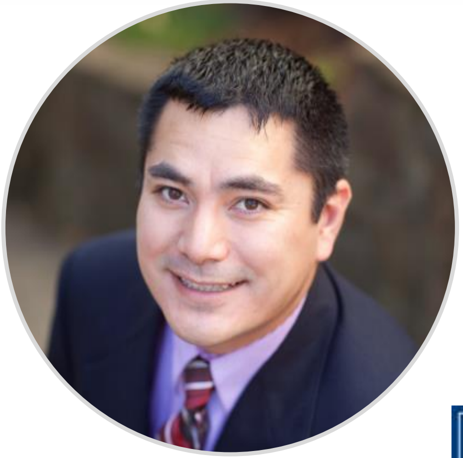
WHEN IOT ATTACKS

UNDERSTANDING THE SAFETY RISKS ASSOCIATED WITH CONNECTED DEVICES

Brought to you by Whitescope

contact@whitescope.io

About:Billy



Billy Kim Rios
Founder

Google

UNIVERSITY OF WASHINGTON 1861
LVX SIT

TEXAS A&M
UNIVERSITY
COMMERCE

Microsoft®

UNITED STATES MARINE CORPS

HAWAI'I PACIFIC UNIVERSITY®

WhiteScope

EY

About:Jonathan

Jonathan Butts, PhD

Founder QED Secure Solutions

I3P

Institute for Information Infrastructure Protection

U.S. DEPARTMENT OF HOMELAND SECURITY

AF INSTITUTE OF TECHNOLOGY

THE UNIVERSITY of TULSA

QED Secure Solutions

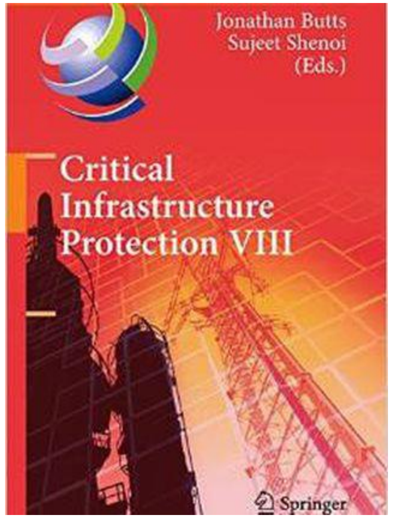
CHAPMAN UNIVERSITY

ὁ χριστὸς καὶ ἡ ἐκκλησία

1861

SRI International®

ifip



Jonathan Butts
Sujeet Shenoi
(Eds.)

Critical Infrastructure Protection VIII

Springer

Shoulders of Giants

- Chris Valasek
- Charlie Miller
- David Litchfield
- Mark Litchfield
- Neel Mehta
- Nate McFeters
- Barnaby Jack
- Mark Dowd
- Chris Evans
- Brian Holyfield
- Eric Cabetas
- Dave Aitel

- Alex Sotirov
- Kingcope
- Skape
- Skywing
- Ryan Smith
- Alex Wheeler
- Tavis Ormandy
- Project Zero
- Microsoft SRD
- Kuzza55
- Eduardo Vela
- Mike Ahmadi

What is IoT?

IoT == Internet of “Things”

26 – 30 billion devices by 2020

From Wikipedia:

> The Internet of Things (IoT) is the ***interconnection*** of uniquely identifiable ***embedded computing devices*** within the existing ***Internet*** infrastructure

What we’re looking for…

- Device(s) connected to the Internet
- In a public space/accessible to the general public
- Exploitation of the device can be leveraged to cause a safety issue

CAR
WASH

Car Wash

PDQ
LASERWASH
www.pdqinc.com

Current Situation

Car wash systems are essentially industrial control systems (ICS)

Current Situation

We’ve written an exploit that can cause a car wash system to physically attack an occupant

Current Situation

Currently, there is no patch for the vulnerability we’ve discovered…

The Setup

Current Situation

Currently, there is no mechanism for researchers to safely test public safety issues without expending their own resources

Case Study

Case Study – Charlie Miller and Chris Valasek - Remote Exploitation of an Unaltered Passenger Vehicle:

http://illmatics.com/Remote%20Car%20Hacking.pdf

Costs – Charlie and Chris

- wiTECH micropod System - **$6,693.00**
- wiTECH Diagnostic Extender Micropod - **$604.00**
- wiTECH VCI System - **$5,482.00**
- Additional wiTECH VCI Pod Kit - **$1,263.00**
- Tech Authority Subscription - **$1,800/year**

Costs – Charlie and Chris

Costs for wiTECH tools

(does not include cost for vehicles and other tools)

$15,842

Costs – Charlie and Chris

Cost of one quarter of tuition, room, board, books, supplies, and other expenses at STANFORD

$15,590

Costs – Charlie and Chris

Page 73 - Remote Exploitation of an Unaltered Passenger Vehicle

While some of the research could proceed without the diagnostic equipment, many active tests and ECU unlocking require an analysis of the mechanic’s tools.

Costs – Charlie and Chris

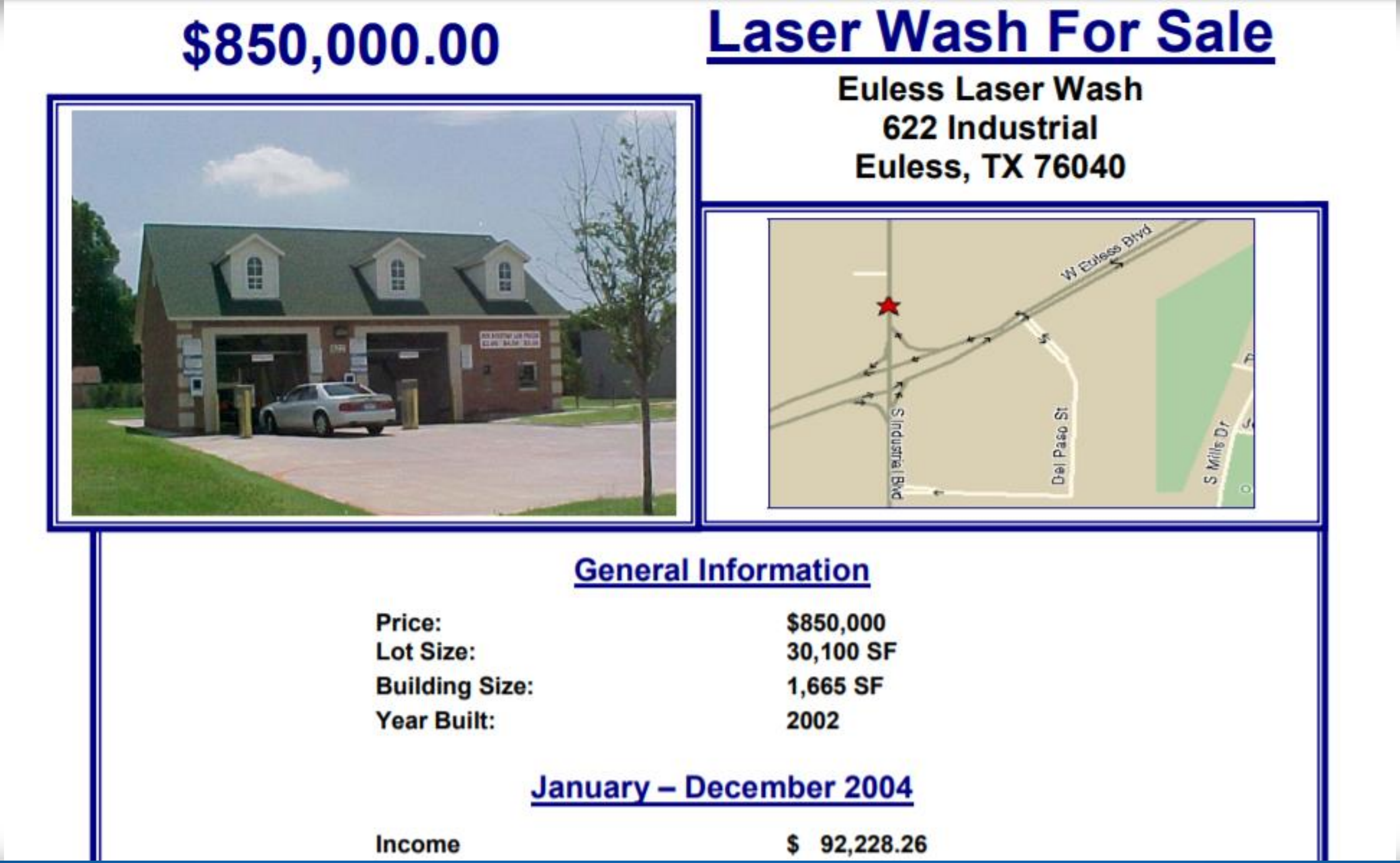
Page 73 - Remote Exploitation of an Unaltered Passenger Vehicle

After both authors of this paper sold plasma for several weeks, we were finally able to afford the system required to do diagnostics on the Jeep Cherokee (and all other Fiat-Chrysler vehicles)

Costs – Charlie and Chris

Thank you Charlie and Chris!

Our Cost Considerations



W Euless Blvd
S Industrial Blvd
Del Paso St
S Mills Dr

$850,000.00

Laser Wash For Sale

Euless Laser Wash
622 Industrial
Euless, TX 76040

General Information

Price:	$850,000
Lot Size:	30,100 SF
Building Size:	1,665 SF
Year Built:	2002

January – December 2004

Income	$ 92,228.26

Our Cost Considerations

- Firmware was acquired in 2014
- Willing owner identified in 2017 and compensated for “academic evaluation of user interfaces”
- Travel and lodging as we could not test against local systems (3 visits)
- Anger and annoyance from spouses (costs are incalculable)

Our Cost Considerations

Research Considerations

If we don’t create a mechanism for researchers to test these systems… they will be forced to:

1. **Give up**
2. **Spend their own $$**
3. **Test against live systems**

Research Considerations

Analysis and responses from manufacturers is great, however we’ve run into challenges in the past

Disclosure Timeline

Feb 2015 – Initial Disclosure, safety issues disclosed
Mar 2015 – No Response
Apr 2015 – No Response
May 2015 – No Response
June 2015 – No Response
July 2015 – No Response
Aug 2015 – No Response
Sept 2015 – No Response
Oct 2015 – No Response
Nov 2015 – No Response
Dec 2015 – No Response

Disclosure Timeline

Jan 2016 – No Response
Feb 2016 – No Response
Mar 2016 – No Response
Apr 2016 – No Response
May 2016 – No Response
June 2016 – No Response
July 2016 – No Response
Aug 2016 – No Response
Sept 2016 – No Response
Oct 2016 – No Response
Nov 2016 – No Response
Dec 2016 – No Response

