# 二次注入攻击

### 原理

二次注入的关键在于：

第一次注入（存储阶段）：攻击者将恶意 SQL 片段（如' OR '1'='1）作为 “正常数据” 提交，应用程序未过滤便存入数据库（此时不触发攻击）。

第二次注入（触发阶段）：当应用程序从数据库读取该恶意数据，并将其拼接进新的 SQL 查询中执行时，恶意代码被触发，导致注入漏洞。

### 测试方法

延迟测试：test' AND SLEEP(5) --

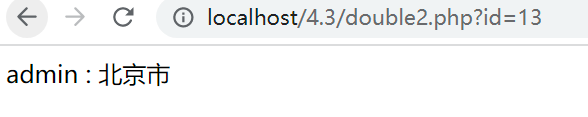
首先存在漏洞密码明文提交hh

### 网站结构:

首先是一个登录页面:

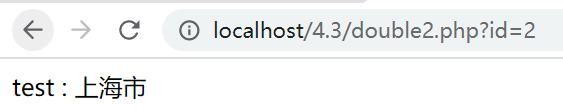


登陆后能够查看用户信息:



这里主要分析最后一个页面

首先构造URL可以在网站横向移动,构造不等同的id

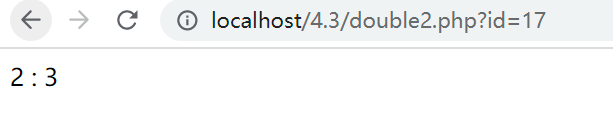


因为最开始的用户名是注册页面

用户名信息会被实体化后,加入到数据库中,所以,在用户注册是构造恶意信息可以忽然数据库,登陆后的查询信息会携带恶意信息

通过构造恶意用户名:

-test’ union select 1,2,3,4--+



发现了回显信息可以执行任意查询(对用户长度没有限制)

同时知道管理员用户名的话可以实现越权 admin ‘ --