

<https://github.com/JuneHck/SQL-injection-bypass>

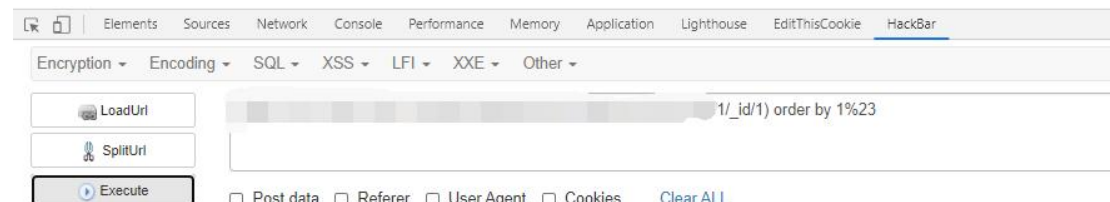
判断列数的时候会提示非法操作

1) order by 1%23

:(

含orSQL注入,非法操作!

页面自动 跳转 等待时间: 3

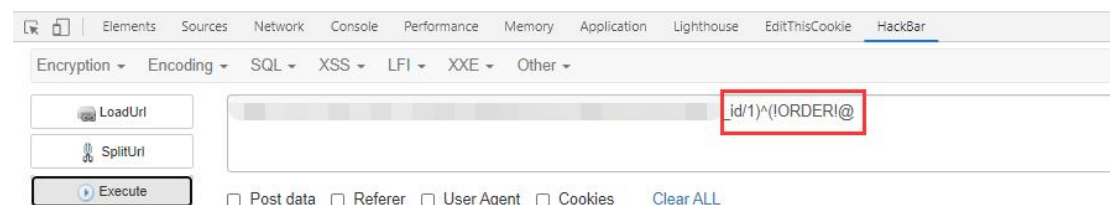


只要含有关键字就拦截

:(

含orSQL注入,非法操作!

页面自动 跳转 等待时间: 3

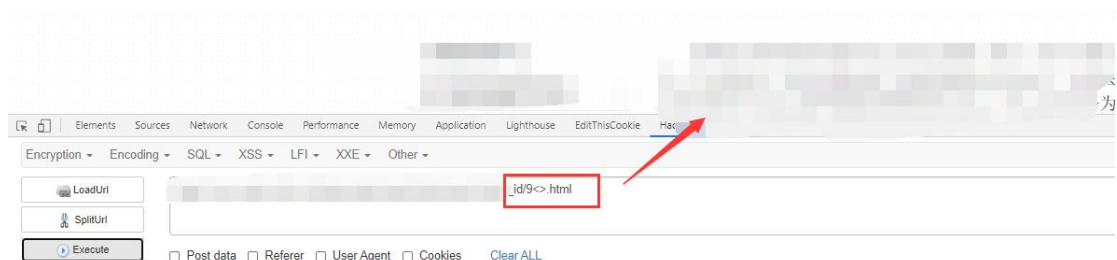


绕过方法是在关键字中穿插<>, 因为会先判断是否存在 sql 注入关键字然后进行全局关键字替换<>来防止 xss 漏洞

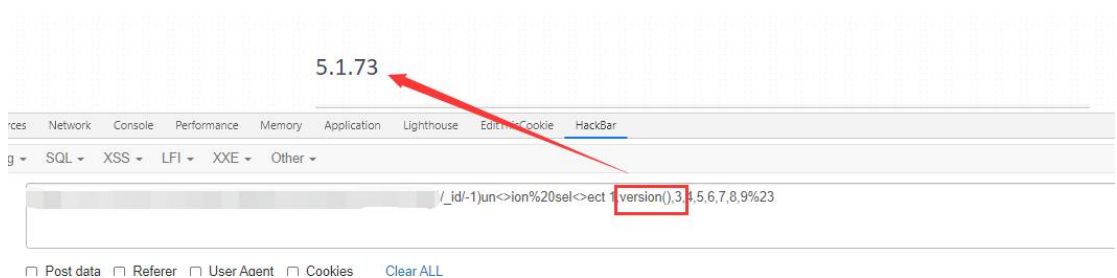
<https://github.com/JuneHck/SQL-injection-bypass>

<https://github.com/JuneHck/SQL-injection-bypass>

可以看到就算加了这两个字符页面还是正常



所以我们直接利用这个方法成功注入



<https://github.com/JuneHck/SQL-injection-bypass>