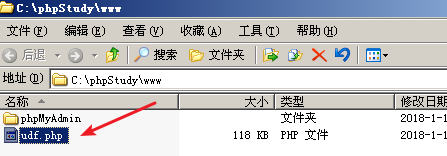
mysql数据库udf提权

## cmdshell提权

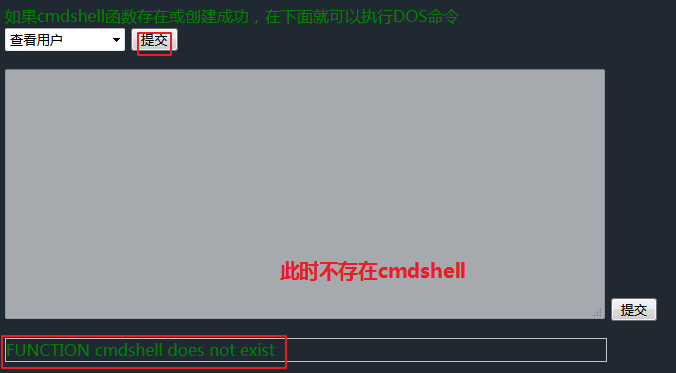
上传UDF提权脚本



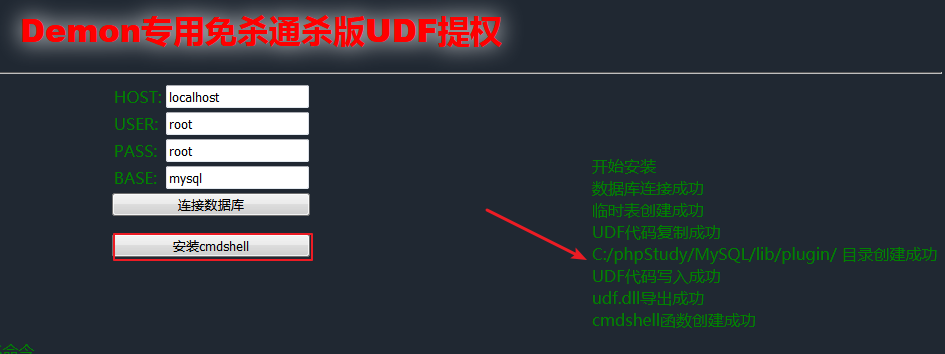
访问，输入数据库账号密码，连接数据库



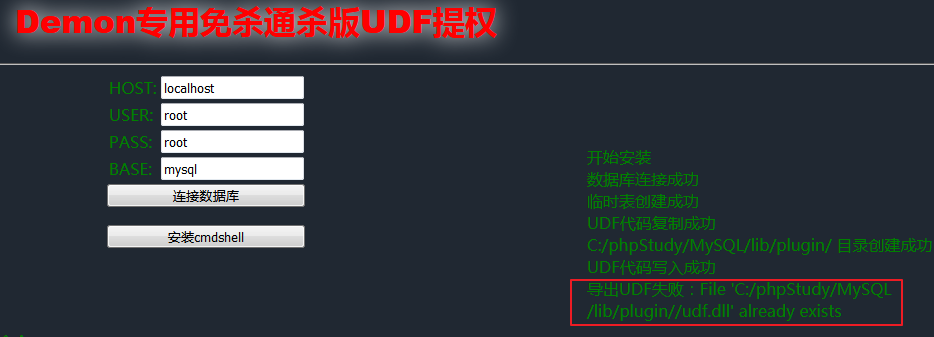
在安装cmdshell之前先使用以下下面功能，看是否已经存在函数cmdshell



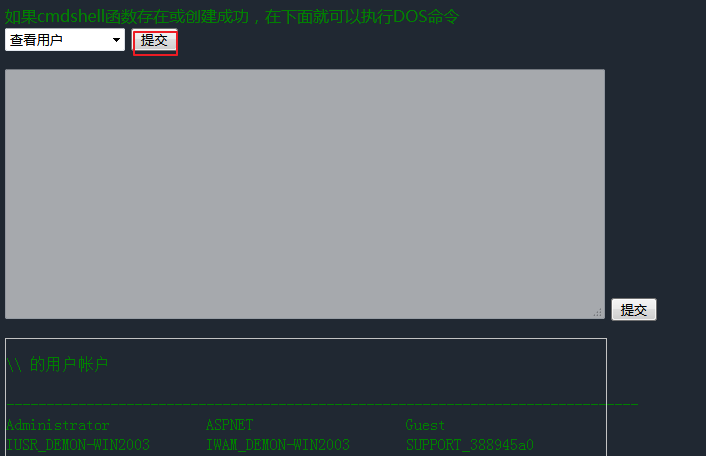
点击安装cmdshell，右边会有安装过程的信息，如果非win2003可能会失败



