i春秋 流量分析 200分

原创

H9_dawn 于 2020-04-11 16:57:40 发布 298 收藏

分类专栏： CTF 文章标签： web 安全

本文链接：https://blog.csdn.net/qq_43622442/article/details/105455160

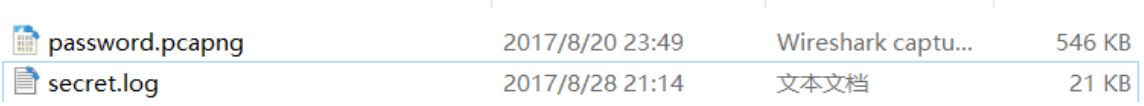
CTF 专栏收录该内容

20 篇文章 2 订阅

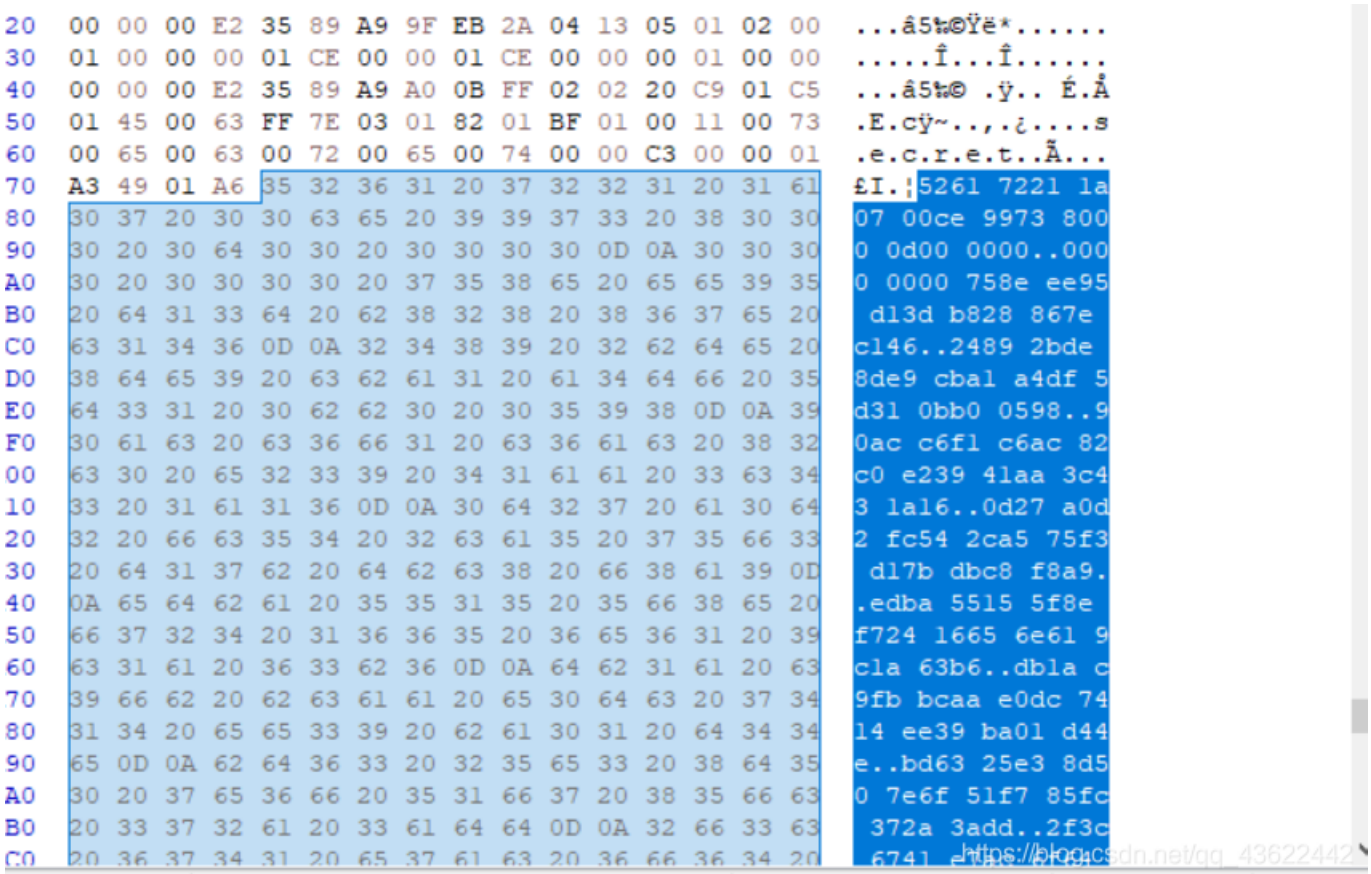
订阅专栏

i春秋 流量分析 200分

1.下载源码发现，比之前多了一个log文件，肯定是有问题的：



2.直接用HxD打开log文件，发现基本上看不懂，这里有点奇怪：



3.我是想新建一个HxD复制进去的，结果发现每次都是复制的左侧的16进制，所以我先把右边的复制进一个txt文件：

```
5261 7221 1a07 00ce 9973 8000 0d00 0000
0000 0000 758e ee95 d13d b828 867e c146
2489 2bde 8de9 cba1 a4df 5d31 0bb0 0598
90ac c6f1 c6ac 82c0 e239 41aa 3c43 1a16
0d27 a0d2 fc54 2ca5 75f3 d17b dbc8 f8a9
edba 5515 5f8e f724 1665 6e61 9c1a 63b6
db1a c9fb bcaa e0dc 7414 ee39 ba01 d44e
bd63 25e3 8d50 7e6f 51f7 85fc 372a 3add
2f3c 6741 e7ac 6f64 e479 2439 758e ee95
d13d b828 32d0 48e0 2f32 9f08 e909 5a52
937e 526b
```

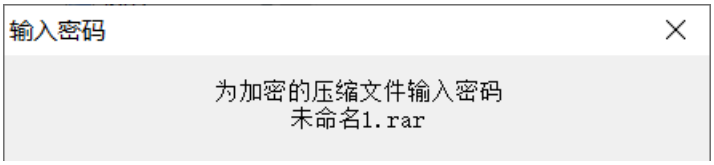

