

ctf (seelog)

原创

[cs_xiaoqiang](#) 于 2018-01-17 19:49:03 发布 1588 收藏 2

分类专栏: [安全 ctf](#) 文章标签: [ctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/cs_xiaoqiang/article/details/79088874

版权



[安全](#) 同时被 2 个专栏收录

11 篇文章 0 订阅

订阅专栏



[ctf](#)

4 篇文章 0 订阅

订阅专栏

这次要说的和上篇一样, 也是一道春秋下的ctf。

给的题目如下图:



依旧是找flag, 题目为seelog, 直接访问连接 <http://106.75.86.18:3333>

本站是内部网站 非请勿入！

http://blog.csdn.net/cs_xiaoqiang

给出的提示是：不是内部网站。我第一时间想到的是会不会这个服务器上还有其他的网站，进过尝试发现方向不对。再仔细从头看，题目为seelog（看日志），解题思路应该与log有关。经过无数的尝试，发现在url后面加上log就可以访问到日志。

Index of /log

Name	Last modified	Size	Description
 Parent Directory	-		
 access.log	2017-10-17 14:40	11M	
 error.log	2017-10-17 14:40	266K	

Apache/2.4.7 (Ubuntu) Server at 106.75.86.18 Port 3333

http://blog.csdn.net/cs_xiaoqiang

逐个访问日志文件，先访问error.log，仔细查找发现里面全部是出错是产生的日志文件。再访问access.log，发现里面大部分也是访问出错是产生的日志文件，还可以看到访问者的ip和访问状态码，以172开头的，一看就是内网。

```

172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] GET /bbs/s8diy.asp HTTP/1.1 404 450 - -
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /upfile.asp HTTP/1.1" 404 447 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /admin_index.asp HTTP/1.1" 404 452 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /reg_upload.asp HTTP/1.1" 404 451 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /bin/login.asp HTTP/1.1" 404 450 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /app/login.asp HTTP/1.1" 404 450 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /bbs/upfile.asp HTTP/1.1" 404 451 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /dzmanager/login.asp HTTP/1.1" 404 456 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /aspcheck/aspcheck.asp HTTP/1.1" 404 458 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /mgyg/admin/login.asp HTTP/1.1" 404 457 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /asp/login.asp HTTP/1.1" 404 450 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /SouthidcEditor/admin_style.asp HTTP/1.1" 404 467 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /eWebEditor/Admin_Default.asp HTTP/1.1" 404 465 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /eWebEditor/Admin_Style.asp HTTP/1.1" 404 463 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /eWebEditor/Upload.asp HTTP/1.1" 404 458 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /eWebEditor/Admin_UploadFile.asp HTTP/1.1" 404 468 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /eWebEditor/eWebEditor.asp HTTP/1.1" 404 462 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /eWebEditor/Admin_Modipwd.asp HTTP/1.1" 404 465 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /flyang/include/Cls_Data.asp HTTP/1.1" 404 464 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /managesite/login.asp HTTP/1.1" 404 457 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /eWebEditor/Admin_Login.asp HTTP/1.1" 404 463 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /WebEdit/db/dbwebedit%23cc495898.asp HTTP/1.1" 404 470
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /admin/manage/login.asp HTTP/1.1" 404 459 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /master/Login.asp HTTP/1.1" 404 453 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /FCKeditor/_samples/asp/sample03.asp HTTP/1.1" 404 472
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /include/FileUpload/admin_upfile.asp HTTP/1.1" 404 472
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /admin/editubb/ewebeditor.asp HTTP/1.1" 404 465 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /admin/southidceditor/admin/admin_login.asp HTTP/1.1"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /admin/editubb/db/dbwebedit%23cc495898.asp HTTP/1.1"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /FCKeditor/_samples/asp/sample02.asp HTTP/1.1" 404 472
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /FCKeditor/_samples/asp/sample04.asp HTTP/1.1" 404 472

