# CYBR-10025 – Lab 2: Electrobuy

# Objective(s):

Check out a cart full of goods from Electrobuy without paying for it!

# Introduction:

Electrobuy is a major re-seller of electronic goods but their website was developed over a long period of time and most of the development team is no longer working for them. They believe that there may be backdoors or other security flaws in the system. You have been hired to test their security.

# Apparatus

* VirtualBox https://www.virtualbox.org/wiki/Downloads
* Electrobuy.ova from Canvas.

# Procedure

1. Import the electrobuy.ova
2. ***Start the electrobuy VM***
3. ***Note the IP address on the boot screen (likely 192.168.99.101)***
4. ***Point your web browser at:*** [***http://192.168.99.101/electrobuy***](http://192.168.99.101/electrobuy)
5. ***When you think you have got it solved click the “checkout” button on your shopping cart for a status message.***

# What To Hand In

* A MS Word file containing:
  + A written step-by-step log of the different things you investigated, information you gathered and what techniques you tried. Doing well on this assignment depends on writing clear instructions on how to gain high level access. If the person marking can’t repeat your steps and get the same effect this will cost you marks.
  + Screenshot from your browser showing the message you get when you checkout with a cart full of free product.

# Rules

1. You may not use an automated tool like Nessus.
2. You may not use a local attack: That is an attack that would require you to be in the same room as the Linux machine if the web application was running on a physical machine instead of a VM. All attacks must be executable using remote tools (browser, ssh, netcat, etc…)
3. ***You may do just about anything else.***

# Hints:

1. Explore the web site and make note of form fields, cookies and how they are sent.
2. Examine the HTML look for other directories you might have access to.
3. Review the slide decks and videos from this course which show specific kinds of attacks.