

# CSS INJECTION

Meetup 18.07.2018 - Sergej Michel

# SCRIPTLESS ATTACKS



<http://constraints.co/img/card/wd1-29.gif>

# WAS SIND SCRIPTLESS ATTACKS?

- Mario Heiderich mit Jahr 2012 - Uni Bochum
- Angriffe kommen ohne JavaScript aus
- NOScript Bypass
- CSP Bypass
- WAF Bypass
- XSS Filter Bypass

# CSS INJECTION AM BEISPIEL VON ROCKETCHAT

- XSS ist so gut wie nicht vorhanden
- Meteor Framework
- Moderne JavaScript Frameworks verhindern effektiv XSS/Web-Content Injection
- Gibt es trotzdem Schächten

# CSS Injection im Dateinamen (in jedem Upload)

```
cat.png');position:absolute;left:-75px;padding-top:1200px;padding-left:1500px;cat.png
```



# CSS Injection im Dateinamen

```
cat.png');CSS-INJECTION;
```

## Generiertes HTML:

```
<div class="inline-image"  
style="background-image: url('https://rocketchat.server/img/cat.png');CSS-INJECTION;');">
```











# IST DIESE CSS-INJECTION AUSNUTZBAR?

<a href="https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet">https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet</a>
<code>&lt;XSS-CAT&gt; &lt;XSS-777&gt; &lt;?xml?&gt;&lt;XSS-777&gt;</code>
STYLE tag (Older versions of Netscape only)
<code>&lt;STYLE TYPE="text/javascript"&gt;alert('XSS');&lt;/STYLE&gt;</code>
STYLE tag using background-image
<code>&lt;STYLE&gt;.XSS{background-image:url("javascript:alert('XSS')");}&lt;/STYLE&gt;&lt;A CLASS=XSS&gt;&lt;/A&gt;</code>
STYLE tag using background
<code>&lt;STYLE type="text/css"&gt;BODY{background:url("javascript:alert('XSS')");}&lt;/STYLE&gt;</code>
<code>&lt;STYLE type="text/css"&gt;BODY{background:url("javascript:alert('XSS')");}&lt;/STYLE&gt;</code>
Anonymous HTML with STYLE attribute
IE6.0 and Netscape 8.1+ in IE rendering engine mode don't really care if the HTML tag you build exists or not, as long as it starts with an open angle bracket and a letter:
<code>&lt;XSS STYLE="xss:expression(alert('XSS'))"&gt;</code>

# GEGENMASSNAHMEN?

```
Convert & to &amp;  
Convert < to &lt;  
Convert > to &gt;  
Convert " to &quot;  
Convert ' to &#39;
```

# NICHT SELBER IMPLEMENTIEREN!

Für Java kann der OWASP Encoder verwendet werden





# GEGENMASSNAHMEN?

## Content-Security-Policy

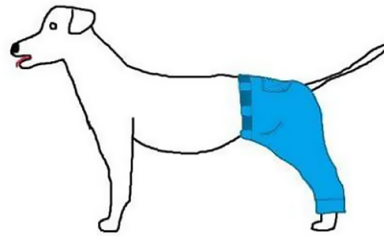
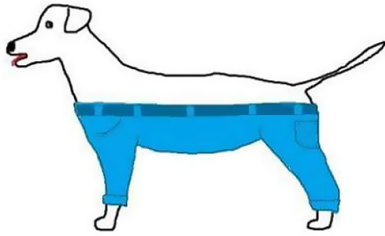
```
Content-Security-Policy: style-src 'self'  
Content-Security-Policy: style-src https://store.example.com  
Content-Security-Policy: default-src 'self'
```





# FRAGEN?

If a dog wore pants would he wear them  
like this                      or                      like this?



<https://static.boredpanda.com/blog/wp-content/uploads/2015/12/tough-questions-funny-if-dog-wear-pants-fb.png>