2018铁三测评题write以及一些想送给你们的话



weixin_34148340 于 2018-01-30 20:01:00 发布 O 117 於 收藏 文章标签: 密码学 php 网络

一、前言

此文献给实验室的萌新们,以及刚刚接触CTF的同学们,希望能对你们的成长起到一些帮助。

二、关于CTF

可能你已经接触过CTF或者对它有所了解,这里我再简单介绍一下。

1.什么是CTF?

CTF(Capture The Flag)中文一般译作夺旗赛,是网络安全技术人员之间进行技术竞技的一种比赛形式, 起源于1996年DEFCON全球黑客大会,以比赛形式模拟代替黑客们之间的真实技术比拼。

2.CTF比赛模式

模式	说明
解题模式	参赛队伍通过互联网或者现场网络参与,类似于各位此次做的线上测评题目,你可以理解为在线答题环节, 通过解决网络安全技术挑战题目的分值和时间来排名,通常用于在线选拔赛。题目主要包含Web安全、逆向、 密码学、数据分析、隐写、安全编程、代码审计与漏洞挖掘利用等。
攻防模式	参赛队伍在网络环境内互相进行攻击和防守,挖掘网络服务漏洞并攻击对手服务器获得分数,并且通过修 补自身服务漏洞进行防御来避免丢分。这种模式竞争较为激烈,比拼参赛队员的智力和技术、团队之间的分工 配合与合作、也比拼体力。
混合模式	结合了上面说的解题模式与攻防模式,赛制较为灵活。

三、测评题目分析

1.你是管理员吗?

解题链接: http://ctf4.shiyanbar.com/web/root/index.php

第一道题目是一个Web题。通常拿到Web题,常做的是右击查看源代码;利用浏览器调试工具F12查看页面 元素、在调试工具的"网络"中观察请求头等。

这题我们打开页面,发现一个登陆框,并且默认用户名为admin。我们查看页面源码,或者直接从title的提示中,我们可以发现一个password.txt文件,于是我们访问一下这个文件http://ctf4.shiyanbar.com/web/root/password.txt,发现这是一个密码字典。既然是密码字典,于是我们便尝试对这个登陆页面进行口令的暴力破解,用户名admin。这里会用到BurpSuite工具,关于使用这个工具暴力破解密码,大家网上搜索,可以参考这篇文章。

II **		200		1941	
79	maek	200		1924	
80	dreamh	200		1924	
81	Shell	200		1924	
82	Nsf0cuS	200		2063	
83	shell	200		1924	
84	10011C120105101	200		1924	
85	fclshark	200		1924	
86	19880118	200		1924	

发现了正确口令组合为: admin/Nsf0cuS

我们利用这组口令去进行登陆,发现页面密码框处限制了字符输入长度。我们可以在前端利用调试工具定位到 密码框处,修改密码字段的长度限制。

	🕑 井友者上具 -	password.txt -	http://ctt4.sh	iyanbar.com/v	web/root/index.
	口 白 査看器	☑ 控制台	□ 调试器	{} 样式编辑	器 🞯 性能
	+				Q 🛔
admin 🕎		<pre> <form <input="" autocom<br="" backgro="" met="" url("da=""></form></pre>	hod="POST" name="usern; ta:image/pn; und-position plete="off"	action="" _: ame" value=" g;base64,iVE n: 98% 50%; type="text"	lpchecked="1" 'admin" style: 30Rw0KGgoAAAA. cursor: point "> co
		>			
False		≺input image: backgro autocom	name="passw url("data:iu und-position plete="off"	ord" <mark>maxleng</mark> mage/png;bas n: 98% 50%; type="passw	<pre>sth="5" value se64,iVBORw0K(cursor: point word"> compared</pre>
		• Kinnut	value="‰ait"	type="subm	i+">

当我们登陆的时候,在开发者调试工具的"网络"数据查看功能的地方发现我们的请求数据

۷	开发	皆工具 -	passwo	ord.txt ·	- http	p://ctf4	shiya	nbar.co	om/web	o/root	/index.	.php			_	—
R	¢	查看器	ŧ	空制台	C)调试	i i i	(} 样式	编辑器	C	性能	₽️ 内存	æ	网络	😫 存储	
11	圃	所有	HTML	CSS	JS	XHR	字体	图像	媒体	WS	其他	□持续日	志		援存	
Y	过滤	URL			⊲											
4.15	*		+			<i>14</i> -			+-8-47		A+4-5	<u>-114 T</u>		1+++	$\pm d_{1}$	