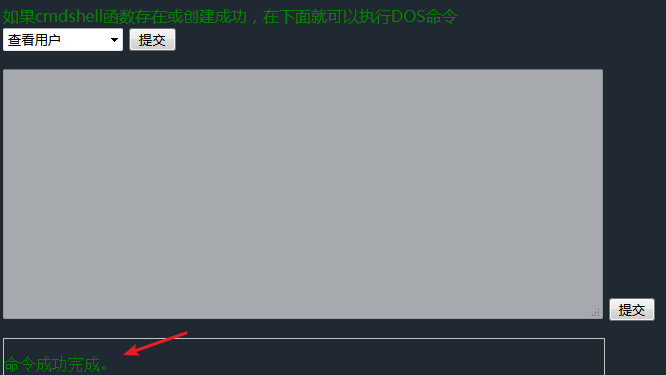
安装成功后，如果重复点击安装会报错。因为函数已经存在

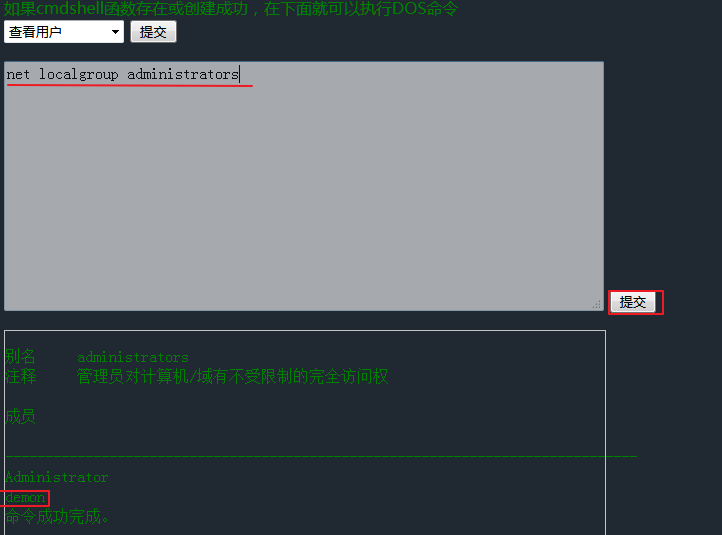


此时可以使用 下拉表单 写好的DOS命令

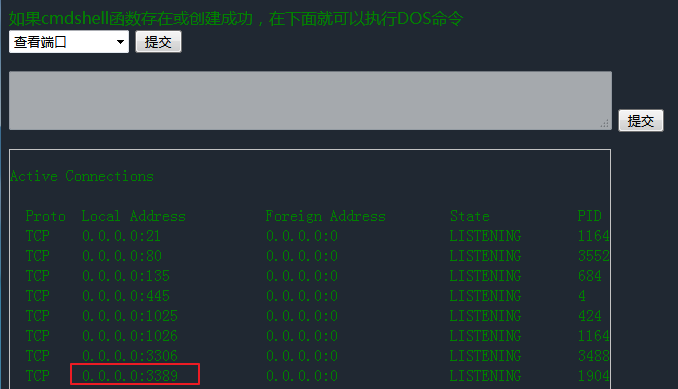
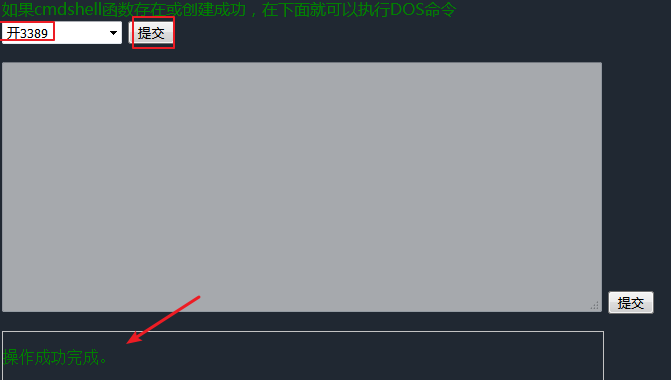


这里简单介绍几个常用功能：创建管理员用户

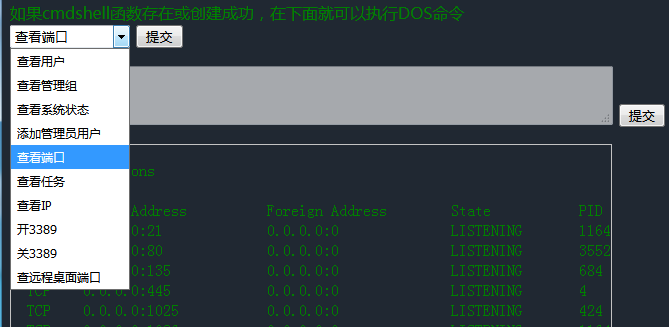


也可以自定义DOS命令，在textarea区域输入提交即可

也集成了开启3389的功能



其他功能也差不多



## backshell反弹提权

使用的仍然是库文件 udf.dll ，不过使用的库里的另一个函数 backshell ，用于主动像远程IP和端口号发送连接，一旦连接成功，拿到的直接是system用户了。访问上传好后的UDF提权工具，用浏览器访问。



