攻防世界XCTF Writeup 之xff_referer

原创

h88z 于 2019-10-27 23:23:53 发布 1855 收藏 6

分类专栏： 网络安全入门 文章标签： XCTF writeup 攻防世界 CTF

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/qq_26012889/article/details/102773547
版权

网络安全入门 专栏收录该内容
2 篇文章 2 订阅
订阅专栏

标题文章极安中国首发

原文地址 https://bbs.secgeeker.net/thread-1401-1-1.html

攻防世界XCTF之xff_referer

题目来源

Cyberpeace-n3k0

打开后浏览题目 要求ip地址必须为123.123.123.123

https://blog.csdn.net/qq_26012889

回看题目为xff_referer
大致便有了思路
本题是考察的HTTP头的伪装修改

HTTP HEAD 复习资料

可参考

HTTP Headers

这里要求我们修改ip地址
也就是修改 X-Forwarded-For 的内容为123.123.123.123

> `X-Forwarded-For` (XFF) 在客户端访问服务器的过程中如果需要经过HTTP代理或者负载均衡服务器，可以被用来获取最初发起请求的客户端的IP地址，这个消息首部成为事实上的标准。在消息流从客户端流向服务器的过程中被拦截的情况下，服务器端的访问日志只能记录代理服务器或者负载均衡服务器的IP地址。如果想要获得最初发起请求的客户端的IP地址的话，那么 X-Forwarded-For 就派上了用场。
> 这个消息首部会被用来进行调试和统计，以及生成基于位置的定制化内容，按照设计的目的，它会暴露一定的隐私和敏感信息，比如客户端的IP地址。所以在应用此消息首部的时候，需要将用户的隐私问题考虑在内。

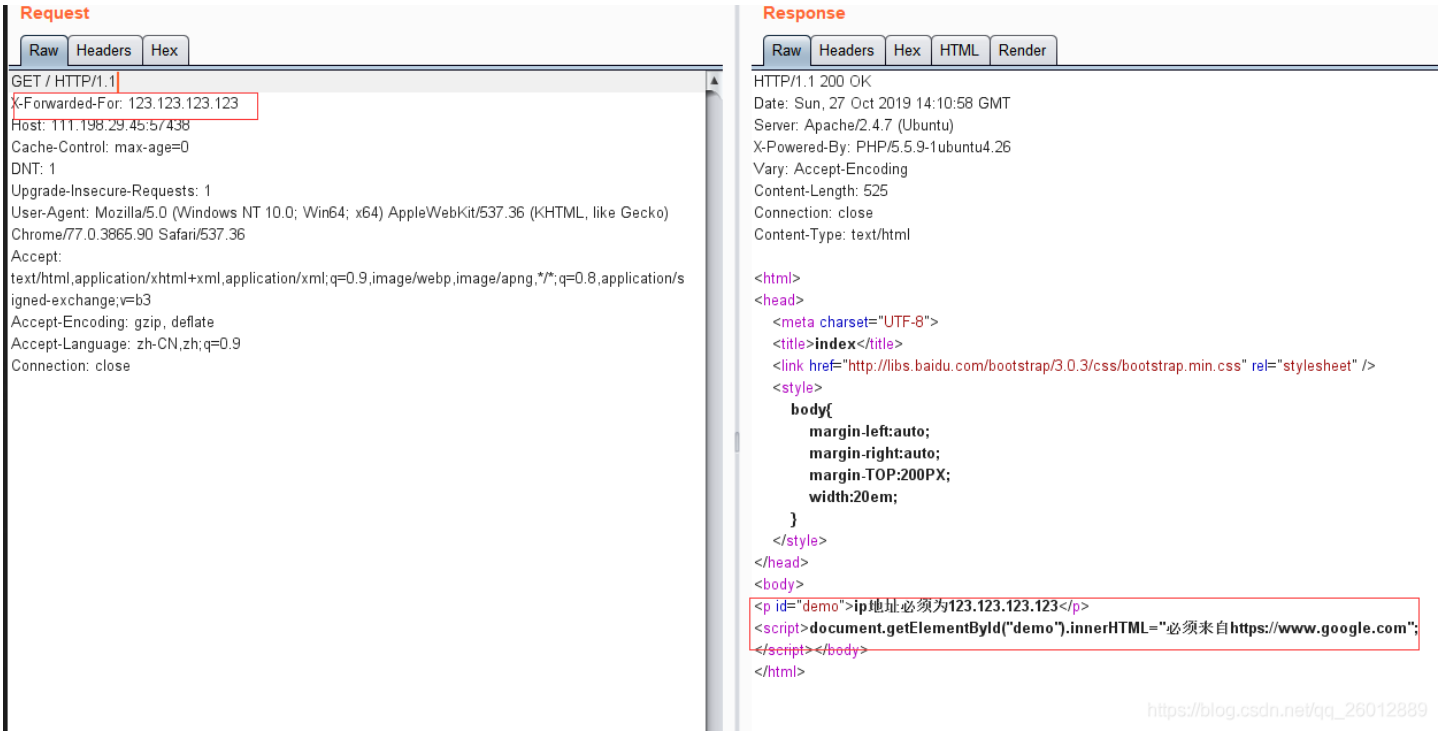
相关资料：

X-Forwarded-For

即

> X-Forwarded-For: 123.123.123.123

我们将上面的X-Forwarded-For 添加上
如图



我们可以发现回显多了一行`<script>`内容为

> 必须来自 [url]https://www.google.com[/url]