这里的cookie一看就是个Base64加密的字符串。当然,这需要一些密码学的知识,关于密码学的学习,你可以参考我转载的这篇博文。

求网址: http://ctf4.shiyanbar.com/web/root/index.php
求方法: POST
程地址: 127.0.0.1:8080
态码:● 200 OK ⑦ 编辑和重发 原始头
本: HTTP/1.1
7 过滤消息头
响应头 (307 字节)
Connection: close
Content-Length: 1756
Content-Type: text/html
Date: Tue, 23 Jan 2018 06:44:03 GMT
Server: nginx
Set-Cookie: newpage=MjkwYmNhNzBjN2RhZTkzZG2018 06:45:03 GMT; Max-Age=60
Vary: Accept-Encoding
X-Powered-By: PHP/5.5.36
清求头 (684 字节)
Accept: text/html,application/xhtml+xmplication/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: keep-alive
Content-Length: 31
Content-Type: application/x-www-form-urlencoded
Cookin Hon htt 24d6f7252ab0015a4c592a4 -1* visitor*** E68 898 898 898 858 AE8 A2

我们对这个字符串进行Base64解密,

MjkwYmNhNzBjN2RhZTkzZGl2NjQ0ZmEwMGl5ZDgzYjkucGhw

得到

290bca70c7dae93db6644fa00b9d83b9.php

当然,上面的我们也可以在burpsuite中直接进行登陆数据的提交

那么,同样的我们就访问一下这个文件,发现是一个留言板页面。



当我们随便进行留言测试的时候,发现没有权限。这里,我们可以修改cookie以及登陆参数进行欺骗。



我们利用burpsuite抓包时,可以发现两个参数: lsLogin和userlevel。很明显, lsLogin的值标识用户是否登 陆, userlevel指明用户身份。当我们把这两个值修改成如图所示内容后,在响应报文里即可发现flag。

这里IsLogin可能比较容易理解,但是userlevel的值为什么要改成root?有没有什么窍门呢?我们回忆题目,"管理员"是一个很重要的提示,一般管理员默认用户名,linux下比如admin,root。windows下是administrator,我们可以合理猜解。得到的Flag有两个字符,需要进行URL解码

flag{C0ngratulati0n}

2.IOS

解题链接: http://ctf4.shiyanbar.com/web/IOS/index.php

这题页面中提示系统升级到了IOS99,我们可以想到修改User-Agent进行欺骗。

关于User-Agent,大家参考我的这篇博文加以了解。User Agent是一个特殊字符串头,是一种向访问网站提供 我们所使用的浏览器类型及版本、操作系统及版本、浏览器内核、等信息的标识。我们访问网页的时候,会自 动提交这个参数。通过这个标识,我们访问的网站可以显示不同的排版从而适应我们的浏览器,提供更好的体 验。

