

- 日志分析课程不考虑日志被删除的情况
 - 删除日志需要管理员权限，且删除日志本身也会留下日志
 - 删除日志的操作会被日志记录设备告警
 - 删除只能删除在受害者机器上的日志，日志设备中的日志不会受影响

一、日志介绍

- 为什么要使用日志
 - 可以在故障刚刚发生时就向用户发送警告信息
 - 可以用来决定故障的根本原因或缩小系统攻击范围
- 分析日志的意义：
 - 如今各式各样的漏洞层出不穷，五花八门的入侵工具更是令人眼花缭乱，稍微懂点网络知识的人都可以利用各种入侵工具进行入侵
 - 虽然经过精心配置的服务器可以抵御大部分入侵，但伴随着新漏洞的出现，也不能保证一台服务器长时间不会被入侵，所以如何检测入侵者行动以保证服务器安全性就会显得十分重要
 - 通过日志，可以分析出各种网络可疑行为、违规操作、敏感信息，协助定位安全事件源头和调查取证，防范和发现计算机网络犯罪活动
- 常见的中间件



Apache



WebLogic
DEVELOPER'S JOURNAL



NGINX
http server

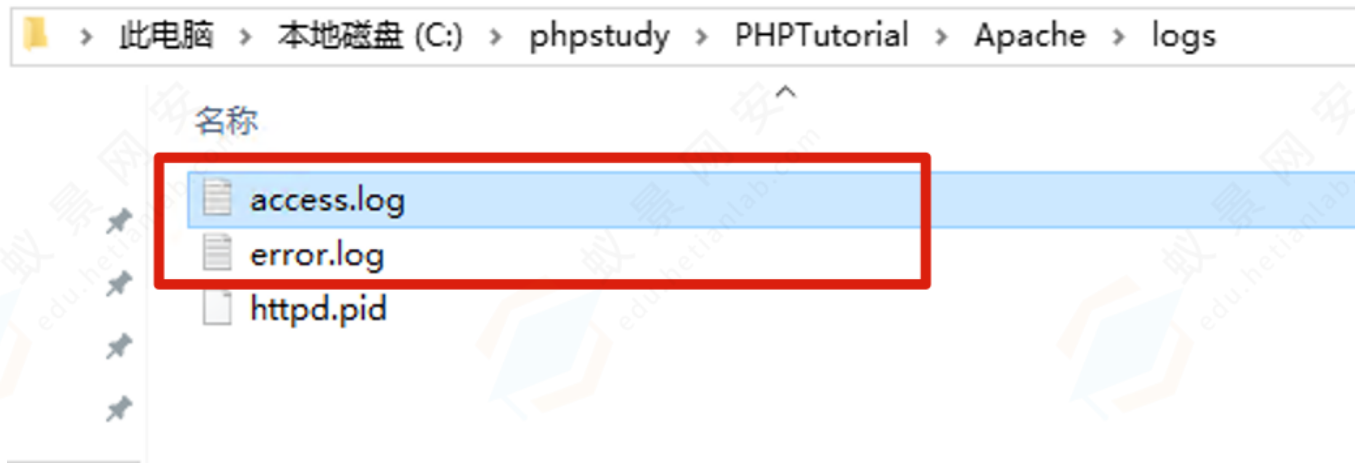
- 中间件日志的关键点

1. 对访问时间进行统计，可以得到服务器在某些时间段的访问情况
2. 对IP进行统计，可以得到用户的分布情况
3. 对请求URL的统计，可以得到网站页面关注情况
4. 对错误请求的统计，可以更正有问题的页面

1. apache

- 日志存放位置
 - Apache日志存放位置

- windows系统，日志文件保存在Apache安装目录的logs子目录中



- Linux系统，默认安装的情况下，在 /var/log/apache2/下

```
(root@kali)-[/var/log/apache2]
# ls
access.log  error.log  error.log.1  error.log.2.gz  other_vhosts_access.log
```

