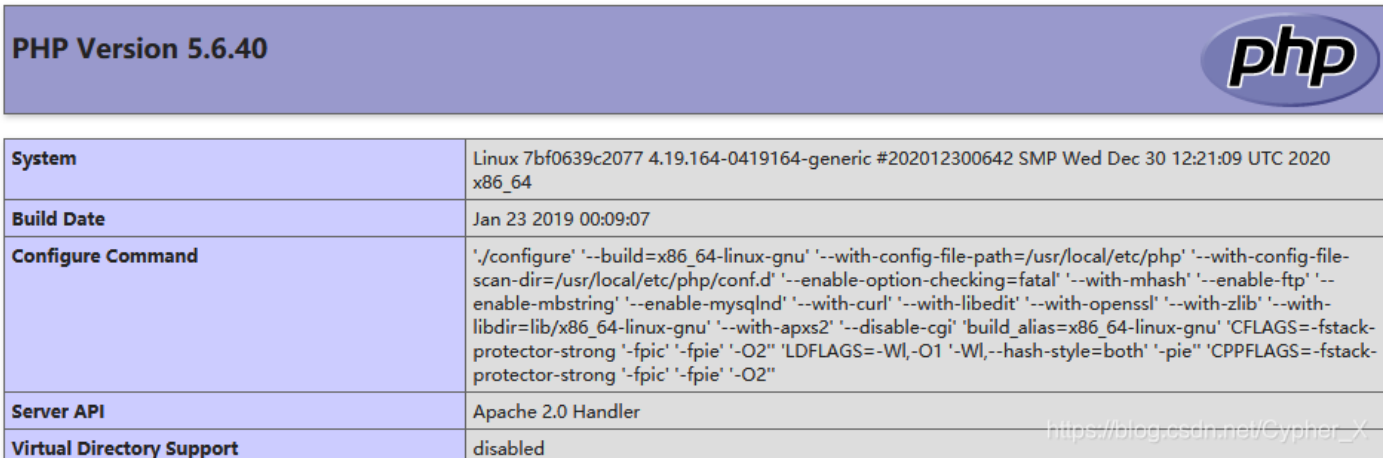
先把文件改成jpg格式的，然后点击upload，用`burp拦截`，再重新改为原本格式

我们选择第一种方式，试着上传一下php文件，内容可以先用`phpinfo()` 测试一下能不能成功



页面提示`nonono bad file!`，看来后端也对后缀名进行了检查，那么我们就用phtml试试，常用的php后缀名绕过见[极客大挑战 2019]Upload 成功上传

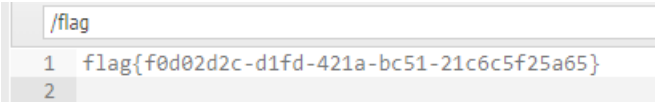
打开后，成功获得执行了`phpinfo()`



PHP Version 5.6.40

System	Linux 7bf0639c2077 4.19.164-0419164-generic #202012300642 SMP Wed Dec 30 12:21:09 UTC 2020 x86_64
Build Date	Jan 23 2019 00:09:07
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu' 'CFLAGS=-fstack-protector-strong '-fpic' '-fpie' '-O2'' 'LDFLAGS=-Wl,-O1 '-Wl,--hash-style=both' '-pie'' 'CPPFLAGS=-fstack-protector-strong '-fpic' '-fpie' '-O2''
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled

接下来只要编写简单的`php一句话木马`就行！后端没有对文件内容进行任何检查。用蚁剑连接后成功在根目录得到flag。



/flag

```
1  flag{f0d02d2c-d1fd-421a-bc51-21c6c5f25a65}
2
```

我们在服务器上找到了.htaccess文件，里面有以下内容

```
<FilesMatch \.phtml$>
 SetHandler application/x-httpd-php
</FilesMatch>
```

可以看到，这里服务器手动把phtml后缀名设置为了php可执行文件，我推测`phtml`与`pht`这种后缀只有在配置文件里添加之后才能生效，正常应该是不能的，因为在这道题里，`pht`后缀无法正常执行。

同时附上`index.php`中的内容，我们可以看到，它在后端也过滤了一些常用的后缀名

```
<?php
 error_reporting(0);
 //设置上传目录
 define("UPLOAD_PATH", "./uplo4d");
 $msg = "Upload Success!";
 if (isset($_POST['submit'])) {
        $temp_file = $_FILES['upload_file']['tmp_name'];
        $file_name = $_FILES['upload_file']['name'];
        $ext = pathinfo($file_name,PATHINFO_EXTENSION);
        if(in_array($ext, ['php', 'php3', 'php4', 'php5'])) {
         exit('nonono~ Bad file! ');
     }
        $new_file_name = md5($file_name).".".$ext;
        $img_path = UPLOAD_PATH . '/' . $new_file_name;
        if (move_uploaded_file($temp_file, $img_path)){
            $is_upload = true;
        } else {
            $msg = 'Upload Failed!';
        }
        echo '<div style="color:#F00">'.$msg." Look here~ ".$img_path."</div>";
    }
```

```
?>
```

参考链接

- [ACTF2020 新生赛]Upload
- [ACTF2020 新生赛]Upload
- apache配置文件AddType application/x-httpd-php .php