

WebGoat Client Side Filtering

Twitter: @BlackSheepSpicy

Twitch: https://twitch.tv/BlackSheepSpicy

2. Oh good, more digging through code:





Shovels out lads, lets look for treasure:

```
<select id="UserSelect" onfocus="fetchUserData()"
</pre>
 name="UserSelect" onchange="selectUser()"> @
   <option value="0" label="Choose Employee">
   Choose Employee</option>
   <option value="101" label="Larry Stooge">Larry Stooge
  </option>
   <option value="103" label="Curly Stooge">Curly Stooge
   </option>
   <option value="104" label="Eric Walker">Eric Walker
  <option value="105" label="Tom Cat">Tom Cat</option>
   <option value="106" label="Jerry Mouse">Jerry Mouse
  </option>
  <option value="107" label="David Giambi">David Giambi
  </option>
  <option value="108" label="Bruce McGuirre">
  Bruce McGuirre</option>
  <option value="109" label="Sean Livingston">
  Sean Livingston</option>
  <option value="110" label="Joanne McDougal">
   Joanne McDougal</option>
 </select>
```

So we come across this option tree right here: lets play around with the values a bit:

Or just skip it and get right to the good stuff:

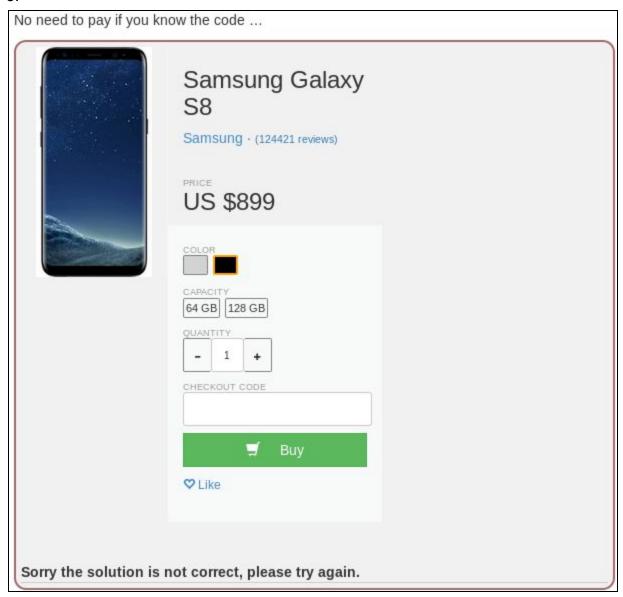
```
<option value="112" label="Larry Stooge">Larry Stooge
</option>
```

Now if we change the employee menu to big larry up here we can get the info that we need:





3.



Get ready for some mega digging

So let's start by digging through the code again, I found this first:

```
<!--Checkout code: webgoat, owasp, owasp-webgoat-->
```



If you play around with these codes, you'll notice nothing goes over the wire, meaning the discount calculation is done locally, also you'll notice when the check out request goes out only the discount code is included:

```
POST /WebGoat/clientSideFiltering/getItForFree HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost:8080/WebGoat/start.mvc
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 13
Cookie: JSESSIONID=D1C1EE6F3C23901AF91E56C4B7E9B634; WEBWOLFSESSION=84E550CB4AAFB5CECA2B8AF9270642C7
Connection: close
checkoutCode=
```

So... the free code is stored somewhere on our machine... and we have to find it...

Thanks to one of my viewers tehEGO, we tracked down the .js function that calculates the discount by searching for ".js" and running through every entry until we found something interesting:

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

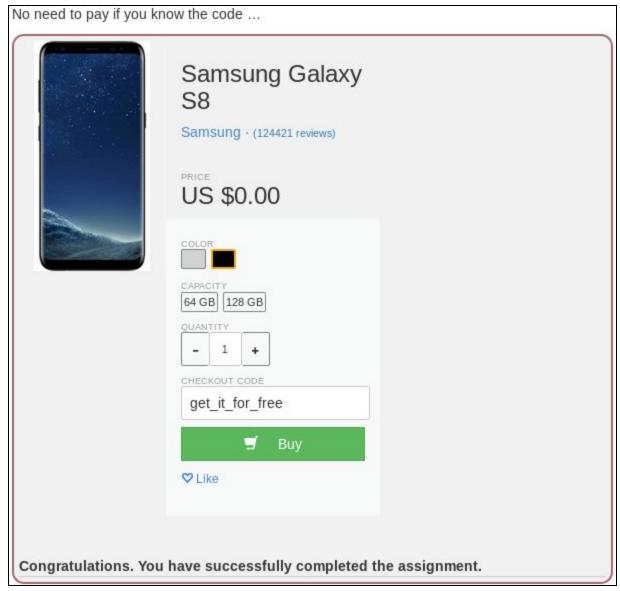
Alright, lets dig thru that code now:

```
0:
                "webgoat"
   code:
   discount:
                25
T1:
   code:
                "owasp"
   discount:
               25
                "owasp-webgoat"
   code:
   discount:
                "get_it_for_free"
    code:
   discount:
               100
```





Slap that code into the challenge and we win ourselves a free phone:



Free and worth the price... because we don't actually get a phone sadly... just like... the concept of one i guess...



So many short write ups when cleaning up the rest of Webgoat. Regardless I hope you enjoyed this write up! If you want to see me overthink these challenges live be sure to drop by my Twitch when I'm live and also follow my Twitter for some fresh memes!