```

有状态码，那就可以进行搜索了。搜索正常访问的状态码200，由于所有的状态码前面都有空格，所以搜索的时候也要加上空格，不然搜索的就是包含有200的这个路径了。

```

172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] GET /SouthidcEditor/admin_style.asp HTTP/1.1 404
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /eWebEditor/Admin_Default.asp HTTP/1.1" 404 46
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /eWebEditor/Admin_Style.asp HTTP/1.1" 404 463
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /eWebEditor/Upload.asp HTTP/1.1" 404 458 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /eWebEditor/Admin_UploadFile.asp HTTP/1.1" 404
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /eWebEditor/eWebEditor.asp HTTP/1.1" 404 462
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /eWebEditor/Admin_Modipwd.asp HTTP/1.1" 404 46
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /flyang/include/Cls_Data.asp HTTP/1.1" 404 464
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /managesite/login.asp HTTP/1.1" 404 457 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /eWebEditor/Admin_Login.asp HTTP/1.1" 404 463
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /WebEdit/db/dbwebedit%23cc495898.asp HTTP/1.1"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /admin/manage/login.asp HTTP/1.1" 404 459 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /master/Login.asp HTTP/1.1" 404 453 "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /FCKeditor/_samples/asp/sample03.asp HTTP/1.1"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /include/FileUpload/admin_upfile.asp HTTP/1.1"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /admin/editubb/ewebeditor.asp HTTP/1.1" 404 46
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /admin/southidceditor/admin/admin_login.asp HT
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /admin/editubb/db/dbwebedit%23cc495898.asp HTT
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /FCKeditor/_samples/asp/sample02.asp HTTP/1.1"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /FCKeditor/_samples/asp/sample04.asp HTTP/1.1"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /FCKeditor/_samples/asp/sample04.asp HTTP/1.1"

```

200 高亮全部(A) 区分大小写(C) 词句匹配(W) 第 56 项, 共找到 56 个匹配项

逐个查找发现有三个状态码为200的，分别是 /index.html 、 /log 、 /wojiushiHouTai888/denglU.php?username=admin&password=af3a-6b2115c9a2c0&submit=%E7%99%BB%E5%BD%95 。

```

2. 16. 3. 1 - - [12/Oct/2016:07:54:50 +0000] "GET /adminmember HTTP/1.1" 404 458
2. 16. 3. 1 - - [12/Oct/2016:07:54:50 +0000] "GET /lwadmin/admlogin.htm HTTP/1.1" 404 458
2. 16. 3. 1 - - [12/Oct/2016:07:54:50 +0000] "GET /addmember HTTP/1.1" 404 446 "-" "-"
2. 16. 3. 1 - - [12/Oct/2016:07:54:50 +0000] "GET /index.html HTTP/1.1" 200 662 "-" "-"
2. 16. 3. 1 - - [12/Oct/2016:07:54:50 +0000] "GET /logout HTTP/1.1" 404 443 "-" "-"
2. 16. 3. 1 - - [12/Oct/2016:07:54:50 +0000] "GET /admin_edit HTTP/1.1" 404 447 "-" "-"
2. 16. 3. 1 - - [12/Oct/2016:07:54:52 +0000] "GET /macadmin HTTP/1.1" 404 445 "-" "-"
2. 16. 3. 1 - - [12/Oct/2016:07:54:52 +0000] "GET /Legman HTTP/1.1" 404 443 "-" "-"
2. 16. 3. 1 - - [12/Oct/2016:07:54:52 +0000] "GET /log/ HTTP/1.1" 200 670 "-" "-"
2. 16. 3. 1 - - [12/Oct/2016:07:54:52 +0000] "GET /log HTTP/1.1" 301 525 "-" "-"
2. 16. 3. 1 - - [12/Oct/2016:07:54:52 +0000] "GET /loginok HTTP/1.1" 404 444 "-" "-"
2. 16. 3. 1 - - [12/Oct/2016:07:54:52 +0000] "GET /links HTTP/1.1" 404 442 "-" "-"
2. 16. 3. 1 - - [12/Oct/2016:07:54:52 +0000] "GET /manage/login%7Bext%7D HTTP/1.1" 404 45
2. 16. 3. 1 - - [12/Oct/2016:07:54:52 +0000] "GET /oa/ewebeditor/admin_login.asp HTTP/1.1" 404 466 "-" "-"
2. 16. 3. 1 - - [12/Oct/2016:07:54:48 +0000] "GET /inc/Editor/admin_login.asp HTTP/1.1" 404 463 "-" "-"
2. 16. 3. 1 - - [12/Oct/2016:07:54:48 +0000] "GET /wojiushiHouTai888/denglU.php?username=admin&password=af3a-6b2115c9a2c0&submit=%E7%99%BB%E5%BD%95 HTTP/1.1" 200 771
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36
2. 16. 3. 1 - - [12/Oct/2016:07:54:48 +0000] "GET /modules/ewebeditor/admin_login.asp HTTP/1.1" 404 471 "-" "-"

```

逐个访问，前面两个都访问失败。只有第三个访问成功，是一个登陆窗口，而flag就在登陆窗口的下面



http://blog.csdn.net/cs_xiaoqiang

需要注意的是：最后访问的ip是http://106.75.86.18:3333加上找到的路径，而不是172.16.3.1，不要看到日志里面这个ip访问的是正常的状态码。172开头的是内网，而我们是访问不到的。

最后将找到的flag填到一开始的网站就完成了。



到这里，就全部完成了。

