# 如何区分GET注入和POST注入

## 一、GET注入

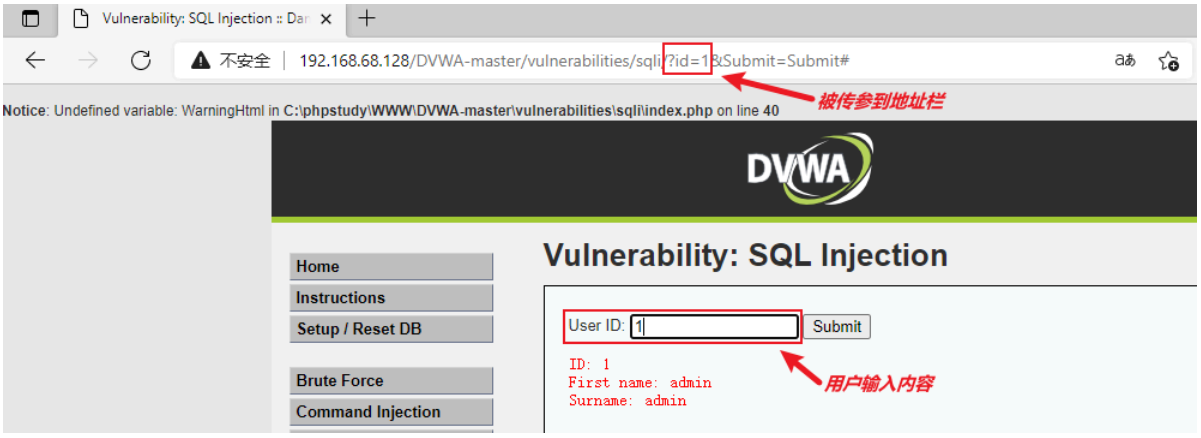
### 1、What is GET注入

要搞懂GET注入之前，先搞懂什么是GET传参。

GET传参：用户输入的内容参数会被传到地址栏（URL栏），是通过GET的方式进行传参

· 特点：传参内容可见，传参长度有限，标识“？”，输入的内容会可能被url编码

GET注入：通过GET传参的方式，传输恶意语句，进行SQL注入




### 2、如何进行GET注入

一般情况判断为传参方式为GET传参方式，首先进行GET注入测试，判断是否存在GET注入

如何判断是否存在GET注入：要想知道是否存在，首先搞原理，弄清楚是如何发生的

