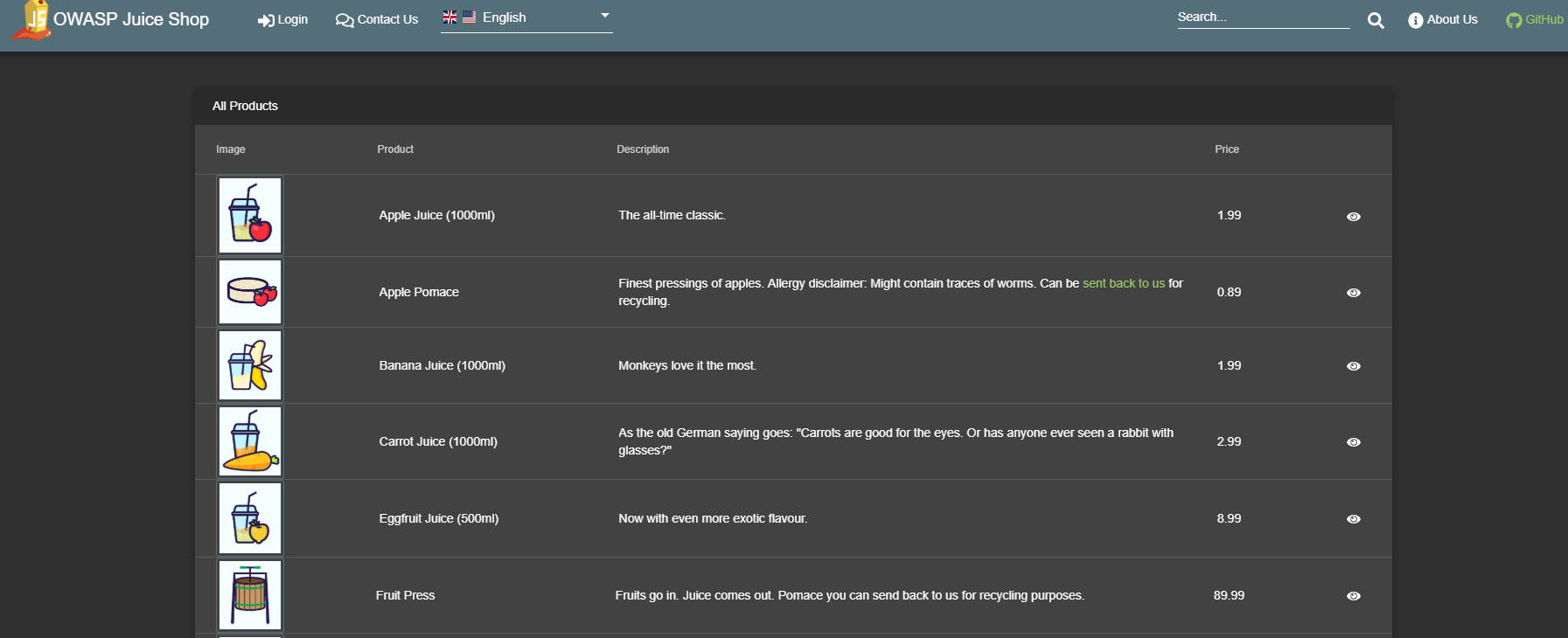
# XSS

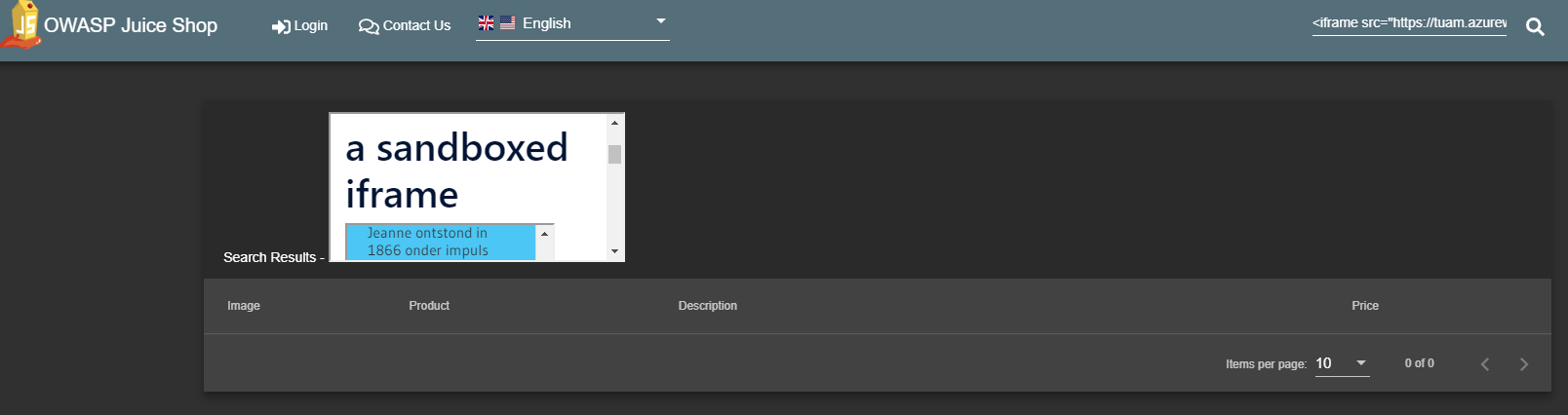
We’re going to discuss XSS. XSS is cross-site scripting. XSS are attacks with scripts that are injected into trusted sites. It happens when the attacker uses a web application to send ‘bad’ code to the end user. The end user almost never expects it and the browser doesn’t know that the script is not trusted. That means that the browser will probably execute the script. The script is most likely JavaScript, but it can also be a HTML, Flash or other code. The script contains private information from the user like the cookies or other session information. The script can rewrite the HTML page, so the user doesn’t know that there is a XSS attack going on.

Now I’m going to explain how to do XSS. First, you have to go to a site. In our case we visited juiceshopap.kurokuapp.com and then I typed the following line of code in the search bar: <iframe src="https://tuam.azurewebsites.net">.





After this, I clicked on the search icon. The page will reload and an Iframe will appear with the according link from the line of code.



So what can be the downside of XSS? You can make a XSS and show your own advertisement. This is a positive thing for the company who’s advertisement is from. You can also make an Iframe that covers the whole original website. This is a dangerous thing because people can put an Iframe above the real website with a login section for example. The user will put his login information and it will go to the person who did the XSS instead of going to the original site owner. The user will not know that his information went to someone else because he thinks he’s on the right site. With this you can steal cookies or other information from the user who’s on the website. You’re kind of creating a portal to an another website and the user will not know it.