

JU的博客

博客园 首页 新随笔 联系 订阅 管理

日志文件包含漏洞

公告

温馨提示

GTL-JU 我的小院子

我用的博客园美化样式

日志文件包含漏洞

日志包含漏洞属于是本地文件包含，同样服务器没有很好的过滤，或者是服务器配置不

个人信息

原理：

apache服务器日志存放文件位置：/var/log/apache/access.log

apache日志文件存放着我们输入的url参数

```
AAE 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
lsb 127.0.0.1 - - [14/Oct/2022:18:11:49 +0800] "GET /upload-labs/ HTTP/1.1" 200 4536
127.0.0.1 - - [14/Oct/2022:18:12:02 +0800] "GET /test/test4.php HTTP/1.1" 200 953
127.0.0.1 - - [14/Oct/2022:18:12:31 +0800] "GET /test/test4.php?file=/var/log/nginx/access.log HTTP/1.1" 200 368
127.0.0.1 - - [14/Oct/2022:18:18:58 +0800] "GET /test/test4.php HTTP/1.1" 200 953
127.0.0.1 - - [14/Oct/2022:18:18:58 +0800] "GET /favicon.ico HTTP/1.1" 404 2659
127.0.0.1 - - [14/Oct/2022:18:19:24 +0800] "GET /test/test4.php?file=/var/log/apache/access.log HTTP/1.1" 200 370
127.0.0.1 - - [14/Oct/2022:18:19:25 +0800] "GET /test/test4.php?file=/var/log/apache/access.log HTTP/1.1" 200 370
127.0.0.1 - - [14/Oct/2022:18:19:25 +0800] "GET /test/test4.php?file=/var/log/apache/access.log HTTP/1.1" 200 370
127.0.0.1 - - [14/Oct/2022:18:19:25 +0800] "GET /test/test4.php?file=/var/log/apache/access.log HTTP/1.1" 200 370
127.0.0.1 - - [14/Oct/2022:18:19:25 +0800] "GET /test/test4.php?file=/var/log/apache/access.log HTTP/1.1" 200 370
127.0.0.1 - - [14/Oct/2022:18:19:25 +0800] "GET /test/test4.php?file=/var/log/apache/access.log HTTP/1.1" 200 370
127.0.0.1 - - [14/Oct/2022:18:19:25 +0800] "GET /test/test4.php?file=/var/log/apache/access.log HTTP/1.1" 200 370
127.0.0.1 - - [14/Oct/2022:18:19:26 +0800] "GET /test/test4.php?file=/var/log/apache/access.log HTTP/1.1" 200 370
```



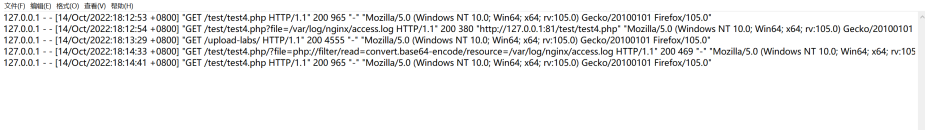
GTL—JU

我们可以通过在url参数中写入一句
句话木马写入到日志文件中，我们可
文件，从而进行命令执行。

没有过人的天赋，没有超人的运气，只有一如既往的坚持，没有原因，只是热爱。

日历

nginx服务器日志存放位置：/var/log/nginx/access.log
和/var/log/nginx/error.log



由本地日志文件可以看到nginx服务器中记录的是每次请求user-agent报文，那么我们可以通过包含nginx'服务器的日志文件，然后在user-agent服务器中写入木马语句进行注入

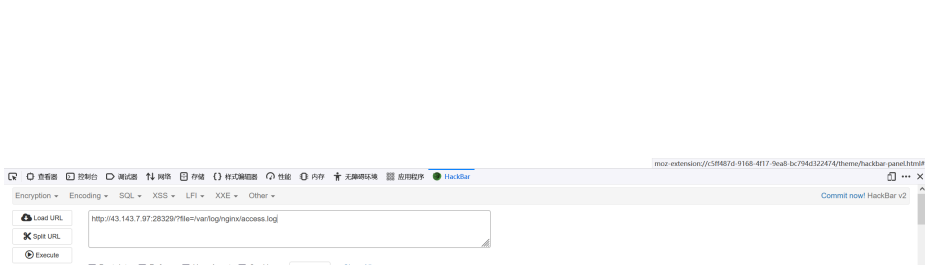
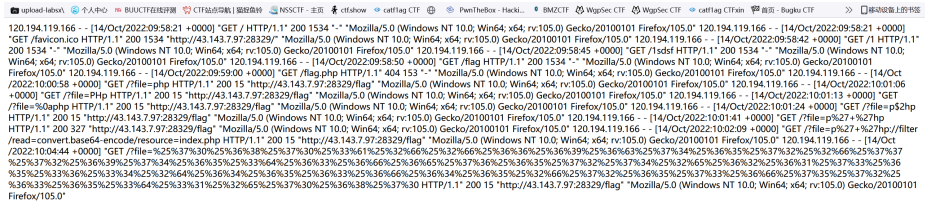
例：

```
<?php
//WEB手要懂得搜索

if (isset ($_GET ['file'])) {
    $file = $_GET ['file'];
    if (preg_match ("/php|flag|data|~|\\|@|_|#|\\$|_|%|^|&|*|(\\|\\-|\\_|\\+|=|/","die ("error");
}
include ($file);
} else {
    highlight_file (__FILE__);
}
```