Disclosure Timeline

Jan 2017 – No Response

Feb 2017 – No Response

Mar 2017 – No Response

Apr 2017 – No Response

May 1, 2016 – Fully working, remote exploit code (PoC) provided
Exploit code causes car wash to physically attack occupants
All that is required is an IP address of a car wash

June 2016 – No Response

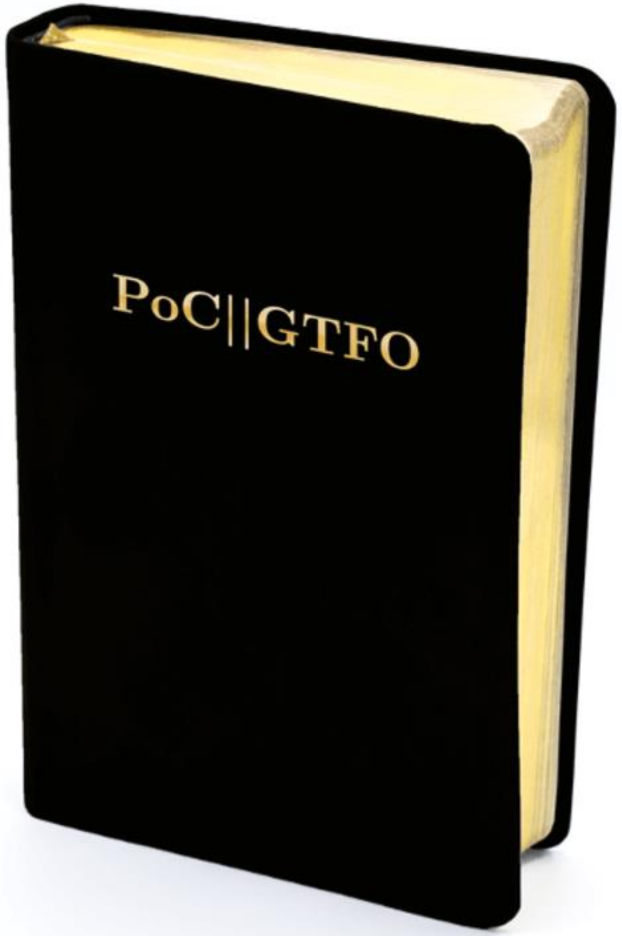
July 2016 – Vendor asks, “Did you test against a demo system?”

Our Cost Considerations

More common responses are like this (different vendor):

1) Refuted – Feature, not a bug
2) Refuted – Not a practical attack
3) Refuted – System doesn’t work in the way we described
4) Refuted – System doesn’t work in the way we described
5) Refuted – System doesn’t work in the way we described
6) Refuted – Vulnerable code not reachable by normal users
7) Refuted – System doesn’t work in the way we described
8) Refuted – Refuted due to safety constraints

PoC or GTFO



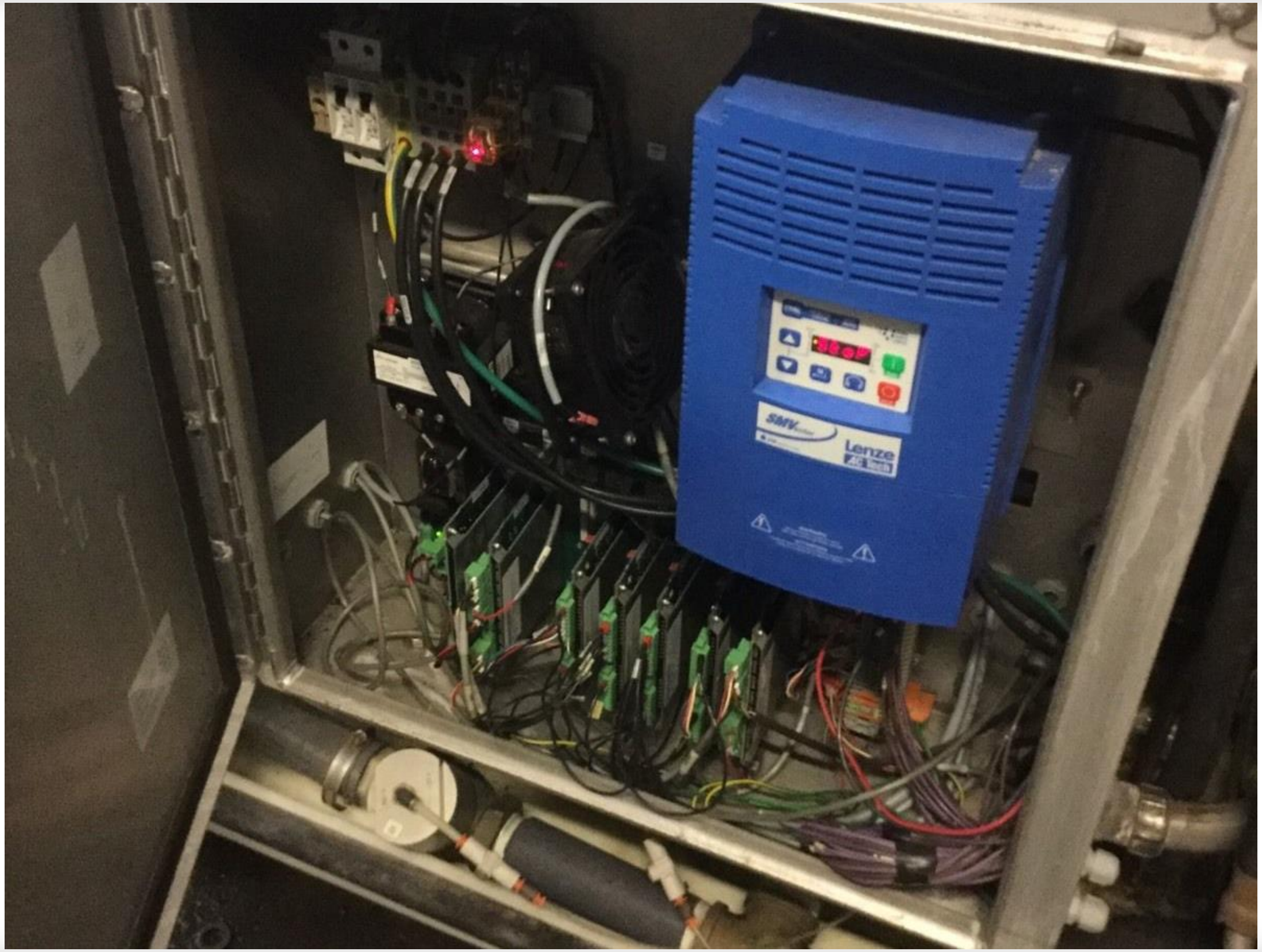
PoC or GTFO

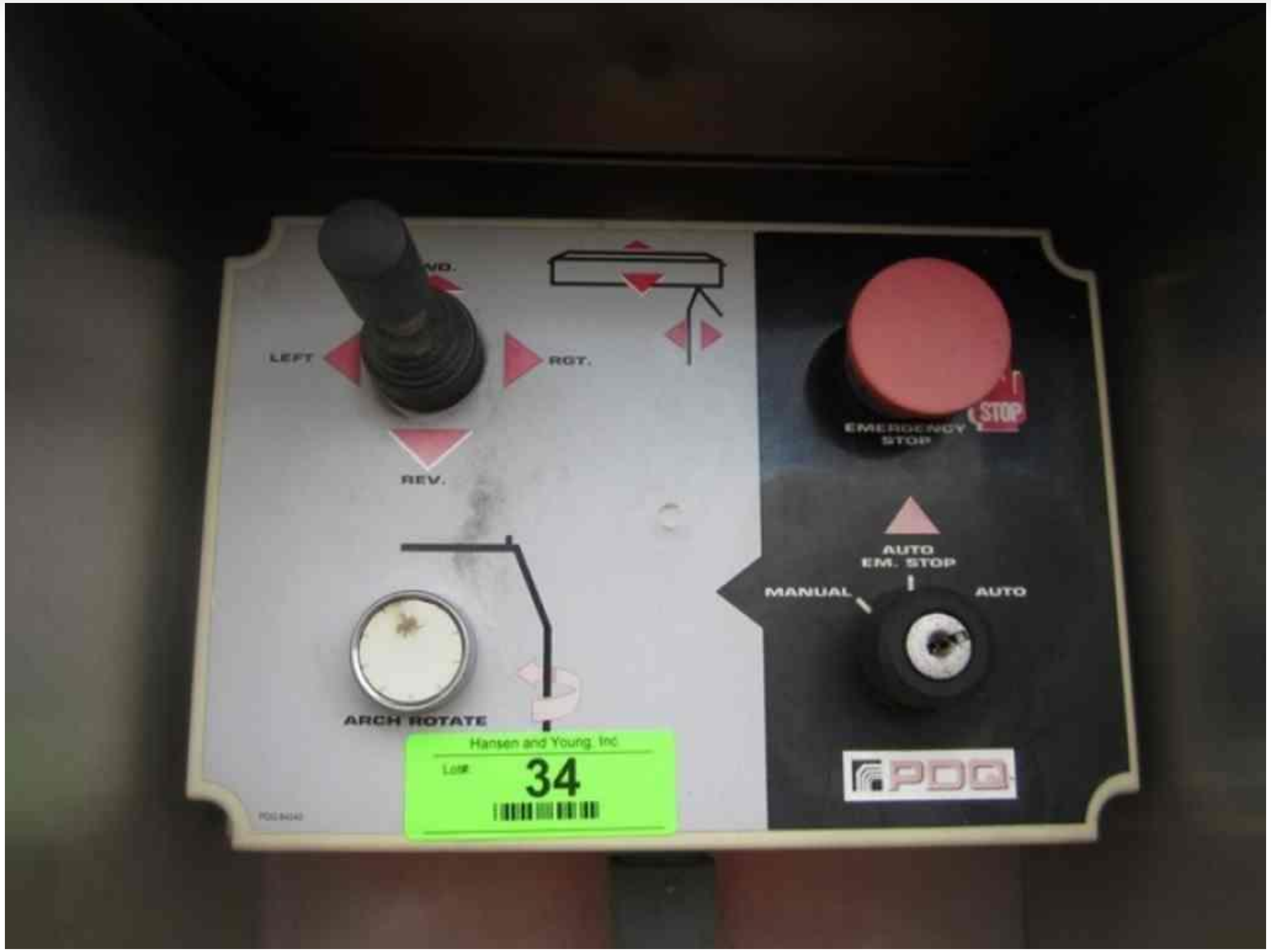
This is how we get PoCs!

