INTERNSHIP STUDIO

TASK 3 REPORT

Spoorthi Udupa

STEPS TAKEN:

STEP 1: VISIT HTTP://TESTASP.VULNWEB.COM/

STEP 2: ON THE TOP MENU YOU WILL FIND A SEARCH OPTION.

STEP 3: CLICK ON IT AND YOU WILL BE PROMPTED WITH THE SEARCH BOX.

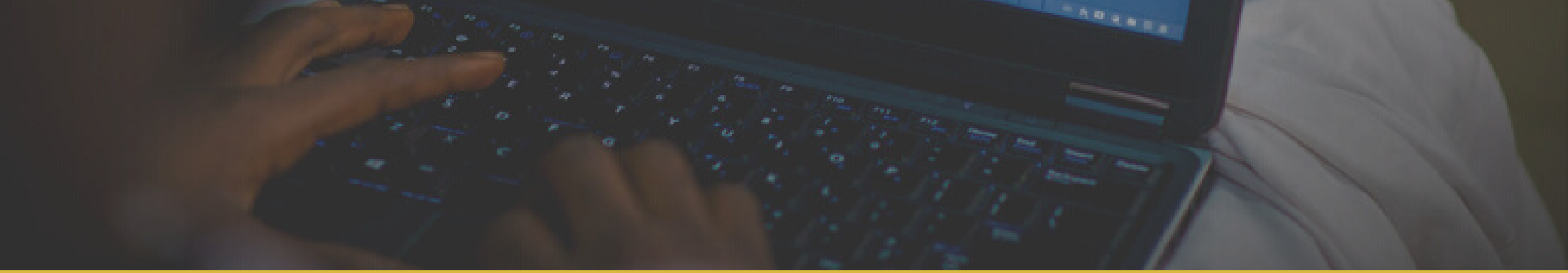
STEP 4: YOU CAN INTERCEPT THE REQUEST IN BURP SUITE

STEP 5: NOW YOU CAN FIND DIFFERENT PAYLOADS FOR XSS.

STEP 6: SEND THE REQUEST TO THE INTRUDER AND PASTE ALL THE PAYLOADS.

STEP 7: TRY TO FIND A SUCCESSFUL PAYLOAD FOR XSS.

STEP 8: PREPARE A REPORT FOR IT.



Report

Cross site scripting (XSS) is a cyberattack method that involves running malicious code as part of a vulnerable web application. Unlike other attack vectors like SQL injections, XSS does not target the application directly—it primarily targets the user.

XSS can have a very large impact on the website and use of it. User accounts can be hijacked, credentials could be stolen, sensitive data could be exfiltrated, and lastly, access to your client computers can be obtained.

One of the most common XSS attack vectors is to hijack legitimate user accounts by stealing their session cookies. This allows attackers to impersonate victims and access any sensitive information or functionality on their behalf.

A practical attack vector for XSS is to use HTML and JavaScript in order to steal user credentials, instead of their cookies. This can be done by cloning the login page of the web application and then using the XSS vulnerability in order to serve it to the victims.

Another powerful attack vector for XSS is to use it in order to exfiltrate sensitive data (for example personal identifiable information or cardholder data) or to perform unauthorized operations, such as siphoning funds.

XSS is also an unexpected source to initiate port scans against the internal network of a client that accesses a vulnerable website.

One of the simplest and yet effective ways for attackers to target businesses or government institutions is to change the visual appearance of a website vulnerable to XSS.

In order to minimize the risks associated with XSS, developers should encode all fields when displaying them in the browser. Additionally, ensure that user input is properly filtered especially in the case of special characters. A common source of XSS are outdated third party libraries integrated in the code, and as such, update these to the latest stable versions.