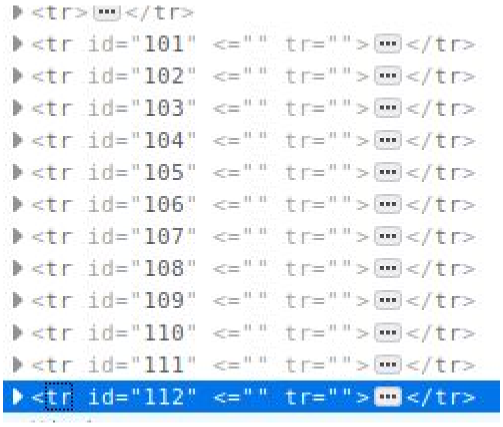
Assignment 4 – Client side Filtering

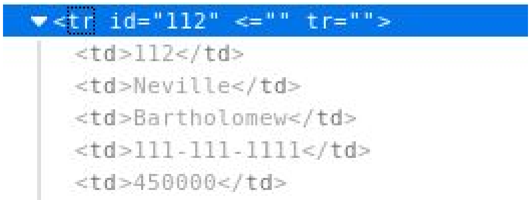
2. **Salary Manager**

- From the hint, I had to examine the drop down menu and I noticed Neville Bartholomew was not listed.
- So I inspected the source code of the page, where I noticed a the tables of the employees and their data.



```
<tr>…</tr>
<tr id="101" <="" tr="">…</tr>
<tr id="102" <="" tr="">…</tr>
<tr id="103" <="" tr="">…</tr>
<tr id="104" <="" tr="">…</tr>
<tr id="105" <="" tr="">…</tr>
<tr id="106" <="" tr="">…</tr>
<tr id="107" <="" tr="">…</tr>
<tr id="108" <="" tr="">…</tr>
<tr id="109" <="" tr="">…</tr>
<tr id="110" <="" tr="">…</tr>
<tr id="111" <="" tr="">…</tr>
<tr id="112" <="" tr="">…</tr>
```

- After which I noticed the additional element that was not seen in the client side.
- The rest was about clicking and opening the html table tags to find out different fields associated with different employees.
- The manager is the last person on the list and his details are clear here

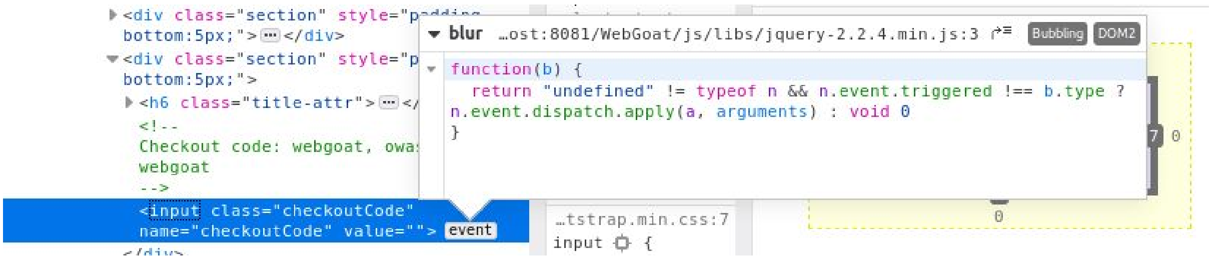


```
<tr id="112" <="" tr="">
    <td>112</td>
    <td>Neville</td>
    <td>Bartholomew</td>
    <td>111-111-1111</td>
    <td>450000</td>
```

Hence, the manager's salary is 450000

3. **Get Samsung Galaxy S8 for free**

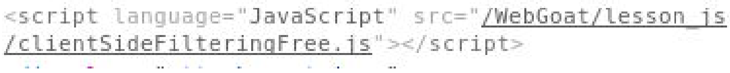
- From the hint, I noticed I needed to inspect the webpage source where I found an js event listener attached to the input field of the coupon code.



```
<div class="section" style="padding-
bottom:5px;">…</div>
<div class="section" style="p
bottom:5px;">
  <h6 class="title-attr">…</
  <!--
  Checkout code: webgoat, owa
  webgoat
  -->
  <input class="checkoutCode"
  name="checkoutCode" value=""> event
</div>
```