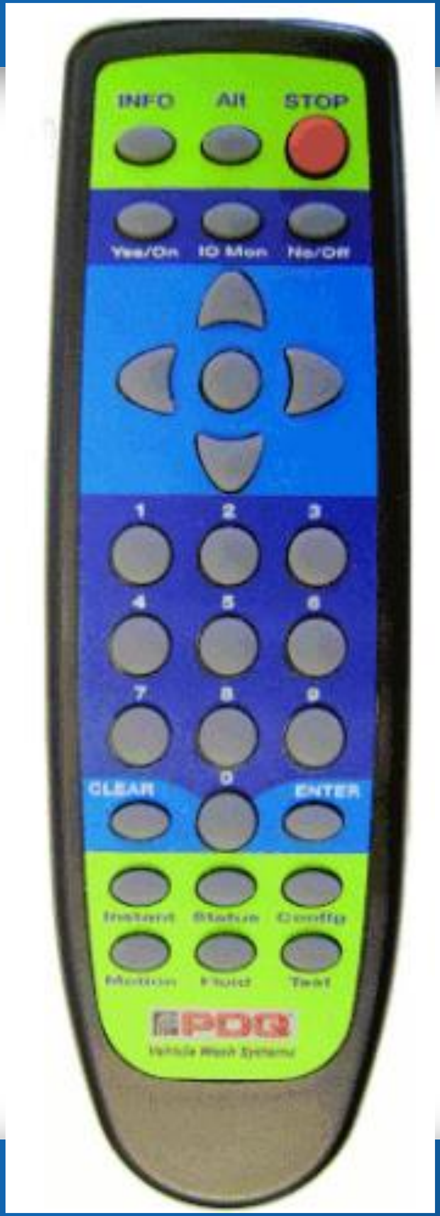
PoCs

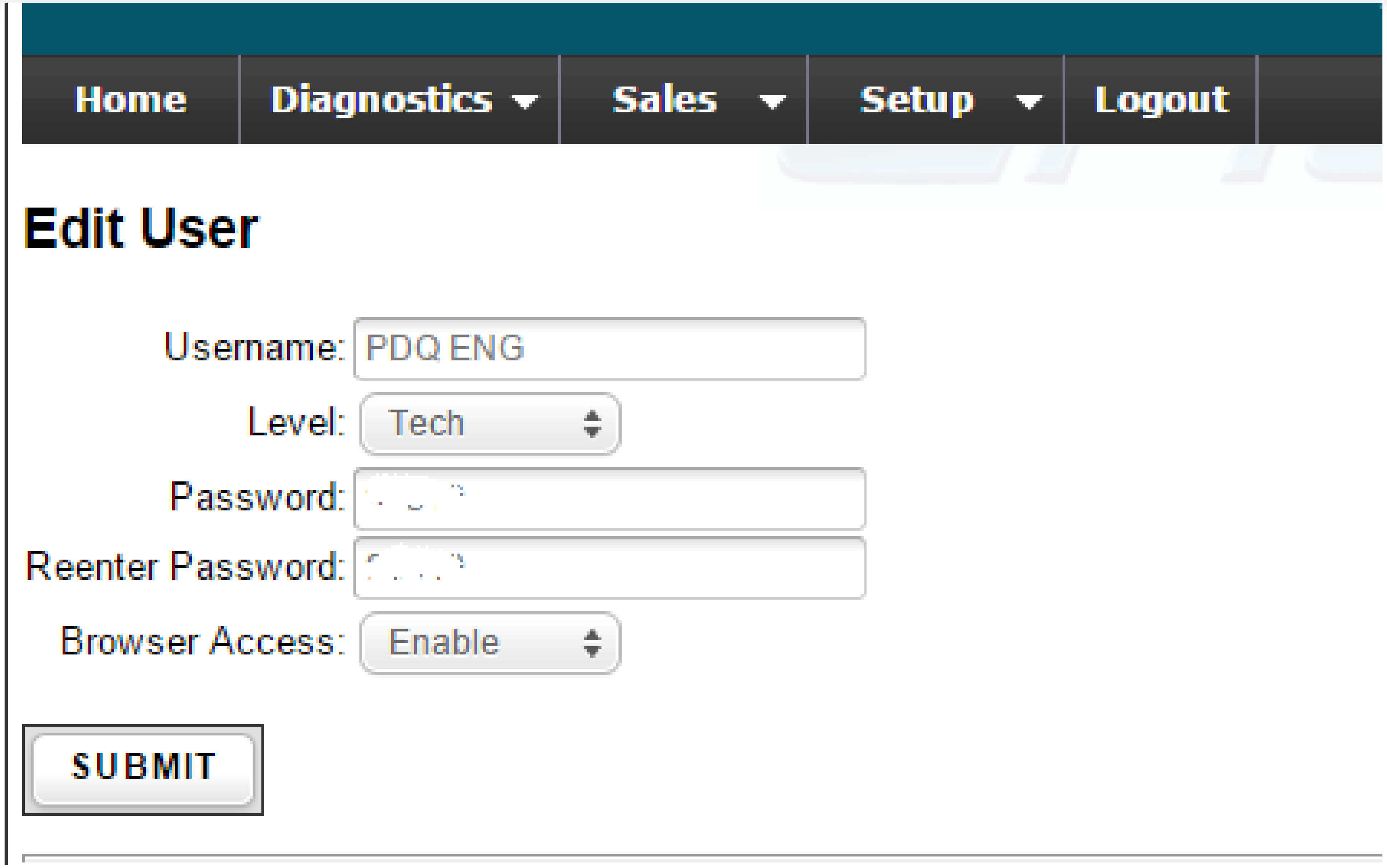
This essentially forces us to write code that can hurt people…

The Technology


SMV
Lenze
AC Tech


FWD.
LEFT
RGT.
REV.
EMERGENCY STOP
STOP
AUTO EM. STOP
MANUAL
AUTO
ARCH ROTATE
PDQ
Hansen and Young, Inc
Lot#
34


INFO
Alt
STOP
Yes/On
IO Mon
No/Off
1
2
3
4
5
6
7
8
9
CLEAR
0
ENTER
Instant
Status
Config
Motion
Hold
Test
PDQ
Vehicle Wash Systems



Edit User

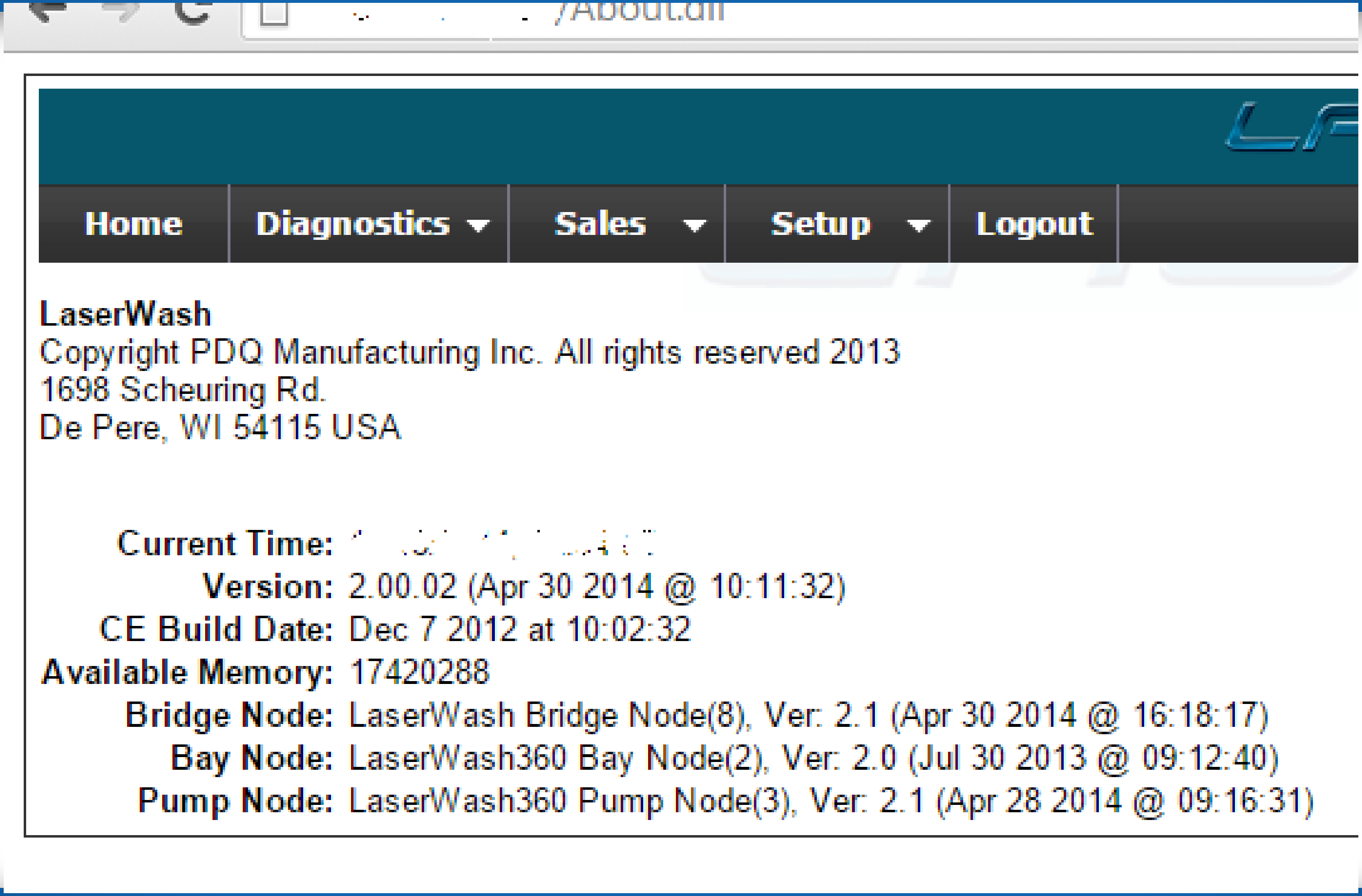
Username: PDQ ENG

Level: Tech

Password: [redacted]

