【F2C】NCTF 南邮攻防平台 Write Up

原创

C

攻防 专栏收录该内容

4 篇文章 0 订阅 订阅专栏

说在前面

大部分参考: NCTF 南京邮电大学网络攻防训练平台 WriteUp

做题网址: CG-CTF (里面时不时出现某同学的名字实在好出戏啊!)

里面只有web。解答比较全,不过我有几题没写出来,以后做出来了会更新。另外也有非web题。 刚接触CTF,很多东西不懂,只是为了做个笔记,比较适合新入门的小萌新看,有一些工具入门的介绍,还有总结出的解题思 路,在dalao们面前肯定是班门弄斧了,有什么错误或者指导意见,请务必在评论区写出来,一定虚心学习! 比较喜欢碎碎念,不要介意~

做题环境

操作系统: Win10 64x 浏览器: firefox 查看器: sublime text, 文本文档 工具: ·burpsuite 用于抓取数据包分析 ·winhex 16进制分析工具 ·firefox hackbar插件

#正题

web

签到题

这题一定是最简单的

你说简单就简单?

第一次接触实在摸不着头脑,结果只需要戳一下F12查看网页源代码就能看到。好嘛,上来就是套路

key在哪里?

🕞 💼 📔 Element	Console	Sources	Network	Performance	Memory	Application	Security	Audits
<html></html>								
<head></head>								
•••• <body> == \$0</body>								
<a <="" style="dis
" td=""><td>play:none"></td><td>nctf{</td><td></td><td>}</td>	play:none">	nctf{		}	>			
key在哪里	?							

md5 collision

来看源代码,顺手加点注释



这段代码还蛮重要的,后面有好几题都是差不多的结构,又套路了? 显然不可能是让我们真去搞碰撞,然后就去百度了一下这个QNKCDZO这个字符串,没想到......

PHP在处理哈希字符串时,会利用"!="或"=="来对哈希值进行比较,它把每一个以"0E"开头的哈希值都解释为0,所以如果两个不同的密码经过 哈希以后,其哈希值都是以"0E"开头的,那么PHP将会认为他们相同,都是0。 也就是说,只要0E开头的就行了,百度一下,人家一下子给列了好几十条,随便找一条就对了,比如找了xxxxxxx 然后用get方式传入参数,只要在url后面加一个 ?a=xxxxxxx 就可以了 顺道也说一下,用post方式传递参数是一样的,至于post和get的差别这里就不讲了,http的知识~ 也就是说在地址栏输入 http://chinalover.sinaapp.com/web19/?a=xxxxxxxx

签到题2

签到题1的套路,上来先戳一戳F12 说真的上面一题要是题目没给代码,上来也是先戳F12,看透.jpg 关键在这里

尚未登录或口令错误<form action="./index.php" method="post"> 输入框: <input type="password" value="" name="text1" maxlength="10">
 请输入口令: zhimakaimen <input type="submit" value="开门">

看到maxlength突然警觉,数了数果然是,zhimakaimen有11个字 直接把10改成11及以上,就成功开门啦~

这题不是web

既然不是web放在隔壁不好吗???

戳进去就一张gif,又不是web...... 只好又跑去看题解,原来是道图片隐写 于是把gif改成txt格式,用文本文档查看末尾获得flag 花了几分钟查了查图片隐写,原来不同文件类型的图片都有特定的结束字段,图片查看器一般只读到结束字段为止,那么在末尾 藏信息就是一种很简单便捷的方式了

层层递进

打个ctf还相亲,居然觉得挺浪漫

点进链接实在不知所措......戳戳F12呗,也没发现什么 可是又发现了什么,切换到网络,刷新一下页面,发现有一个404.html,点进去一看

来来来,听我讲个故事:

- •从前,我是一个好女孩,我喜欢上了一个男孩小A。
- 有一天,我终于决定要和他表白了!话到嘴边,鼓起勇气...
- 可是我却又害怕的<u>后退</u>了。。。

为什么? 为什么我这么懦弱?

最后,他居然向我表白了,好开森...说只要骗足够多的笨蛋来这里听这个蠢故事浪费时间,

他就同意和我交往!

```
谢谢你给出的一份支持!哇哈哈\(^o^)/~!
```

查看网页源代码,一首藏尾诗 0110 0110 0110 。flag get

AAencode

题目提示太明显了,百度一下aaencode,有很多说明,js转换可以用sublime自带的package实现 但是!这题我卡了一天!你问我为什么?

