pikachu漏洞测试：

1：

暴力：

服务器验证码绕过：

失败后没有刷新验证码， 验证码5分钟有效

前端验证码绕过：

js函数

token：

即每一次请求都是需要token的，请求必须携带token才可以，token每一次都不一样 这是怎么实现的呢？防爆力无效 脚本可以获取

2： xss

反射xss 拼接script到地址里面触发

有个页面会把get后面的内容放到页面之间；

post类型： 有个后端脚本 把post里面的参数 返回前端渲染，脚本里面放js

存储型xss 论坛的脚本

3：csrf

给出一个url表示修改操作，用户一点 就完成了操作自己的；使得用户在不知情的情况下完成操作的漏洞

解决方式就是加token，每一次请求都需要获得token以后 才能操作;

4:sql注入：

分类讨论：

5：文件上传漏洞和文件包含漏洞

上传php脚本文件， 利用包含， 完成一句话木马；

php伪协议的概念，在包含存在的时候 获得源码的内容；

6: