

Was Symfony für IT-Sicherheit unternimmt und was nicht

Eine kurze Betrachtung des Frameworks



Andreas Sperber

aramido



aramido.de/blog



[@aramido_de](https://twitter.com/aramido_de)

Was kann denn schon schief gehen?

*Symfony is a set of reusable **PHP** components...*

The standard foundation on which the best PHP applications are built. Choose any of the 30 stand-alone components available for your own applications.

[Browse components →](#)



*... and a **PHP** framework for web projects*

Speed up the creation and maintenance of your PHP web applications. End repetitive coding tasks and enjoy the power of controlling your code.

[What is Symfony →](#)

Projects using Symfony

Drupal™

phpBB®

 laravel

 eZ®
Where Content Means Business

 OROCRM

PIWIK

Häufige Schwachstellen von Webanwendungen



XSS + CS



Injections



CSRF



Verlust sensibler
Daten

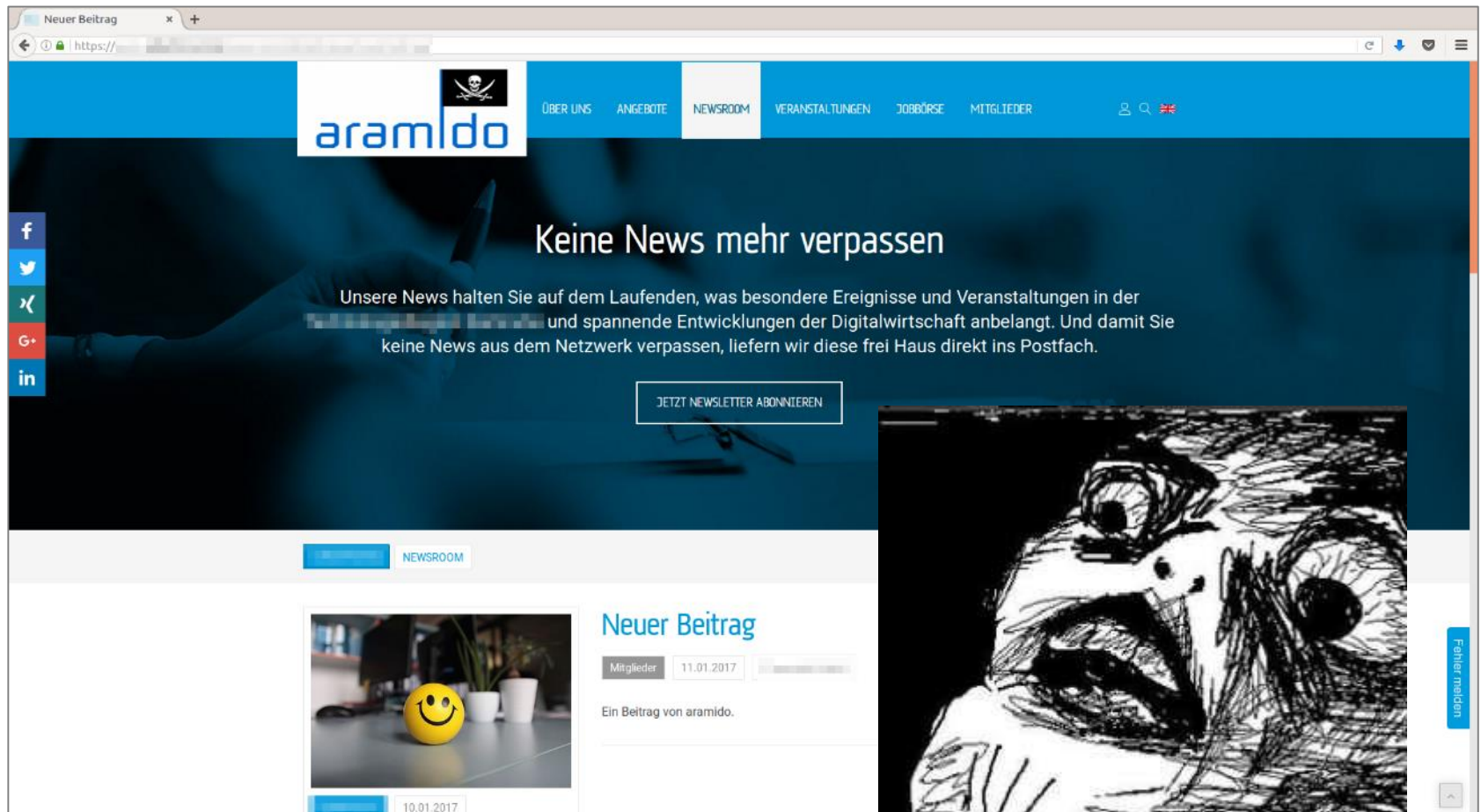


Brute Force

Cross Site Scripting und Content Spoofing



Cross Site Scripting und Content Spoofing



Output-Escaping mit Twig

```
{% autoescape %}  
    HTML-Autoescaping für den gesamten Inhalt  
{% endautoescape %}
```



