

The traditional/inevitable update: OWASP Juice Shop



for German OWASP Day 2018

by Björn Kimminich / @bkimminich

<http://owasp-juice.shop>

Maturity Promotion #2



Fun Fact: Juice Shop is probably the most shipwrecked [Flagship Project](#) at OWASP!

Juice Shop Success Pyramid™

contributors 39

owasp flagship project

code style

standard

cii best practices

silver



maintainability

A



test coverage

87%

downloads

8k total

downloads

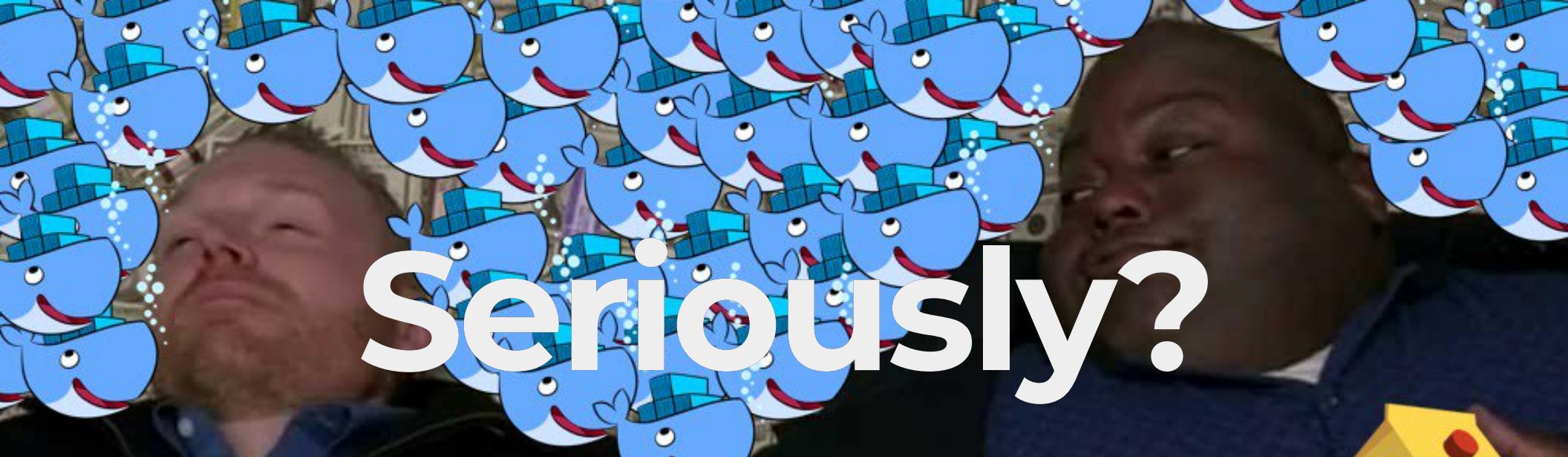
3k

docker pulls

2M

Seriously?

docker pulls 2M



Seriously?

docker pulls

2M

No, really, seriously???

