攻防世界xff_referer解析

原创

nwpuhkp 于 2021-10-30 10:35:11 发布 140 收藏

分类专栏： web 攻防世界 文章标签： web php

本文链接：https://blog.csdn.net/chlet/article/details/121047423

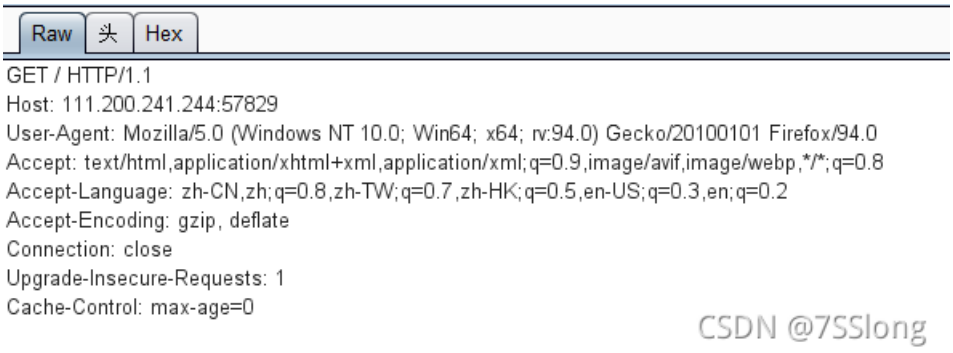
攻防世界xff_referer解析

ip地址必须为123.123.123.123

获取场景后发现，要求IP为123.123.123.123；

可以使用火狐浏览器的X-Forwarded-For插件；

这里使用Burpsuit；



抓到请求信息；

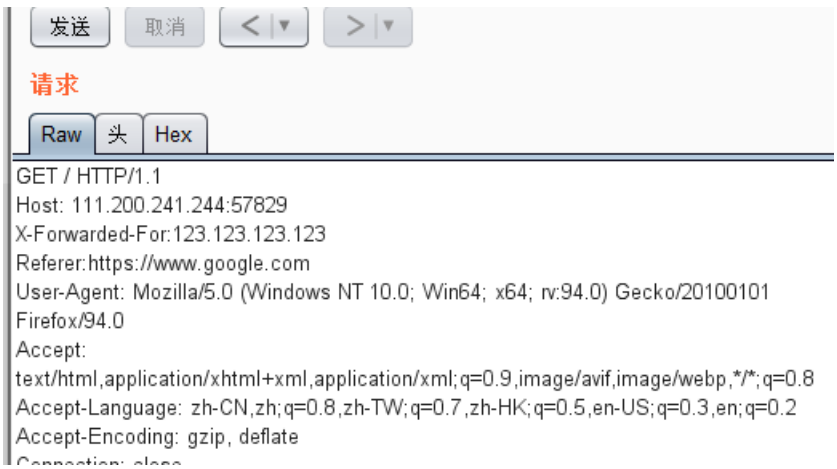
在host后添加X-Forwarded-For:123.123.123.123；

在重发器中发送；

```
    }
  </style>
</head>
<body>
<p id="demo">ip地址必须为123.123.123.123</p>
<script>document.getElementById("demo").innerHTML="必须来自https://www.google.com";</script><
```

发现有了另一个限制；

要求来自谷歌；



```
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```


在X-Forwarded-For:123.123.123.123后面加上Referer:https://www.google.com；

响应

Raw | 头 | Hex | HTML | Render

```
HTTP/1.1 200 OK
Date: Fri, 29 Oct 2021 05:56:16 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Vary: Accept-Encoding
Content-Length: 631
Connection: close
Content-Type: text/html

<html>
<head>
    <meta charset="UTF-8">
    <title>index</title>
    <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />
    <style>
        body{
            margin-left:auto;
            margin-right:auto;
            margin-TOP:200PX;
            width:20em;
        }
    </style>
</head>
<body>
<p id="demo">ip地址必须为123.123.123.123</p>
<script>document.getElementById("demo").innerHTML="必须来自https://www.google.com";</script><
script>document.getElementById("demo").innerHTML="cyberpeace{00d718277bcc2e5603be581be7122
4d2}";</script></body>
</html>
```


得到flag；

cyberpeace{00d718277bcc2e5603be581be71224d2}