Output-Escaping mit Twig

```
{% autoescape 'js' %}  
    JS-Autoescaping für den gesamten Inhalt  
{% endautoescape %}
```



Output-Escaping mit Twig

```
{% autoescape false %}  
    Kein Escaping des Inhalts  
{% endautoescape %}
```



CSP-Header gegen Client-Injections

Content-Security-Policy:

```
default-src 'none';  
script-src 'self';  
connect-src 'self';  
img-src 'self';  
style-src 'self';  
report-uri /csp/report
```

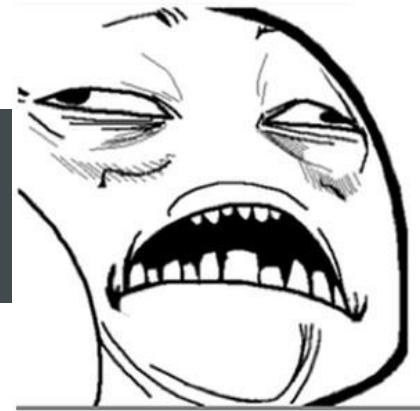


Injections



Prepared Statements

```
self::createQueryBuilder('u')  
    ->where("u.username = '$username'")  
    ->getQuery()  
    ->execute();
```



```
self::createQueryBuilder('u')  
    ->where('u.username = :username')  
    ->setParameter('username', $validatedUsername, \PDO::PARAM_STR)  
    ->getQuery()  
    ->execute();
```



Eingabedatenvalidierung

```
// src/AppBundle/Entity/User.php
namespace AppBundle\Entity;

use Symfony\Component\Validator\Constraints as Assert;

class User
{
    /**
     * @ORM\Column(name="googleAuthenticatorSecret", type="string", nullable=true)
     *
     * @Assert\Regex(
     *     pattern="/^(?:[A-Z2-7]{8})*(?:[A-Z2-7]{2}={6}|[A-Z2-7]{4}={4}|[A-Z2-7]{5}={3}|[A-Z2-7]{7}=)?$/",
     *     match=true,
     *     message="The authenticator secret is not valid. Please reload the page."
     * )
     *
     */
    protected $googleAuthenticatorSecret;
}
```



Cross Site Request Forgery



CSRF: Löschen per GET-Request

```
http://heise-security-n... x +
view-source:http://heise-security-news.de/Deutsche-Bahn-fixt-Schwachstelle-im-neuen-WLAN-von-ICEs.html | c | Suchen

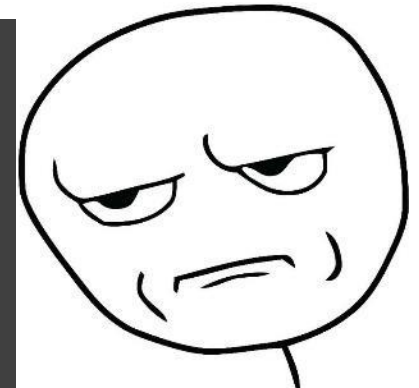
730
731     <li class="right"><a href="https://www.heise-medien.de/">Copyright © 2017 Heise Medien</a></li>
732
733
734
735
736
737
738 </ul>
739
740
741
742
743
744 <script src="res/suche.js"></script><ul class="ui-autocomplete ui-menu ui-widget ui-widget-content ui-corner-all" role="listbox" aria-activedescendant="ui-active-i
745
746 <script src="res/heise.js"></script><section class="heise-modal newsletter_2014_modal"><div class="wrapper-transparent"></div><div class="stage"><button data-role=
747
748
749 
750 
751 
752 
753 
754 
755 
756 
757 
758 
759 
760 
761 
762 
763 
764 
765 
766 
767 
768 
769 
770 
771 
772 
773 
774 
775 
776 
777 
778 
779
780
781
782 </body></html>
```

Löschen per GET-Request

```

```

```
/**
 * @Route("/{id}/delete", name="admin_post_delete")
 * @Method("GET")
 * @Security("is_granted('delete', post)")
 */
public function deleteAction(Post $post)
{
    $entityManager = $this->getDoctrine()->getManager();
    $entityManager->remove($post);
    $entityManager->flush();
    ...
}
```



Synchronizer (CSRF) Token

```
<input id="csrf_token" name="_csrf_token" value="0gjKUIJa2trwx0K-Drx80h2XA9akQUe60XzGHwFcC0" type="hidden">
```



Same Origin

Source Origin === Target Origin



Verlust sensativer Daten



Schutz ruhender Daten

\$2y\$13\$NPidMJQTICFl/UaSRjFwvu4jzj8g5zzWBJDW4WSeIIoqXFdrithk.



Brute Force



Brute Force



12,4 Mio.



1,55 Mrd.



1,37 Mrd.



68,7 Mio.



