java代码审计
深度解析

第八课 DOM型XSS及总结
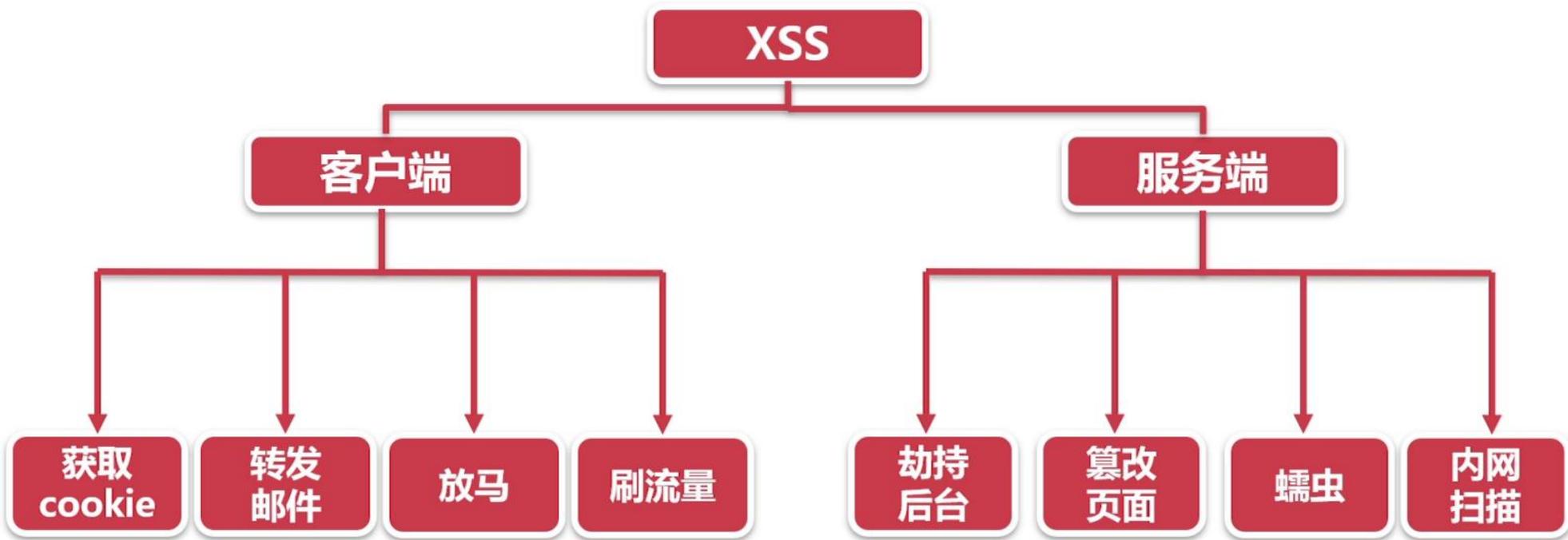
DOM型XSS

可能触发DOM型XSS的属性

◆ document.referer属性

◆ location属性

◆ innerHTML属性

赛博梦工厂
Cyber Works

```
"shenjisaomiaojieguo - WebRoot/jsp/repair/ckupRecordList.jsp - Audit Workbench
ile  Edit  Tools  Options  Help

addInventorylog.jsp    Project Summary    right_news.jsp    exequipment.jsp    BaseAction.java    exwarehouseequip.jsp    inequipment.jsp    ckupRecordList.jsp

10  <html>
11  <head>
12      <title>检定管理</title>
13
14  <meta http-equiv="pragma" content="no-cache">
15      <meta http-equiv="cache-control" content="no-cache">
16      <meta http-equiv="expires" content="0">
17      <meta http-equiv="keywords" content="keyword1,keyword2,keyword3">
18      <meta http-equiv="description" content="This is my page">
19      <link href="<%=basePath %>css/reset.css" rel="stylesheet" type="text/css" />
20      <link href="<%=basePath %>css/style.css" rel="stylesheet" type="text/css">
21      <script src="../js/jquery-1.4.min.js" type="text/javascript"> </script>
22      <script src="<%=basePath %>js/public.js" type="text/javascript"> </script>
23      <script type="text/javascript" src="../js/My97DatePicker/WdatePicker.js"></script>
24      <script language="javascript" >
25
26      function search(){
27          var checkupnumber=document.getElementById("checkupnumber").value;
28          var ckupresult=encodeURI(encodeURI(document.getElementById("ckupresult").value));
29          var begintime=document.getElementById("begintime").value;
30          var endtime=document.getElementById("endtime").value;
31
32          window.location.href="<%=basePath%>repair/searchCkupHistoryPages.action?checkupnumber="+checkupnumber+"&ckupresult="+ckupresult+"&begintime="+begintime+"&
33      }
34      </script>
35  </head>
36
37  <BODY bgColor="#dee7ff" leftMargin="0" background="" topMargin="0"
38      marginheight="0" marginwidth="0">
39      <center>
40          <table class="navposition" cellpadding="0" cellspacing="0">
41              <tr>
42                  <td class="titleBg leftwidth">
43                      <div class="titleLeft">
44                           
45                      </div>
46                  </td>
47                  <td class="titleBg title">
48                      <span>当前位置: </span><span>维修检定 &gt;&gt; 检定记录</span>
49                  </td>
50                  <td class="titleBg rightwidth">
51                      <div class="titleRight">

html/head/script/#text                                    Writable    Smart Insert    32 : 98
```

谢谢观赏