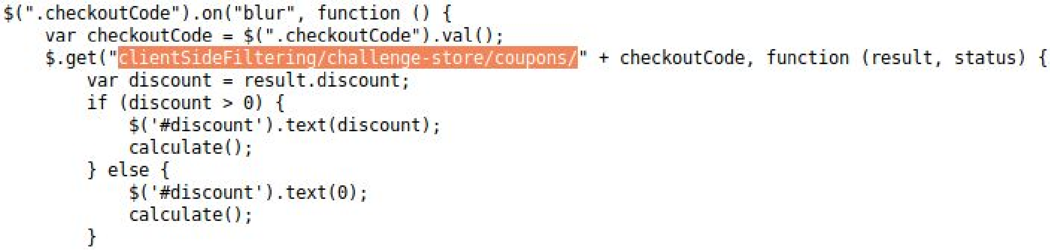
```
blur …ost:8081/WebGoat/js/libs/jquery-2.2.4.min.js:3
function(b) {
  return "undefined" != typeof n && n.event.triggered !== b.type ?
n.event.dispatch.apply(a, arguments) : void 0
}
```

- The next hint stated that check the response to the backend page. So I inspected the source code closely and noticed the an outer javascript file called in this html page.



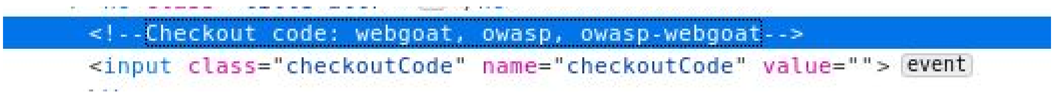
```
<script language="JavaScript" src="/WebGoat/lesson_js
/clientSideFilteringFree.js"></script>
```

- I copied the url, appended the webgoat url at the beginning and pasted it on a new tab on firefox to examine the javascript file carefully.
- After careful examination, I noticed the event listener attached to the input field of the coupon code.



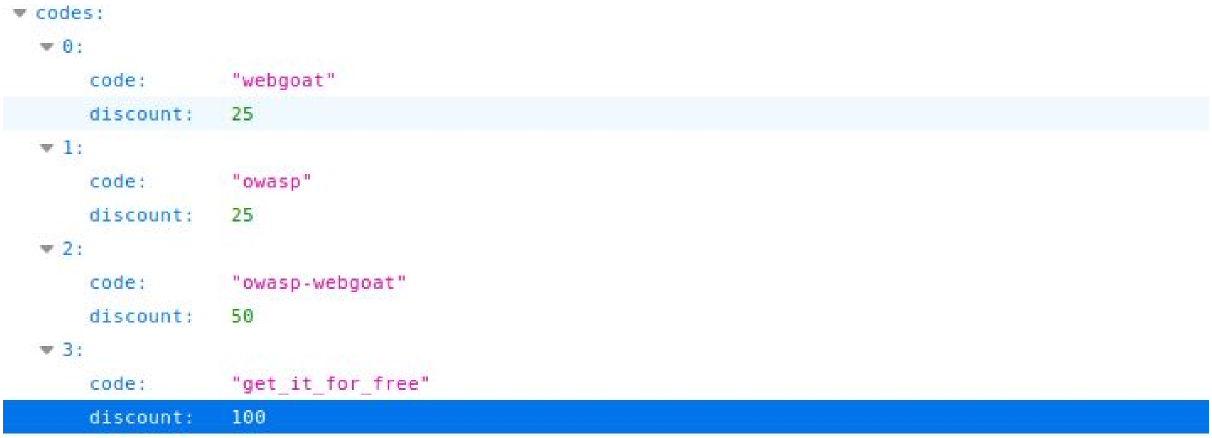
```
$(".checkoutCode").on("blur", function () {
    var checkoutCode = $(".checkoutCode").val();
    $.get("clientSideFiltering/challenge-store/coupons/" + checkoutCode, function (result, status) {
        var discount = result.discount;
        if (discount > 0) {
            $('#discount').text(discount);
            calculate();
        } else {
            $('#discount').text(0);
            calculate();
        }
```

- The calculate() function here is calculating the free coupons and we also notice the get function is getting the free coupons from another page. The url is highlighted in the image above.
- I copied the url, appended the webgoat url at the beginning and pasted it on a new tab on firefox. This time, it a json file with same items listed on the comment section here.



```
<!--Checkout code: webgoat, owasp, owasp-webgoat-->
<input class="checkoutCode" name="checkoutCode" value=""> event
```

The content of the json file is below:



```
▼ codes:
  ▼ 0:
      code:       "webgoat"
      discount:   25
  ▼ 1:
      code:       "owasp"
      discount:   25
  ▼ 2:
      code:       "owasp-webgoat"
      discount:   50
  ▼ 3:
      code:       "get_it_for_free"
      discount:   100
```

Now, we can see each code with it corresponding discount and because we want a 100% discount, our answer is: ‘get_it_for_free’