Sql 注入无回显，盲注又被封怎么办？

1、Sql 注入无回显怎么办？

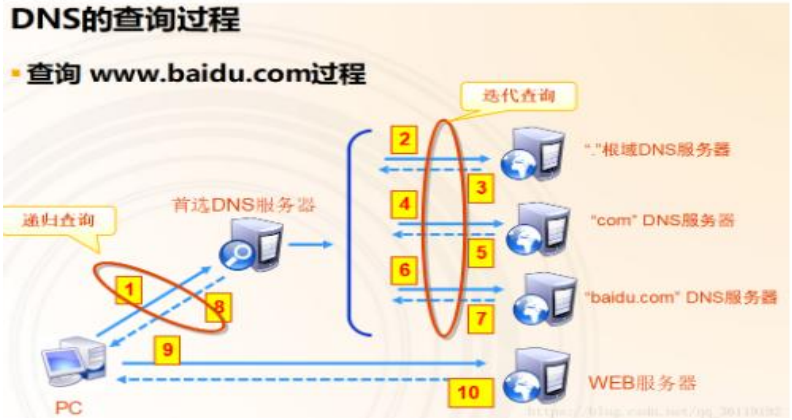
我们可以采用盲注，基于时间的盲注，基于布尔值的盲注

2、sql 盲注被封了怎么办？

盲注，这种注入速度非常慢，需要一个一个字符猜解，需要像服务器发送的大量请求，而且很容易被网站 WAF 或者防火墙 BAN 掉 IP，虽然也可以使用代理 IP 池，但是还是需要一种快速有效的方法来获取数据。此时我们就可以利用 DNSlog 来快速的获取回显数据。

3、DNSLog 平台

（1）DNS 解析过程



（2）UNC

UNC 是一种命名惯例，主要用于在 Microsoft Windows 上指定和映射网络驱动器.。UNC 命名惯例最多被应用于在局域网中访问文件服务器或者打印机。我们日常常用的网络共享文件就是这个方式。UNC 路径就是类似\softer 这样的形式的网络路径

格式： \servername\sharename ，其中 servername 是服务器名，sharename 是共享资源的名称。

目录或文件的 UNC 名称可以包括共享名称下的目录路径，格式为：\servername\sharename\directory\filename

（3）查询 DNS 解析记录来获得命令执行的回显

DNSLog 部署过程：
申请一个域名，如 wasj.com
在我们的 VPS 上安装并配置 DNS 服务器
将 wasj.com 的 DNS 服务器设置为我们的 VPS 地址
这样，所有访问 wasj.com 的二级三级四级等等子域名都会被解析到我们的 VPS 上。
我们就可以通过查询 DNS 解析记录来获得命令执行的回显了。
但是由于部署非常麻烦，所以我们可以通过一些在线的 DNSLog 平台：
http://ceye.io
http://www.dnslog.cn

4、 Sql 注入盲注的 DNSlog 利用条件

- DBMS 中需要有可用的，能直接或间接引发 DNS 解析过程的子程序，即使用到 UNC
- Linux 没有 UNC 路径，所以当处于 Linux 中的数据库管理系统时，不能使用该方式获取数据