Report – Project 3, Computer Security

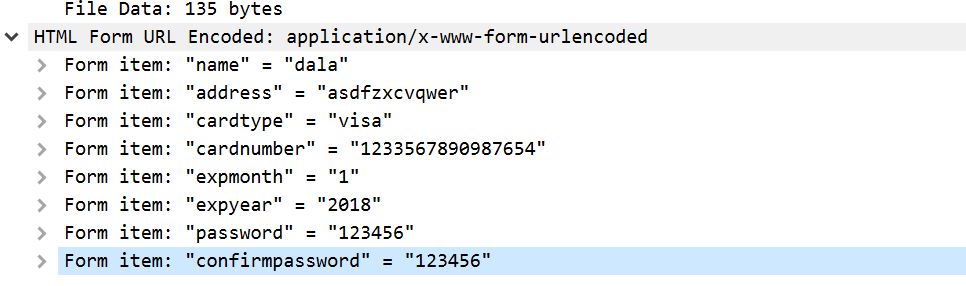
By: Zhou Shen, Subhash Rajapaksha

# Vulnerabilities in lucy.mscs.mu.edu

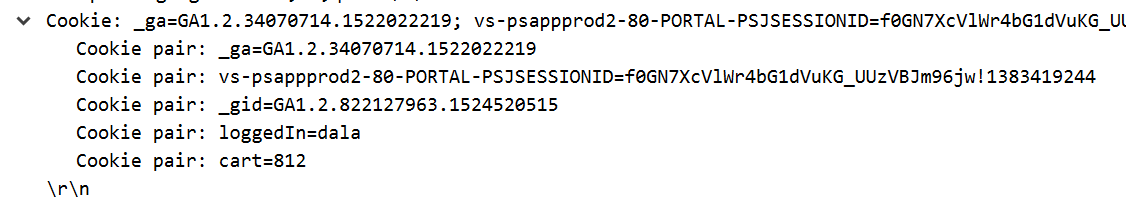
The web site lucy.mscs.mu.edu has below vulnerabilities.

## Spoofing the network traffic

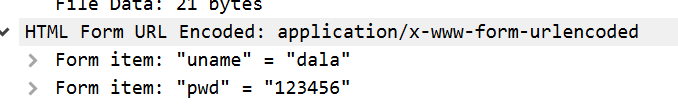
* Change data page in Terba Mate shop posts data openly. No encryption. Wireshark traces extracts data.



* Cookie information can be seen.



* Login information can be seen.



