hackthebox-Toxic writeup

原创

qq_40952713 于 2021-08-19 11:49:09 发布 663 收藏

文章标签： 渗透测试 靶机

本文链接：https://blog.csdn.net/qq_40952713/article/details/119795157

hackthebox-Toxic writeup

cookie解码

分析源代码发现cookie是文件读取目录经过序列化之后再进行base64编码后生成的

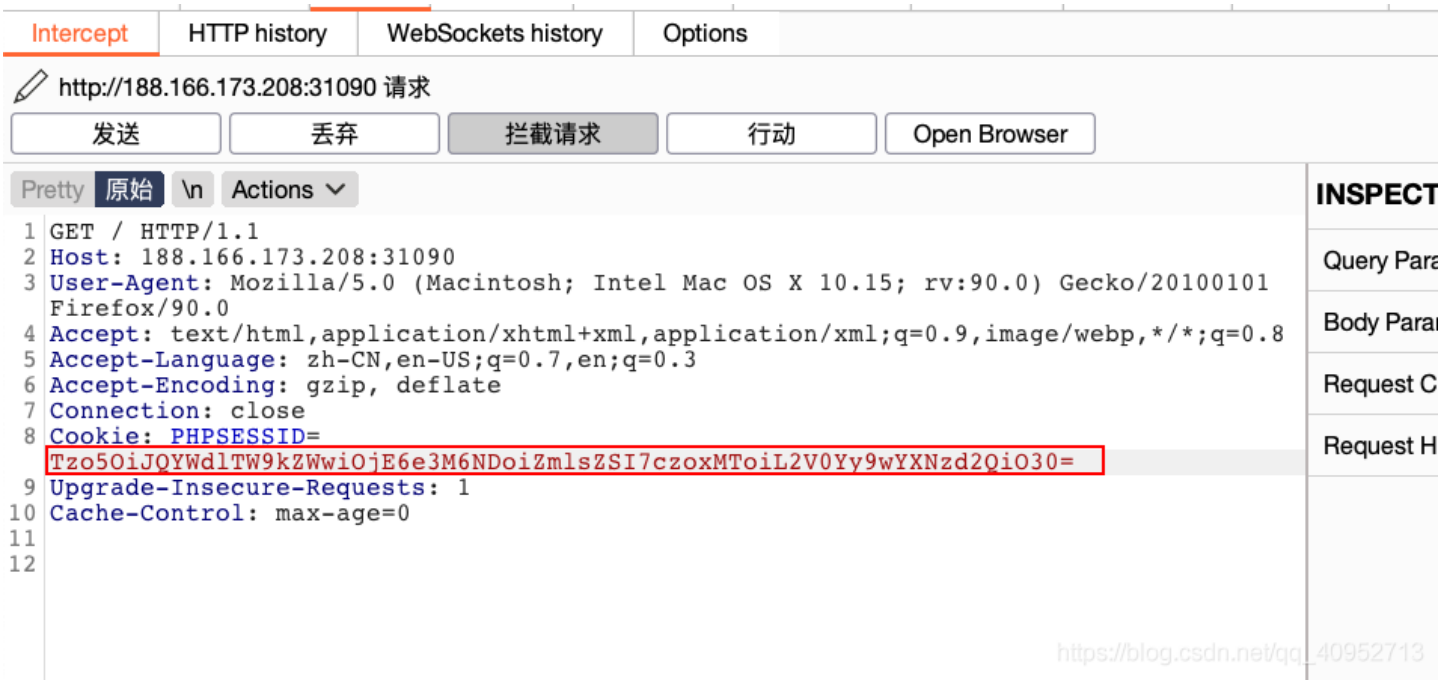
```php
if (empty($_COOKIE['PHPSESSID']))
{
    $page = new PageModel;
    $page->file = '/www/index.html';

    setcookie(
        'PHPSESSID',
        base64_encode(serialize($page)),
        time()+60*60*24,
        '/'
    );
}

$cookie = base64_decode($_COOKIE['PHPSESSID']);
unserialize($cookie);
```


