06 - XSS - DOM Lab

We can see that everything is being processed using JavaScript locally because no request has been sent to the server, and data have been processed and added to the page. We cab see this by going to the network tab in the developers tools, and observing there is no request going or coming from the server.

This is DOM-Based Cross Site Scripting. Now, we can start by trying a basic payload script:

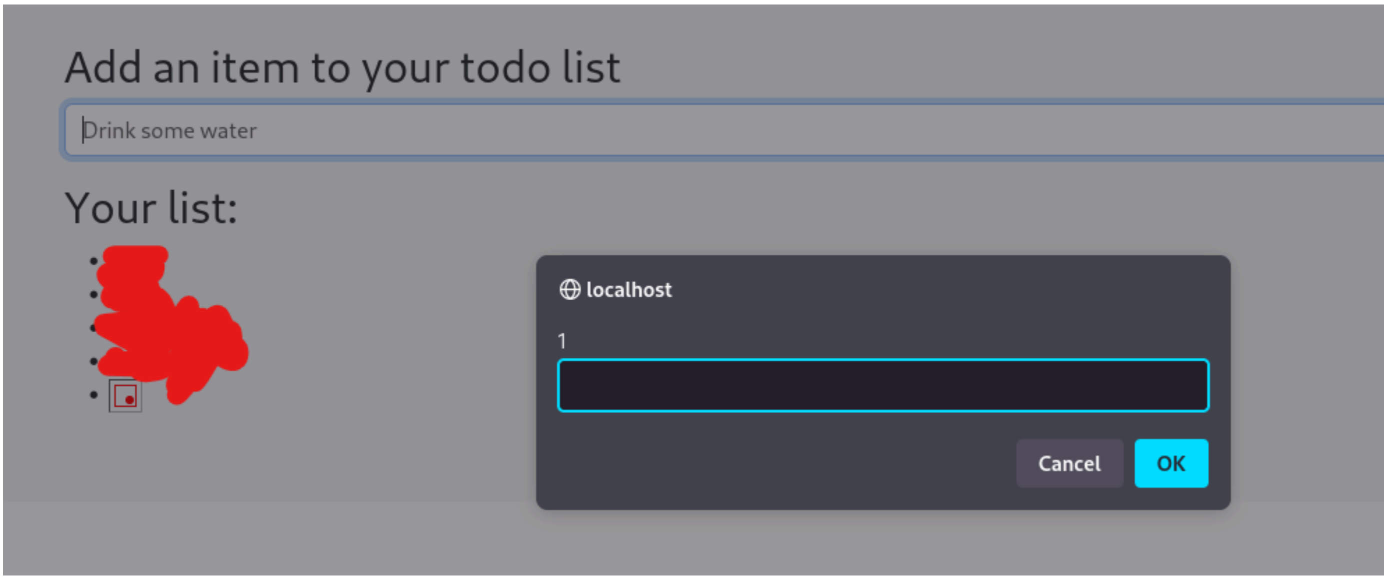
```
<script>prompt(1)</script>
```

But, this does not work. And, the reason is that even though the code is being added to the page is not actually being called, so we need some type of trigger. Now, if this was part of the page as we loaded the page, this would be triggered. But, in this case, we need to find another way to trigger this.

We can do something like:

```
<img src=x onerror="prompt(1)">
```

So, the idea behind the payload is, the browser is going to try to load x, it is going to fail and throw an error, and on the error we are able to execute JavaScript.



Add an item to your todo list

Drink some water

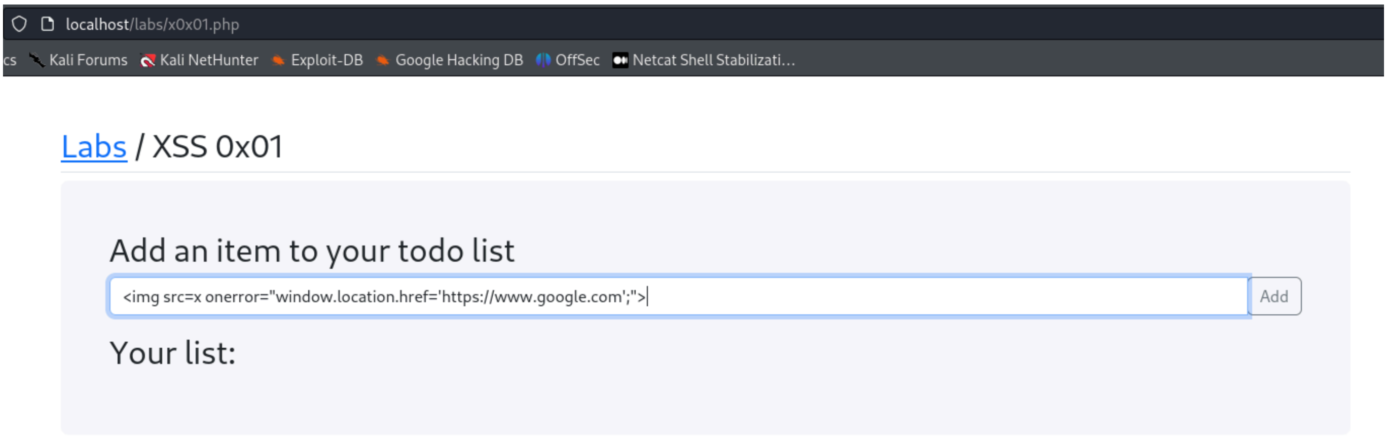
Your list:

