Hands-on: Smart Bulb Security Demonstration and Basic Testing

Learning Objectives

After completing this activity, students will be able to:

- Understand basic IoT device functionality
- Identify common IoT security vulnerabilities
- Execute basic security tests
- Observe real-time attack impacts
- Understand the importance of IoT security

Required Materials

- Computer with Windows OS
- Internet connection
- Web browser
- Command Prompt/PowerShell
- Text editor (Notepad or similar)

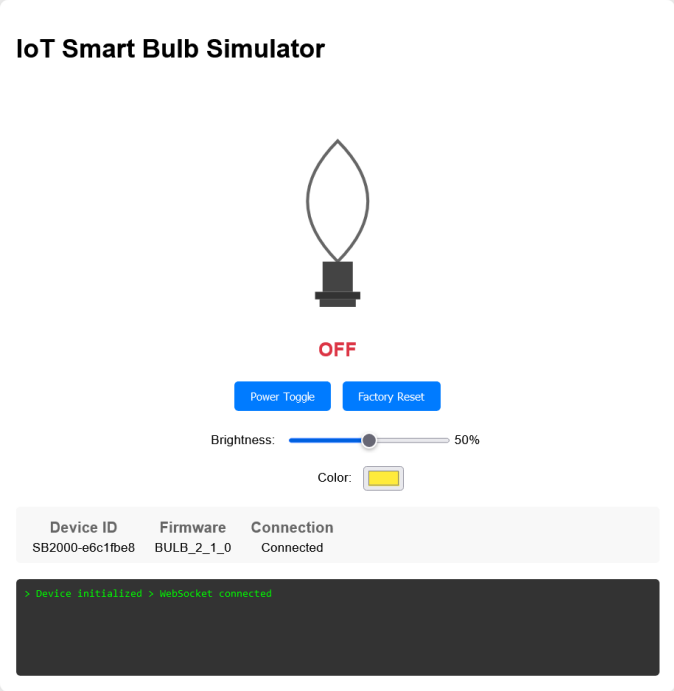
Instructions

1. Environment Preparation
    - Download https://github.com/mitayag/iotsecurity.git
    - Create a folder name smartbulb and copy the file in the download repository folder **/lab/smartbulb**.
2. Open the folder in VSCode.
3. Install Python packages
    - Open a terminal on your VSCode
    - Type `pip install flask flask-socketio`
4. Run the application type `python smart_bulb_server.py`

Understanding the Smart Bulb Interface

5. Access the Smart Bulb

```
# Open web browser and navigate to:
http://localhost:8080
```



Basic Interface Testing

- ☐ Click the power button to turn the bulb on/off
- ☐ Move the brightness slider
- ☐ Use the color picker to change colors
- ☐ Note the device information displayed

Record Observations

- ☐ What information can you see about the device?
- ☐ What controls are available?
- ☐ Was any password required to access the device?

API Endpoints

An API (Application Programming Interface) is a set of rules, protocols, and tools that allow software applications to communicate with each other. It acts as a bridge between different software systems, enabling them to share data or functionality in a standardized way.

- ☐ GET / # Web interface
- ☐ POST /api/control/power # Power control
- ☐ POST /api/control/brightness # Brightness control
- ☐ POST /api/control/color # Color control
- ☐ POST /api/control/factory_reset # Factory reset

Basic Security Testing

6. Check Device Status

```
# Open Command Prompt and type:
curl http://localhost:8080/api/status
```

- ☐ Record the information received
- ☐ Note any sensitive data exposed

7. Control Testing

Note: Each commands will be executed on the terminal of you VSCode

 # Turn the bulb on

```
curl -X POST http://localhost:8080/api/control/power -H "Content-Type: application/json" -d "{\"state\": true}"
```

 # Turn the bulb off

```
curl -X POST http://localhost:8080/api/control/power -H "Content-Type: application/json" -d "{\"state\": false}"
```

- ☐ Did the commands work?
- ☐ What happened on the web interface?

 # Setting Maximum Brightness...

```
curl -X POST http://localhost:8080/api/control/brightness -H "Content-Type: application/json" -d "{\"brightness\": 100}"
```

 # Changing Colors

```
curl -X POST http://localhost:8080/api/control/color -H "Content-Type: application/json" -d "{\"color\": \"#FF0000\"}"
```

Summary:

After completing this hands-on IoT security laboratory activity, students have gained practical experience in analyzing and testing the security of IoT devices through a simulated smart bulb system. Through this interactive session, they've learned to identify and exploit common security vulnerabilities found in IoT devices, while understanding the potential real-world implications of these security flaws.