More Languages

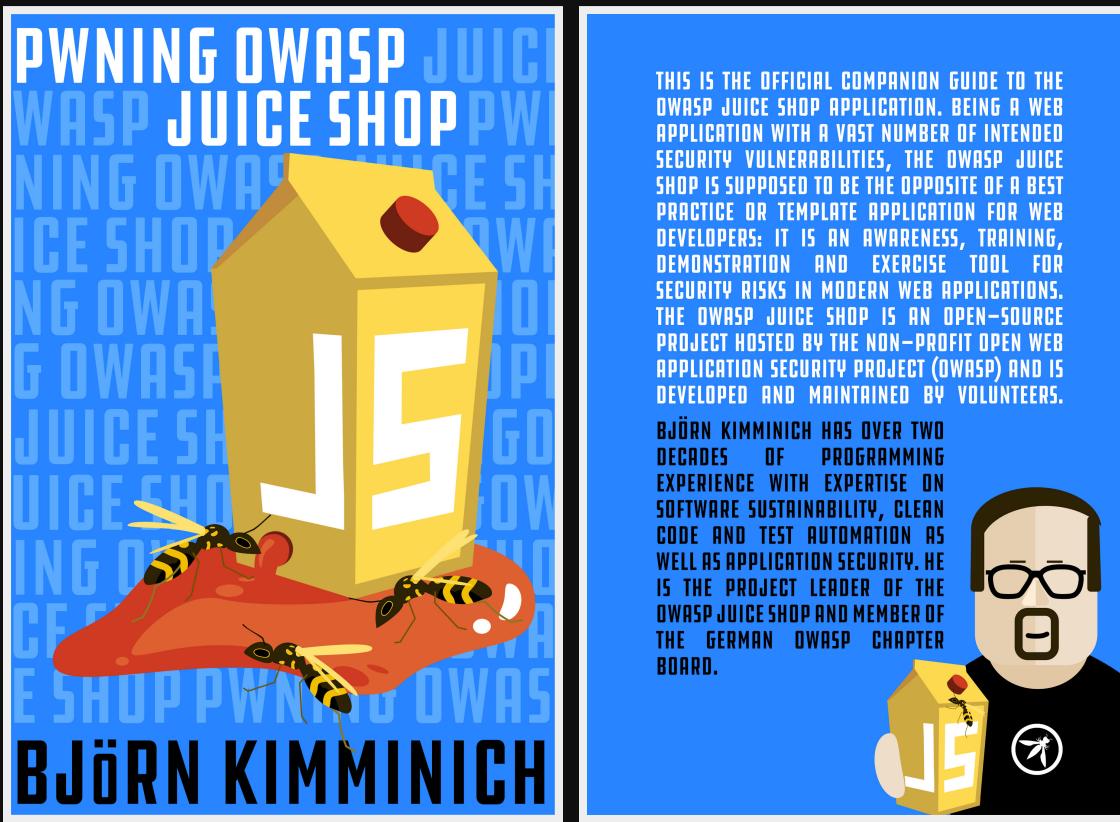
≥85% UI translation available for



<85% translation available for



>2,800 LeanPub Readers



THIS IS THE OFFICIAL COMPANION GUIDE TO THE OWASP JUICE SHOP APPLICATION. BEING A WEB APPLICATION WITH A VAST NUMBER OF INTENDED SECURITY VULNERABILITIES, THE OWASP JUICE SHOP IS SUPPOSED TO BE THE OPPOSITE OF A BEST PRACTICE OR TEMPLATE APPLICATION FOR WEB DEVELOPERS: IT IS AN AWARENESS, TRAINING, DEMONSTRATION AND EXERCISE TOOL FOR SECURITY RISKS IN MODERN WEB APPLICATIONS. THE OWASP JUICE SHOP IS AN OPEN-SOURCE PROJECT HOSTED BY THE NON-PROFIT OPEN WEB APPLICATION SECURITY PROJECT (OWASP) AND IS DEVELOPED AND MAINTAINED BY VOLUNTEERS.

BJÖRN KIMMINICH HAS OVER TWO DECADES OF PROGRAMMING EXPERIENCE WITH EXPERTISE ON SOFTWARE SUSTAINABILITY, CLEAN CODE AND TEST AUTOMATION AS WELL AS APPLICATION SECURITY. HE IS THE PROJECT LEADER OF THE OWASP JUICE SHOP AND MEMBER OF THE GERMAN OWASP CHAPTER BOARD.



Fun Fact: The book is *free* but made **≈1,000\$** revenue thanks to voluntary buyers so far!

CTF Multi-Framework-Support

```
root@55fba87d027f:~# npm i -g juice-shop-ctf-cli
/usr/bin/juice-shop-ctf -> /usr/lib/node_modules/juice-shop-ctf-cli/bin/juice-shop-ctf.js
+ juice-shop-ctf-cli@0.0.0
updated 1 package in 1.741s
root@55fba87d027f:~# juice-shop-ctf

Generate OWASP Juice Shop challenge archive for setting up CTFd (>=1.1.0) or FBCTF score server
? CTF framework to generate data for? CTFd
? Juice Shop URL to retrieve challenges? https://juice-shop.herokuapp.com
? Secret key <or> URL to ctf.key file? https://raw.githubusercontent.com/bkimminich/juice-shop/master/ctf.key
? Insert a text hint along with each challenge? Free text hints
? Insert a hint URL along with each challenge? Paid hint URLs

Backup archive written to /root/OWASP_Juice_Shop.2018-08-22.CTFd.zip

For a step-by-step guide to import the ZIP-archive into CTFd, please refer to
https://bkimminich.gitbooks.io/pwning-owasp-juice-shop/content/partI/ctf.html#running-ctfd
root@55fba87d027f:~# juice-shop-ctf

Generate OWASP Juice Shop challenge archive for setting up CTFd (>=1.1.0) or FBCTF score server
? CTF framework to generate data for? FBCTF
? Juice Shop URL to retrieve challenges? https://juice-shop-staging.herokuapp.com
? Secret key <or> URL to ctf.key file? https://raw.githubusercontent.com/bkimminich/juice-shop/master/ctf.key
? URL to country-mapping.yml file? https://raw.githubusercontent.com/bkimminich/juice-shop/master/config/fbctf.yml
? Insert a text hint along with each challenge? (Use arrow keys)
> No text hints
  Free text hints
  Paid text hints
```



Useful Fact: With `juice-shop-ctf --config myconfig.yml` you can now fully automate CTF setups!

