DESIGN MANUAL

WEB BROWSER ADDON FOR DETECTING SQL AND XSS VULNERABILITIES

COLIN BROPHY

CYBERCRIME & IT SECURITY

30/04/21

Contents

INTRODUCTION

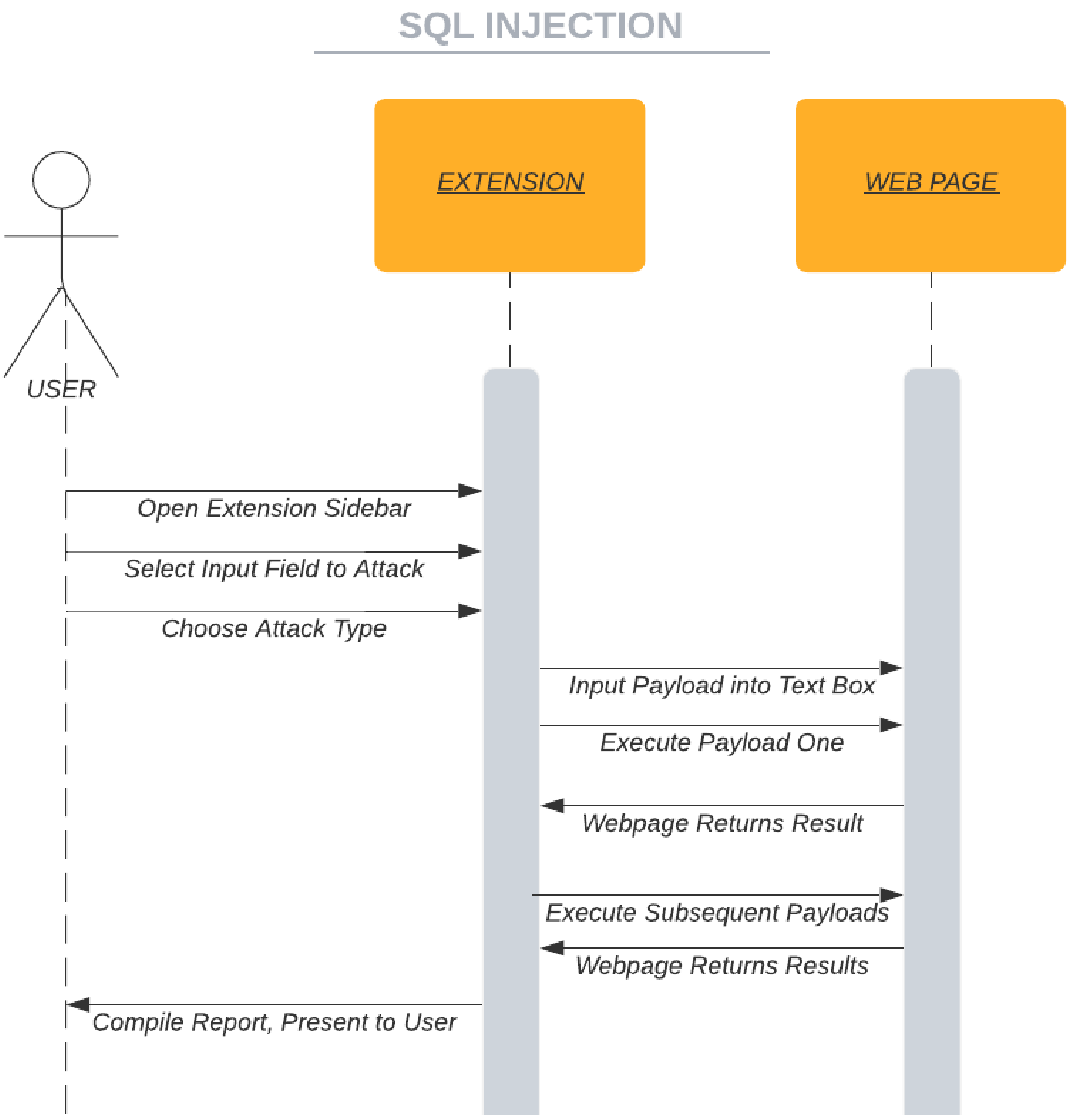
This document will outline the design process when creating the extension, the thoughts behind each decision, as well as use case diagrams for the intended functionality. The document will feature mock-ups of the UI using Balsamiq. The idea is that, by using this document, anyone can create the extension from scratch. The design will be kept as simple as possible to appeal to a broad range of target markets.

