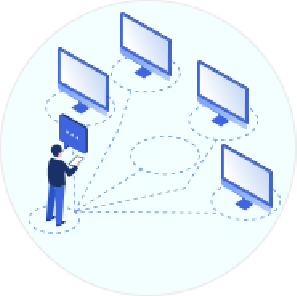
2021年中国工业互联网安全大赛核能行业赛道writeup之Webshell密码

原创

苦行僧(csdn) 于 2021-10-23 11:15:00 发布 37 收藏
分类专栏： 信息安全 文章标签： CTF

本文链接：https://blog.csdn.net/qpeity/article/details/120896180
版权



信息安全 专栏收录该内容
12 篇文章 0 订阅
订阅专栏

附件题：Webshell密码

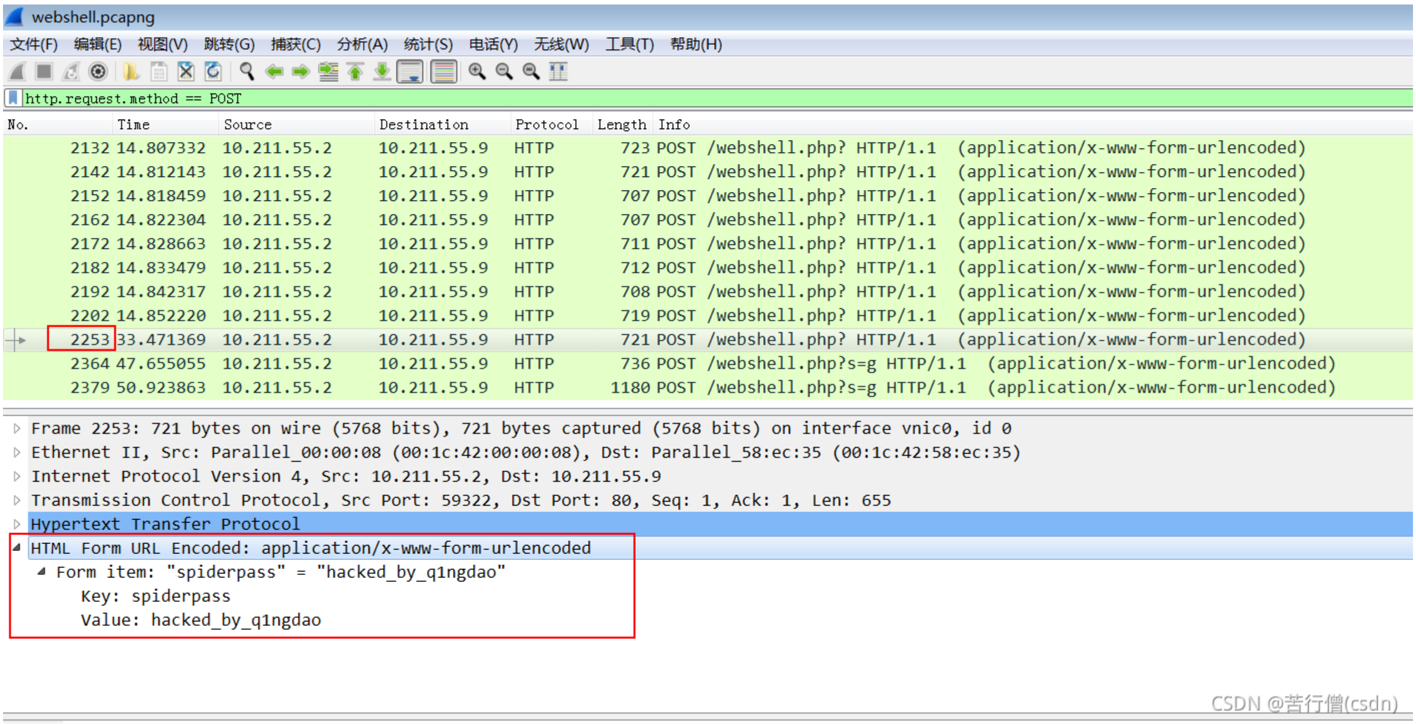
题目描述：

> 某次攻防演练中，抓到了一个webshell的流量，请分析出密码，flag形式：flag{密码}

附件下载：

https://download.csdn.net/download/qpeity/33675356
https://download.csdn.net/download/qpeity/33675356附件解压缩得到一个webshell.pcapng，全局搜索flag，没有发现有用信息。

因为是Webshell，一般HTTP请求会用到POST方法，筛选 http.response.method == POST。发现攻击者在不断的尝试用户spiderpass的弱口令，一直尝试到 No.2253 包，在此之后就得手了。所以 No.2253 包里面尝试的口令就是flag中{}的部分。


webshell.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
http.request.method == POST
```

```
No.     Time      Source       Destination   Protocol  Length Info
   2132 14.807332 10.211.55.2  10.211.55.9   HTTP       723 POST /webshell.php? HTTP/1.1  (application/x-www-form-urlencoded)
   2142 14.812143 10.211.55.2  10.211.55.9   HTTP       721 POST /webshell.php? HTTP/1.1  (application/x-www-form-urlencoded)
   2152 14.818459 10.211.55.2  10.211.55.9   HTTP       707 POST /webshell.php? HTTP/1.1  (application/x-www-form-urlencoded)
   2162 14.822304 10.211.55.2  10.211.55.9   HTTP       707 POST /webshell.php? HTTP/1.1  (application/x-www-form-urlencoded)
   2172 14.828663 10.211.55.2  10.211.55.9   HTTP       711 POST /webshell.php? HTTP/1.1  (application/x-www-form-urlencoded)
   2182 14.833479 10.211.55.2  10.211.55.9   HTTP       712 POST /webshell.php? HTTP/1.1  (application/x-www-form-urlencoded)
   2192 14.842317 10.211.55.2  10.211.55.9   HTTP       708 POST /webshell.php? HTTP/1.1  (application/x-www-form-urlencoded)
   2202 14.852220 10.211.55.2  10.211.55.9   HTTP       719 POST /webshell.php? HTTP/1.1  (application/x-www-form-urlencoded)
   2253 33.471369 10.211.55.2  10.211.55.9   HTTP       721 POST /webshell.php? HTTP/1.1  (application/x-www-form-urlencoded)
   2364 47.655055 10.211.55.2  10.211.55.9   HTTP       736 POST /webshell.php?s=g HTTP/1.1  (application/x-www-form-urlencoded)
   2379 50.923863 10.211.55.2  10.211.55.9   HTTP      1180 POST /webshell.php?s=g HTTP/1.1  (application/x-www-form-urlencoded)
```

```
▷ Frame 2253: 721 bytes on wire (5768 bits), 721 bytes captured (5768 bits) on interface vnic0, id 0
▷ Ethernet II, Src: Parallel_00:00:08 (00:1c:42:00:00:08), Dst: Parallel_58:ec:35 (00:1c:42:58:ec:35)
▷ Internet Protocol Version 4, Src: 10.211.55.2, Dst: 10.211.55.9
▷ Transmission Control Protocol, Src Port: 59322, Dst Port: 80, Seq: 1, Ack: 1, Len: 655
▷ Hypertext Transfer Protocol
◢ HTML Form URL Encoded: application/x-www-form-urlencoded
  ◢ Form item: "spiderpass" = "hacked_by_q1ngdao"
      Key: spiderpass
      Value: hacked_by_q1ngdao
```

根据提示flag的格式为flag{密码}得到 —— flag{hacked_by_q1ngdao}