1.延时注入 好事最多
2. sqlmap -r 参数，对应bp抓的包，使用post的方法传参
例如网站需要cokie，用户登录的方式。

3. 联合查询：

order by 1 语句成功后在采用二分法找长度。

联系网址：http://192.168.1.55:8000/DVWA0/login.php
admin/password

中间件：
apatch-》php
tomcat -》java

重点，文件读写
union -》 UnioN/ununionion/ un/**/ion/(un)(ion)

渗透的工具：
burp Suite
python
一句话： 蚁剑，冰蝎，菜刀

上传文件流程：
1.上传正常的图片，确定功能正常
2.逐项更改（检查项）

文件包含：