Since the TAs were very happy with your performance in the mini-exams so far, they decided to give you access to a website where you can get answers to all the tricky questions you always wanted to ask. Unfortunately, when they built their question answering website they did not pay enough attention to *input sanitization* which makes their website vulnerable to cross-site scripting (XSS).
In this exercise your goal will be to craft malicious input queries to the question answering system so that instead of giving you an answer the website raises an alert. The content of the alert must be the cookie that is set when you visit the website. If you managed to raise an alert (with the correct cookie content), you will receive a token that you can submit. Along with the token, please submit the URL you crafted to exploit the vulnerability and raise the alert (in the Code section on the submission page). The exercise proceeds in three levels (of increasing difficulty) and each level is complete when you successfully raised an alert.

An alert is a dialog box that pops up on the screen. A sample alert is shown in Figure 1.

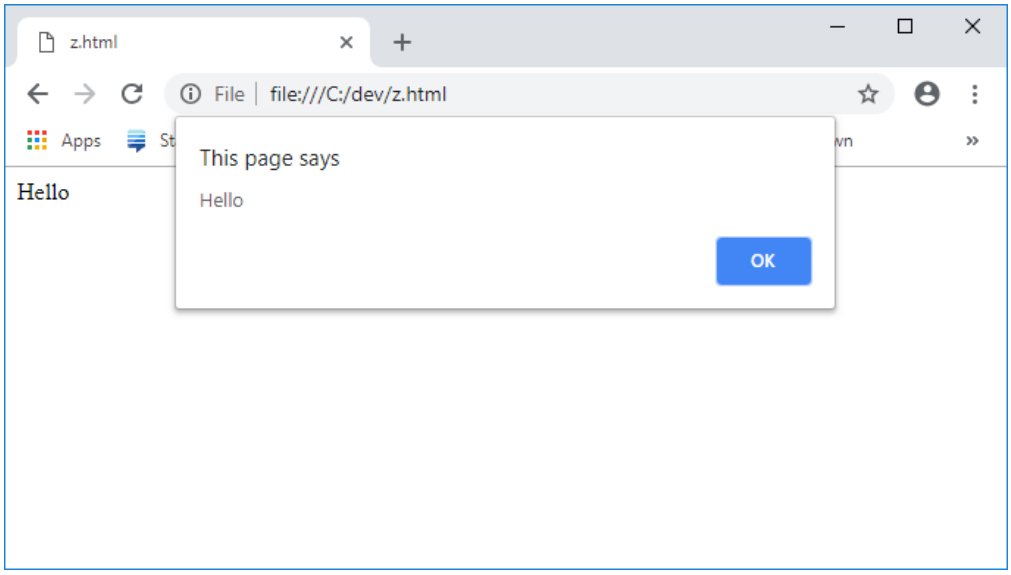


Figure 1: Example alert with the content 'Hello'.

To get started, head over to the TA's website at https://com301-vuln.epfl.ch/ and try to craft a question that raises an alert.

**Important note:** It is possible to execute commands via the console window of your browser, which could include raising alerts. However, *these are not XSS attacks*. Thus, any solution based on, at any point, executing commands on the console will not be accepted as a correct solution to the exercise. This is why we also ask you to submit the URL you created.

*Questions to reflect upon*:

1. In this exercise, you tried to get the website to raise an alert with your own cookie. How would you exploit this vulnerability to get someone else's cookie?

2. What measures should the TAs take to protect against such vulnerabilities?

You do not need to write an answer to these questions.