过滤了很多，php和-被过滤导致不能使用php伪协议

通过产生报错，可以看到题目使用的服务器是nginx，访问默认日志文件



通过返回信息可以看到日志文件记录了传入参数的值以及user-agent的值

但是由于file通过正则匹配过滤了php所以我们无法在url参数里面直接写入木马，但是user-agent位置并没有进行过滤，所以我们可以在这里进行注入

可以通过包含这个日志文件，然后在user-agent报文里面添加木马，进行注入

<	2024年9月						>
日	一	二	三	四	五	六	
1	2	3	4	5	6	7	
8	9	10	11	12	13	14	
15	16	17	18	19	20	21	
22	23	24	25	26	27	28	
29	30		2	3	4	5	
6	7		9	10	11	12	

搜索

搜索关键词~

常用链接

- 我的随笔
- 我的评论
- 我的参与
- 最新评论
- 我的标签

我的标签

- web学习(25)
- CTF比赛wp(9)
- misc(1)
- 环境搭建(1)

随笔档案

- 2023年4月(1)
- 2023年3月(1)
- 2023年2月(5)
- 2022年12月(2)
- 2022年11月(4)
- 2022年10月(14)
- 2022年5月(1)
- 2022年4月(4)
- 2022年3月(5)

阅读排行榜

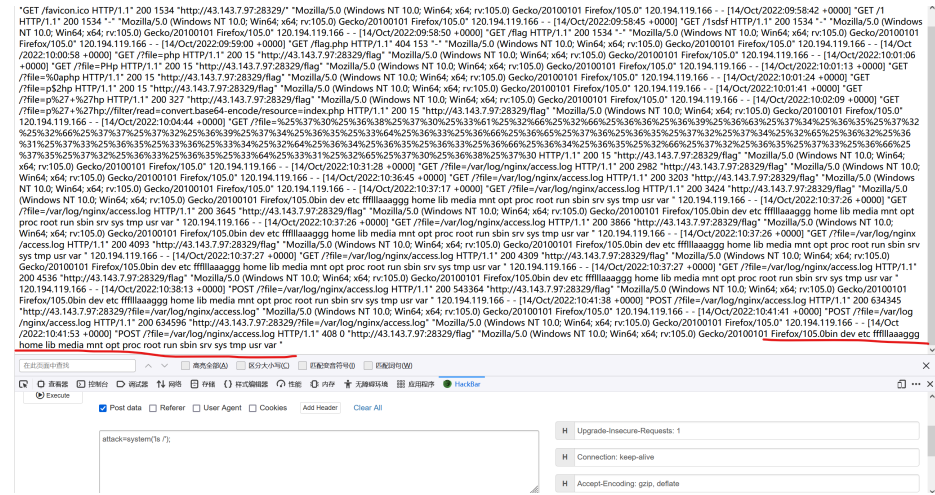
- 报错注入常用的三种注入方式(flool , extractvalue、updatexml)(6092)
- 对flask session伪造的学习(2113)
- sql注入之文件的读写-----上传一句活木马(1339)
- sql注入中关于group by 和 with n p 函数运用(1182)
- F5隐写(1080)

评论排行榜

- 对flask session伪造的学习(1)



通过执行phpinfo();发现以及执行成功。



标签: web学习

- 2. 网刃杯部分题目wp(1)
- 3. 报错注入常用的三种注入方式(flool , extractvalue、updatexml)(1)

推荐排行榜

- 1. NKCTF2023&数字人才挑战赛web部分wp(1)
- 2. 对flask session伪造的学习(1)
- 3. 报错注入常用的三种注入方式(flool , extractvalue、updatexml)(1)
- 4. sql注入----极客大挑战 (hardsql) (1)
- 5. sql注入----极客大挑战 (babysql) (1)

最新评论

- 1. Re:对flask session伪造的学习
如果直接把session储存在客户端，那和token机制有什么区别呢？不太懂

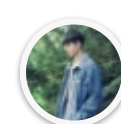
- 2. Re:网刃杯部分题目wp
大佬！

- 3. Re:报错注入常用的三种注入方式 (flool ,extractvalue、updatexml)
慕名而来

好文要顶

关注我

收藏该文



GTL_JU

粉丝 - 3 关注 - 1

+加关注

« 上一篇: 伪随机数种子爆破

» 下一篇: creat_function()代码注入

posted @ 2022-10-27 11:21

阅读(912)

评论(0)

会员力量, 点亮园子希望

刷新页面

返回顶部

登录后才能查看或发表评论, 立即 [登录](#) 或者 [逛逛](#) 博客园首页

https://www.cnblogs.com/GTL-JU/p/16831597.html

3/4



编辑推荐:

- 利用分布式锁在 ASP.NET Core 中实现防抖
- 写在临近40岁的年龄
- 一场 Kafka CRC 异常引发的血案
- 记录荒废了三年的四年.net开发的第三次面试
- 架构实战

阅读排行:

- 利用分布式锁在ASP.NET Core中实现防抖
- .NET 8.0 文档管理系统网盘功能的实现
- C#设计模式入门实战教程
- 图穷匕见-所有反DDD模式都是垃圾
- 神奇的C语言输出12天圣诞节歌词代码

