## i春秋-在线挑战-真的很简单-过程记录



adedeens 在下方输入目标网址:	X		
www.test.ichunqiu	一键爆账号密码		
2 44 40 46 26 9 DEDE <mark>C/M</mark> E			
推荐:  ichunqiu adab29e084ff095	ce3eb		
你好友的Email: @			

## 0x01 获取hash值对应的密码

资料可知,dedeCMS的密码hash是32位的hash截取来的,因此对其前三位和最后一位进行裁剪后可得到16位的hash。破解可得密码only\_system。

## 0x02 获取管理员后台目录

网上大量教程和经验总结获取后台的路径,但是绝大部分都是差之毫厘因此没有得到后台路径。

/data/mysql\_error\_trace.inc是各大经验教程总结的第一方法。但是在这个实验中不生效。最后获 悉/data/mysqli\_error\_trace.inc才能爆破出路径。因为在这个实验环境中使用的mysqli函数集,因此也需要通过 mysqli\_error\_trace.inc来爆破路径。



## 0x03 登录并获取shell

后台功能丰富,既有上传点也有修改上传附件限制的设置功能。对上传附件的限制进行修改,并进行上传获取 shell。





	EDE C/AS	V5.7										EIN HERS
	1.18.18.18 🖬 1.518.14							12562	建業	3	1 112	iete 🔹 æikk
-	- 370mt	*	N/DETS									(上帝順文件)
0	• 网站栏目管理	8	关键字:		文件类型 •	用户组	•	182				
极助	<ul> <li>防有档案列表</li> <li>等率权的档案</li> </ul>		法师	文件都题		文件大小	1	上传会员	上保时间	4	文件类型	管理
4	<ul> <li>現実率的文档</li> </ul>		0	1492		0.0 1		ichangin	2016-10-05	10:50	射件/其它	現代 新秋
JR.	0 评论管理		- 60	KITHR T-IL-	AND 101005	1 1050061	lil. ale	i chengi n	2010-04-07	15:30	相种/其它	更次(最終
来	。内容即於站	0	8	我的服务	殿片	34-3.E		i chungi u	2010-04-07	15:30	相性/東宅	第三日 第三日
*	- 内容管理		8	我的眼界一些关于花的	調片	41.2 K		Telengin	2010-04-07	15:30	相件/其它	現法   新除
슢	a 40000	2	8	我的服务	開始	32.7 K		i chungi n	2010-04-07	15:30	附件/其它	更改 細味

0x04 连接shell初步探查主机



虽然是系统权限,但是做了一些限制。而且桌面上的flag文件也做了限制,无法通过type直接读取。

自行上传net.exe实现net,直接修改ichunqiu的账户密码。

		Copyright @ 1985-2003 Microsoft Corporation Microsoft					
		用户名创:	admin				
		ares (L)					
<ul> <li>(2) 第二日</li> <li>(2) 第二日</li> <li>(3) 第二日</li> <li>(3) 第二日</li> <li>(4) 第二日</li></ul>	这合远程;	+算机,悠必须	[被授予允许通过终端服务登录的权限。	X 默认地,"远程桌面用户"组			
的成员拥 面用户锁	有该权限。 1没有该权	,如果您不是"近 限,您必须被引	远程桌面用户"组或其他拥有该积限的组 F助授予该权限。	的成员,或者如果"远程桌			
			確定				

使用远程登录则发现所有账户都不在远程登录组里面。

0x05通过共享获取flag文件



转载于:https://blog.51cto.com/12125295/1858795