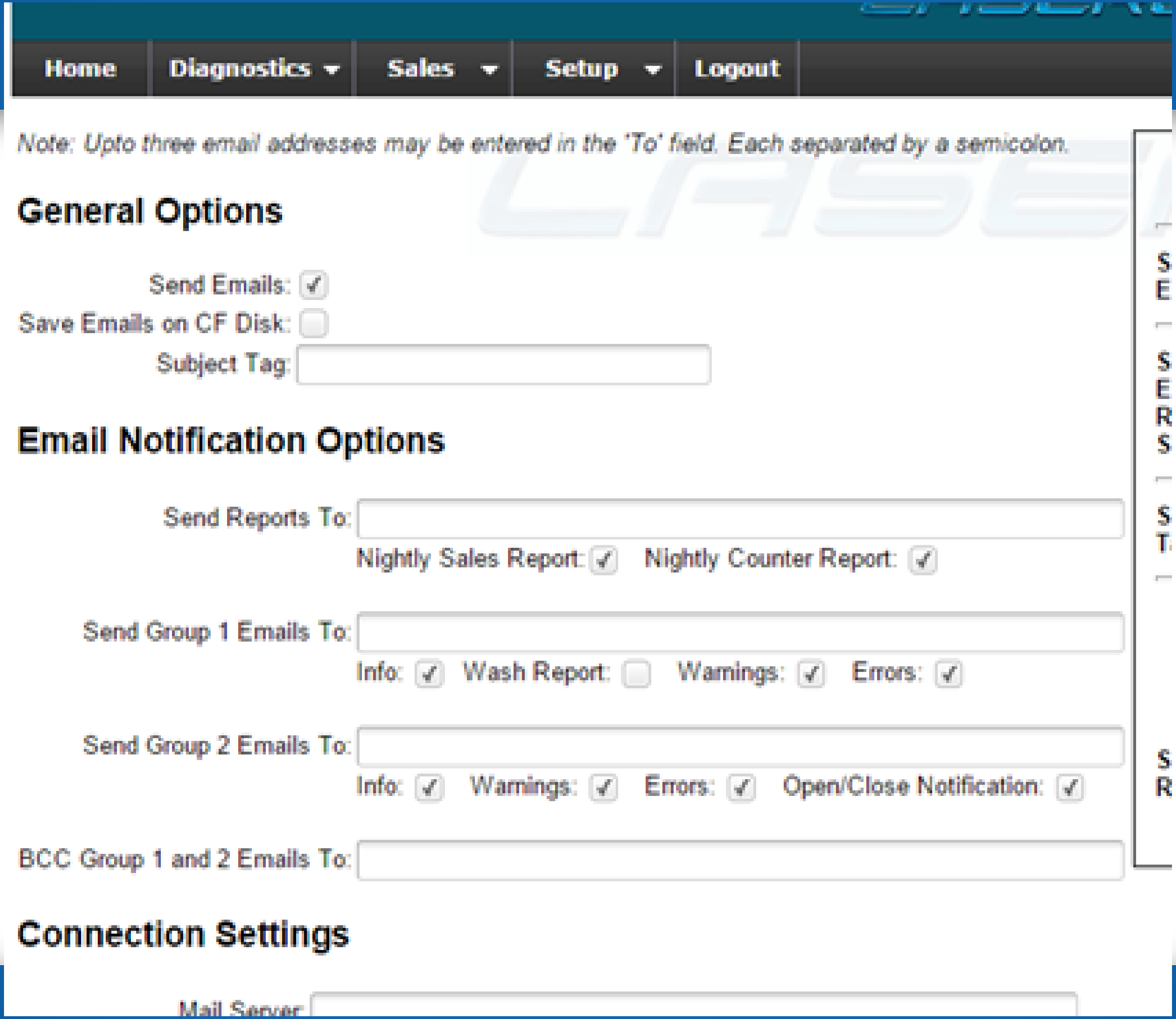
Reenter Password: [redacted]

Browser Access: Enable



LaserWash
Copyright PDQ Manufacturing Inc. All rights reserved 2013
1698 Scheuring Rd.
De Pere, WI 54115 USA

```
     Current Time: [redacted]
          Version: 2.00.02 (Apr 30 2014 @ 10:11:32)
    CE Build Date: Dec 7 2012 at 10:02:32
 Available Memory: 17420288
      Bridge Node: LaserWash Bridge Node(8), Ver: 2.1 (Apr 30 2014 @ 16:18:17)
         Bay Node: LaserWash360 Bay Node(2), Ver: 2.0 (Jul 30 2013 @ 09:12:40)
        Pump Node: LaserWash360 Pump Node(3), Ver: 2.1 (Apr 28 2014 @ 09:16:31)
```



Note: Upto three email addresses may be entered in the 'To' field. Each separated by a semicolon.

General Options

Send Emails: ☑

Save Emails on CF Disk: □

Subject Tag:

Email Notification Options

Send Reports To:

Nightly Sales Report: ☑ Nightly Counter Report: ☑

Send Group 1 Emails To:

Info: ☑ Wash Report: □ Warnings: ☑ Errors: ☑

Send Group 2 Emails To:

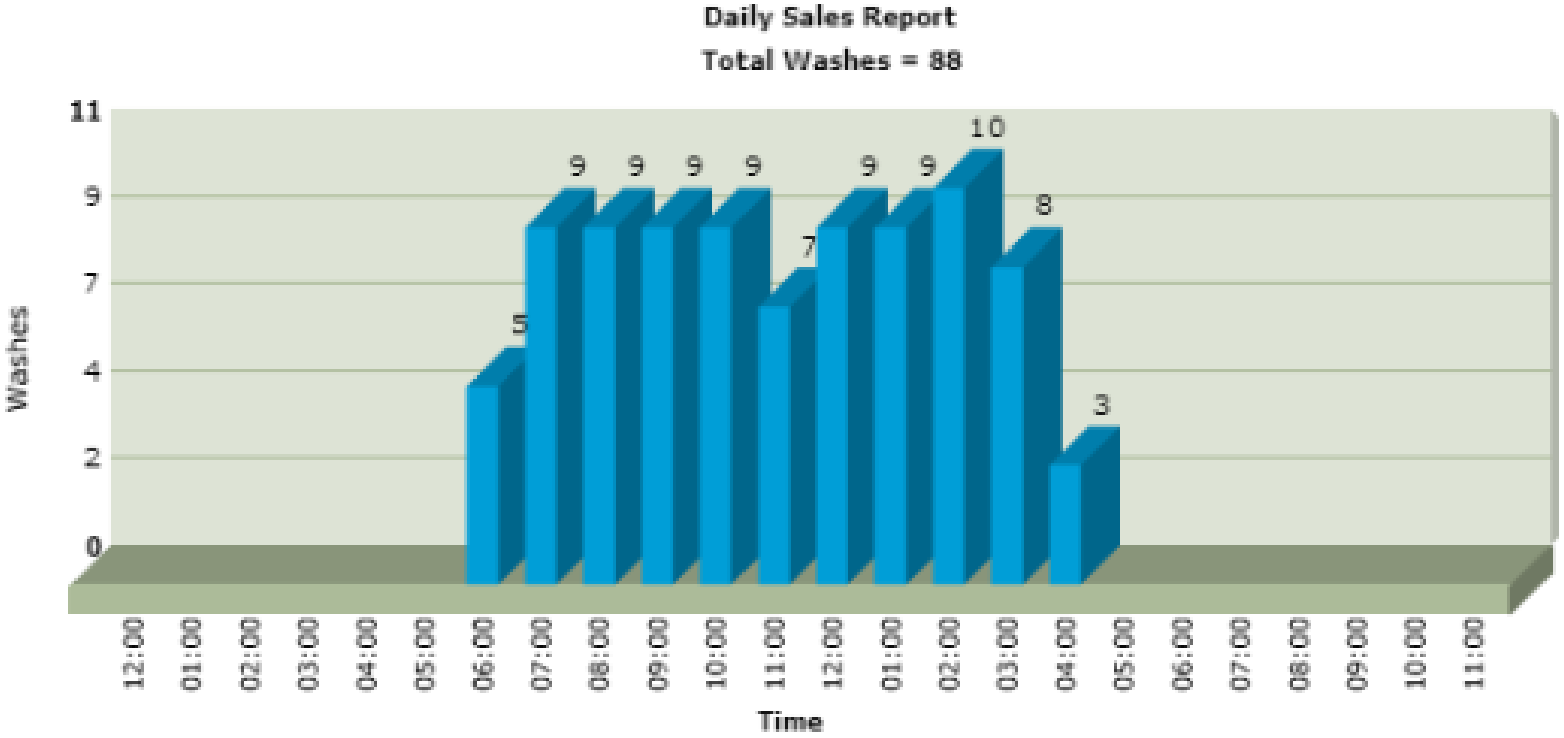
Info: ☑ Warnings: ☑ Errors: ☑ Open/Close Notification: ☑

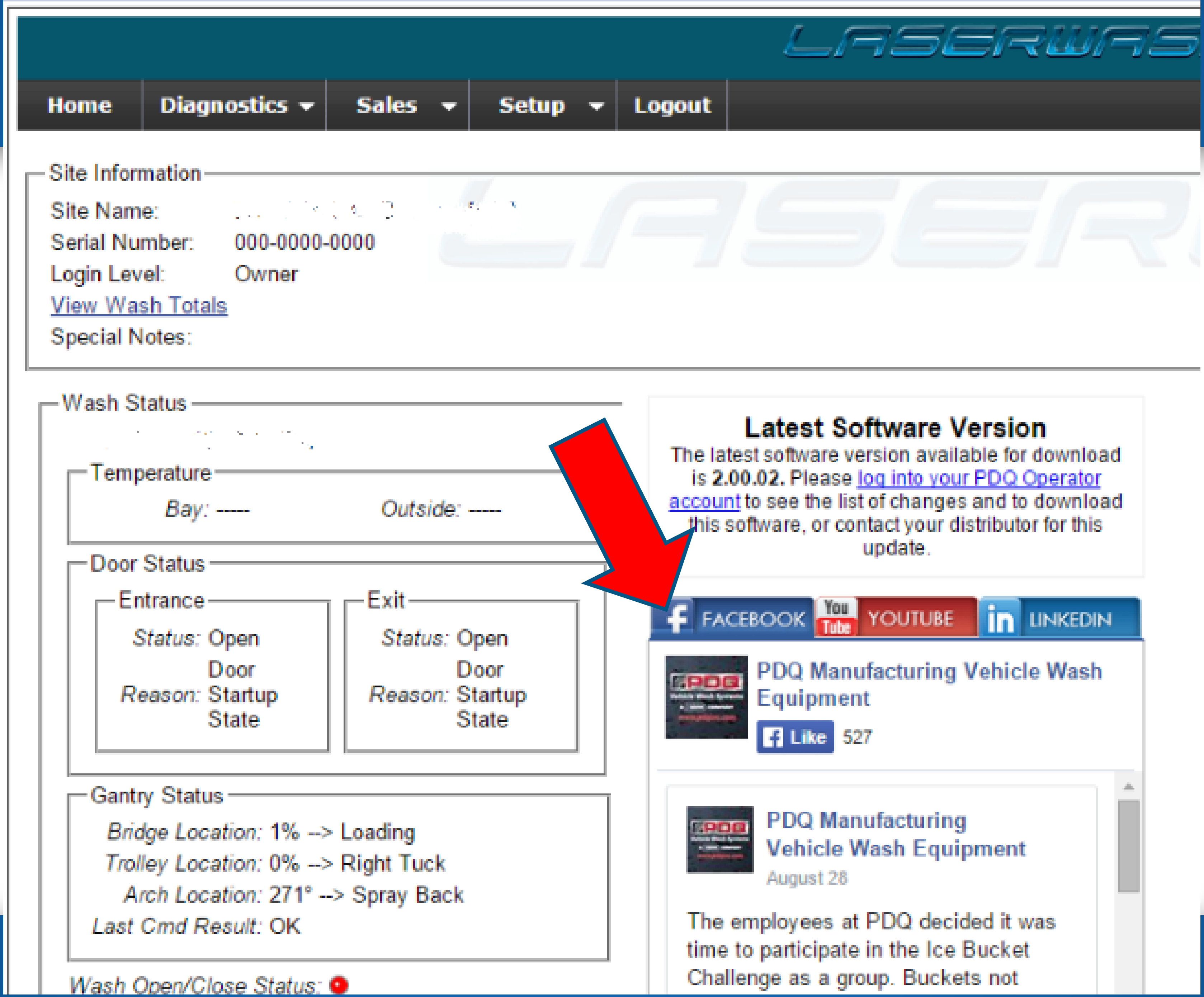
BCC Group 1 and 2 Emails To:

Connection Settings

Mail Server:

YES! The carwash can send email!