4.然后再复制粘贴进HxD：

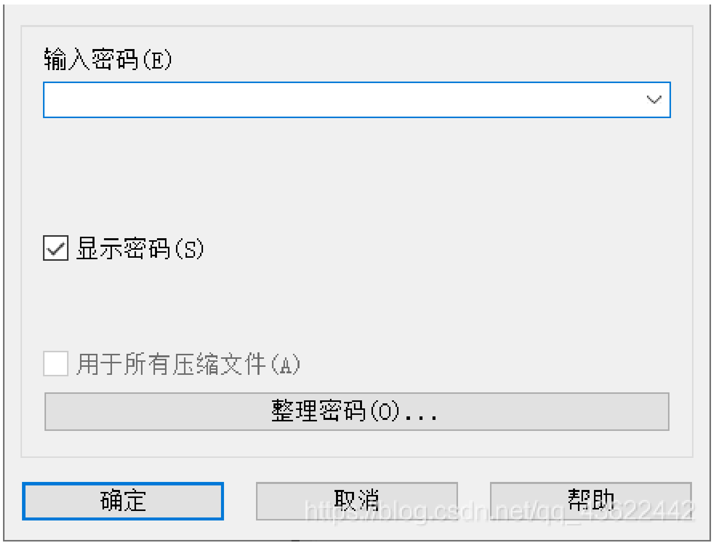
et(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	对应文本
0000	52	61	72	21	1A	07	00	CE	99	73	80	00	0D	00	00	00	Rar!...Î™s€.....
0010	00	00	00	00	75	8E	EE	95	D1	3D	B8	28	86	7E	C1	46	....uŽî•Ñ=¸(†~ÁF
0020	24	89	2B	DE	8D	E9	CB	A1	A4	DF	5D	31	0B	B0	05	98	$‰+Þ.éË¡¤ß]1.°.˜
0030	90	AC	C6	F1	C6	AC	82	C0	E2	39	41	AA	3C	43	1A	16	.¬ÆñÆ¬‚Àâ9Aª<C..
0040	0D	27	A0	D2	FC	54	2C	A5	75	F3	D1	7B	DB	C8	F8	A9	.' ÒüT,¥uóÑ{ÛÈø©
0050	ED	BA	55	15	5F	8E	F7	24	16	65	6E	61	9C	1A	63	B6	íºU._Ž÷$.enaœ.c¶
0060	DB	1A	C9	FB	BC	AA	E0	DC	74	14	EE	39	BA	01	D4	4E	Û.Éû¼ªàÜt.î9º.ÔN
0070	BD	63	25	E3	8D	50	7E	6F	51	F7	85	FC	37	2A	3A	DD	½c%ã.P~oQ÷…ü7*:Ý
0080	2F	3C	67	41	E7	AC	6F	64	E4	79	24	39	75	8E	EE	95	/<gAç¬odäy$9uŽî•
0090	D1	3D	B8	28	32	D0	48	E0	2F	32	9F	08	E9	09	5A	52	Ñ=¸(2ÐHà/2Ÿ.é.ZR
00A0	93	7E	52	6B													"~Rk