- 可以通过配置文件查看这些日志文件配置到了什么地方

```
<IfModule log_config_module>
#
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common

<IfModule logio_module>
# You need to enable mod_logio.c to use %I and %O
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
</IfModule>

#
# The location and format of the access logfile (Common Logfile Format).
# If you do not define any access logfiles within a <VirtualHost>
# container, they will be logged here. Contrariwise, if you *do*
# define per-<<VirtualHost> access logfiles, transactions will be
# logged therein and *not* in this file.
#
CustomLog "logs/access.log" common


#
# If you prefer a logfile with access, agent, and referer information
# (Combined Logfile Format) you can use the following directive.
#
#CustomLog "logs/access.log" combined
</IfModule>
```

如果实在找不到：

- Linux: `find / -name="access.log" 2>/dev/null`




```
(root@kali)-[/var/log/apache2]
# find / -name "access.log" 2>/dev/null
/var/log/nginx/access.log
/var/log/apache2/access.log
/var/lib/docker/overlay2/45a43b14bd0a0cc13156d3e56ac
```

- windows: everything <https://www.voidtools.com/zh-cn/>

 access.log - Everything

文件(F) 编辑(E) 视图(V) 搜索(S) 书签(B) 工具(T) 帮助(H)

access.log

名称	路径
 access.log	C:\phpstudy\PHPTutorial\Apache\logs
 access.log	C:\phpstudy\PHPTutorial\nginx\logs
 access.log.lnk	C:\Users\Administrator\AppData\Roamin...

- apache标准中规定了4类日志，分别为：

1. 错误日志
2. 访问日志
3. 传输日志
4. Cookie日志

传输日志 与 Cookie 日志现已废除

- 访问日志介绍 (access_log)
 - access_log 为访问日志，记录所有对 apache 服务器进行请求的访问

访问的IP	浏览时间	访问的资源	使用的浏览器
192.168.3.3	[14/Feb/2020:23:01:04 +0800]	"GET /del.php HTTP/1.1" 200 1220 "http://192.168.3.17/del.php"	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
192.168.3.3	[14/Feb/2020:23:20:15 +0800]	"GET /del.php HTTP/1.1" 200 1220 "http://192.168.3.17/add.php"	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
192.168.3.3	[14/Feb/2020:23:20:15 +0800]	"GET /del.php HTTP/1.1" 200 1220 "http://192.168.3.17/del.php"	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36

1. 远程主机IP：表明访问网站的是谁
2. 空白（Email）：为了避免用户的邮箱被垃圾邮件骚扰，第二项用 "-" 取代
3. 空白（登录名）：记录浏览者进行身份验证时提供的名字
4. 请求时间：[] 中的内容是时间，最后的+0800表示服务器所处时区位于UTC之后8小时
5. 方法+资源+协议：服务器收到的是一个什么样的请求，格式为 "方法 资源 协议"

- 6. 状态代码：请求是否成功，或是遇到了什么样的错误
- 7. 发送字节数：表示发送给客户端的字节数，告诉我们传输是否被打断

- 错误日志介绍 (error_log)
 - 错误日志记录了服务器运行期间遇到的各种错误，以及一些普通的诊断信息，比如服务器何时启动、何时关闭等
 - 错误日志的一般格式：

日期和时间	错误等级	错误消息
[Fri Feb 14 20:42:19.767790 2020]	[auth_digest:notice] [pid 873] AH01757:	generating secret for digest authentication ...
[Fri Feb 14 20:42:19.770668 2020]	[lbmethod_heartbeat:notice] [pid 873] AH02282:	No slotmem from mod_heartbeat
[Fri Feb 14 20:42:20.032032 2020]	[mpm_prefork:notice] [pid 873] AH00163:	Apache/2.4.6 (CentOS) PHP/5.4.16 configured -- resuming normal operations
[Fri Feb 14 20:42:20.032123 2020]	[core:notice] [pid 873] AH00094:	Command line: '/usr/sbin/httpd -D FOREGROUND'
[Wed May 13 22:24:55.152421 2020]	[suexec:notice] [pid 838] AH01232:	suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.localdomain. Set the 'ServerName' directive global to suppress this message		
[Wed May 13 22:24:55.314153 2020]	[auth_digest:notice] [pid 838] AH01757:	generating secret for digest authentication ...
[Wed May 13 22:24:55.314954 2020]	[lbmethod_heartbeat:notice] [pid 838] AH02282:	No slotmem from mod_heartbeat
[Wed May 13 22:24:56.664164 2020]	[mpm_prefork:notice] [pid 838] AH00163:	Apache/2.4.6 (CentOS) PHP/5.4.16 configured -- resuming normal operations
[Wed May 13 22:24:56.664362 2020]	[core:notice] [pid 838] AH00094:	Command line: '/usr/sbin/httpd -D FOREGROUND'