Daily Sales Report
Total Washes = 88
Washes
11
9
7
4
2
0
5
9
9
9
9
7
9
9
10
8
3
12:00
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
Time



Site Information

Site Name: [illegible]

Serial Number: 000-0000-0000

Login Level: Owner

View Wash Totals

Special Notes:

Wash Status

[illegible]

Temperature

Bay: -----   *Outside:* -----

Door Status

Entrance

Status: Open Door

Reason: Startup State

Exit

Status: Open Door

Reason: Startup State

Gantry Status

Bridge Location: 1% --> Loading

Trolley Location: 0% --> Right Tuck

Arch Location: 271° --> Spray Back

Last Cmd Result: OK

Wash Open/Close Status: ●

Latest Software Version

The latest software version available for download is **2.00.02**. Please log into your PDQ Operator account to see the list of changes and to download this software, or contact your distributor for this update.

PDQ Manufacturing Vehicle Wash Equipment

Like 527

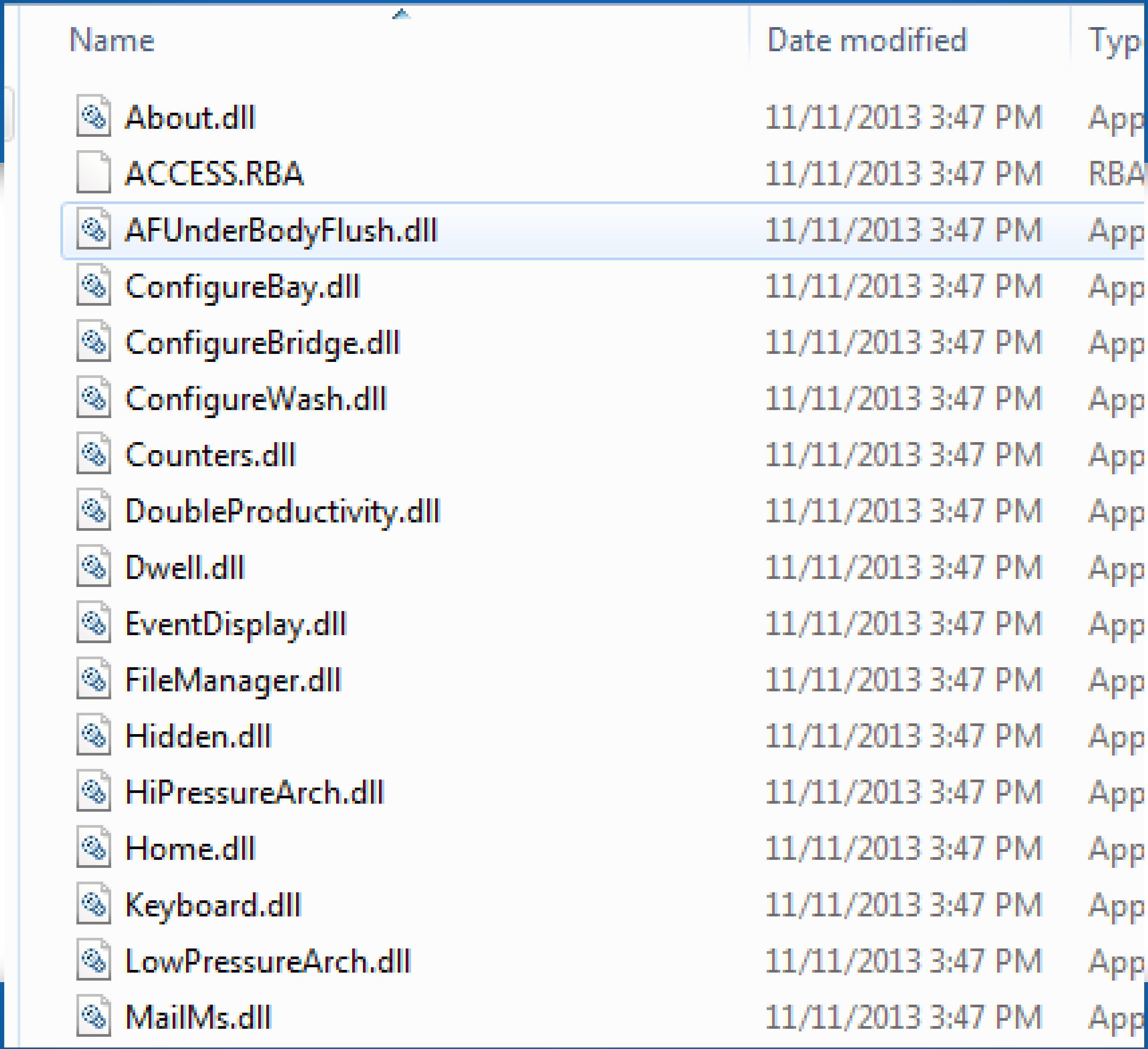
PDQ Manufacturing Vehicle Wash Equipment

August 28

The employees at PDQ decided it was time to participate in the Ice Bucket Challenge as a group. Buckets not

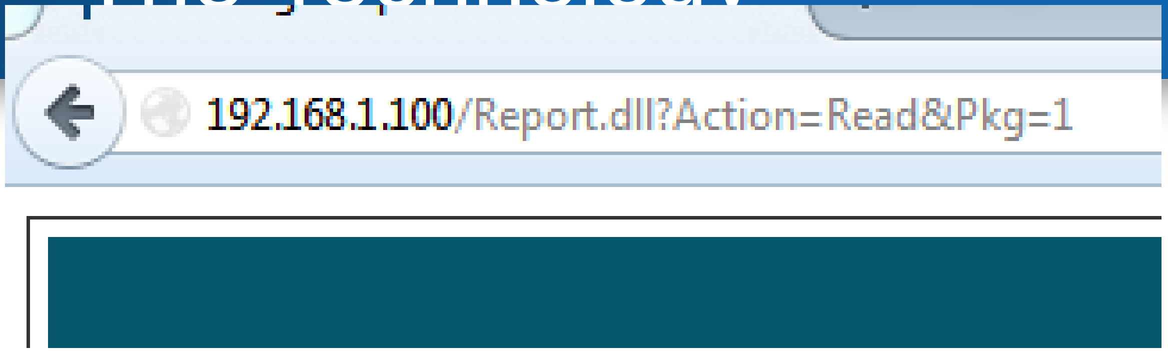
The Technology

- WinCE on ARM
- rbhttp22.dll == Intrinsyc Rainbow web server
- Web server calls mapped to an unmanaged ARM DLLs
- “BGI” – Binary Gateway Interface

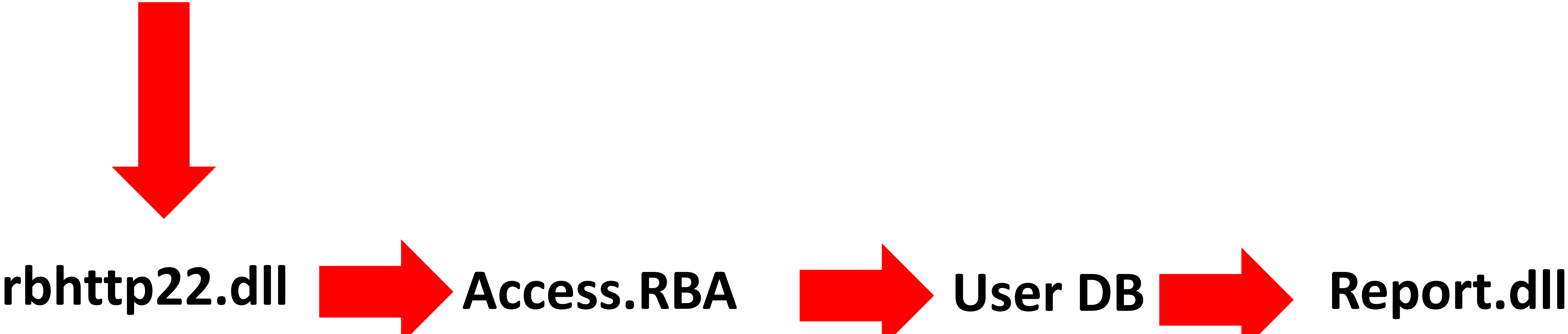


Name	Date modified	Typ
About.dll	11/11/2013 3:47 PM	App
ACCESS.RBA	11/11/2013 3:47 PM	RBA
AFUnderBodyFlush.dll	11/11/2013 3:47 PM	App
ConfigureBay.dll	11/11/2013 3:47 PM	App
ConfigureBridge.dll	11/11/2013 3:47 PM	App
ConfigureWash.dll	11/11/2013 3:47 PM	App
Counters.dll	11/11/2013 3:47 PM	App
DoubleProductivity.dll	11/11/2013 3:47 PM	App
Dwell.dll	11/11/2013 3:47 PM	App
EventDisplay.dll	11/11/2013 3:47 PM	App
FileManager.dll	11/11/2013 3:47 PM	App
Hidden.dll	11/11/2013 3:47 PM	App
HiPressureArch.dll	11/11/2013 3:47 PM	App
Home.dll	11/11/2013 3:47 PM	App
Keyboard.dll	11/11/2013 3:47 PM	App
LowPressureArch.dll	11/11/2013 3:47 PM	App
MailMs.dll	11/11/2013 3:47 PM	App

