第十届极客大挑战部分writeup



SyOung ● 于 2020-05-22 18:43:56 发布 ● 330 ☆ 收藏 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u> 版权协议,转载请附上原文出处链接和本声明。本文链接: <u>https://blog.csdn.net/Karol_agan/article/details/103098155</u> 版权

MISC

1.是谁杀了谁:注意自己的HP,别被气死了。

1.解压文件是一个exe文件,打开

2.来回试了几次发现**会在目录中生成HP** 文件,应该要对HP文件处理

3.用 **010editor** 打开HP文件得到flag Syc{I_kill3d_myself_Orz}

2.嘿,你喜欢吃鲱鱼罐头吗?:实验室禁止吃鲱鱼罐头!

1.这个题纠结了N年,开始以为对图片处理,修改了宽高都没用

2. hint: English & Google (very easy, do not think too much) & 高层潇闻钦为了让大家牢记实验室不能吃鲱鱼罐头,专门去打了个 备注

3. 此题给了两个Hint,都是指向寻找解密网站。hint1:English&google 意思用英文去谷歌搜索。hint2:要搜索的东西在图片中,也就是罐头装的死鱼。

4. 去谷歌搜索deadfish code关键字,可以

发现在线解密网站(deadfish decode) ((https://www.dcode.fr/deadfish-language)。 5.010打开图片发现后半部分有一段异常数据,放到解密网站中解密拿到flag。

ctf图片隐写(修改宽高示例)



https://blog.csdn.het/Kafoljagah

现在我们右击这个图片,查看它的详细信息,宽度:500像素;高度:420像素。注意看操作——这个时候,我们知道图片是因 为高度不够而没有完全显示出flag,所以我们只需要修改他的高度,它的高度是420像素,将十进制的420转换成16进制的 数据,420的十六进制是 01a4,把图片拖到010editor中,查找01,这个01就是我们需要改的图片的高度,看到他的宽度 像素为 500,将500转换为16进制数据,500的16进制是 01f4,我们只需要把420像素的 01a4 改成 500 像素的 01f4 然后 点击保存就好了,再打开这个图片flag就出现了

3.啊啊啊啊啊啊啊!!!: 我好兴奋!!!: 啊啊啊啊, 让我嗨!!! 我要打一辈子极 客!!!

先用010editor打开,根据JPEG图片以"FF D8"开头,"FF D9"结尾,发现GIF中隐藏着JPEG图片,用binwalk来分离图片

方法: kali终端: binwalk+图片路径

DECIMAL	HEXADECIMAL	DESCRIPTION
	一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	isban.gif
0	0×0	GIF image data, version "89a", 40 x 40
4051	0xFD3	JPEG image data, JFIF standard 1.01
4081	0xFF1	TIFF image data, big-endian, offset of first image
directory	: 8	
root@Agan:	~/图片#	

发现隐藏有jpeg图片,从4051偏移开始是另一张jpeg dd if=jsban.gif of=j.jpg skip=4051 bs=1

使用dd命令分离出隐藏文件

dd分离

命令: dd if=要分离的图片名.jpg of=分离出来的图片名.jpg skip=偏移量 bs=1

规安全	详细信息 以前的版本	
属性	值	^
说明		
标题		
主题		
分级	$\begin{array}{c} \begin{array}{c} \begin{array}{c} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} $	
标记		
备注	Syc{Do_You_know_Ayrain}	
来源		
作者	418700665	
拍摄日期	2000/11/11 19:19	
程序名称		
获取日期		
版权		
图像 ———		
图像 ID		
分辨率	1280 x 1920	
宽度 1280 像素		
高度 1920 像素		
水平分辨率 96 dpi		
垂直分辨率	96 dpi	
位深度	24	
n ve		v

注:

CTF中图片隐藏文件分离方法总结

前言

可以使用winhex之类的工具先行分析其是否为图片,可以看其头部信息,还有就是JPG图片有一个特性最后的应用数据块为FF E0 活着直接使用binwalk看看图片下有什么鬼玩意儿的。

应用(A)

binwalk分离

命令: binwalk -e 图片路径

foremost分离

命令: foremost 图片地址 #会在图片地址的目录下生成一个output的文件夹。输出到里面了。

dd分离

命令: dd if=要分离的图片名.jpg of=分离出来的图片名.jpg skip=偏移量 bs=1

https://blog.csdn.net/Karol_agan

4: 散打黑客的压缩包: 我拼着生命危险从散打黑客的电脑里偷来的压缩包,大家快跟我 一起破解开。看看藏着什么东西

用ARCHPR暴力破解,选中所有数字,两次解压包爆破密码都是四位数字,最终得到flag。



RPG真是太有趣了吧:做题也太累了,不如来打会游戏吧##

下载后发现与rpgmaker软件有关,在网上下载rpgmaker,发现打不开exe文件,下载rpgmaker的RGSSAD解包器,解开数据包 后发现.rxproj文件

	12 M TO 12	
📕 Data	2019/11/18 23:09	文件夹
🌼 Game.exe	2004/6/25 0:00	应用程序
🕤 Game.ini	2019/10/7 19:29	配置设置
🗊 Game.rxproj	2008/1/31 20:31	RXPROJ 文件
📄 rgssad_sp.log	2019/11/18 23:09	文本文档

然后用rpgmaker打开Game.rxproj文件,

📸 Project1 - RPG Maker XP 文件(F) 编辑(E) 视图(V) 模式(M) 绘图(D) 比例(S) 工具(T) 游戏(G) 帮助(H) 🖂 🗕 🖉 🗶 📖 🧖 🗟 🍌 1 🖻 5 0 18 를 Ж h 3 S × 0 ~ 1 -1 1 v 1 前旅店 ^) 练级点 1 土之洞窟