5.看到了rar头，那么我们把这个数据包 文件-》另存为：未命名1.rar

secret.log	2017/8/28 21:14	文本文档	21 KB
未命名1.rar	2020/4/11 16:35	WinRAR 压缩文件	1 KB

6.发现直接解压的话需要密码：





7.那密码肯定就在鲨鱼包里了，这次我学乖了，上来就追踪流，看看干了些啥，有些什么不同。翻着翻着发现了卡住了：

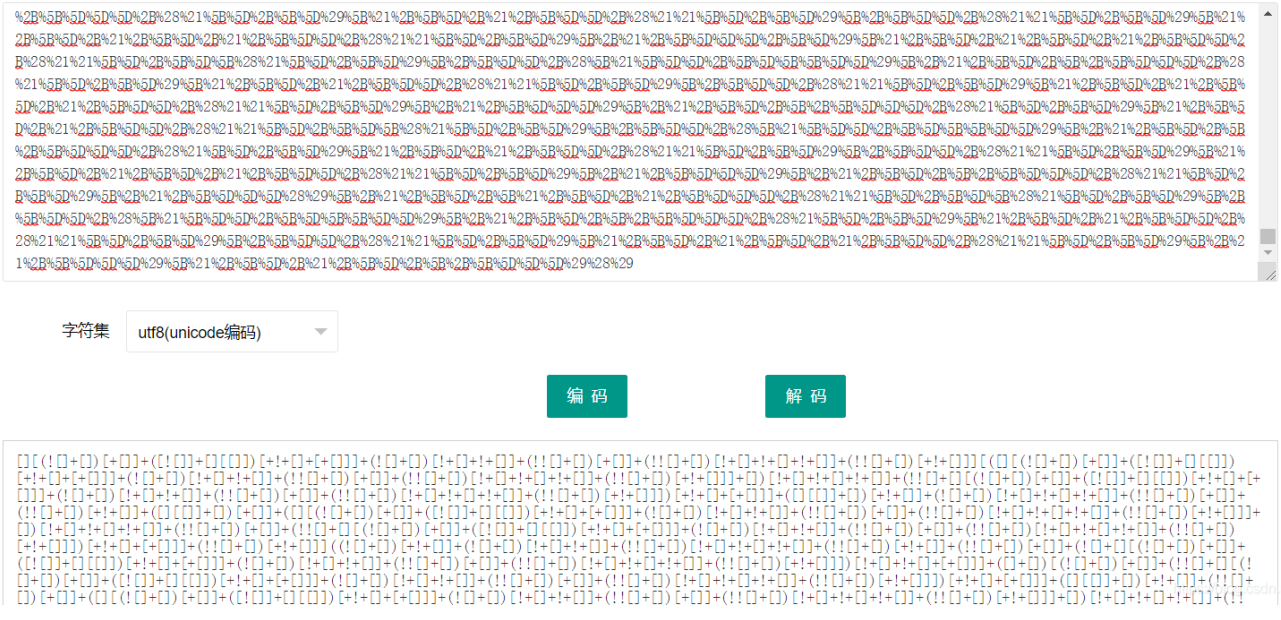
```
POST / HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Referer: http://paste.ubuntu.com/
Accept-Language: zh-CN
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/
537.36 Edge/15.15063
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: paste.ubuntu.com
Content-Length: 115348
Connection: Keep-Alive
Cache-Control: no-cache

poster=pwd&syntax=text&content=%5B%5D%5B%28%21%5B%5D%2B%5B%5D%29%5B%2B%5B%5D%5D%2B%28%5B%21%5B%5D%5D%2B%5B%5D%5B%5B%5D%5D%
29%5B%2B%21%2B%5B%5D%2B%5B%2B%5B%5D%5D%5D%2B%28%21%5B%5D%2B%5B%5D%29%5B%21%2B%5B%5D%2B%21%2B%5B%5D%5D%2B%28%21%21%5B%5D%2B
%5B%5D%29%5B%2B%5B%5D%5D%2B%28%21%21%5B%5D%2B%5B%5D%29%5B%21%2B%5B%5D%2B%21%2B%5B%5D%2B%21%2B%5B%5D%5D%2B%28%21%21%5B%5D%2
B%5B%5D%29%5B%2B%21%2B%5B%5D%5D%5D%5B%28%5B%5D%5B%28%21%5B%5D%2B%5B%5D%29%5B%2B%5B%5D%5D%2B%28%5B%21%5B%5D%5D%2B%5B%5D%5B%
5B%5D%5D%29%5B%2B%21%2B%5B%5D%2B%5B%2B%5B%5D%5D%5D%2B%28%21%5B%5D%2B%5B%5D%29%5B%21%2B%5B%5D%2B%21%2B%5B%5D%5D%2B%28%21%21
%5B%5D%2B%5B%5D%29%5B%2B%5B%5D%5D%2B%28%21%21%5B%5D%2B%5B%5D%29%5B%21%2B%5B%5D%2B%21%2B%5B%5D%2B%21%2B%5B%5D%5D%2B%28%21%2
1%5B%5D%2B%5B%5D%29%5B%2B%21%2B%5B%5D%5D%5D%2B%5B%5D%29%5B%21%2B%5B%5D%2B%21%2B%5B%5D%2B%21%2B%5B%5D%5D%2B%28%21%21%5B%5D%