- 注意：默认情况下 Apache 在发生warn及以上事件时会记录，这个级别在配置文件中可以进行修改

```
ErrorLog "logs/error_log"

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel error
```

- 1. debug：最详细的日志级别，记录所有调试信息，通常只在开发和测试环境中使用。
- 2. info：记录有关正常操作的信息，例如服务器启动和停止、模块加载等。
- 3. notice：记录需要注意但不是错误的事件，例如非致命性的配置问题或客户端请求的异常情况。
- 4. warn：记录警告信息，表示可能存在问题，但不会影响系统的正常运行。
- 5. error：记录错误信息，表示出现了某种错误，但仍然可以继续运行。
- 6. crit：记录严重错误信息，表示出现了严重问题，需要立即采取措施解决。
- 7. alert：记录需要立即采取行动的事件，例如硬件故障或安全漏洞。
- 8. emerg：记录紧急事件，表示系统已经无法正常运行，需要立即采取行动。
- 查看日志时，经常使用的命令

- 1. 查看 IP

```
cat access.log | awk '{print $1}'
```

```
192.168.97.1
192.168.97.1
192.168.97.1
192.168.97.1
192.168.3.3
192.168.3.3
192.168.3.3
192.168.3.3
192.168.3.3
```

2. 显示访问前10位的IP地址，便于查找攻击源

```
cat access.log|awk '{print $1}'|sort|uniq -c|sort -nr|head -10
```

```
[root@localhost logs]# cat access_log | awk '{print $1}' | sort|uniq -c |sort -nr|head -10
 46 192.168.97.1
 30 192.168.3.3
  5 172.16.206.1
```

3. 显示指定时间以后的日志

```
cat access.log |awk '$4>="[1/Jan/2020:00:00:00"'
```

```
192.168.3.3 - - [14/Feb/2020:22:51:20 +0800] "GET /logout.php HTTP/1.1" 302 - "http://192.168.3.17/add.php" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_0; rv:80.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36"
192.168.3.3 - - [14/Feb/2020:22:51:20 +0800] "GET /login.php HTTP/1.1" 200 1055 "http://192.168.3.17/add.php" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_0; rv:80.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36"
192.168.3.3 - - [14/Feb/2020:22:51:23 +0800] "POST /login.php HTTP/1.1" 302 1396 "http://192.168.3.17/login.php" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_0; rv:80.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36"
192.168.3.3 - - [14/Feb/2020:22:51:23 +0800] "GET /add.php HTTP/1.1" 200 1437 "http://192.168.3.17/login.php" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_0; rv:80.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36"
192.168.3.3 - - [14/Feb/2020:22:51:23 +0800] "GET /add.php HTTP/1.1" 200 1437 "http://192.168.3.17/add.php" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_0; rv:80.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36"
```

4. 查看某一时间内的IP连接情况

```
grep "2020:05"access.log |awk '{print $4}'|sort|uniq -c |sort -nr
```

```
[root@localhost logs]# grep "2020:23" access_log | awk '{print $4}' | sort|uniq -c |sort -nr
  3 [14/Feb/2020:23:00:58
  2 [14/Feb/2020:23:20:15
  2 [14/Feb/2020:23:01:04
  2 [14/Feb/2020:23:00:47
  2 [14/Feb/2020:23:00:44
  2 [14/Feb/2020:23:00:15
  1 [14/Feb/2020:23:00:43
  1 [14/Feb/2020:23:00:17
```

5. 查看指定的IP做了什么

```
cat access.log |grep 192.168.3.3| awk '{print 1"\t"$8}'| sort|uniq -c |sort -nr|less
```

```
[root@localhost logs]# cat access_log |grep 192.168.3.3|awk '{print $1"\t"$8}' |sort|uniq -c|sort -nr|less
 30 192.168.3.3      HTTP/1.1"
```