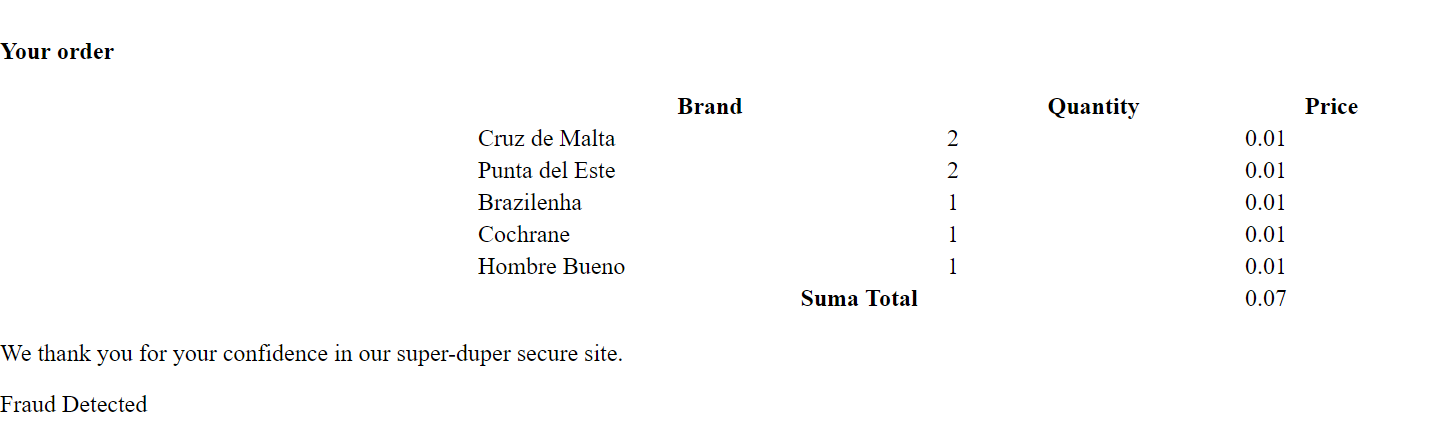
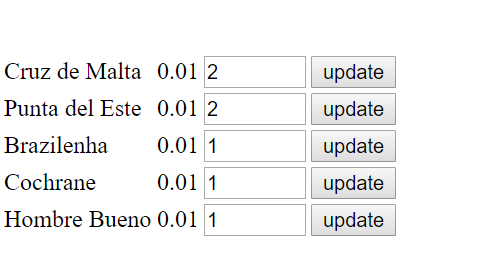
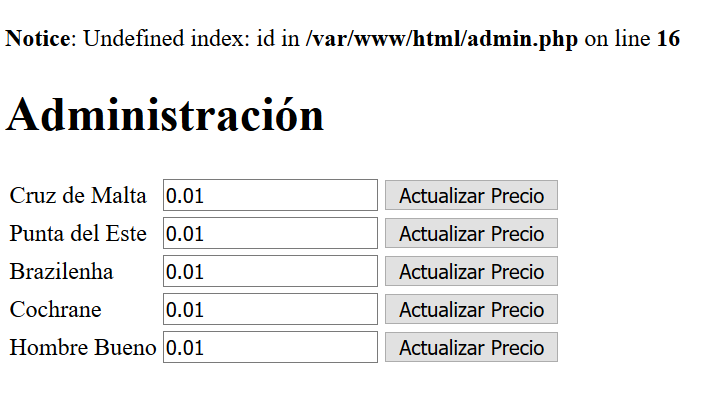
## Banner grabbing

Banner grabbing with telnet command, server information could be obtained.



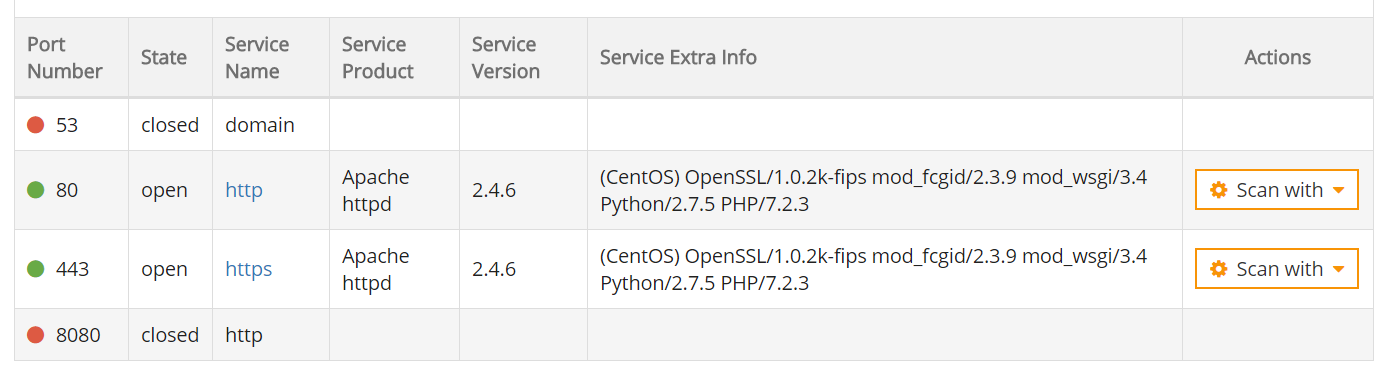
## URL guessing

Guessing the url admin.php and register.php worked. Admin.php allows changing unit prices of the products.



## Port scanning

TCP port scan using Nmap (<https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap>) gave information about open ports.



## SQL injection

The example 1 and login to the Yerba Mate Shop is vulnerable to below injection attacks.

Option 1: If the username is known, using the user name followed symbols ‘/\* and password \*/’ will let the intruder to log in. For example, if the user is ‘test’, then the username= test’/\* and password=\*/’

Option 2: When there is no any user name, username = 1’ or ‘1’=’1 and password = 1’ or ‘1’=’1 will let the intruder log in.