 $\begin{array}{l} & g = -1 \\ g$

谁能告诉我这堆中文怎么解?:)去问隔壁的dalao并获得两个直男专属笑脸表情后

知道了是编码的问题,就开始百度怎么转成UTF-8。结果chrome不! 支! 持! 编码转换

得,拜拜了您嘞。火速换成firefox,点击选项窗口(就是设置所在的那个)右键添加更多项目,里面有个文字编码,改成UTF-8 就可以。sublime text/notepad++也支持编码转换





终于看到了可爱的颜文字,转成js之后进入题目页面,戳F12,切换到命令行窗口,把整个js放进去运行就得到flag了

单身二十年

这题可以靠技术也可以靠手速! 老夫单身二十年,自然靠的是手速! 看题目完全不知道在说啥,两个页面都戳了F12也没用,好吧再去看看dalao的题解 原来要抓包!是时候掏出burpsuite了。官网有free版本的,下载后是一个jar包,直接双击就能打开,不分操作系统 在使用之前先改一下代理,打开firefox的设置

<mark>回</mark> 常规	高级 Step2	(?)
Q 搜索	堂规 数据反馈 网络 更新 证书	
➡ 内容		
▲ 应用程序	连接	
∞ 隐私	配置 Firefox 如何连接至国际互联网	Step3 ~~ 设置(E)
🔒 安全	网络内容缓存 _{连接设置} ×	
🗘 同步	您的网络内容缓存当了 配置访问国际互联网的代理	立即清除(<u>C</u>)
🛓 高级	无视自动缓存管 不使用代理(Y) 初始是这个 缓存最大为 (L) □ 自动检测此网络的代理设置(W) ○ 使用系统代理设置(U)	
ſ	离线 Web 内容和用	Step4
Step1	您的应用程序缓存当i	立即清除(<u>N</u>)
	 ✓ 网站请求保存数 SSL代理:端□:(Q) 0 	例外(<u>X</u>)
	以下网站已被允许存 ETP 代理: 端口:(R) 0 €	
	http://newtab.fire SO <u>C</u> KS 主机:	0 字节
	http://offlintab.fire ○ SOC <u>K</u> S v4 ● SOCKS <u>v</u> 5 □ 远程 <u>D</u> NS 不使用代理:(N)	127 KB
	https://outlook.liv localhost, 127.0.0.1	2.0 MB 移除(R)

通常burpsuite的配置不用改了,如果改过的可以看这里

other tools or another installation of Durn

Target Proxy Sp	pider Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts			
Intercept HTTP history WebSockets history Options												
Proxy Listeners Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use												
Add	Running Int	erface	Invisible	Redirect		Certificat	te					
	12	7 N N 1·9N9N				Per-host						
Edit 127.0.0.1:8080 Per-host												
Remove												
Each installat	ion of Burp gene	rates its own	n CA certific	ate that Prox	y listeners	can use whe	n negotiating	g SSL conr	nections. Y	'oı		

CA certificate ...

好了,开始抓包吧

Burp	Burp Intruder Repeater Window Help												
Targ	e	roxy	spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts	
Inter	Intercept HTTP history WebSockets history Options												
	Request to http://ctf.njupt.edu.cn:7080 [180.209.64.77]												
F	Forward Drop Intercept is on Action												
Raw	Pa	ams	Headers	Hex									
GET 7a	p1/ch	alleng	e/detail/	2 HTTP/1	.1								

刚才打开的界面刷新一下,burpsuite里就会出现抓到的数据包了。点击页面上的链接会发现无法跳转,在burpsuite上戳forward 按钮,将截断的数据包重新发出去,就会跳到下一个页面了,没跳过去就多戳几下

Tar	get	Proxy	Spider	canner	Intruder	Repeater	Sequencer	Decoder	Com	parer	Extender	Options	Alerts			
Inte	rce	HTTP	history	VebSoci	kets histo	ry Options										
Filter	Filter: Hiding CSS, image and general binary content															
#	Ho	st		1	Method	URL		F	Params	Edited	Status	Length	MIME t	Extension	Title	Comment
		.									200	1100	script	js		
6	•					1.404				~		100				
8	R			,												
9																
10	hı.					emaati	15									
11	htt	p://china	alover.sinaa	app.c (GET	/web8/					200	343	HTML			
12	htt	p://china	alover.sinaa	арр.с (GET	/web8/search	_key.php			U.	200	250	HTML	php		
13	htt	p://china	alover.sinaa	ipp.c (GET	/web8/no_key	/_is_here_fore	ever.php			200	402	HTML	php		
				_					_	-						<u> 7</u> F
Re	quest	Resp	onse													
Ra	w H	leaders	HexH	TML R	nder											
HTTP	/1.1	200 OK														
Serve	r: sa	е														
Date:	Tue,	14 Nov	2017 07:0	6:59 GM	Г											
Conte	nt-T	ype: text	t/html													
Conn	ection	n: keep-:	alive													
Conte	ວ∠ວ nt-L	enøth: 1	00													
1		Berry T														
le i				1			<td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>									

……原来这就是需要多戳几下的理由,明明只有两个界面中间多出来的那个是啥玩意儿? 点开看数据包,查看数据包的response message,原来flag就在里面了

但是我不服输!不单身也必须有手速?! 所以来来回回看了好几遍 好吧,中间的确飞速闪过一个路径为search_key.php的url。

.....

下一题

php decode

```
<?php
function CLsI($ZzvSWE) {
    $ZzvSWE = gzinflate(base64_decode($ZzvSWE));
    for ($i = 0; $i < strlen($ZzvSWE); $i++) {
        $ZzvSWE[$i] = chr(ord($ZzvSWE[$i]) - 1);
    }
    return $ZzvSWE;
}
eval(CLsI("+7DnQGFmYVZ+eoGmlg0fd3puUoZ1fkppek1GdVZhQnJSSZq5aUImGNQBAA=="));
?>
```