2B%5B%5D%5B%28%21%5B%5D%2B%5B%5D%29%5B%2B%5B%5D%5D%2B%28%5B%21%5B%5D%5D%2B%5B%5D%5B%5B%5D%5D%29%5B%2B%21%2B%5B%5D%2B%5B%2B
%5B%5D%5D%5D%2B%28%21%5B%5D%2B%5B%5D%29%5B%21%2B%5B%5D%2B%21%2B%5B%5D%5D%2B%28%21%21%5B%5D%2B%5B%5D%29%5B%2B%5B%5D%5D%2B%2
8%21%21%5B%5D%2B%5B%5D%29%5B%21%2B%5B%5D%2B%21%2B%5B%5D%2B%21%2B%5B%5D%5D%2B%28%21%21%5B%5D%2B%5B%5D%29%5B%2B%21%2B%5B%5D%
5D%5D%29%5B%2B%21%2B%5B%5D%2B%5B%2B%5B%5D%5D%5D%2B%28%5B%5D%5B%5B%5D%5D%2B%5B%5D%29%5B%2B%21%2B%5B%5D%5D%2B%28%21%5B%5D%2B
%5B%5D%29%5B%21%2B%5B%5D%2B%21%2B%5B%5D%2B%21%2B%5B%5D%5D%2B%28%21%21%5B%5D%2B%5B%5D%29%5B%2B%5B%5D%5D%2B%28%21%21%5B%5D%2
B%5B%5D%29%5B%2B%21%2B%5B%5D%5D%2B%28%5B%5D%5B%5B%5D%5D%2B%5B%5D%29%5B%2B%5B%5D%5D%2B%28%5B%5D%5B%28%21%5B%5D%2B%5B%5D%29%
5B%2B%5B%5D%5D%2B%28%5B%21%5B%5D%5D%2B%5B%5D%5B%5B%5D%5D%29%5B%2B%21%2B%5B%5D%2B%5B%2B%5B%5D%5D%5D%2B%28%21%5B%5D%2B%5B%5D
%29%5B%21%2B%5B%5D%2B%21%2B%5B%5D%5D%2B%28%21%21%5B%5D%2B%5B%5D%29%5B%2B%5B%5D%5D%2B%28%21%21%5B%5D%2B%5B%5D%29%5B%21%2B%5
B%5D%2B%21%2B%5B%5D%2B%21%2B%5B%5D%5D%2B%28%21%21%5B%5D%2B%5B%5D%29%5B%2B%21%2B%5B%5D%5D%5D%2B%5B%5D%29%5B%21%2B%5B%5D%2B%
21%2B%5B%5D%2B%21%2B%5B%5D%5D%2B%28%21%21%5B%5D%2B%5B%5D%29%5B%2B%5B%5D%5D%2B%28%21%21%5B%5D%2B%5B%5D%5B%28%21%5B%5D%2B%5B
%5D%29%5B%2B%5B%5D%5D%2B%28%5B%21%5B%5D%5D%2B%5B%5D%5B%5B%5D%5D%29%5B%2B%21%2B%5B%5D%2B%5B%2B%5B%5D%5D%5D%2B%28%21%5B%5D%2
```

