## 基本信息

IP：101.37.30.224

操作系统用户名/密码：root/Jgw@0792!

后台管理端：[www.0792gw.cn/jgw](http://www.0792gw.cn/jgw)

管理员用户名/密码：duanss/Passw0rd!

## 文件路径

网站源文件根目录：/data/wwwroot/default

备份文件路径：/data/wwwroot/backup

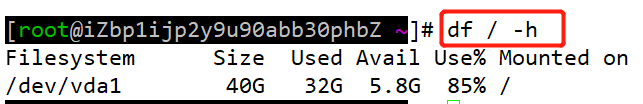
相关脚本：

* 备份脚本：/data/wwwroot/rum\_backup
* 检查index文件有没有被替换的脚本：/data/wwwroot/backup/check\_index.sh

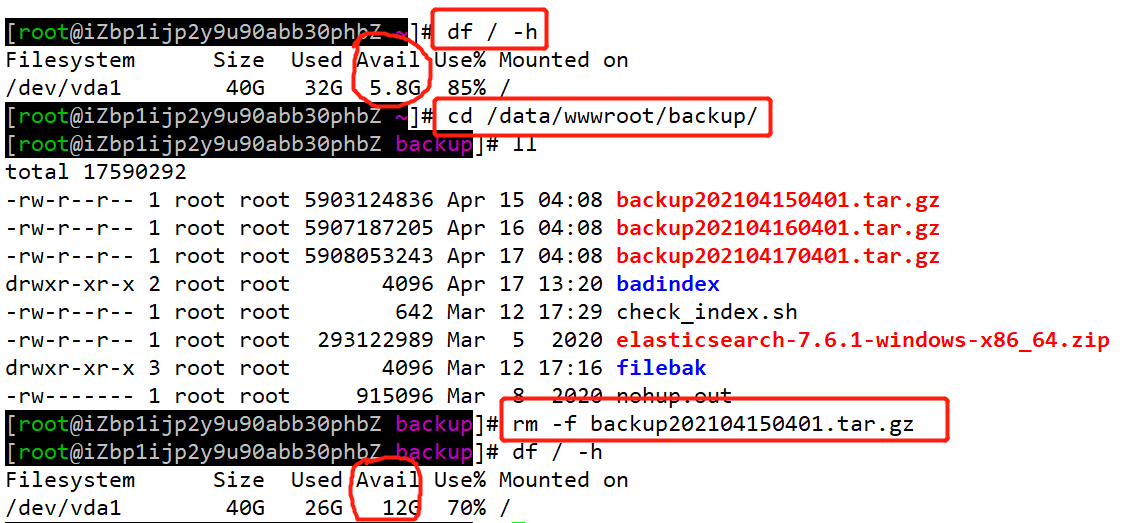
## 一些日常操作

1. 适当清理备份文件：

* 登录系统，查看空闲空间：**df / -h**

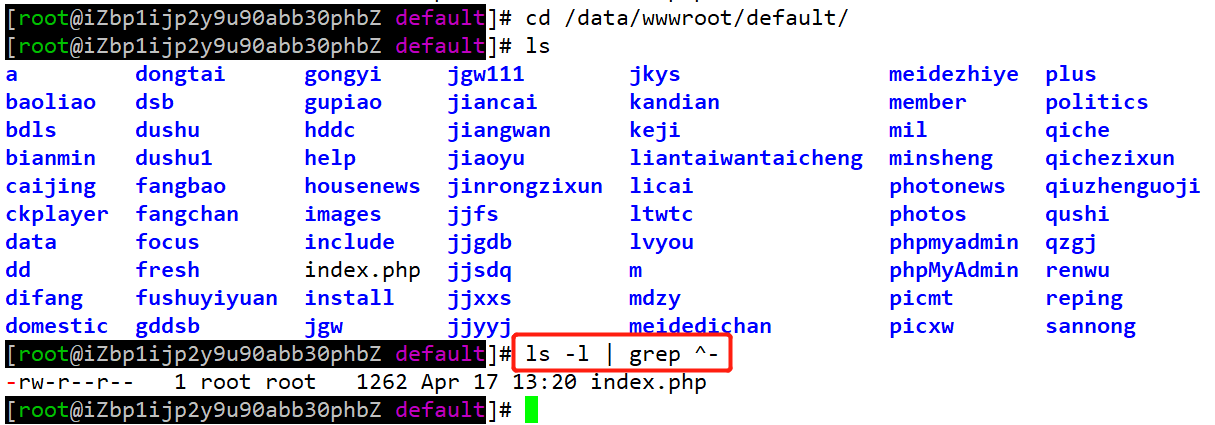


* 此时可以到backup目录下把备份文件删除一个，基本上保留一到两个备份文件即可：



（使用rm命令的时候要小心）

1. 检查index文件状态



**ls -l | grep ^-** 这个命令是详细列出当前路径下所有的文件，不包含文件夹。因为从目前情况来看，攻击者一般都是替换index文件，有时候会多放一个index.html 或者 index.htm等，所以如果这里突然多出了别的文件，一般都是恶意文件，删除即可。而且index.php这个文件本身大小也只有1262字节，如果突然变大，也是被替换了，check\_index.sh脚本也会检查这个。

备份的index.php文件位置：**/data/wwwroot/backup/filebak/index.php**

1. 广告图片的位置：**/data/wwwroot/default/style/adimg**

有的广告需要把几张jpg文件合成一个gif，同时注意首页广告图片一般大小都是1200\*50，尤其注意宽度1200，有时候对方发来的图片宽度很大，这时候需要适当的裁剪。