我们可以在网上搜索一个IOS99的User-Agent值示例,也可以自己构造,比如

Mozilla/5.0 (iPhone; CPU iPhone OS 99 like Mac OS X) AppleWebKit/0 Safari/536

我们根据要求,提交信息之后,即可获得flag。



这里检测了浏览器标识、操作系统标识、渲染引擎标识、版本信息。顺带提一下,最后的浏览器字段,只能使用Safari,你改成其他浏览器就不行,

因为Safari是苹果研发的浏览器,也是iPhone手机、iPodTouch、iPad平板电脑中iOS指定默认浏览器。

flag{LMvBi8w9\$m1TrgK4}

3. 照猫画虎

解题链接: http://ctf4.shiyanbar.com/web/copy/index.php



这题,右击查看源代码,页面元素,没有发现。于是我们分析其网络请求

∑ ‡	空制台	口调	式器 {	} 样式編	輯器	C (性能	₽₽ 内存	計 网络	89 存储	₽⊤⋗	3 ھ	\$ □	
TML	CSS	JS XHP	く 字体	图像	媒体	WS	其他	□持续日	志 □禁	用缓存				
		₽												
文作		消息头		Cool	kie		参数	<u>۲</u>	响应	耗时		堆村	観踪	
in	请求	之 之 同 址: ht	tp://ct	f4.shi	yanbai	c.com/	/web/	copy/inde	x.php					
	请求	大法: GE	т											
	远和	呈地址: 1 2:	1.194.2	.44:80										
	状态	祸: ● 2	00 OK (? 编	辑和重	发质	融头							
	版本	: HTTP/1	.1											
	Y	过滤消息的	¥.											
		Content	-Type: t	ext/htm	d									1
		Date: Tu	.ie, 30 Ja	n 2018	10:34:3	87 GM	т							
		Server:	nginx											
		Set-Coo	kie: Vis	itor=MjY	(50To)	wNDE1	NzQw	ZWFhNGQ	5ZGVjYmM4	ZGEwMDFkN	12ZkODA1	Zg%3I	D%3D	
	?	Transfer	-Encodi	ng: chui	nked									
		Vary: Ac	cept-En	coding										
		X-Powe	red-By:	PHP/5.5	.36									
	₩Ì	青求头 (631	字节)											
		۸ ـ ـ ـ . ـ ـ ـ				المتغمان		- Paratana A.		s0 0				

看到Set-Cookie,是不是熟悉了?一回生,二回熟。我们先把最后两个%3D字符串解码得到"==",进行base64 解密

MjY5OTowNDE1NzQwZWFhNGQ5ZGVjYmM4ZGEwMDFkM2ZkODA1Zg==

得到

2699:0415740eaa4d9decbc8da001d3fd805f

如果你已经有了一些密码学的基础,你应该会发现2699后面是一串经过32位md5加密的数据,如果看不出来,回头在看看密码学的东西去,至少熟悉各种形式的密文,知道其使用的加密算法。

我们继续,给大家推荐一个加解密md5的网站:http://www.cmd5.com/。

	密文: 0415740eaa4d9decbc8da001d3fd805f											
	类型: 自动			▼ [帮助]								
		查询	加密									
查询结果:												

2699

说明后半段的值,是前一个数字的32位md5加密字符串。于是我们"照猫画虎",把"1234567890"md5之后,组 合起来



1234567890:e807f1fcf82d132f9bb018ca6738a19f

然后把这段字符串经过Base64编码后,修改成cookie地值,提交,即可获得flag



flag{T4mmL9GhpaKWunPE}

4.问题就在这

解题链接: http://ctf4.shiyanbar.com/ste/gpg/john.tar.gz.gpg

提示: 找答案 GPG key: GhairfAvvewvukDetolicDer-OcNayd#

这题下载到的是一个gpg文件,文件名为john.tar.gz.gpg。我们可以从网上了解到这是一个经过GPG加密的数据,加密前的文件很可能是john.tar.gz,linux下的一种压缩文件。

自然地想到,我们要对这个文件进行解密,但是无论是解题前,还是解题后,我都强烈建议你深入了解一下GPG的知识。

windows下有很方便的工具可以进行解密,下载链接: https://gpg4win.org/download.html。当然,kali也自带了gpg工具,关于它的使用,你可以参考我的另一篇博

文: http://www.cnblogs.com/ssooking/p/8378407.html。解密命令:

解密时,需要输入密钥:GhairfAvvewvukDetolicDer-OcNayd#。密钥不会在控制台上显示。

解密完成后,我们解压压缩包,会得到一个pcap数据包文件。

> 测i	> 测试题目 > john-in-the-middle >											
	名称	^	修改日期									
	HTTP		2018/1/2									
<u>_</u>	🚡 john-in-th	ie-middle.pcap	2015/4/2									
<i>"</i>												