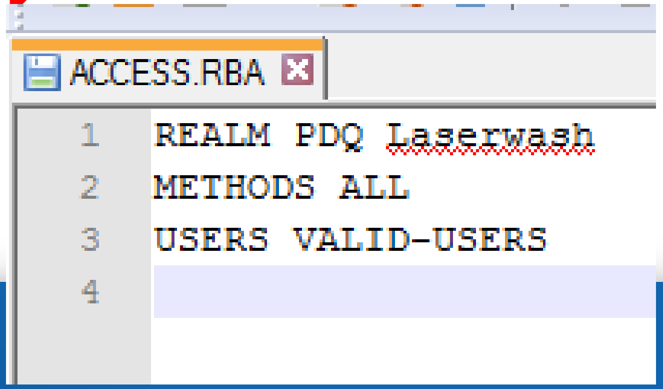
The Technology



192.168.1.100/Report.dll?Action=Read&Pkg=1



rbhttp22.dll → Access.RBA → User DB → Report.dll

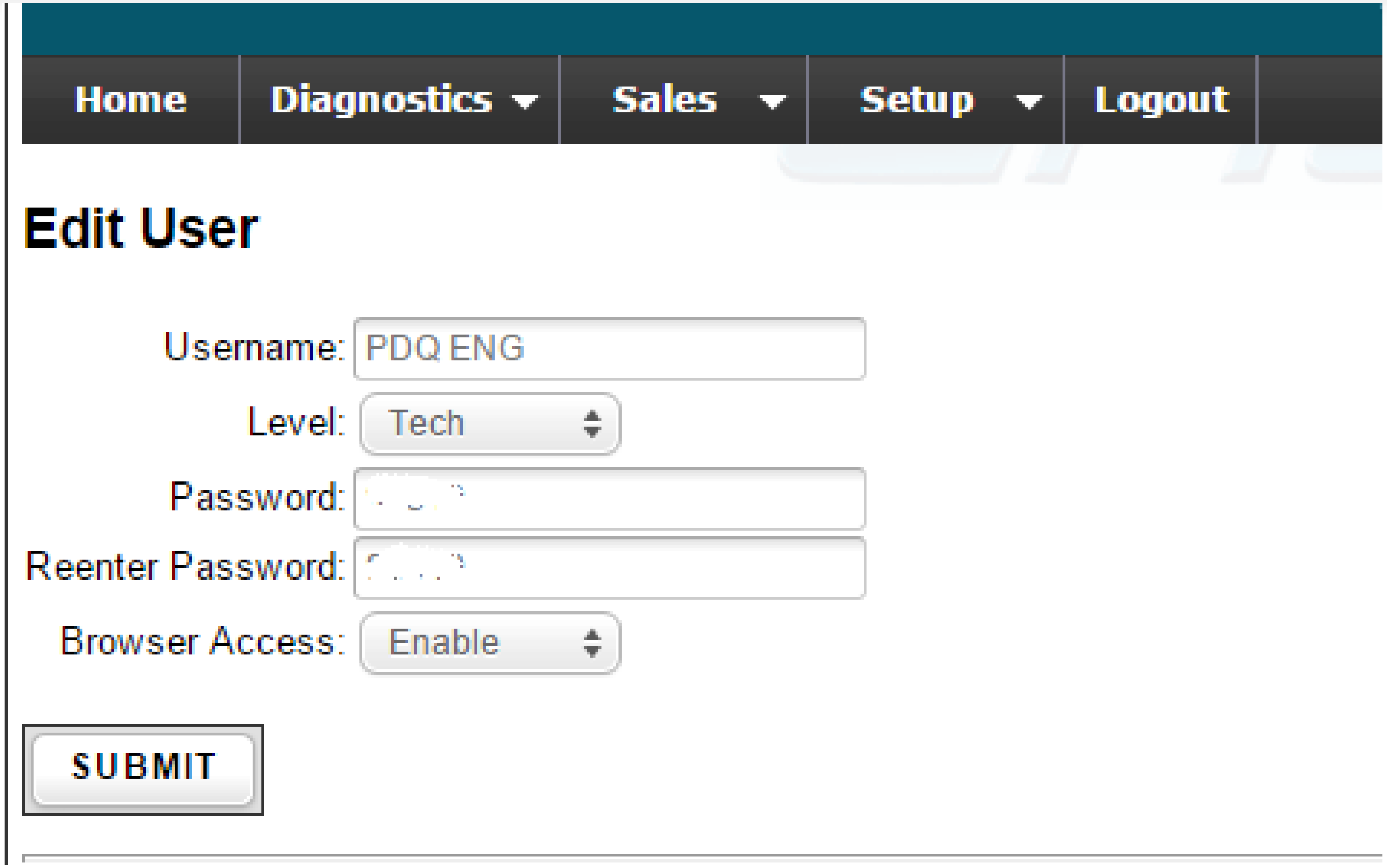


```
REALM PDQ Laserwash
METHODS ALL
USERS VALID-USERS

```

Credentials

- Owner – 12345
  - Full control, including free car washes ☺
- PDQ ENG - 83340
  - Engineering control, but no access to sales information and no free car washes
- Both sets of creds can cause safety issues



Edit User

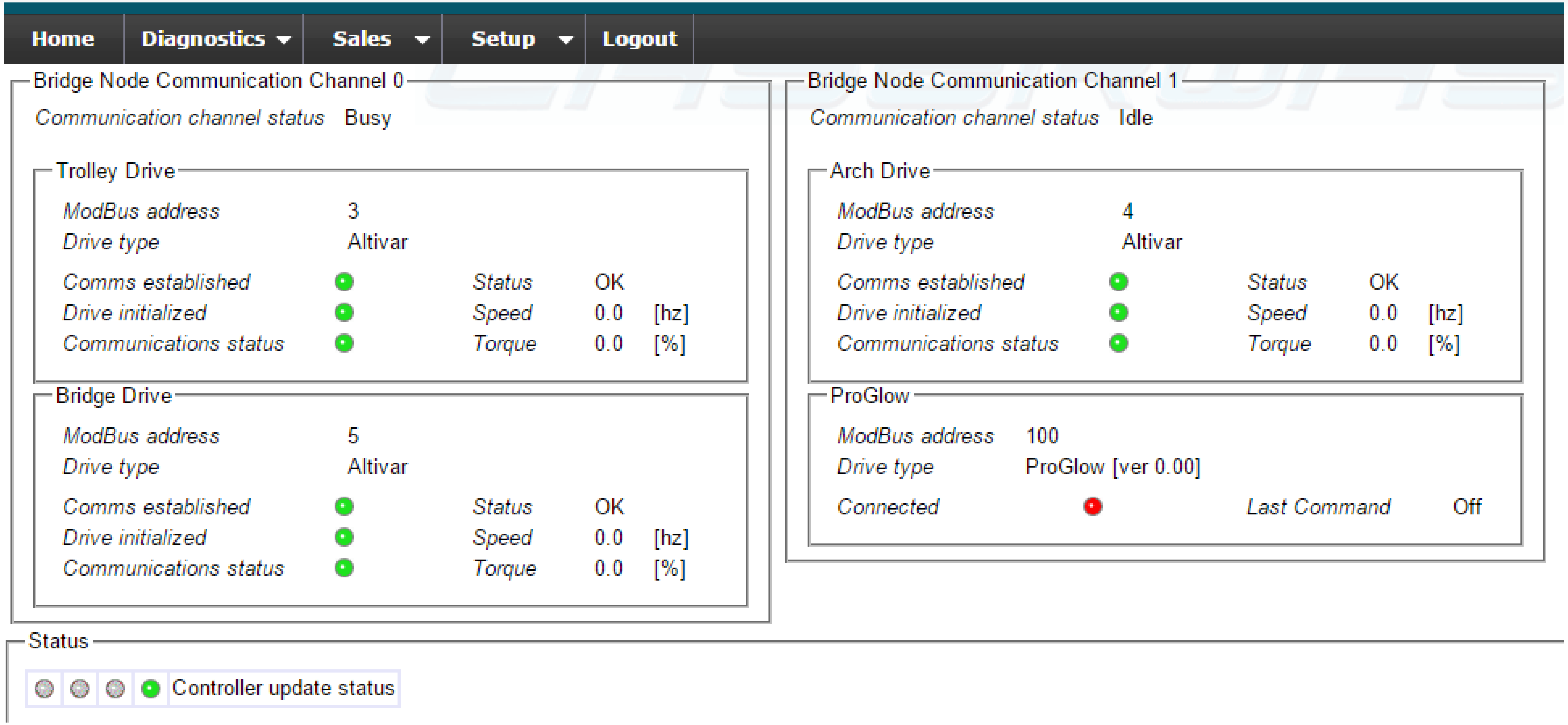
Username: PDQ ENG

Level: Tech

Password:

Reenter Password:

Browser Access: Enable



Bridge Node Communication Channel 0

Communication channel status Busy

Trolley Drive

ModBus address	3			
Drive type	Altivar			
Comms established	🟢	*Status*	OK	
Drive initialized	🟢	*Speed*	0.0	[hz]
Communications status	🟢	*Torque*	0.0	[%]

Bridge Drive

ModBus address	5			
Drive type	Altivar			
Comms established	🟢	*Status*	OK	
Drive initialized	🟢	*Speed*	0.0	[hz]
Communications status	🟢	*Torque*	0.0	[%]

Bridge Node Communication Channel 1

Communication channel status Idle

Arch Drive

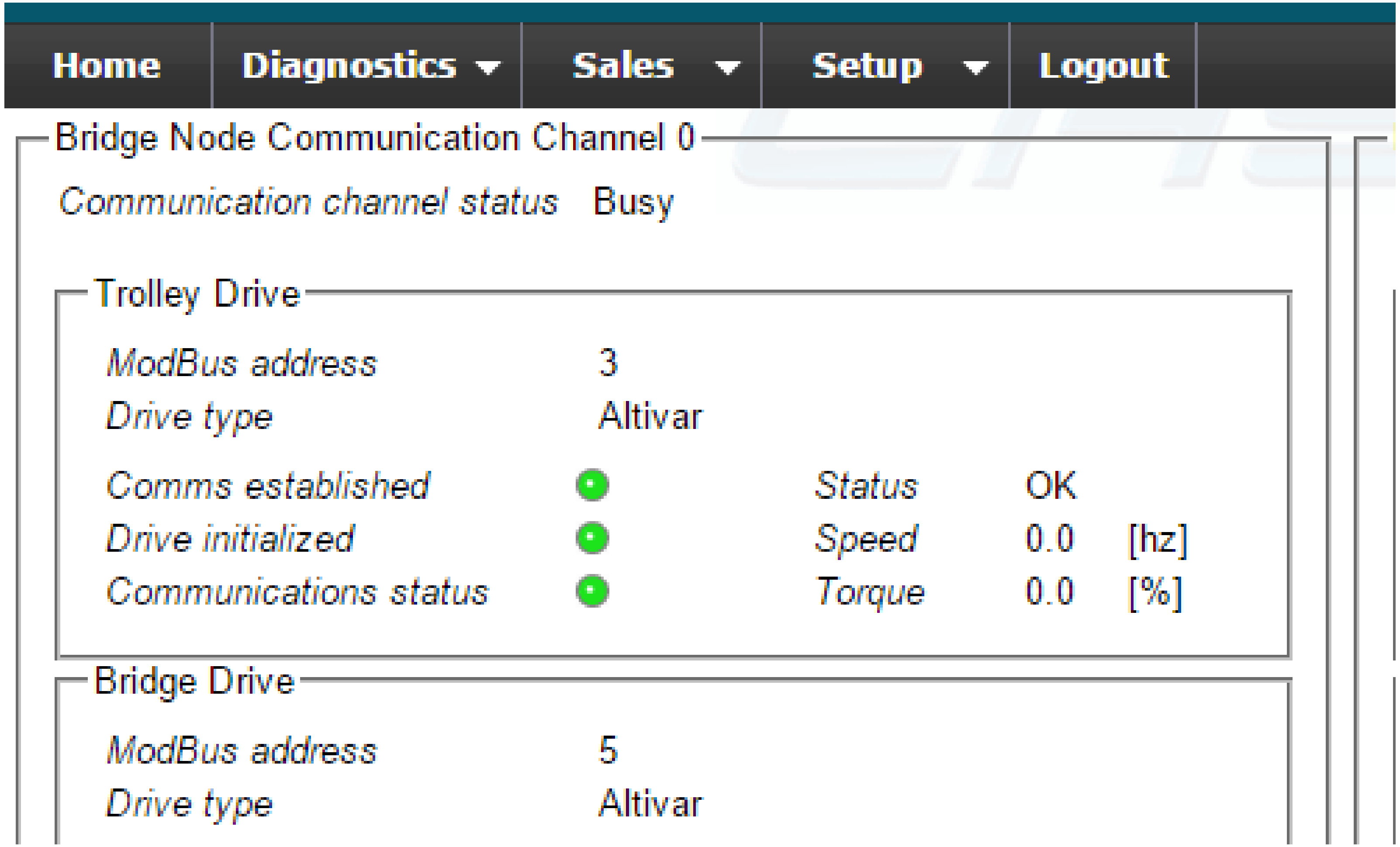
ModBus address	4			
Drive type	Altivar			
Comms established	🟢	*Status*	OK	
Drive initialized	🟢	*Speed*	0.0	[hz]
Communications status	🟢	*Torque*	0.0	[%]