6. 查看最近访问量最高的文件

cat access.log |tail 10000| awk '{print \$7}' | sort|uniq -c |sort -nr|less

```
root@localhost logs]# cat access_log |tail -10000|awk '{print $7}'|sort|uniq -c |sort -nr|less
11 /add.php
7 /
5 /login.php
4 /reg.php
4 /del.php
3 /page_3.php?id=1
3 /page_2.php?id=1%27%20and%201=2%20union%20select%201,user(),3%23
3 /page_2.php?id=1
3 /page_1.php?id=1
3 /logout.php
3 /favicon.ico
2 /page_3.php?id=1%27%20and%201=2%20union%20select%201,user(),3%23
2 /page_3.php?id=1%27
2 /page_2.php?id=1%27
```

2. iis

- IIS提供了一套相当有效的安全管理机制，并且也提供了一套强大的日志文件系统
 - 通过对日志文件的监测，可以找出有疑问的痕迹、得到网站的访问、操作记录、以及系统的问题所在
 - IIS日志记录了网站服务器接收，处理请求以及运行错误等各种原始信息
 - 即它可以记录访问者的一举一动，不管访问者是访问网站，还是上传文件，不管是成功还是失败，日志都以进行记录

windows server 如何安装 IIS 服务器：



- IIS7.5: %SystemDrive%\inetpub\logs\LogFiles
- IIS6.0: %systemroot%\system32\logfiles\w3svc1

```
2020-03-26 07:14:30 192.168.124.51 GET / - 80 - 192.168.124.55 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:74.0)Firefox/74.0 200 0 0 62
2020-03-26 07:14:30 192.168.124.51 GET /css/css.css - 80 - 192.168.124.55 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:74.0)Firefox/74.0 200 0 0 0
2020-03-26 07:14:30 192.168.124.51 GET /css/menu.css - 80 - 192.168.124.55 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:74.0)Firefox/74.0 200 0 0 0
2020-03-26 07:14:30 192.168.124.51 GET /js/jquery.js - 80 - 192.168.124.55 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:74.0)Firefox/74.0 200 0 0 0
```

- 访问时间: 2020-03-26 07:14:30
- 所访问的服务器IP地址: 192.168.124.51
- 执行的操作: GET /css/css.css
- 访问的端口: 80
- 客户端IP地址: 192.168.124.55
- 浏览器的类型: Mozilla/5.0+
- 系统相关信息: (Windows+NT+10.0;+Win64;+x64;+rv:74.0)
- 操作代码状态: 200 (正常)
- Wondows状态代码: 0 (操作成功完成)

3. 日志分析工具

- 360 星图

1. 配置

修改配置文件: /conf/config.ini, 指定日志文件路径或者日志文件目录

```
1 #360星图系统配置文件
2
3 #日志文件存放路径, 可以是直接目录也可以是文件, (如: d:\logs\1.log 或 d:\logs\, 如果使用d:\logs
4 log_file:C:\phpstudy\PHPTutorial\Apache\logs\access.log
5
6 #日志文件类型设置, 1:自动识别iis/apache/nginx日志 2:自定义格式
7 xingtu_logtype:1
8
9 #是否生成Html分析报告(包括常规报告及安全分析报告), 1:不开启;2:开启
10 common_analysis:2
11
12 #默认host, 建议替换default为网站域名, 不带http://
13 host:default
```