5 Mio.



85 Mio.

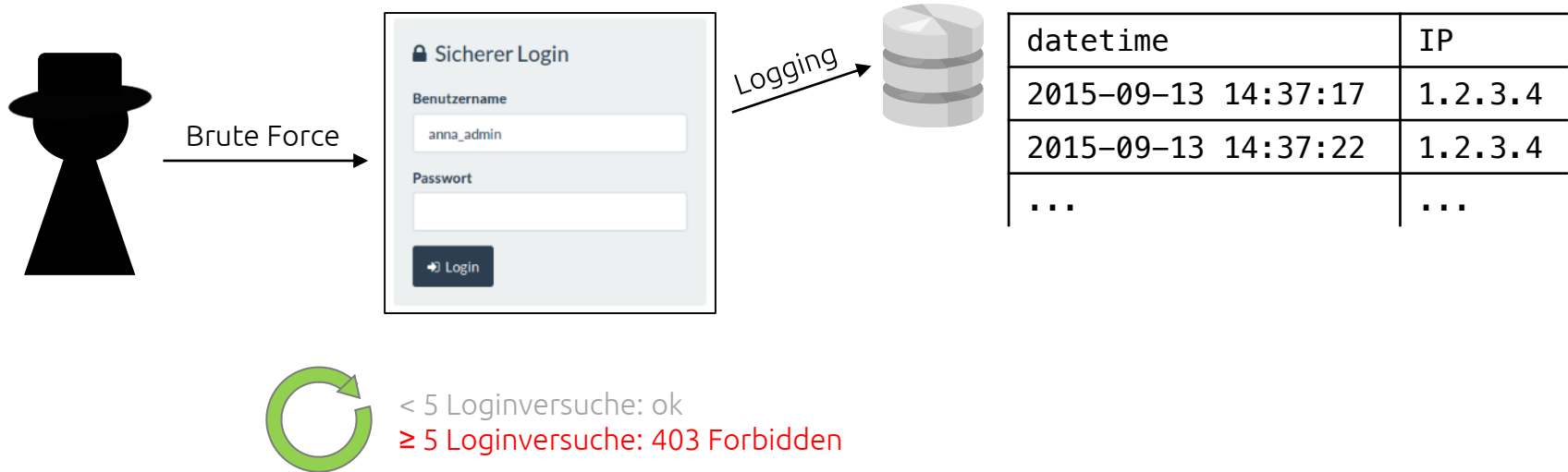


Dictionary-Angriff durch zahlreiche Leaks

```
Tested for password "AVOHISUK064" without success
Tested for password "avohai" without success
Tested for password "avogas3n" without success
Tested for password "AVOGADRO1991" without success
Tested for password "avogadro" without success
Tested for password "avoelec" without success
Tested for password "avodva14" without success
Tested for password "avods111" without success
Tested for password "avofoz" without success
Tested for password "avogadina" without success
Tested for password "avogtil" without success
Tested for password "avoeavoe" without success
Tested for password "avoid2525" without success
Tested for password "avoid1iblis" without success
Tested for password "avoidtheplague" without success
Tested for password "avoidshel" without success
Tested for password "avoidit1" without success
Tested for password "avoidn" without success
Tested for password "avoine12" without success
Tested for password "avoid7.7Z" without success
Tested for password "avoir68102" without success
Tested for password "Avoidyar4ne" without success
Tested for password "avoir01" without success
Tested for password "Avoidus7" without success
Tested for password "avoidthejerks" without success
Tested for password "avoidgals" without success
Tested for password "Avoider1" without success
Tested for password "avoinn505215" without success
Tested for password "avoid78" without success
Tested for password "avoine" without success
Tested for password "Avoir#15" without success
Tested for password "AVOID9990~" without success
Tested for password "avoirscriinels" without success
```

```
Tested for password "avokagimaj" without success
Tested for password "avokt2sd" without success
Tested for password "avoisn9394" without success
```

Brute Force Schutz



Smarte Schutzmechanismen

Achtung: Google hat einen verdächtigen Anmeldeversuch in Ihrem Konto verhindert. **Waren Sie das?** ✕

← **Zuletzt verwendete Geräte** ?

Geräte, die in den letzten 28 Tagen in Ihrem Konto aktiv waren oder momentan angemeldet sind [Weitere Informationen](#)

Jemand kennt Ihr Passwort. Google hat den Log-in verhindert. [Weitere Informationen](#)

**Unbekanntes Gerät**

Uhrzeit: 25. August, 20:36

Standort: Nürnberg, Deutschland

IP-Adresse: 1.1.1.1 



Google - Kartendaten Nutzungsbedingungen

Ungefäher Standort ([kann Städten in der Nähe entsprechen](#))

Erkennen Sie diese Aktivität? Falls nicht, könnte jemand anderes im Besitz Ihres Passworts sein.

Symfony und IT-Sicherheit: ein Ausschnitt



XSS + CS



Injections



CSRF



Verlust sensibler
Daten



Brute Force

Zum Mitnehmen

1. Kenne dein Threat Model
2. Kenne das Framework
3. Sorge für Defense in Depth

Andreas Sperber

andreas.sperber@aramido.de

 @aramido_de