ftp -21 :直接访问，匿名账户，看文件，可能是后面爆破的字典

扫后台：zip ，phpmyadmin

御剑 - burp

web

- 暴力破解
- 注入
-上传

数据库：

- ms   -- sa xp_cmdshell
- mysql -- udf提权