简单说，*原本程序要执行的代码拼接了用户输入的数据然后执行，就是本来用户输入的数据是要被查询的，但是被数据库当作代码执行*

*OK，AND，只需知道输入的数据有没有被数据库当作代码，可以判断存不存在注入点*

*AND，用户输入的数据一定不是输入everying都行的，如果用户随便输入的数据都被当做代码执行，那么这个网站就失去了它的功能，这是网站开发者不允许的*

## 三、POST注入

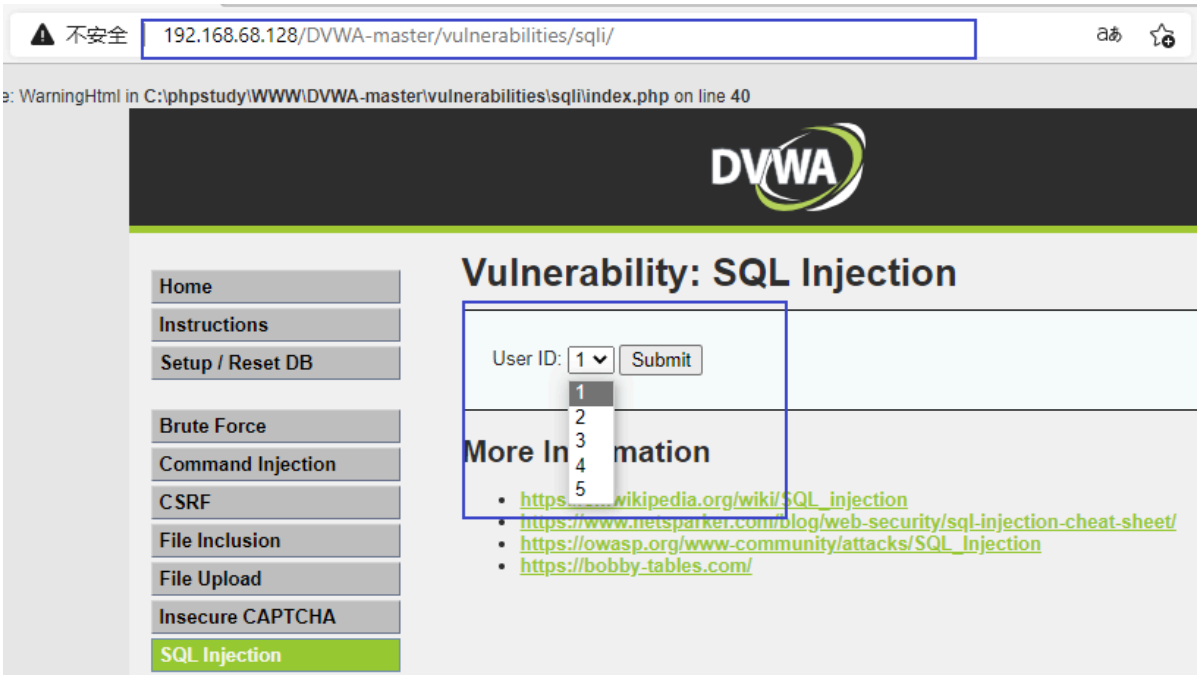
### 1、What is POST注入

要搞懂POST注入，先搞懂POST传参

POST传参：用户输入的内容被隐藏了起来，地址栏看不到

特点：*传参内容不可见，传参长度无限制*