选择时间点,然后双击图中位置得到flag

◆文章: 你赢了,我的flag是
 ◆文章: Syo{I_love_Rpg_VErY_Much!!!!!}

Web

1.BurpSuiiiiiit!!!: 拿起你的burp,开始战斗吧

1.将jar文件导入burp

3	Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz														
Bur	Burp Intruder Repeater Window Help														
Та	Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Froject options User options Alerts														
Ex	Extensions BApp Store APIs Options														
Bui	Burp Extensions Extensions let you customize Burp's behavior using your own or third-party code.														
	Add		Loaded	Туре	N	ame									
	lemov	/e	V	Java	S	yc welcome y	ou!!! Happy (game!!!!!!!							
	Lla														
	υp														
1	Down														
-															
	Details Output Errors														
	Output to system console														
C	O Save to file: Select file														
	Show in UI:														
	Be	efore I	give you th	e flag, I wa	nt to tell yo	ou something	about BurpE>	tender.							
	Bu	irp loo	oks for a cla	ass called E	BurpExtend	der to instantia	ate (with no c	onstructor p	arameters)	and then call	s regis	sterExtender	rCallbacks() on	this obje	ct passing in a "callback
	Think of this as the entrypoint for your extension, allowing you to tell Burp what your extension is capable of, and when Burp should as your extension again														

flag在error里

2.你看见过我的菜刀么

直接用菜刀连接,根目录下有flag文件夹,打开得到flag

3.Jiang's Secret:我在那放了一个秘密

F12看源码发现一个链接,打开:





点Secret提示

用BurpSuite抓包, Send to repeate -> GO

	Raw	Headers	Hex	HTML	Render	
GET /Archive_room.php HTTP/1.1 Host. 110.25.14.40.0100 Pragma: no-cache Cache-Control: no-cache Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36 Accept: text/html.application/xhtml+xml.application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.9 Connection: close st fFr ali G	<he tyle="b: tyle="b tyle="b FFF;lef <di lign="c; eorgia, <td>ead> <meta c<br=""/><title>绝 nead> ody ackground- ch1 ont-family:ve 我把他们 ob <a id="n
ackground-
it:44%;"> iv style="po enter" style serif;color:v oody></title></td><td>harset= 會省家 color:bl erdana;; 门都放行 r> naste color:re nt size sition: ="font;i white;"></td><td>**utf-8*> ack;*><!--<br-->color:red 在这里了</td><td>br> <t ;text-align: , 去看看f > iction.php" :50px;widtl RET;bottom: 0 x er @ cl4y</t </td><td>r> <center;"> </center;"></td></di </he 	ead> <meta c<br=""/> <title>绝 nead> ody ackground- ch1 ont-family:ve 我把他们 ob <a id="n
ackground-
it:44%;"> iv style="po enter" style serif;color:v oody></title>	harset= 會省家 color:bl erdana;; 门都放行 r> naste color:re nt size sition: ="font;i white;">	**utf-8*> ack;*> <br color:red 在这里了	br> <t ;text-align: , 去看看f > iction.php" :50px;widtl RET;bottom: 0 x er @ cl4y</t 	r> <center;"> </center;">
GET /action.php HTTP/11 Host: 118.25.14.40:8106 Pragma: no-cache Cache-Control: no-cache Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36 Accept: text/html.application/xhtml+xml.application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.9 Connection: close		HTTP/1.1 3 Server: ngi Date: Mon Content-Ty Connection: e Content-Le Content-Le 	302 For nx/1.14 , 25 No -Pe: tex -By: Pl end.php ength: 6 PE htm hp	und 4.2 vv 2019 f tt/html; e HP/7.3.5 53 h/>	14:55:51 (charset=U	.nevx.aroi_agan GMT JTF-8

III #	用 🚺 成都信息工程大学 📸 百度一下,你	就知道 Umcode编码转换…	MagkuCTF - 练习	Ex 扩展迷 - Chrome	242 决
<html></html>					
	<pre><title>secret</title> <meta_charset="htf-8"></meta_charset="htf-8"></pre>				
php</td <td></td> <td></td> <td></td> <td></td> <td></td>					
	highlight_file(_FILE);				
	<pre>\$file=\$_GET['file'];</pre>				
	if(strstr(\$file, "/") stristr(\$file,	"tp") stristr(\$file,"input")	stristr(\$file, "data")){	
	echo Uh no!;				

	exit();
} inclu	de (\$file)
//flag放在了f	flag.php里
?>	

https://blog.csdn.net/Karol_agan

考点是PHP伪协议,filter输出流 https://blog.csdn.net/nzjdsds/article/details/82461043

0x01 php://filter

php://filter 是一种元封装器,设计用于数据流打开时的筛选过滤应用。这对于一体式 (all-in-one) 的文件函数非常有用,类 似 <u>readfile()</u>、<u>file()</u>和 <u>file_get_contents()</u>,在数据流内容读取之前没有机会应用其他过滤器。

-----php.net

简单说经常利用它进行base64编码,如

php://filter/read=convert.base64-encode/resource=file:///c:/windows/win.ini"

可以运用多种过滤器 (字符串/转换/压缩/加密)

常用于读取文件/源码:

https://blog.csdn.net/Karol_agan



Base64解码:

4.Easysql:最近我做了一个小网站,我把flag放在里面了,不过我没有把登陆密码告诉任何人,所以你们是拿不到flag的!

简单的万能密码: 用户名随意 密码 1' or '1'='1



