XSS (CROSS-SITE SCRIPTING)-

DOM-based XSS (Document Object Model)- Attack payload is executed as a result of modifying the the original client side script, so that the client side code runs in an "unexpected" manner.

Reflected (non-persistent)- We will be injecting scripts using some tools as a payload. Delivering a payload directly to the victim. Victim requests a page containing the payload and the payload comes embedded in the response as a script.

We will be doing following harm using XSS-

-Session-hijack-
Hijacking a user session and logging in to the account to collect information.
We will posts a malicious script to a form so when another user clicks the link, an asynchronous HTTP Trace call is triggered which collects the user's cookie information from the server, and then sends it over to another malicious server that collects the cookie information.

Using session hijack we will do following-

-**Changing the password of the victim**. This is possible when the application allows changing or resetting passwords without having to enter the old password
-**can transfer any specified amount of money** to their accounts.

-**Capture keystrokes**- capture the keystrokes by injecting a keylogger. On every keypress, a new XMLHttp request will be generated and sent towards the keylog.php page hosted at the attacker-controlled server.

-Stealing info- We can also fetch the entire page source of the page by using the required payload scripts and read the current balance, transaction information, personal data.

-**Stealing credentials** (**phishing** using XSS)- XSS can also be used to inject a form into the vulnerable page and use this form to collect user credentials. The payload below will inject a form with the message ***Please login to proceed***, along with **username** and **password** input fields.

TOOLS-
detection- blurpsuite, XSS Scanner, XSpear, XSStrike
Attack- XSSER, blurpsuite,

The request will be captured by Burp. The vast majority of XSS vulnerabilities can be found quickly and reliably using Burp Suite's web vulnerability scanner.
The XSS Scanner uses the OWASP ZAP scanning engine which is one of the world's most popular open source security tools, actively maintained by hundreds of international developers.
XSStrike analyses the response with multiple parsers and then crafts payloads that are guaranteed to work by context analysis integrated with a fuzzing engine.

XSSER- It contains several options to try to bypass certain filters, and various special techniques of code injection.

Burp Suite- It is used in order to intercept the request and then send intercepted data into Intruder. It helps in decoding the received data in the Burp Decoder gives us the cleartext page source of the vulnerable page.

XSS (CROSS-SITE SCRIPTING)-

2 types of XSS attacks used- DOM-based XSS (Document Object Model), Reflected (non-persistent) XSS attack. We will be doing the following harm using XSS- Session-hijack, Capturing keystrokes by injecting a keylogger, Stealing information like current balance, transaction information, Stealing credentials by injecting a form into the vulnerable page.

TOOLS-

Detection- XSS Scanner-The XSS Scanner uses the OWASP ZAP scanning engine. , **XSStrike**- XSStrike analyses the response with multiple parsers and then crafts payloads.

Attack- XSSER- It contains several options to try to bypass certain filters, and various special techniques of code injection.

Burp Suite- It is used to intercept the request and then send intercepted data into Intruder.