使用用Wireshark分析数据包,里面有许多HTTP数据,我们直接导出HTTP对象

文件(E)	编辑(E)	视图(⊻)	跳转(G)	捕获(<u>C</u>) 分析(<u>A</u>) 统计
打开	Ŧ		Ctrl+O		2 👔	<u>₽</u> 📃
打开	干最 近			•		
合并	‡(<u>M</u>)					De
从日	Hex 转储导	≹入([]			.154	1
关闭	8		Ctrl+W		.154	19
/₽≠	=(C)		Challer		.154	19
1841	F(<u>5</u>)		Ctri+S		.154	19
另代	齐为(<u>A</u>)		Ctrl+Sh	itt+S	.154	19
文件	抹合			+	.154	19
					.154	19
导出	出特定分组.				.154	19
导出	分组解析	結果		•	.154	19
导出	分组字节	츘(<u>B</u>)	Ctrl+H		.154	19
导出	님 PDU 到方	之件			.154	19
导出	님 SSL 会话	密钥			.154	1
导出	对象			•	DIC	ом
打印	D(P)		Ctrl+P		HTT	P🖊
					IMF.	

我们也可以将数据包导入Charles工具中分析http



我们可以看到有很多图片,我们想到了考察内容中的隐写。隐写术是信息隐藏,即不让计划的接收者之外的任何人知道信息的传递事件或信息内容的一门技巧与科学。CTF中隐写术的题目,如果给图片,一般会把一些信息隐藏到图片里。我们可以使用stegsolve工具来分析这些图片。

stegsolve是一个java程序,电脑上需要装有java环境,正确配置了环境变量才能运行。一般双击即可,命令行环境下的运行命令

java -jar stegsolve.jar

当我们使用该工具对logo.png图片进行分析时,可以发现隐藏的flag。至于为什么找到了logo.png这张图片,当你运气不好的时候,你可能需要一个一个试试了。



flag{J0hn_th3_Sn1ff3r}

5.你最美

解题链接: http://ctf4.shiyanbar.com/misc/123/123.exe

这题下载到了一个exe文件,一般给这种文件,基本是考察逆向分析。但是,我们从这个链接中,发现这个题目属于安全杂项分类(密码学、隐写术、数据包分析等)

eb/copy/int 🗙 🛛 🕂

C ctf4.shiyanbar.com/misc/123/123.exe

「具 🗀 安全学习 🗀 辅助站点 🗀 漏洞预警 💪 Gooale 🎇 IP138音)

我们把这个程序放进十六进制编辑器中,这里我用的工具是HxD

1 HxD - [C:\\	₩ HxD - [C:\Users\ssooking\Desktop\测试题目\123.exe]																
📓 文件(F) 编	圖 文件(F) 编辑(E) 搜索(S) 视图(V) 分析(A) 工具(T) 窗口(W) 帮助(H)																
🗋 👌 🕶 🗐	📄 🚵 🖝 💭 🧼 😃 🖬 16 🔤 Windows (At 🔄 十六进制 🖂																
😰 123.exe	📓 123.exe																
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	64	61	74	61	3A	69	6D	61	67	65	2F	70	6E	67	3B	62	data:image/png;b
00000010	61	73	65	36	34	2C	69	56	42	4F	52	77	30	4B	47	67	ase64,iVBORw0KGg
00000020	6F	41	41	41	41	4E	53	55	68	45	55	67	41	41	41	52	OAAAANSUhEUgAAAR
00000030	67	41	41	41	45	59	43	41	49	41	41	41	41	49	37	48	gAAAEYCAIAAAAI7H
00000040	37	62	41	41	41	46	52	45	6C	45	51	56	52	34	6E	4F	7bAAAFRE1EQVR4n0
00000050	33	64	55	57	34	62	4F	78	41	41	51	53	74	34	39	37	3dUW4bOxAAQSt497
00000060	2B	79	63	77	4D	69	34	47	75	4E	5A	36	32	71	33	79	+ycwMi4GuNZ62q3y
00000070	44	79	65	71	30	47	50	77	59	6B	58	39	2F	66	33	31	Dyeq0GPwYkX9/f31
00000080	2F	41	2F	2F	50	6E	70	78	38	41	66	67	4D	68	51	55	/A//Pnpx8AfgMhQU
00000090	42	49	45	42	41	53	42	49	51	45	41	53	46	42	51	45	BIEBASBIQEASFBQE
000000A0	67	51	45	42	49	45	2F	6A	76	38	32	2B	76	31	47	6E	gQEBIE/jv82+vlGn
000000B0	75	4F	33	47	48	51	66	50	69	39	38	76	48	30	33	54	uO3GHQfPi98vH03T
000000C0	75	38	65	2F	6A	38	41	35	65	38	6A	53	58	4F	62	38	u8e/j8A5e8jSXOb8
000000D0	4F	4B	42	41	45	68	51	55	42	49	45	42	41	53	42	49	OKBAEhQUBIEBASBI