[redacted]

localhost

1

We can also try to use the same payload and see if we can forward the user to a different location.



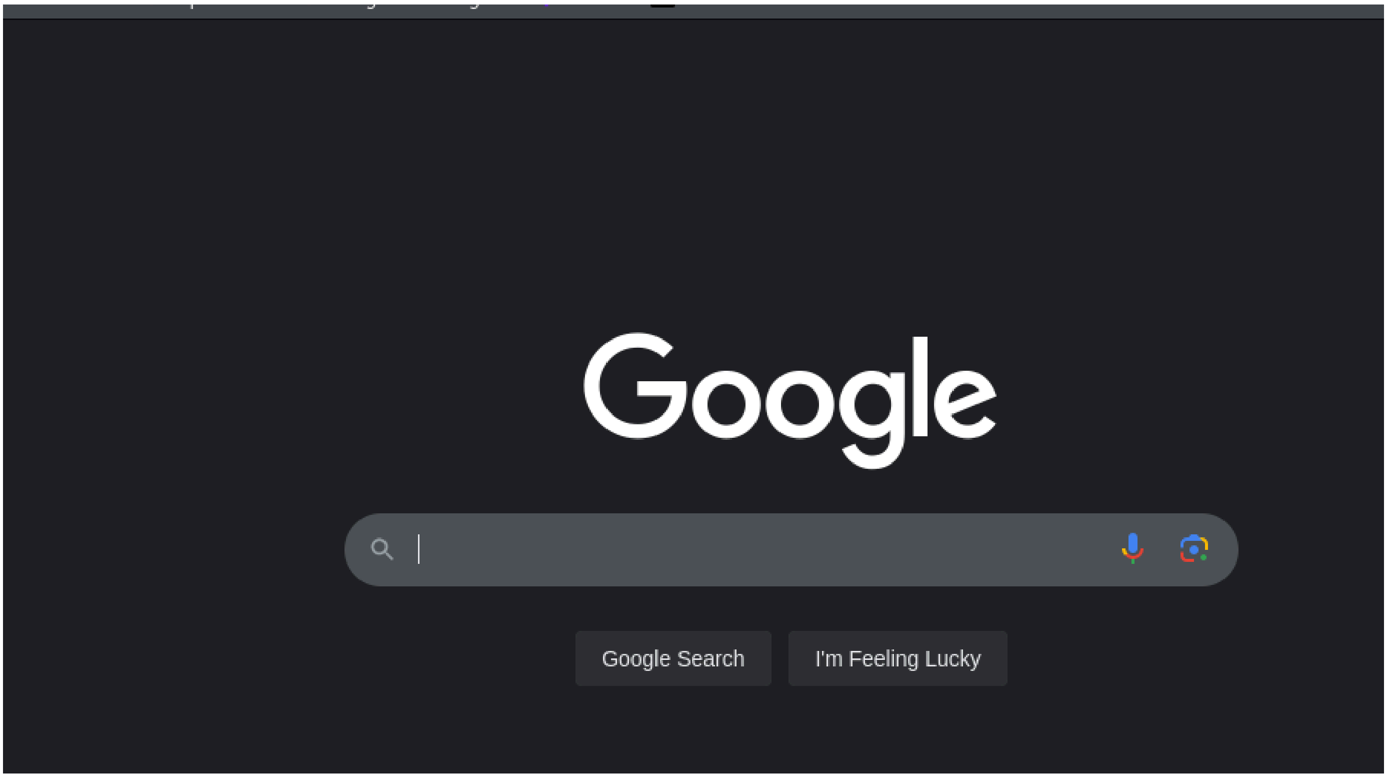
localhost/labs/x0x01.php

Labs / XSS 0x01

Add an item to your todo list

```
<img src=x onerror="window.location.href='https://www.google.com';">
```

Your list:



It works!

This gives me ideas on how to complete other challenges I haven't been able to complete.