2. 启动

双击打开 start.bat,开始自动日志分析

```
C:\Windows\system32\cmd.exe

*****

360星图-Web日志分析引擎
Copyright©2014 360网站卫士 [http://wangzhan.360.cn]
交流QQ群: 12803537

*****

运行前检查...
设置的host为:default
日志路径为:C:\phpstudy\PHPTutorial\Apache\logs\access.log
加载系统配置文件:C:\Users\Administrator\Downloads\360星图网站日志分析\xingtu_full网站日志分析\conf\config.ini
加载分析规则文件:C:\Users\Administrator\Downloads\360星图网站日志分析\xingtu_full网站日志分析\conf\rules.ini
当前分配的系统内存为: 437M
检查完毕!

开始分析,请耐心等待(分析1G日志大约需要200秒)...

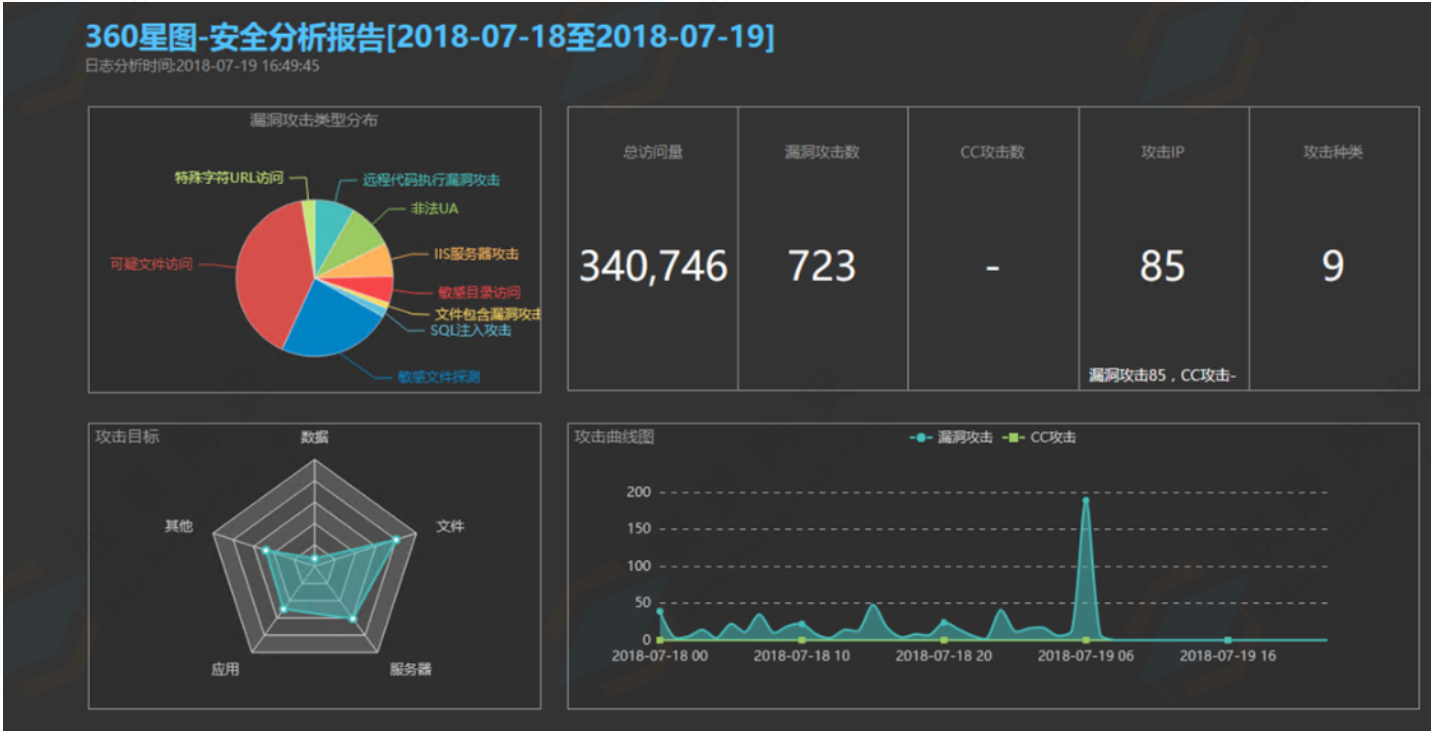
当前文件为: access.log;文件大小为: 0K

本次进行了[Web攻击分析、日常分析]
共分析了5条访问日志
分析耗时:18秒
其中异常访问0条
常规日志分析报告已生成

分析结果请打开[星图安装目录result文件夹]查看
本次分析完成!
```

