# Introduction to Computer Security

## Lab 4 - Google's XSS game

Report
of
Andreas Wilhelm

February 27, 2019

# 1 Level 1

Added the following line in the query bar.

```
<script>alert(1)</script>
```

# 2 Level 2

Because the message box uses html, you can use the html syntax to load a picture in the message. However if the img does not exist you can define an onerror-action, which is in this case the alert. In following listing the code.

```
<img src="http://doesnotexist" onerror="javascript:alert(1)"/>
```

# 3 Level 3

For the execution of the function chooseTab(num) scripting is used. Additionally you can change the img url by typing something after *frame#2* which will be executed by the script. So similiar to level 2, you can add the onerror-action into the url.

```
https://xss-game.appspot.com/level3/frame#2'onerror='alert(1)';
```

# 4 Level 4

If you type in something different than a number the developer console gives the output *Syntax Error: Invalid or unexpected token*. So there is no error handling and you can use the semicolon to concatenate and finally execute several commands. However you have to use the ascii code of the semicolon wich is %3B. So add the following code at the end of the line.

```
')%3Balert(1)%3Bvar xx=('
```

# 5 Level 5

If you navigate to the sign-up page you see *signup?next=confirm*. So that was after next is written will be executed after clickung on the next button. So simply by changing *confirm* to the *javascript:alert(1)*. and after reloading the page, you can execute your code snipped by clicking on next.

# 6 Level 6

So in this level you can load gadgets and other JS things. The url for that has to be typed in after the *frame#*. For the evil alert js file you can use google callback as described in the fourth hint. But if you type in *https://www.google.com/jsapi?callback=alert* an exception occur which says that you're not allowed to load a url with *http*. Though if you use capital letters you can use it. So by adding following code snippet you create the alert.

```
HTTPS://www.google.com/jsapi?callback=alert
```