南邮CTF自练

原创

Jerui-v- 于 2017-08-08 21:55:48 发布 359 收藏

小白自练南邮平台的CTF, 借鉴了好多其他的writeup QAQ

W...Web

一、md5 collision

源代码

```
<?php
$md51 = md5('QNKCDZO');
$a = @$_GET['a'];
$md52 = @md5($a);
if(isset($a)){
if ($a != 'QNKCDZO' && $md51 == $md52) {
    echo "nctf{*****************}";
} else {
    echo "false!!!";
}}
else{echo "please input a";}
?>
```

1.MD5值的作用是防止伪造，对字符串的改动会引起MD5值的变化

$md51 = md5('QNKCDZO')的结果为0e830400451993494058024219903391

$md52的结果为a的md5值

2.php中==的弱类型，使其只要保证md52与md51匹配开头的0e即可

二、这题不是WEB

打开连接后保存gif图片，用IDA或txt打开，转化成二进制形式，在末尾找到flag,所以这是一道图片隐写题

三、层层递进

way1:用brupsuite截断，在httphistory中找到一个状态码为200(成功状态码）但链接中显示web/404.html的叛徒（这个得等很久。。），打开后查看源代码，看到竖着的flag

way2:右键看源代码，在<body>中找到

src="SO.html"，点进去有出现一样的，再点进去（所谓层层递进），直到出现

src="404.html"，点开后到一个瞎讲故事的网页，看源代码即可。

四、单身二十年

~~用brupsuite截断，在httphistory中找到search_key.php，在这个http页面的响应（response)中找到flag.~~

打开后查看源代码，看到

五、单身100年也没用

用火狐右键查看元素，在网络中打开状态为302的http包，在响应头中找到flag

六、phpdecode

把最后的eval改成echo运行一下，，，就出来了

七、文件包含

参考php中的文件包含漏洞

1.php://filter/可用于处理打开的数据流，起到过滤作用。如果源文件为.php则很有可能在前台显示不出来。
2.先让文件转化为base64格式（convert.base64-encode）然后再输出，这样不论是什么格式的文件都可以在前台输出。
3.再次解码就可得到源代码

通过构造含有漏洞的语句：file=php://filter/read=convert.base64-encode/resource=index.php 查看想看的代码
（http://4.chinalover.sinaapp.com/web7/index.php?file=php://filter/read=convert.base64-encode/resource=index.php）

得到经过base64加密后的字符串去解密即可~）

八、Download~

查看页面源代码，看到

```
<p><a href="download.php?url=eGluZ3hpbmdkaWFuZGVuZy5tcDM=" target="_blank">星星点灯</a></p>
<p><a href="download.php?url=YnV4aWFuZ3poYW5nZGEubXAz" target="_blank">不想长大</a></p>
```

发现在下载链接中有一个download.php的东西，结合url后面的字符串是下载文件的base64加密字符串（可以试着将eGluZ3hpbmdkaWFuZGVuZy5tcDM= 解码，结果为xingxingdiandeng.mp3）

因此，将download.php也用base64加密，得到的结果构造出一个下载链接

http://way.nuptzj.cn/web6/download.php?url=ZG93bmxvYWQucGhw 既可以下载download.php文件，下载后用记事本打开：

```
??<?php
error_reporting(0);
include("hereiskey.php");
$url=base64_decode($_GET[url]);
if( $url=="hereiskey.php" || $url=="buxiangzhangda.mp3" || $url=="xingxingdiandeng.mp3" || $url=="download.
 $file_size = filesize($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!";
}
?>
```

在其中看到一个hereiskey.php的文件，用同样的方法将hereiskey.php用base64加密，构造下载链接

http://way.nuptzj.cn/web6/download.php?url=aGVyZWlza2V5LnBocA==，下载的php文件用记事本打开既得flag

九、COOKIE

用火狐的查看元素分析http，将里面的cookie=0改成=1再发送即可

十、Mysql

在url中打开robots.txt文件：http://chinalover.sinaapp.com/web11/robots.txt，看到一段php代码，发现其中需要进行sql注入，http://chinalover.sinaapp.com/web11/sql.php?id=1024.1

密码学

一、KeyBoard

奇奇怪怪的脑洞题，居然是根据字母在键盘上敲出的轨迹来得到结果，开始还一直在想置换。。。

ytfvbhn tgbgy hjuygbn yhnmki tgvhn uygbn uygbn yhnijm

a r e u h a c k

二、base64全家桶

```
print
(base64.b16decode(base64.b32decode(base64.b64decode('R1pDVE1NWlhHUTNETU4yQ0dZWkRNTUpYR
OOzREtNWldHTTJES1JSVOdJMORDTlpUR1kyVEdNWlRHSTJVTU5SUkdaQ1RNTkJWSVkzREVOU1JHNFpUTU5KVEd
FWlRNTjJF'))))
```

三、n次base64

说了用pyhton,就写一个循环不停解下去吧

```
s = '''#题目中的密文#'''
while True:
    s = base64.b64decode(s)
    print(s)
```