

攻防世界 Crypto高手进阶区 4分题 工业协议分析1

原创

思源湖的鱼  于 2020-12-26 14:24:57 发布  270  收藏

分类专栏: [ctf](#) 文章标签: [ctf](#) [攻防世界](#) [crypto](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_44604541/article/details/111741383

版权

CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的4分题

本篇是工业协议分析1的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

得到一个流量包

发现一个长度异常的流量

No.	Time	Source	Destination	Protocol	Length	Info
	1801 150.466006	192.168.2.53	192.168.2.112	TCP	10120	102 → 2817 [PSH, ACK] Seq=1103156 Ack=5906 Win=6656
	8508 393.840663	192.168.2.53	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
	8507 393.840651	192.168.2.53	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
	8505 393.840402	192.168.2.53	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
	8504 393.840294	192.168.2.53	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
	8502 393.840114	192.168.2.53	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]
	8501 393.839937	192.168.2.53	192.168.2.112	COTP	1094	DT TPDU (0) [COTP fragment, 1021 bytes]

```

0060 09 64 61 74 61 20 3d 20 22 64 61 74 61 3a 69 6d  .data = "data:im
0070 61 67 65 2f 70 6e 67 3b 62 61 73 65 36 34 2c 69  age/png; base64,i
0080 56 42 4f 52 77 30 4b 47 67 6f 41 41 41 41 4e 53  VBORw0KGgoAAAANS
0090 55 68 45 55 67 41 41 41 64 41 41 41 41 42 69 43  UhEUgAAA dAAAABiC
00a0 41 59 41 41 41 44 67 4b 49 4c 4b 41 41 41 41 41  AYAAADgK ILKAAAAA
00b0 58 4e 53 52 30 49 41 72 73 34 63 36 51 41 41 41  XNSR0IAr s4c6QAAA
00c0 41 52 6e 51 55 31 42 41 41 43 78 6a 77 76 38 59  ARnQU1BA ACxjwv8Y
00d0 51 55 41 41 41 41 41 63 45 68 5a 63 77 41 41 41  QIAAAATc Ek7cAAD

```

里面传了一张png图片

把这段base64复制
转为图片

在线调色板 网页常用色彩 中日传统色彩 传图识色 WEB安全色 网页颜色选择器 颜色代码查询、RGB颜色值 **base64图片在线转换工具**

flag{ICS-mms104}

```


KAAAAAXNSR0IArs4c6QAAARnQU1BAACxjwv8YQUAAAJcEhZcwAADsMAAA7D
AcdvqGQAAABzXSURBVHhe7Z2Js11Fncfn75maqZmaqZkaS0elXAp1GHRUHGFQHY
QFQRFBWQRiBoBWQyyKaBsxo0tCagkQHAYQEL2jSxAYEoSIAHOvM/JPTPn9fv1Od1
9+9z3bvh+qr5FkXe77z33ntO/7l//fr/+m0IIlYQQ0ciACiGEEAnlgAohhBAJyIAKIYQQ
ciACiGEEAnlgAohhBAJyIAKIYQQCciACiGEEAnlgAohhBAJyIAKIYQQCciACiGEEAnlgA
ohhBAJyIAKIYQQCciACiGEEAnlgAohhBAJyIAKIYQQCciACiGEEAnlgAohhBAJyIAKIYQ
QCciACiGEEAnlgAohhBAJyIAKIYQQCciACiGEEAnlgAohhBAJyIAKIYQQCciACiGEEAnl
gAohhBAJyIAKIYQQCciACiGEEAIOZkDff78oNm/ZV8xfuK2Y8fxrxex5W4vK3cVe/Ye6
L1CCCGEF6yGtC33n63uOPuNcW/fHJG8bcffsarf/3UjNLAvtz/h/Xm6/h3IYQQYIKSz
YBufePt4thT55qG0NXxp8/ttqIDGj/vP3Oe+VKf/L1y4qTzppffOq/ni/+6bDpxY+ve7n
3irHw/VrKzdsjE6tFL24v7p26rrhsOpLy8x3+pZnFhz/zbdNz+th/PfD86auzi3MuWFhcc

```

*请上传小于300KB的.jpg/.jpeg/.gif/.bmp/.png/.ico格式图片，不建议将大图转换。

图片转成Base64
Base64还原图片
清空结果

https://blog.csdn.net/walxin_44604541

得到flag

结语

base64转图片