USE CASE DIAGRAMS

RUN SQL TEST

The basic idea of how the SQL Test runs currently is as follows:

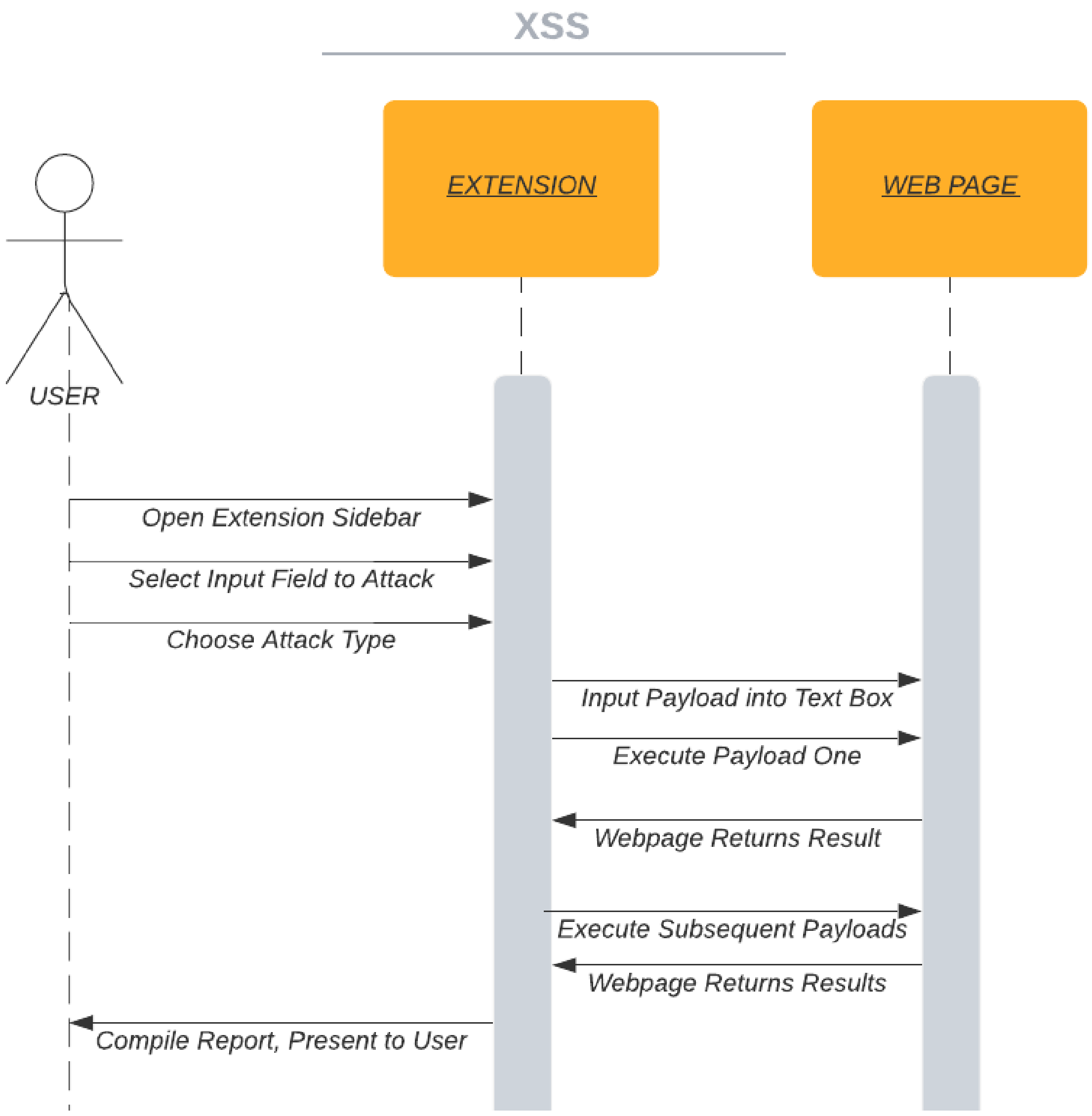
- User selects the input field they wish to attack.
- User chooses automated or custom attack, extension runs attack against web page.
- The extension compiles a report for each payload run and returns the result to the user.