*POST注入：**通过POST传参的方式，传输恶意语句，进行SQL注入，本质和GET注入是一样的***

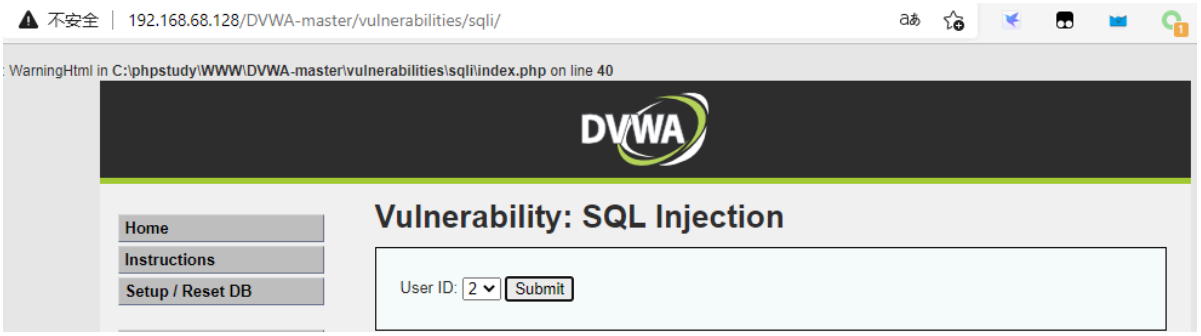


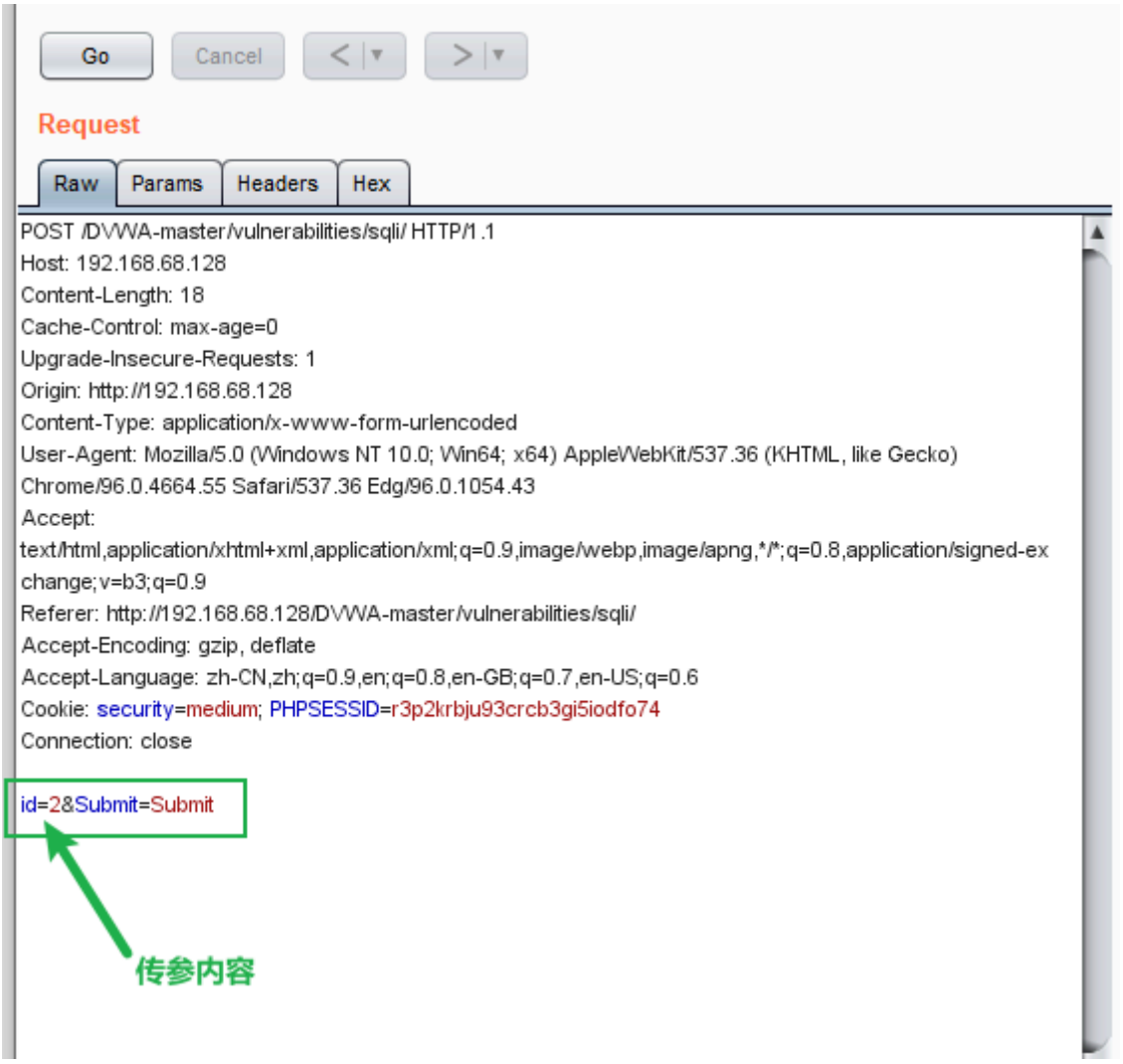

**如上图，所示，没有输入地方，只有选项框，最重要的一点是，地址栏不可见传参内容**

**WC，这怎么搞，这怎么进行传参，TMD不按套路来**

**那好吧，来搬个救兵吧 >>>>> BURP**

**BURP来抓个包吧，既然地址栏不能显示传参内容，抓包总可以吧**






**OK，，来来来，，传参内容出现了吧，，**

**那就在burp里测试吧**

**剩下的步骤就和GET注入一模一样了，修改传参内容**