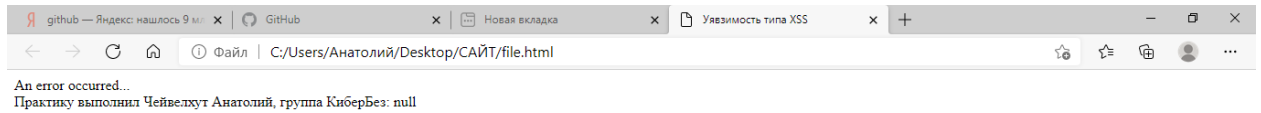
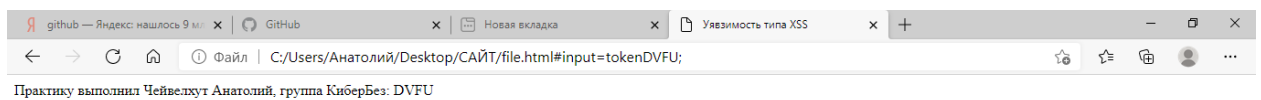


Практическая работа. XSS уязвимости на примере html-документа



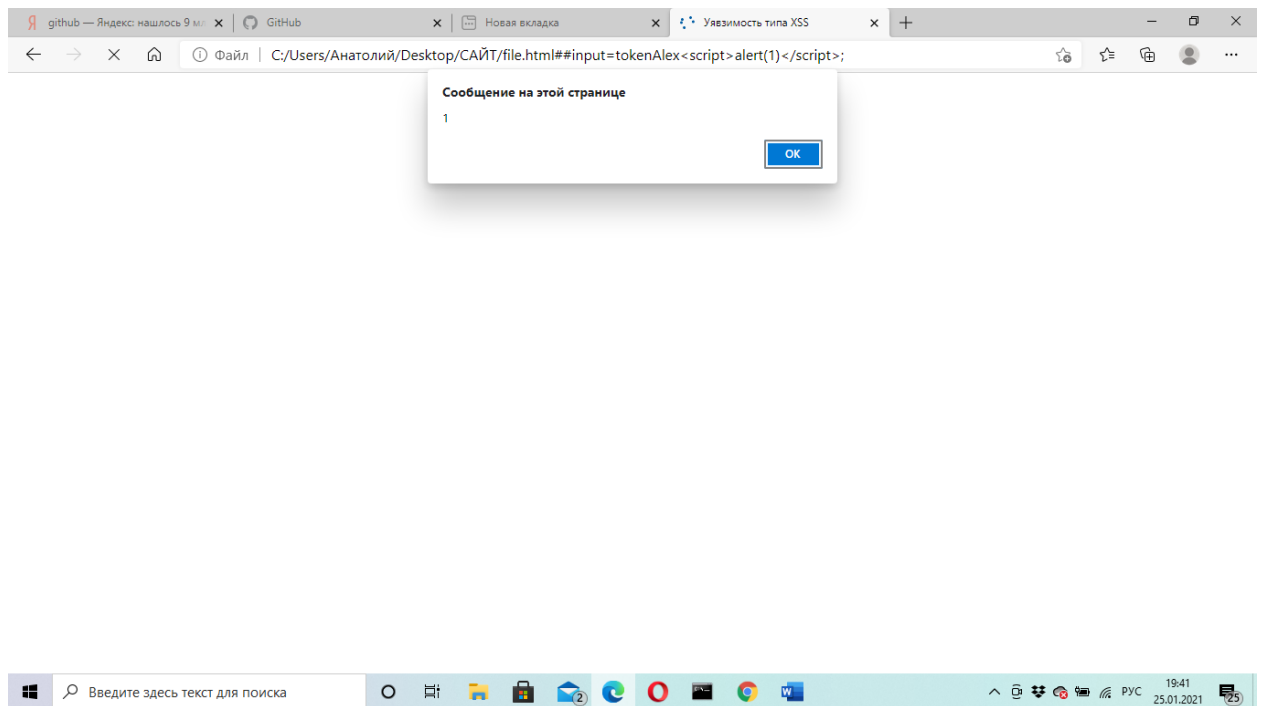
Добавим в адресную строку к текущему адресу следующее значение: **#input=tokenDVFU;**



При обновлении адресной строки значение, которое находилось в адресной строке присвоилось переменной внутри скрипта, которое впоследствии вывелось на экран.

Затем 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.