SQL注入之数据提交方式

GET方式注入

get注入方式比较常见，主要是通过url中传输数据到后台，带入到数据库中去执行，可利用联合注入方式直接注入

POST方式注入

post提交方式主要适用于表单的提交，用于登录框的注入

方法：利用BurpSuite抓包进行重放修改内容进行，和get差别是需要借助抓包工具进行测试，返回结果主要为代码，也可转化为网页显示

Request方式注入

概念：超全局变量 PHP中的许多预定义变量都是“超全局的”，这意味着它们在一个脚本的全部作用域中都可以用，这些超全局变量是：
$*REQUEST*（获取*GET/POST/COOKIE*）*COOKIE*在新版本已经无法获取了
*$*POST（获取POST传参）
$*GET*（获取*GET*传参）
*$*COOKIE（获取COOKIE传参）
$_SERVER（包含了诸如头部信息(header)、路径(path)、以及脚本位置(script locations)等等信息的数组）

HTTP头注入

什么是Header头？

通常HTTP消息包括客户机向服务器的请求消息和服务器向客户机响应消息。 这两种类型的消息有一个起始行，一个或者多个头域，一个只是头域结束的空行和可选的消息体组成。
HTTP的头域包括通用头，请求头，响应头和实体头四个部分

什么是Header头部注入？

header注入，该注入是指利用后端验证客户端信息（比如常用的cookie验证）或者通过header中获取客户端的一些信息（比如User-Agent用户代理等其他header字段信息），因为这些信息在某些地方是会和其他信息一起存储到数据库中，然后再在前台显示出来，又因为后台没有经过相对应的信息处理所以构成了sql注入。