8.这些字符太多，加载太久了，看着这个就感觉不对劲，往下一翻，发现了这个，研究过xss，我知道这是jsfuck编码后的：

```
<h1>Paste from pwd at Sun, 20 Aug 2017 15:48:11 +0000</h1>
<div class="paste">
<a class="pturl" href="/25355581/plain/">Download as text</a>
<div class="paste">
<table class="pastetable"><tr><td class="linenos"><div class="linenodiv"><pre>1</pre></div></td><td class="code"><div
class="paste"><pre>[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+
[]]+(!![]+[])[+!+[]]][([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]
+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+
[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+
[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!!
[]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+
[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]((![]+
[])[+!+[]]+(![]+[])[!+[]+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]+(!![]+[])[+[]]+(![]+[][(![]+[])[+[]]+([![]]+[]
[[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]]+([]+
[])[(![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+
[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(!![]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+
```

9.这里第二个坑点来了，不能直接复制下面的jsfuck，因为中间有些特殊的数字之类的：

10.把上面url中content后面的内容url解码一下：



11.坑点三到了，直接用ctf这个网站的jsfuck解出来看不懂的--还是要拿去http://www.jsfuck.com/# 去执行一下：

programming style based on the atomic parts of
t characters to write and execute code.

ou can even run it on Node.js.

ı script. Uncheck "eval source" to get back a

val Source

```
+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+
+(!![]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[]
]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+
+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+
+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+
]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+
])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])
]]]()[+!+[]+[!+[]+!+[]]]+(!![]+[][(![]+[])[+
[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+
+!+[]+[+[]]])()
```

Run This

12.发现弹窗出现了密码，拿去解压得到flag：

flag{COnGr4t5_H4ck3r_YOu_Ge7_Secr3t:)}