RUN XSS TEST

The basic idea of how the XSS Test runs currently is as follows:

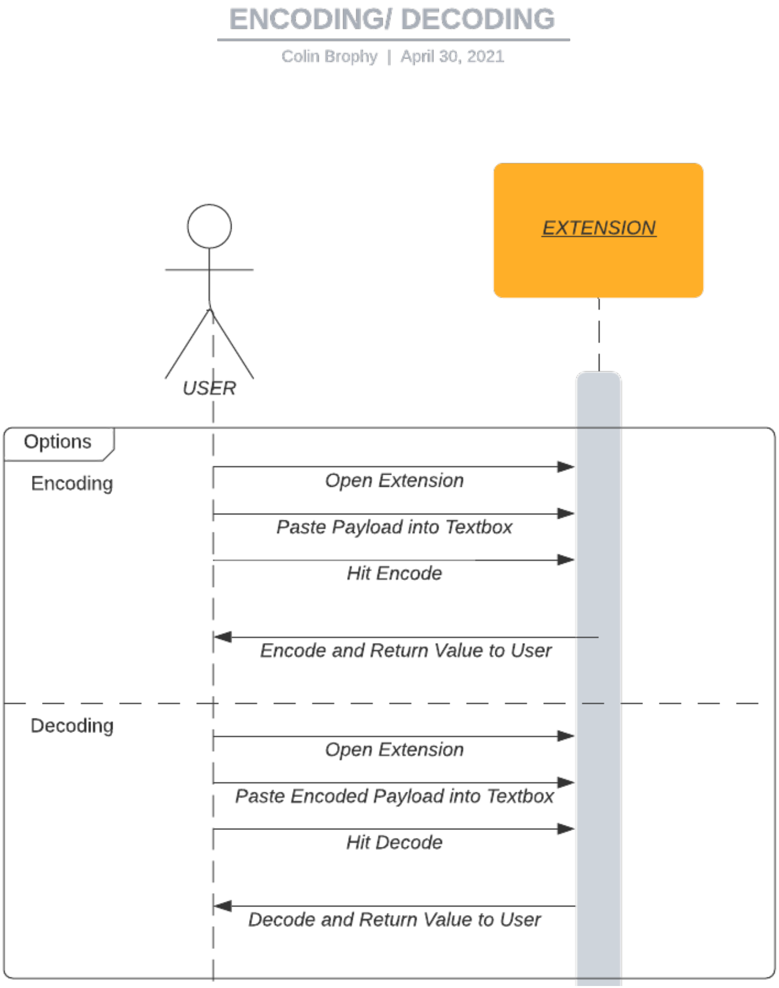
- User selects the input field they wish to attack.
- User chooses automated or custom attack, extension runs attack against web page.
- The extension compiles a report for each payload run and returns the result to the user.



PAYLOAD ENCRYPTION/ DECRYPTION

The operation of the payload encoder/ decoder is simple, as follows:

- User opens the Encoder/ Decoder tab.
- User pastes in the payload they wish to encode/ decode.
- The user selects encode or decode as they wish.
- The text in the box is replaced with the encoded/ decoded version.

