CSS INJECTION

Meetup 18.07.2018 - Sergej Michel

SCRIPTLESS ATTACKS

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

WAS SIND SCRIPTLESS ATTACKS?

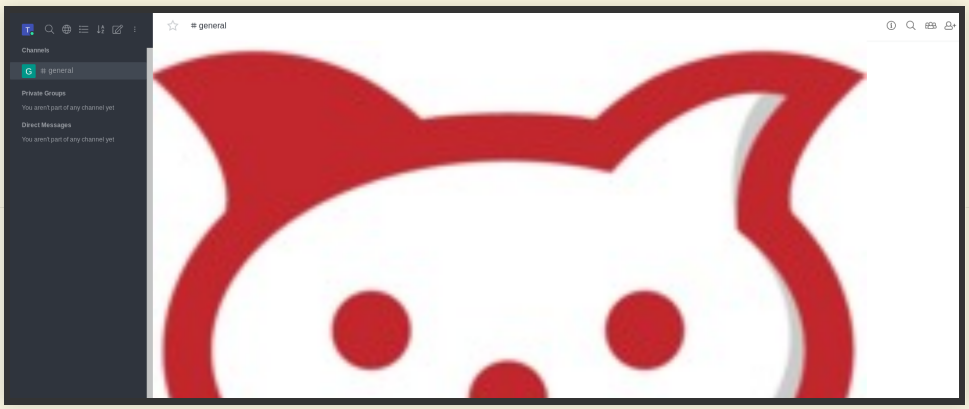
- Mario Heiderich mit Jahr 2012 - Uni Bochum
- Angriffe kommen ohne JavaScript aus
- NOScript Bypass
- CSP Bypass
- WAF Bypass
- XSS Filter Bypass

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;');">
```

Demo

IST DIESE CSS-INJECTION AUSNUTZBAR?

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

SCHWÄCHEN IM ESCAPING SIND EINIGEN IN FRAMEWORKS VORHANDEN

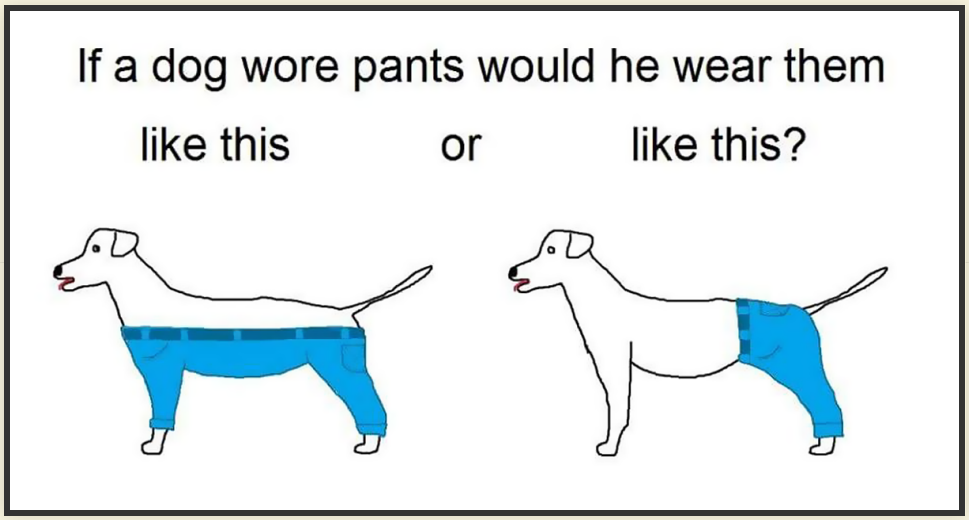
GEGENMASSNAHMEN?

Content-Security-Policy

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

ZUSAMMENFASSUNG

FRAGEN?



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