一看到这个,我们就可以发现,这是一张图片,只是经过了base64编码(别问为什么了,见多了你就知道啦。这种格式很好记),关于这种base64图片存在的意义,你可以看看这篇文 章:https://www.cnblogs.com/coco1s/p/4375774.html。我们利用在线工具 (http://imgbase64.duoshitong.com/),把这么长的一大串数据转回图片。



发现是一个二维码,扫码即可获得flag。当然,不使用工具,我们也可以新建一个html文件,把这么长的数据引入img图片标签里,也能够看到图片。类似于

flag{you are beautiful}

6.shellcode 解题链接: http://ctf4.shiyanbar.com/re/shellcode/shellcode.txt

这道题目给了一段十六进制代码,分类在逆向里,如果你懂逆向和PWN,会写shellcode,可能会顺着它的 思路,顺手就写个shellcode出来了。但是写完之后,会发现没法运行,直接崩溃。而且,对萌新来说,可能会 一脸懵,也不会写shellcode。所以这题需要换个思路。

我们重新观察这些十六进制数据

\x6a\x0b\x58\x99\x52\x66\x68\x2d\x63\x89\xe7\x68\x2f\x73\x68\x00\x68\x2f\x62\x69\x6e\x89\xe3\x52\xe8\x34\x00
\x00\x00\x65\x63\x68\x6f\x20\x5a\x6d\x78\x68\x5a\x33\x74\x54\x53\x45\x56\x73\x62\x47\x4e\x76\x5a\x47\x56\x66
\x53\x56\x4e\x66\x63\x32\x39\x66\x51\x32\x39\x76\x62\x48\x30\x4b\x7c\x62\x61\x73\x65\x36\x34\x20\x2d\x64\x00
\x57\x53\x89\xe1\xcd\x80

既然是十六进制,我们就把这些数据放到十六进制编辑器中看看。在文档里,把"\X"全都去掉

6a0b58995266682d6389e7682f736800682f62696e89e352e8340000006563686f205a6d78685a3374545345567362474e765a475666 53564e6663323966513239766248304b7c626173653634202d6400575389e1cd80

我们拷贝这些数据,在HxD中新建一个空白二进制文档,把这些内容粘贴进去。

🔊 HxD - [Unt	itled	1]															- 0
📓 文件(F) 编辑(E) 搜索(S) 视图(V) 分析(A) 工具(T) 窗口(W) 帮助(H)																	
📄 🚵 🖌 💭 🧼 😃 🖬 🖌 💽 16 🔤 V Windows (At 🚽 十六进制 🚽																	
📓 Untitled1																	
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	OF	
00000000	6A	0B	58	99	52	66	68	2D	63	89	E7	68	2F	73	68	00	j.X™Rfh-c‰çh/sh.
00000010	68	2F	62	69	6E	89	E3	52	E8	34	00	00	00	65	63	68	h/bin‰ãRè4ech
00000020	6F	20	5A	6D	78	68	5A	33	74	54	53	45	56	73	62	47	o ZmxhZ3tTSEVsbG
00000030	4E	76	5A	47	56	66	53	56	4E	66	63	32	39	66	51	32	NvZGVfSVNfc29fQ2
00000040	39	76	62	48	30	4B	7C	62	61	73	65	36	34	20	2D	64	9vbH0K base64 -d
00000050	00	57	53	89	E1	CD	80										.WS‰áÍ€

发现了一段经过了base64编码的数据: ZmxhZ3tTSEVsbGNvZGVfSVNfc29fQ29vbH0K

base64解码,发现它就是flag

flag{SHEllcode_IS_so_Cool}

四、最后的一些话

时刻保持一颗不断学习和进取的心,在坚持不懈的努力中奋勇前进!一路征途,风雨无阻(共勉!)



<u>创作打卡挑战赛</u> 赢取流量/现金/CSDN周边激励大奖