日志文件包含

发布于 2023-07-31 413 次阅读

- 当环境存在文件包含漏洞的时候,伪协议用不了,url_allow_include也没有开启,就可以尝试包含日志文件

方法

- 日志文件包含和sql的日志写马的原理类似,都是利用日志记录了查询语句,构造恶意的查询语句将木马写入到日志文件,然后利用文件包含漏洞包含日志文件执行木马
- 先看看日志文件长什么样子吧

```
127.0.0.1 - - [06/Aug/2022:16:02:22 +0800] "GET /sqli-labs-master/Less-1/ HTTP/1.1" 200 881
127.0.0.1 - - [06/Aug/2022:16:03:46 +0800] "GET /sqli-labs-master/Less-1/ HTTP/1.1" 200 557
127.0.0.1 - - [06/Aug/2022:16:04:01 +0800] "GET /sqli-labs-master/Less-1/%EF%BC%9Fid=1 HTTF
127.0.0.1 - - [06/Aug/2022:16:04:06 +0800] "GET /sqli-labs-master/Less-1/id=1 HTTP/1.1" 404 26
127.0.0.1 - - [06/Aug/2022:16:04:14 +0800] "GET /sqli-labs-master/Less-1/%EF%BC%9Fid=1 HTTF
127.0.0.1 - - [06/Aug/2022:16:04:23 +0800] "GET /sqli-labs-master/Less-1/?id=1 HTTP/1.1" 200 55
127.0.0.1 - - [06/Aug/2022:16:22:54 +0800] "GET /sqli-labs-master/ HTTP/1.1" 200 7933
127.0.0.1 - - [06/Aug/2022:16:22:54 +0800] "GET /sqli-labs-master/index.html_files/freemind2htm
127.0.0.1 - - [06/Aug/2022:16:22:54 +0800] "GET /sqli-labs-master/index.html_files/freemind2htm
127.0.0.1 - - [06/Aug/2022:16:22:54 +0800] "GET /sqli-labs-master/index.html_files/image.png H
127.0.0.1 - - [06/Aug/2022:16:22:56 +0800] "GET /sqli-labs-master/sql-connections/setup-db.php
127.0.0.1 - - [06/Aug/2022:16:23:18 +0800] "GET /sqli-labs-master/Less-1 HTTP/1.1" 301 249
127.0.0.1 - - [06/Aug/2022:16:23:18 +0800] "GET /sqli-labs-master/Less-1/ HTTP/1.1" 200 691
127.0.0.1 - - [06/Aug/2022:16:23:18 +0800] "GET /sqli-labs-master/images/Less-1.jpg HTTP/1.1" 2
127.0.0.1 - - [06/Aug/2022:16:23:29 +0800] "GET /sqli-labs-master/Less-1/?id=1 HTTP/1.1" 200 72
```

- ==可以看到,apache的默认日志记录了访问的路径,但是不一定在所有情况下都是如此,既然存在文件包含漏洞,可以先利用文件包含漏洞把文件包含进来看看日志文件记录了那些信息,再有针对性的构造,比如后面的例题就是日志文件记录了UA的信息而不是路径==
- 既然要包含日志文件,就需要知道日志文件的路径,常见路径如下

/var/log/httpd/access_log

(2) nginx 日志文件
日志文件在用户安装目录logs目录下
以我的安装路径为例/usr/local/nginx,
那我的日志目录就是在/usr/local/nginx/logs里