3. 结果

打开 result 文件夹可以查看分析结果



360星图	360星图-常规日志分析报告					
数据概况	日志分析时间:2018-07-19 16:49:45					
IP流量分析	数据概况					
访问页面分析	总访问量	PV数	UV数	独立IP数	异常访问数	消耗流量
静态资源请求分析	340,746	45,131	24,086	16,488	14,249	-
死链分析	IP流量分析(TOP200)					
来源分析	基于IP，分析IP对应地域、访问量、流量消耗					
搜索引擎爬虫分析	ID	访问次数	访问占比	IP	国家/地区	流量
关键字分析	1	10,180	2.988%	222.88.94.218	中国-河南洛阳	-
地域分布	2	3,850	1.130%	120.24.255.192	中国-浙江杭州	-
操作系统分析	3	1,743	0.512%	59.175.199.99	中国-湖北武汉	-
浏览器分析	4	1,618	0.475%	59.175.199.97	中国-湖北武汉	-
状态码分析	5	1,512	0.444%	123.126.68.102	中国-北京	-
	6	1,259	0.369%	39.104.53.180	中国-香港	-
	7	1,206	0.354%	112.125.89.4	中国-北京	-
	8	1,057	0.310%	118.190.215.68	中国-中国	-
	9	1,025	0.301%	61.183.175.0	中国-湖北武汉	-

• http Logs Viewer

http Logs Viewer						
File Edit Reports Statistics Node Graph Help						
Sort Filter Status IP Address All						
Advanced Filter Date Request User Agent Referer						
access.log						
IP Address	Date	Request	Sta...	Size	Country	
127.0.0.1	2023/9/26 14:50:23	GET / HTTP/1.1	200	11	N/A	
127.0.0.1	2023/9/26 14:50:26	GET /dwwa/ HTTP/1.1	302	148	N/A	
127.0.0.1	2023/9/26 14:50:26	GET /dwwa/login.php HTTP/1.1	200	1543	N/A	
127.0.0.1	2023/9/26 14:50:29	POST /dwwa/login.php HTTP/1.1	302	148	N/A	
127.0.0.1	2023/9/26 14:50:29	GET /dwwa/login.php HTTP/1.1	200	1582	N/A	
127.0.0.1	2023/9/26 15:54:38	GET / HTTP/1.1	200	11	N/A	
127.0.0.1	2023/9/26 15:58:17	GET / HTTP/1.1	200	11	N/A	

http Logs Viewer							
File Edit Reports Statistics Node Graph Help							
Sort Filter Status IP Address All Apply Filter							
Advanced Filter Date Request User Agent Referer							
access.log access.log							
IP Address	Date	Request	Sta...	Size	Country	Referer	User Agent
127.0.0.1	2023/9/26 14:50:23	GET / HTTP/1.1	200	11	N/A		
127.0.0.1	2023/9/26 14:50:26	GET /dwwa/ HTTP/1.1	302	148	N/A		
127.0.0.1	2023/9/26 14:50:26	GET /dwwa/login.php HTTP/1.1	200	1543	N/A		
127.0.0.1	2023/9/26 14:50:29	POST /dwwa/login.php HTTP/1.1	302	148	N/A		
127.0.0.1	2023/9/26 14:50:29	GET /dwwa/login.php HTTP/1.1	200	1582	N/A		
127.0.0.1	2023/9/26 15:54:38	GET / HTTP/1.1	200	11	N/A		
127.0.0.1	2023/9/26 15:58:17	GET / HTTP/1.1	200	11	N/A		
127.0.0.1	2023/9/26 16:10:07	POST /dwwa/login.php HTTP/1.1	302	148	N/A	http://127.0.0.1/dwwa/login.php	Mozilla/5.0 (Windows NT...
127.0.0.1	2023/9/26 16:10:07	GET /dwwa/login.php HTTP/1.1	200	1582	N/A	http://127.0.0.1/dwwa/login.php	Mozilla/5.0 (Windows NT...
127.0.0.1	2023/9/26 16:10:07	POST /dwwa/login.php HTTP/1.1	302	148	N/A	http://127.0.0.1/dwwa/login.php	Mozilla/5.0 (Windows NT...
127.0.0.1	2023/9/26 16:10:07	GET /dwwa/login.php HTTP/1.1	200	1582	N/A	http://127.0.0.1/dwwa/login.php	Mozilla/5.0 (Windows NT...
127.0.0.1	2023/9/26 16:10:10	GET /dwwa/login.php?wafaw HTTP/1.1	404	218	N/A	-	Mozilla/5.0 (Windows NT...