ProGlow

ModBus address	100		
Drive type	ProGlow [ver 0.00]		
Connected	🔴	*Last Command*	Off

Status

○ ○ ○ 🟢 Controller update status



Bridge Node Communication Channel 0

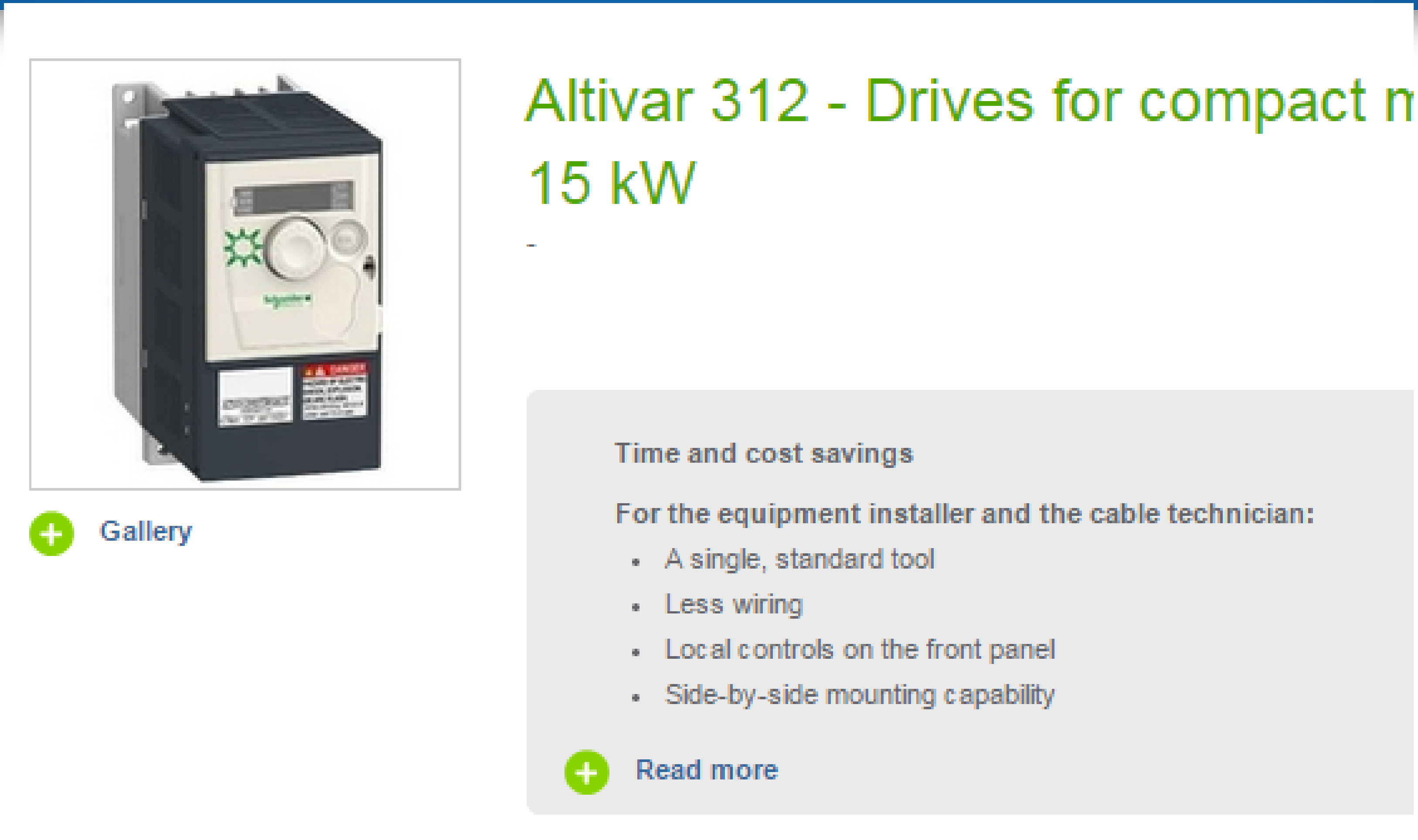
Communication channel status Busy

Trolley Drive

ModBus address	3			
Drive type	Altivar			
Comms established	●	*Status*	OK	
Drive initialized	●	*Speed*	0.0	[hz]
Communications status	●	*Torque*	0.0	[%]

Bridge Drive

ModBus address	5
Drive type	Altivar



Altivar 312 - Drives for compact m
15 kW

-

+ Gallery

Time and cost savings

For the equipment installer and the cable technician:

- A single, standard tool
- Less wiring
- Local controls on the front panel
- Side-by-side mounting capability

+ Read more

The Exploits

The Exploits

Additional detail will be added before the presentation

The Exploits

Identification of hardware safety mechanisms

The Exploits

Identification of software safety mechanisms

The Exploits

Authentication Bypass

The Exploits

Disabling of safety signals

The Exploits

Door exploits

The Exploits

Arm exploit

Safety Implications

Safety Implications

Additional detail will be added before the presentation

Safety Implications

Trapping an occupant inside the carwash

Safety Implications

Striking the occupant with the bay doors

Safety Implications

Striking the occupant with the arm

Moving Forward

Risk Measurement

CVSS does not adequately capture safety risks

CVSS Inadequacies

- Hospira Symbiq (Infusion Pump)
- Remote exploit - CVE-2015-3965
- A CVSS v2 base score: 7.1
- CVSS vector string: (AV:N/AC:M/Au:N/C:N/I:C/A:N)

CVSS Inadequacies

- Pyxis (Medical Supply Cabinet)
- Remote exploit - CVE-2014-5422
- A CVSS v2 base score: 9.7
- CVSS vector string: (AV:N/AC:L/Au:N/C:C/I:C/A:P)

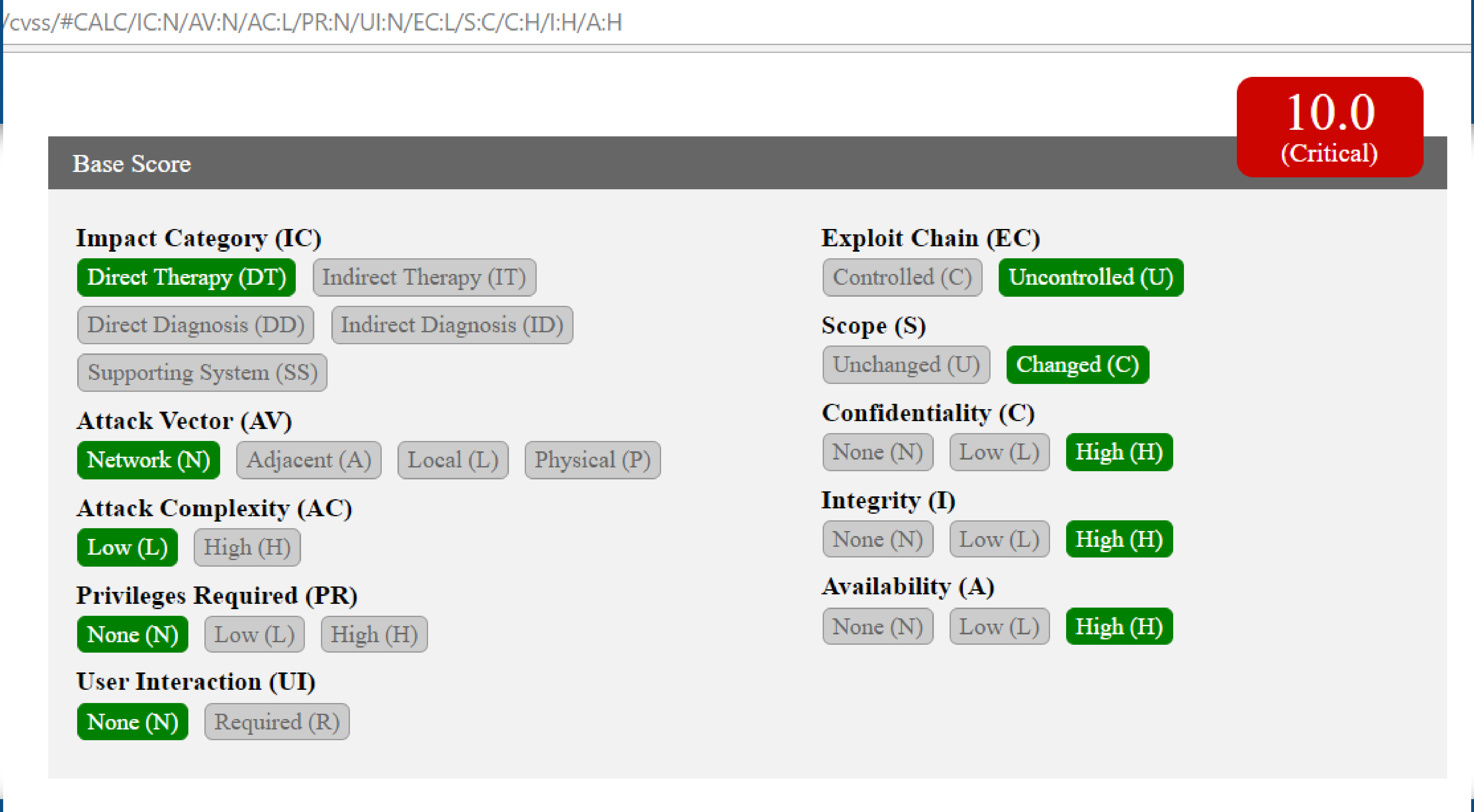
CVSS Inadequacies

Hospira Symbiq: 7.1 ← Can be used to kill someone

Pyxis Supply Station: 9.7 ← Can be used to steal supplies

Risk Measurement

Here is a system that considers “effect”