- 如果用户专门设置过,那么也可以先包含web服务器的配置文件,然后查找日志文件的路径

(1) apache+linux 默认配置文件
/etc/httpd/conf/httpd.conf
/etc/init.d/httpd

测试

- 这里拿[HNCTF 2022 WEEK2]easy_include做测试吧

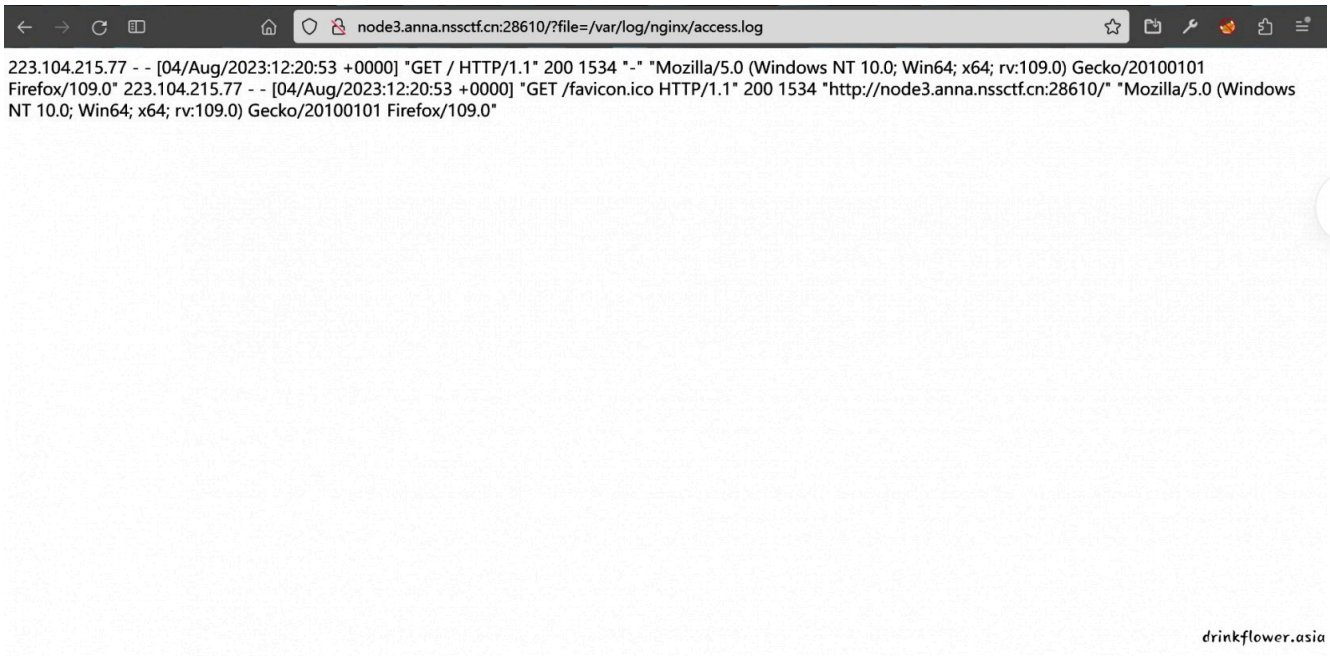
```
<?php
//WEB手要懂得搜索

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

- 过滤的比较死,无法直接读取flag 而且无法使用伪协议,尝试使用日志包含
- 无论是apache还是nginx,都有日志文件,当服务器在linux上面的时候其位置一般是

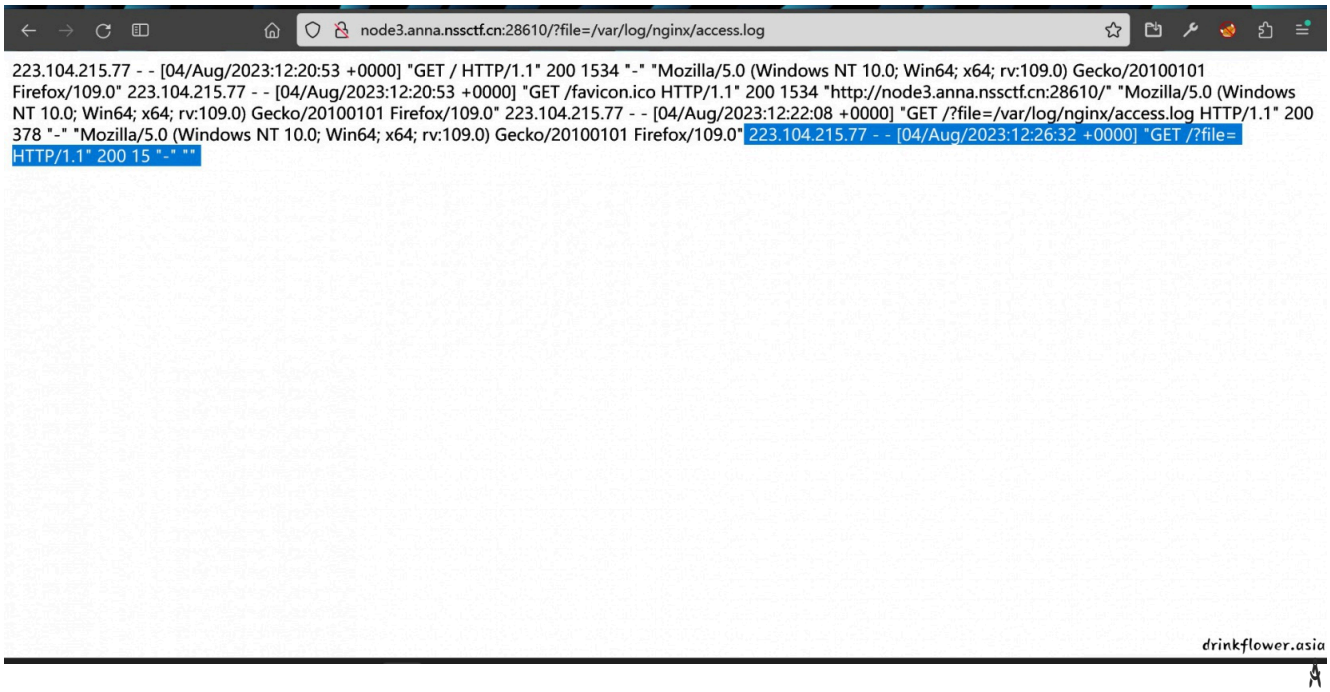
/var/log/apache/access.log
/var/log/nginx/access.log
/var/log/nginx/error.log

?file=/var/log/apache/access.log
?file=/var/log/nginx/access.log
?file=/var/log/nginx/error.log



(只有?file=/var/log/nginx/access.log有回显)

- 可以看到日志文件里面存的是访问者的UA和访问网址,那么我们可以构造一个含有木马的路径或者UA,即可将木马写入到日志文件
- 这里出了一点问题,可以看到,当路径和UA中有木马的时候会被自动过滤掉,不会被写入到文件,响应的字段都是空的



- 卡了很久,最后发现原来可以rce,只是不知道为什么不能写马