Online XSS Scripting Tools

Aim:

To perform and practice how to avoid XSS scripting using online tools

XSS Scripting:

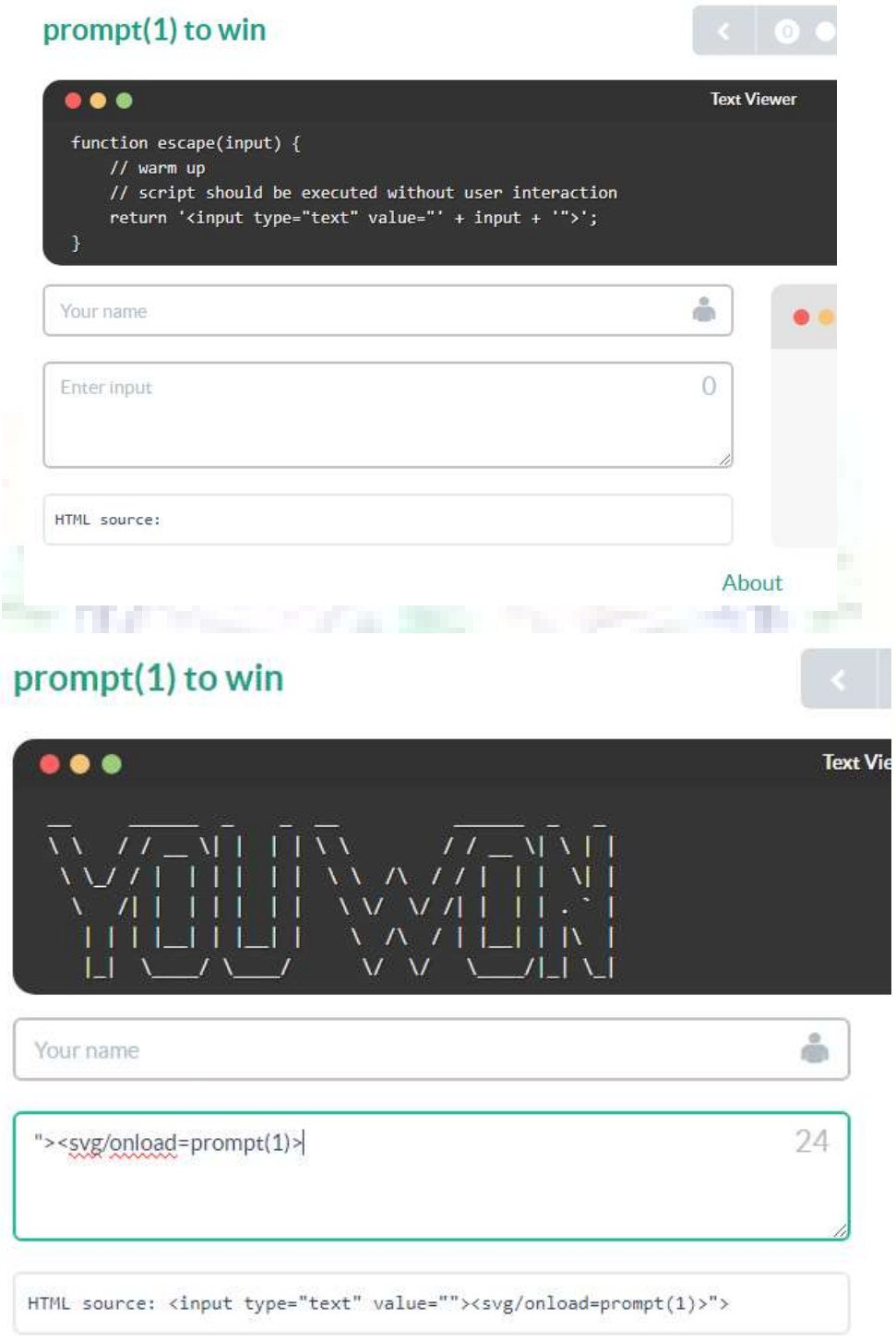
Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same origin policy, which is designed to segregate different websites from each other.

Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data. We can confirm most kinds of XSS vulnerability by injecting a payload that causes our own browser to execute some arbitrary JavaScript. Here prompt.ml site is used to study XSS scripting and analysing various payloads.

Procedure:

1. Use the url prompt.ml in the web browser (Use Chrome, IE, Firefox)
2. There are up to 15+ levels of task with XSS scripting challenges
3. User can go to the next level only if the user found answer in the current level
4. The main concept used in this online tool is that the user should be displayed with prompt(1) as output

Output Screenshot:



Answer for Level 0: SVG is always good for a short and crisp attack vector. This solution works with 24 characters and the answer is "><svg/onload=prompt(1)>

Similarly for Level-1, answer is <svg/onload=prompt(1)

Answers for all the levels are available in the below link:
https://github.com/cure53/XSSChallengeWiki/wiki/prompt.ml