/cvss/#CALC/IC:N/AV:N/AC:L/PR:N/UI:N/EC:L/S:C/C:H/I:H/A:H

10.0
(Critical)

Base Score

Impact Category (IC)

[✓ Direct Therapy (DT)] Indirect Therapy (IT)
Direct Diagnosis (DD) Indirect Diagnosis (ID)
Supporting System (SS)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

[✓ None (N)] Low (L) High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Exploit Chain (EC)

Controlled (C) [✓ Uncontrolled (U)]

Scope (S)

Unchanged (U) [✓ Changed (C)]

Confidentiality (C)

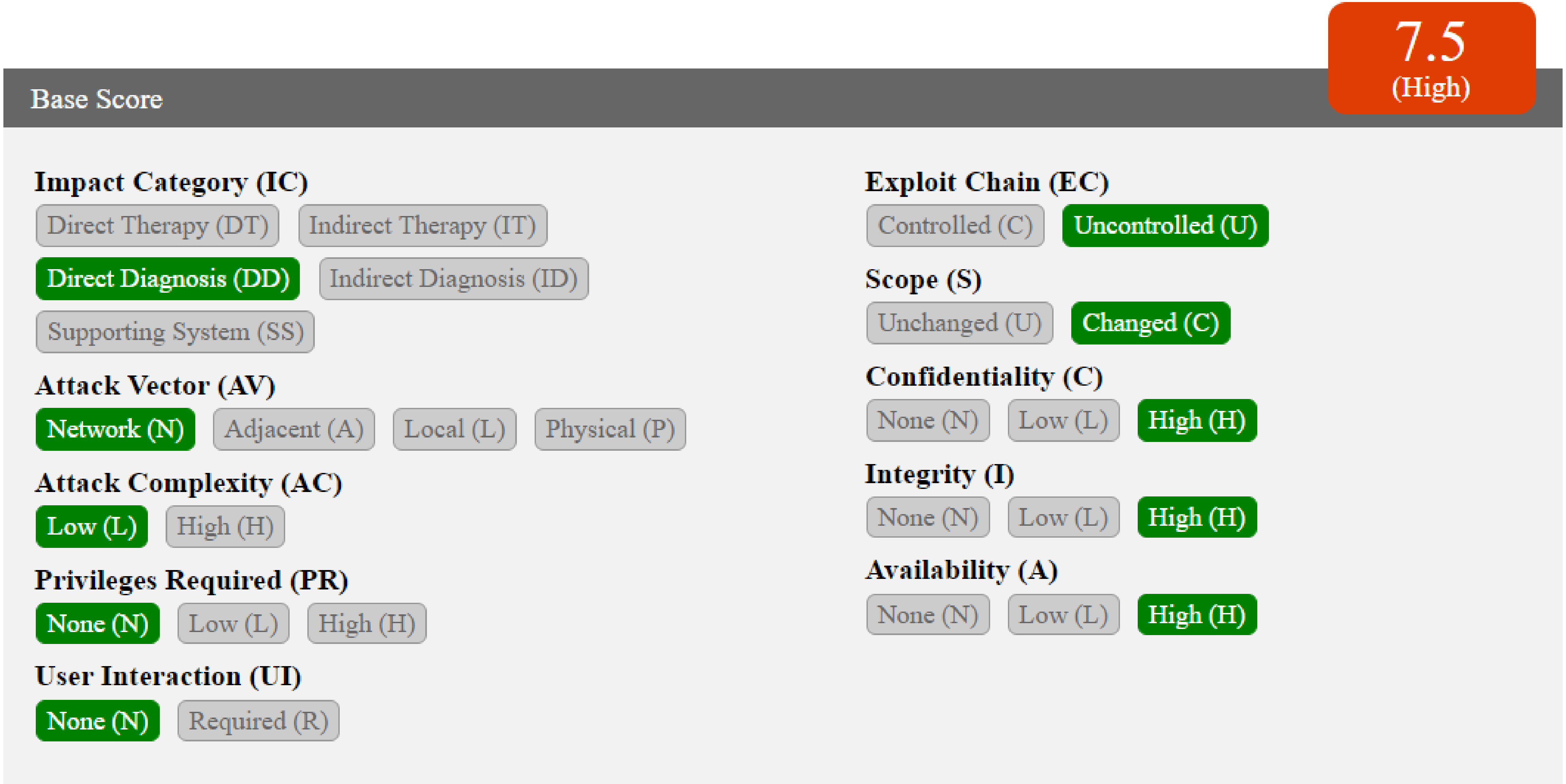
None (N) Low (L) [✓ High (H)]

Integrity (I)

None (N) Low (L) [✓ High (H)]

Availability (A)

None (N) Low (L) [✓ High (H)]



7.5
(High)

Base Score

Impact Category (IC)

Direct Therapy (DT) Indirect Therapy (IT)
[✓ Direct Diagnosis (DD)] Indirect Diagnosis (ID)
Supporting System (SS)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

[✓ None (N)] Low (L) High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Exploit Chain (EC)

Controlled (C) [✓ Uncontrolled (U)]

Scope (S)

Unchanged (U) [✓ Changed (C)]

Confidentiality (C)

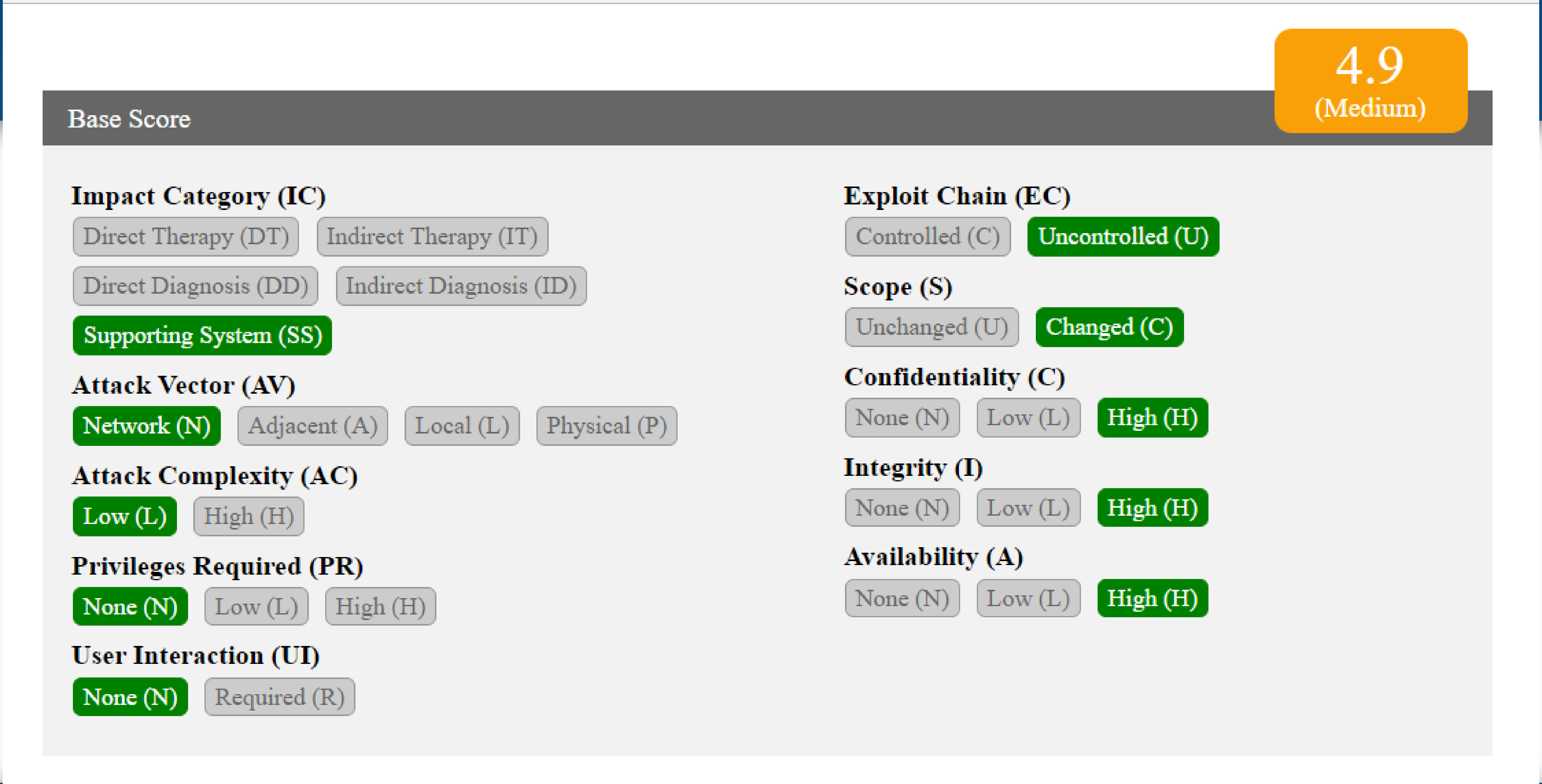
None (N) Low (L) [✓ High (H)]

Integrity (I)

None (N) Low (L) [✓ High (H)]

Availability (A)

None (N) Low (L) [✓ High (H)]



4.9
(Medium)

Base Score

Impact Category (IC)

Direct Therapy (DT) Indirect Therapy (IT) Direct Diagnosis (DD) Indirect Diagnosis (ID) [✓ Supporting System (SS)]

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

[✓ None (N)] Low (L) High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Exploit Chain (EC)

Controlled (C) [✓ Uncontrolled (U)]

Scope (S)

Unchanged (U) [✓ Changed (C)]

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

Integrity (I)

None (N) Low (L) [✓ High (H)]

Availability (A)

None (N) Low (L) [✓ High (H)]

Software and Safety

Design ≠ Implementation ≠ Reality

The Butts-Rios Law

The Security Law of Cyber-Physical Systems:

The mechanical functions of a cyber-physical system are bounded only by the physical limits of the hardware components.

Prediction

Exploitation of a system that relies on software controls for implementing mechanical safety will result in the loss of life

Thanks!

WhiteScope

Billy Rios - Founder

Billy.Rios@Whitescope.io

http://whitescope.io