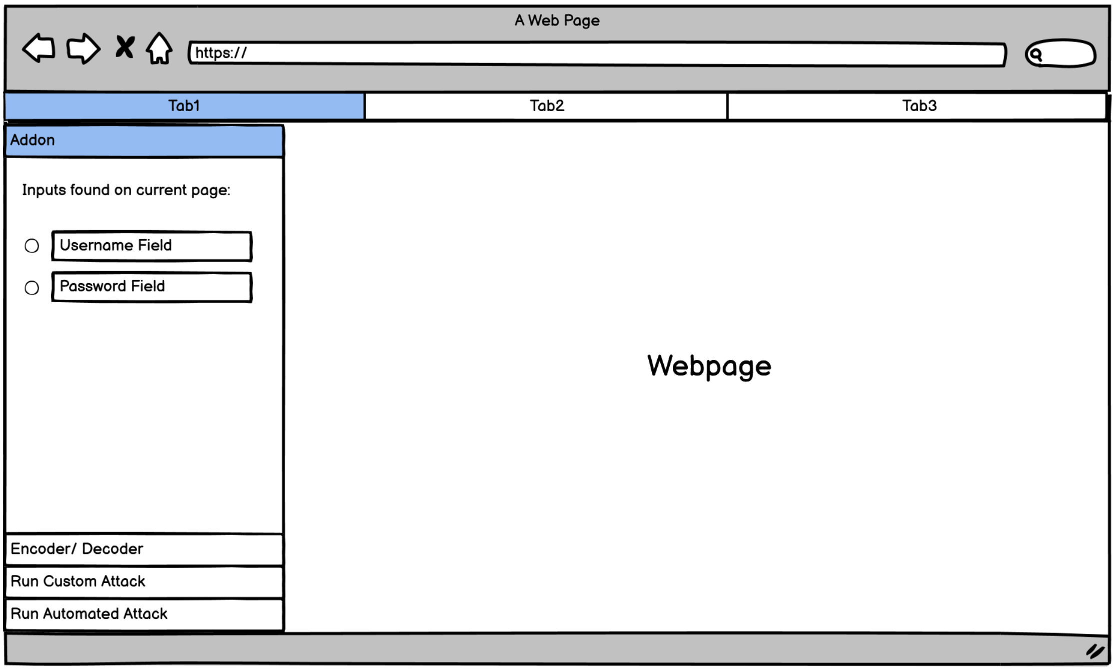

ENCODING/ DECODING
Colin Brophy | April 30, 2021
USER
EXTENSION
Options
Encoding
Open Extension
Paste Payload into Textbox
Hit Encode
Encode and Return Value to User
Decoding
Open Extension
Paste Encoded Payload into Textbox
Hit Decode
Decode and Return Value to User

WIRE DIAGRAMS

MAIN PAGE

Below is a wire diagram is how I perceive my extension will look. It is to be a sidebar over the current active web page, which would display to the user all the input fields on the current active page. These could then be selected using the radio buttons beside them to be chosen for an attack.

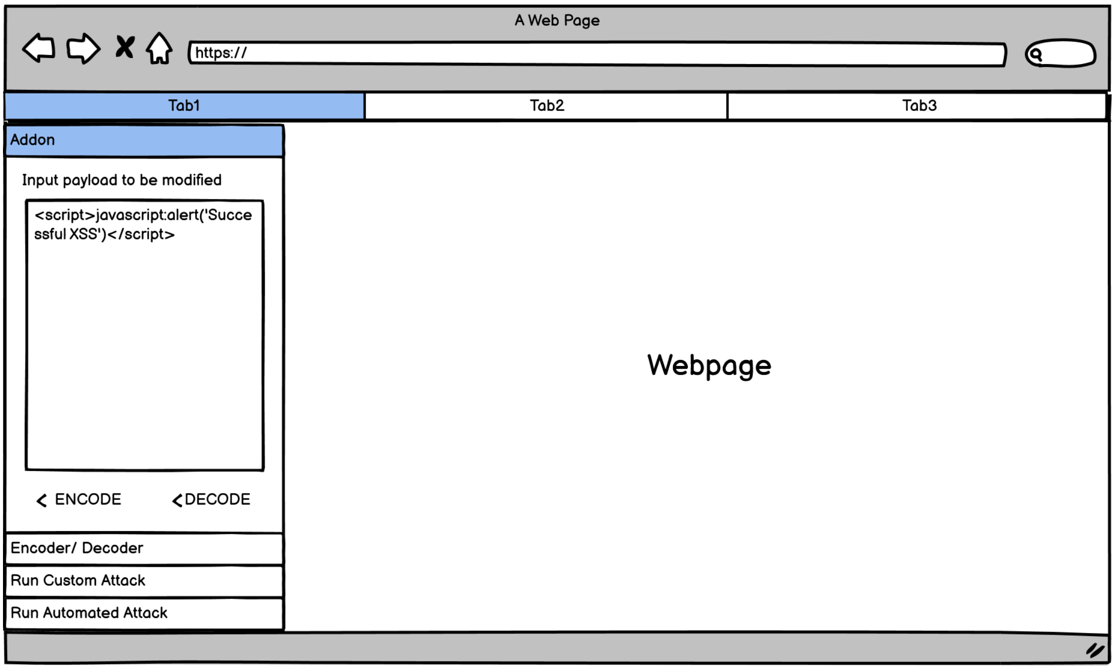
Once the input field in question is selected, the user has the option to run a custom payload against the site, or run automated attacks from a list of well-known payloads. The extension will either run the one custom payload, and let the user know the result, or it will automate the testing of multiple payloads, compile a report and return that to the user, perhaps by opening another browser tab and showing it in a basic HTML page.



EXTRA FEATURE

There will be extra functionality such as a payload encoder and decoder. The user can click on the relevant option in the extension and they will be brought to another page within the extension. From here, there will be a text box they can input the payload into and hit "encode" or "decode" as they wish.

The following is a wire diagram showing how this will work:



COMMENTS

This is the basic idea of how I picture my extension will look. This is, of course, subject to change throughout the development of the extension if I find ways to streamline certain features. I will contrast and compare this idea to my final design in the final report.