将抓取到的cookie进行base64解码

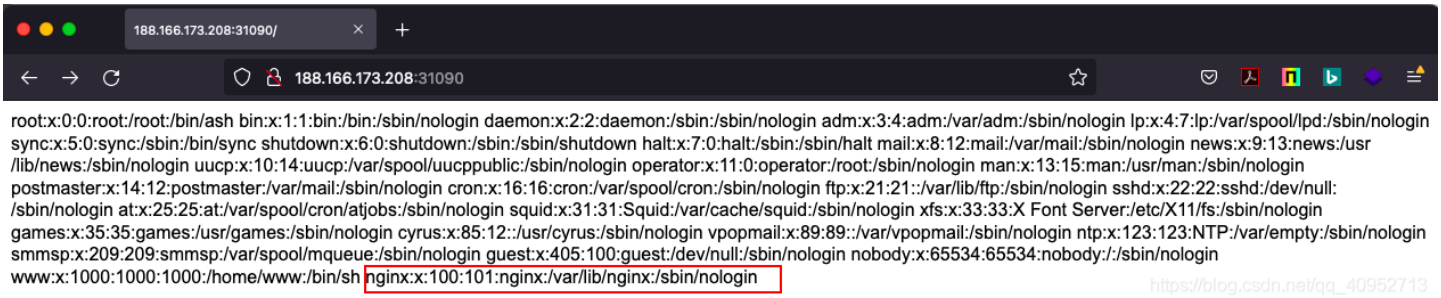
尝试敏感文件读取

修改路径，重新编码

替换原有的cookie值

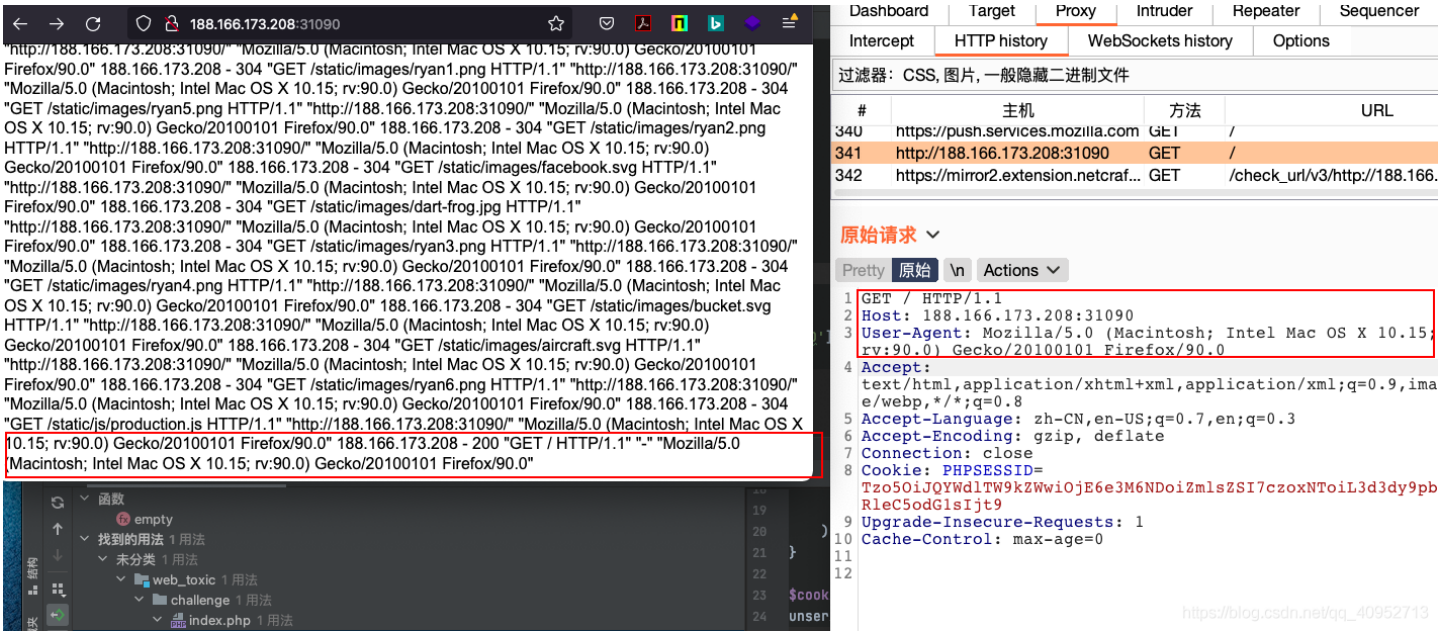


读取成功，发现nginx用户



读取nginx日志文件

发现日志文件记录的信息为用户请求头的个别信息（User-Agent:字段内容是可修改的）

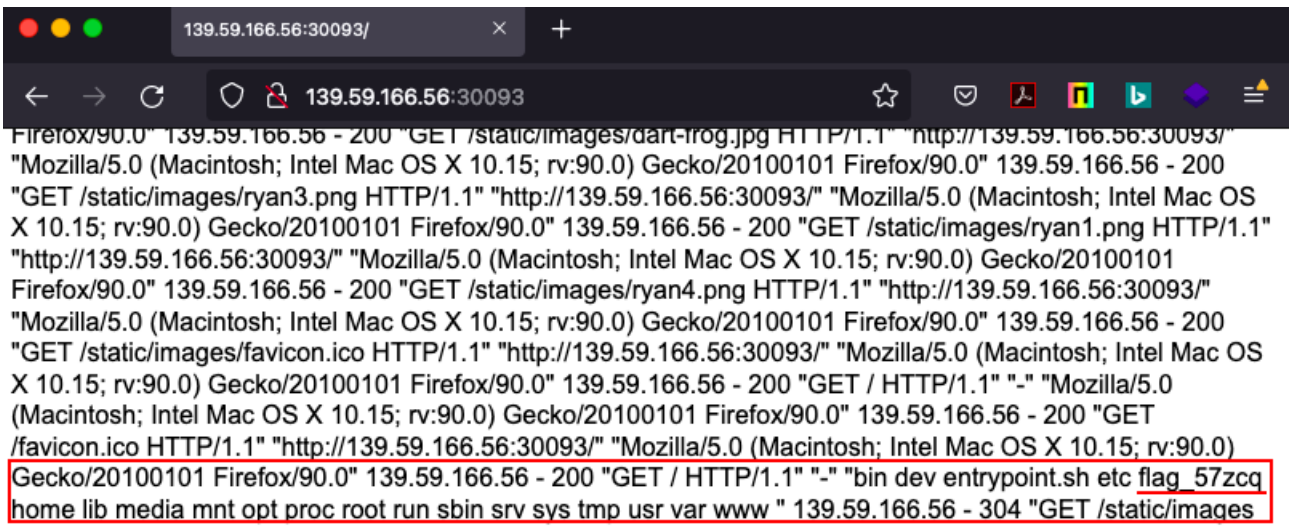


寻找flag

修改User-Agent:内容，将PHP代码存入日志文件中，来查看当前目录下的文件（中途靶机被玩坏了，重新启动了靶机，IP变了）

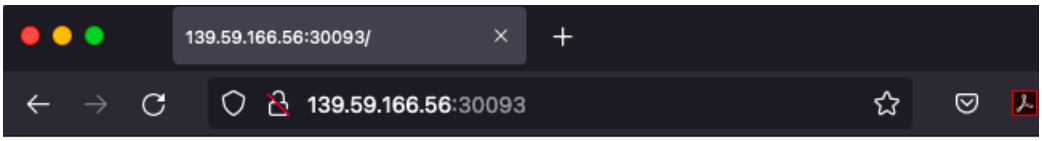
再次读取日志文件

日志文件中的PHP代码被执行后，成功显示出文件列表，发现一个名为flag_57zcq的文件



```
/dart-frog.jpg HTTP/1.1" "http://139.59.166.56:30093/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0)
Gecko/20100101 Firefox/90.0" 139.59.166.56 - 304 "GET /static/js/production.js HTTP/1.1"
"http://139.59.166.56:30093/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101
Firefox/90.0" 139.59.166.56 - 304 "GET /static/images/ryan4.png HTTP/1.1" "http://139.59.166.56:30093/"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0" 139.59.166.56 - 304
"GET /static/images/twitter.svg HTTP/1.1" "http://139.59.166.56:30093/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0" 139.59.166.56 - 304 "GET /static/images/ryan6.png HTTP/1.1"
```

读取



HTB{P0i5on_1n_Cyb3r_W4rF4R3?!}