意思是需要请求头包含当前请求页面的来源页面的地址[url]https://www.google.com[/url]
也就是修改请求头中的Referer内容为[url]https://www.google.com[/url]

Referer请求头包含了当前请求页面的来源页面的地址，即表示当前页面是通过此来源页面里的链接进入的。服务端一般使用 `Referer` 请求头识别访问来源，可能会以此进行统计分析、日志记录以及缓存优化等。

需要注意的是 referer 实际上是 “referrer” 误拼写。参见 HTTP referer on Wikipedia （HTTP referer 在维基百科上的条目）来获取更详细的信息。

在以下两种情况下， `Referer` 不会被发送：

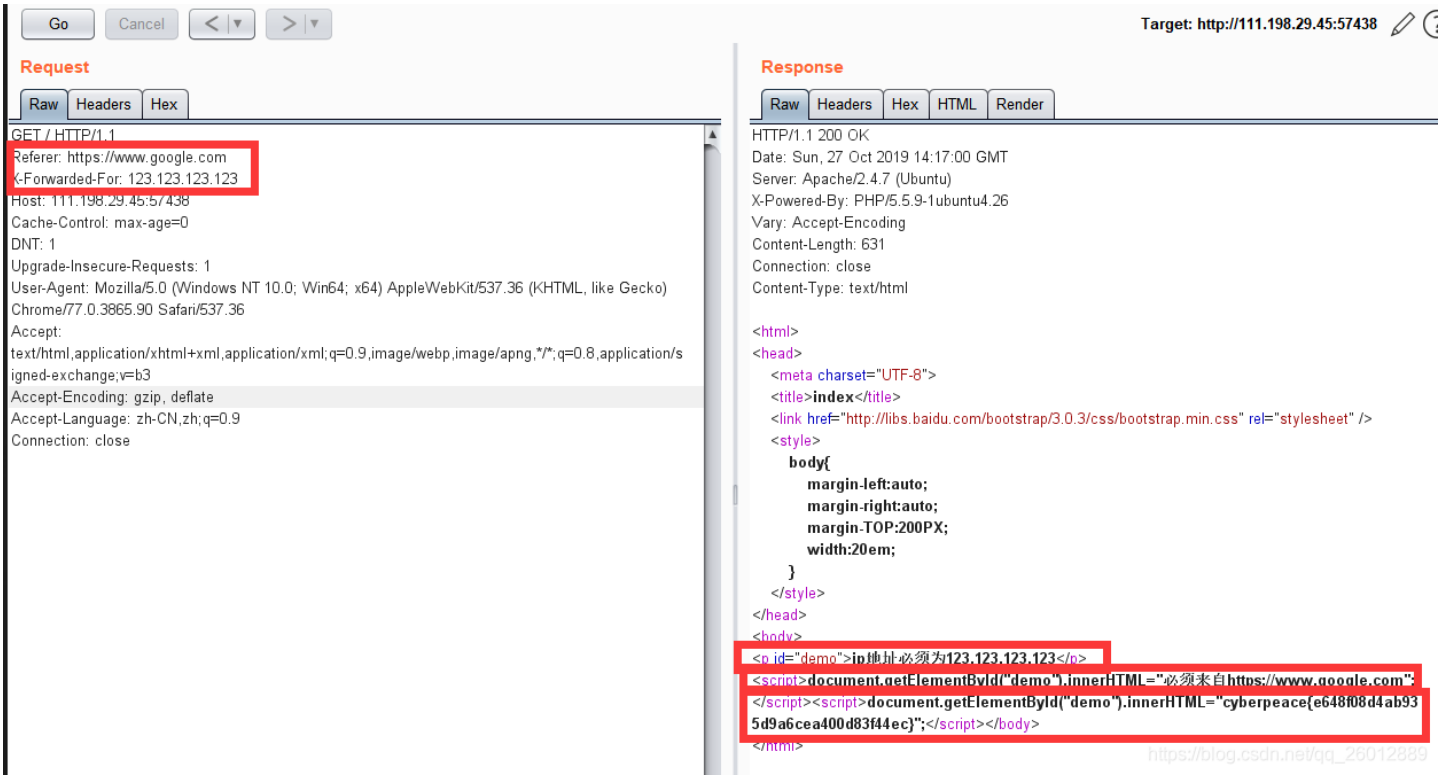
- 来源页面采用的协议为表示本地文件的 “file” 或者 “data” URI；
- 当前请求页面采用的是非安全协议，而来源页面采用的是安全协议（HTTPS）。

相关资料

Referer

即

> Referer: [url]https://www.google.com[/url]
> 下面我们添加上Referer: [url]https://www.google.com[/url]



可以看到flag就出现了。
又增加了一行 `<script>` 内容里就有flag
本题目flag即为

> cyberpeace{e648f08d4ab935d9a6cea400d83f44ec}