



# Modbus

📅 2021-09-01 | 📁 Challenge, 2021, 工业信息安全技能大赛, 巡回赛-上海站

Challenge | 2021 | 工业信息安全技能大赛 | 巡回赛-上海站 | Modbus

[点击此处](#)获得更好的阅读体验

## WriteUp来源

来自 **Venom** 战队

## 题目描述

某工业企业被黑客攻击，工业安全运维人员记录下了网络数据包，需要分析数据包中的异常，找出flag。


## 题目考点

- 流量分析
- modbus协议分析

## 解题思路

分析流量，在流量中找到一串base64加密，解密后即为flag

TCP 44 502 → 49715 [ACK] Seq=537 Ack=109 Win=10232 Len=0														
0000	02 00 00 00 45 00 00 6b 54 9c 40 00 80 06 00 00	...	E	k	T	@	...							
0010	c0 a8 2f 81 c0 a8 2f 81 01 f6 c2 33 8c 0b f0 79	..	/	..	/	..	3	..	y					
0020	87 e1 fe f6 50 18 27 f8 4c ce 00 00 04 9f 00 00	...	P	.	L	...								
0030	00 3d 01 03 3a 00 00 00 5a 00 6d 00 78 00 68 00	=	:	:	Z	m	x	h	.					
0040	5a 00 33 00 74 00 7a 00 61 00 47 00 6c 00 6c 00	Z	3	t	z	a	G	l	l	.				
0050	63 00 45 00 4e 00 30 00 5a 00 6b 00 31 00 76 00	c	E	N	0	.	Z	k	1	v	.			
0060	5a 00 47 00 4a 00 31 00 63 00 33 00 30 00 3d	Z	G	J	1	.	c	3	0	=				



CTFHub



## Flag



1 flag{shiepCtfModbus}

**本文作者：** CTFHub

**本文链接：** <https://writeup.ctfhub.com/Challenge/2021/工业信息安全技能大赛/巡回赛-上海站/dLQvsnMw2yxzcJrNaAzaq8.html>

**版权声明：** 本博客所有文章除特别声明外，均采用 [CC BY-NC-SA](#) 许可协议。转载请注明出处！

[# Challenge](#)

[# 2021](#)

[# 工业信息安全技能大赛](#)

[# 巡回赛-上海站](#)

[< Malware](#)

[WiFi >](#)

© 2019 – 2022 ❤ CTFHub

由 [Hexo](#) & [NexT.Gemini](#) 强力驱动