10/10/19 Francesco Penasa, homework-4

exercise 2

We tried to observer the requests done to the server in order to see if something was changeable in order to discover Bartholomew's salary. To start such requests we tried to open the webpage and specify the user displayed in the table. Using OWASP ZAP, we have noticed that only one request to the web server is done even while changing the employee multiple times. Such observation lead us to think that the employee information are not request every time for a specific user but that there is some kind of client side filter. Intercepting the first webserver response after reloading the page with OWASP ZAP we are able to see that the webserver gives us a JSON containing the data of all users, that are then filtered and displayed. In fact we see only the selected user in the browser page, yet the JSON contains all users data. If we explore such JSON we are able to check the CEO'S information, which are the following.
Results:

```
"Salary" : "450000",
"UserID" : "112",
"FirstName" : "Neville",
"LastName" : "Bartholomew",
"SSN" : "111-111-1111"
```

exercise 3

We can inspect the page to see if it is possible to change some hidden values to grant us the discount. While doing such research we can see the following comment in the webpage.
`<!-- Checkout code: webgoat, owasp, owasp-webgoat -->`
After checking the checkout codes in the comment we can say that such codes work and it is possible to use them to have a discount.
Results: use one of the following codes `webgoat`, `owasp`, `owasp-webgoat` to have a discount on the purchase.