Google Summer of Code 2018



Project Challenge Pack

Student Shoeb Patel

Mentor Jannik Hollenbach Mentor Timo Pagel

Project Angular Migration

Student Aashish Singh

Mentor Björn Kimminich

Live Demo

OWASP Juice Shop 8.x

<http://demo.owasp-juice.shop>

Last but not least...

...I made (kind of) a promise in the abstract...

The screenshot shows a conference agenda page with a modal window displaying a detailed abstract for a talk.

Agenda:

- 13:00 - 13:40 Invited Talk **Entwicklung von APT-** Christoph Fischer
- 13:40 - 14:05 **Der Feind in meiner App** Ingo Hanke
- 14:05 - 14:50 **Lightning Talks**
 - IT security weaknesses
 - Mapping techniques
 - Fun with Apache
- 14:50 - 15:20 Kaffeepause / Coffee Break
- 15:20 - 16:00 Invited Talk **Daniel Gruss**
Transient Execution Attacks
- 16:00 - 16:25 **Efail: Angriffe gegen E-Mails** Christian Dresen
- 16:25 - 16:50 **PostScript Undead: PDF-Exploit** Jens Müller
- 16:50 - 17:00 **The traditional/inevitable OWASP Juice Shop update** Björn Kimminich
- 17:00 Ende der Veranstaltung

Abstract Details (Modal Window):

The traditional/inevitable OWASP Juice Shop update
Björn Kimminich

In the last year a lot has happened, so it is time for the traditional/inevitable OWASP Juice Shop update of 2018:

- Two students and three mentors did amazing work during the Google Summer of Code, which will culminate in the v8.0.0 release some time this year
- The AngularJS frontend is currently being completely rewritten into the latest Angular with Material Design and all kinds of extra fanciness
- Over 20 new challenges have been added over the last year, including JWT issues, XXE, RCE, more Injection, more XSS, more of probably even worse stuff
- The official CTF setup-utility now supports not only CTFd but Facebook's FBCTF framework
- The Juice Shop is seeing more usage world-wide than ever before with a total of over 250.000 pulls of its Docker image and hundreds of clone operations of its GitHub repository per week

A lot more might still happen in the time between the submission of this abstract and the actual German OWASP Day. It might even have its own "commercial" jingle or song by then...

Bio

Björn Kimminich works as an IT architect and application security officer for Kuehne + Nagel. On the side, he gives IT Security lectures at the non-profit private university Nordakademie. Björn also is the project leader of the OWASP Juice Shop and a board member for the German OWASP chapter.

SCHLIESSEN

...and luckily, my good pal Brian from 7MS Podcast...

A lot more might still happen in the time between the submission of this abstract and the actual German OWASP Day. It might even have its own "commercial" jingle or song by then...

...gave in to the massive     pressure...

braimee / bpatty

Watch 23 Unstar 61 Fork 24

Code Issues 1 Pull requests 0 Projects 0 Wiki Insights

OWASP Juice Shop jingle / song #13

 Open bkimminich opened this issue on 28 Jun · 13 comments

bkimminich commented on 28 Jun

Hi @braimee! You thought I wouldn't seriously open this ticket, did you?
(Visitors, please upvote  to increase pressure on Brian! Thank you!)

Assignees
No one assigned

Labels
None yet

Projects

 5  1  3  1

...so that I can proudly present...

...the alpha-release of the

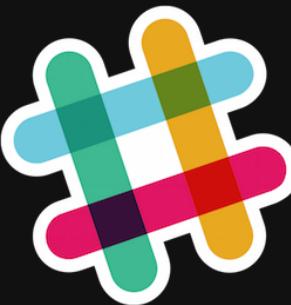
Juice Shop jingle



...in front of live audience for the first time exclusively at **GoD 2018!**

*(Naturally, finding this soundfile and its lyrics will become two new challenges *very soon!*)*

Thank you for your continued interest in the project!



Copyright (c) 2018 Björn Kimminich

Licensed under the MIT license.