

TALK BY **BJÖRN KIMMINICH** / **@BKIMMINICH**

---

[https://www.owasp.org/index.php/OWASP\\_Juice\\_Shop\\_Project](https://www.owasp.org/index.php/OWASP_Juice_Shop_Project)

# YOU MISSED LAST YEAR'S TALK?

*Juice Shop is an intentionally insecure webapp written in Node.js, Express and AngularJS. It contains over 30 challenges of varying difficulty tracked on a score board.*

# WHAT'S NEW?

# OWASP += JUICE SHOP

Juice Shop is now an [official OWASP Tool Project](#)



# MULTI-LANGUAGE SUPPORT

Complete UI translations available for several languages



# MORE RUN OPTIONS

One-click-Cloud-deployment without hacking restrictions\*



Deploy to Heroku

\*Written confirmation of Heroku tech support: **Everything** except DDoS attacks is okay!

# EVEN MORE RUN OPTIONS

Automatic provisioning of a Juice Shop VirtualBox VM



VAGRANT

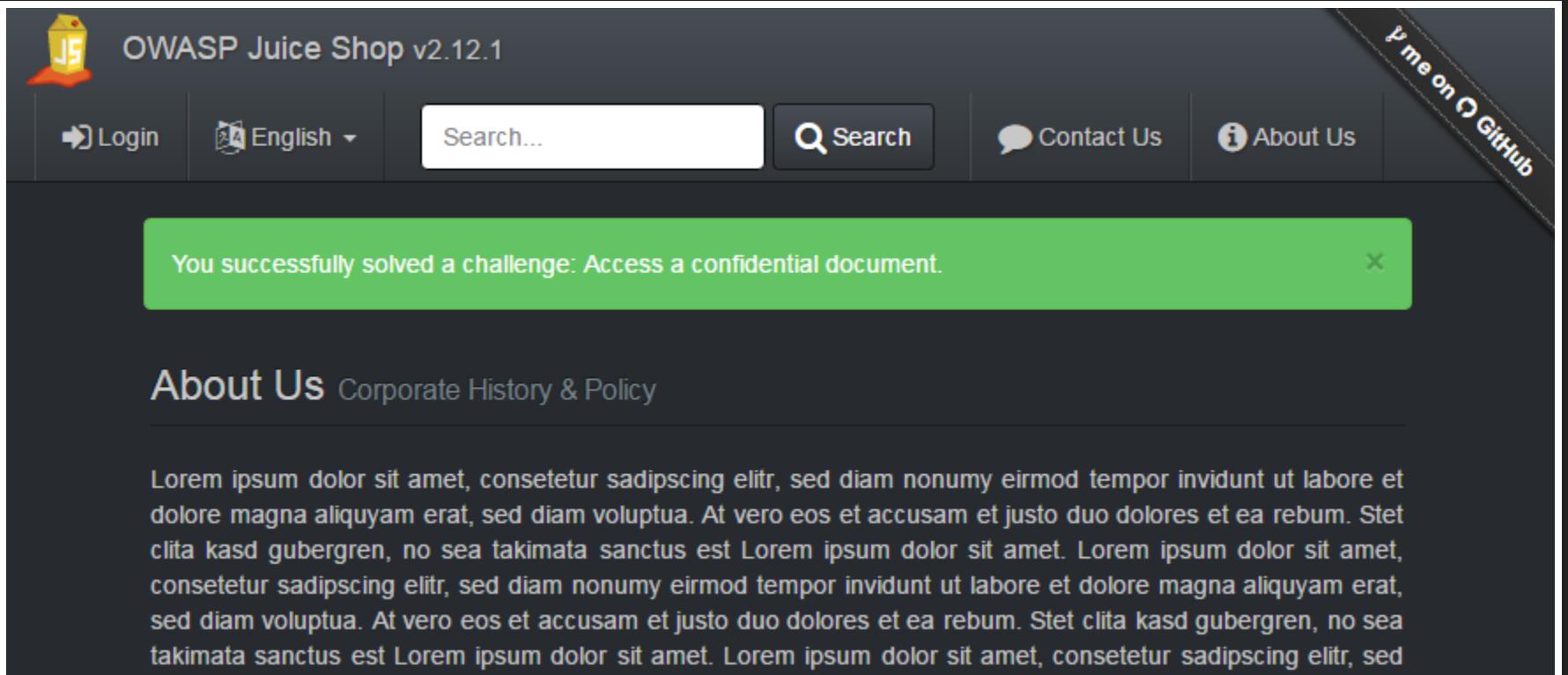
# LOGIN VIA OAUTH 2.0

You can now use your Google account to log in



# INSTANT SUCCESS FEEDBACK

Solved challenges are announced as push notifications



The screenshot shows the OWASP Juice Shop v2.12.1 web application. The top navigation bar includes a logo, the text "OWASP Juice Shop v2.12.1", and links for "Login", "English", "Search", "Contact Us", and "About Us". A GitHub link "View me on GitHub" is also present. A green success notification box in the center of the page states: "You successfully solved a challenge: Access a confidential document." A small "X" icon is at the end of the notification box. Below the notification, the "About Us" section is visible, featuring the heading "About Us" and the sub-section "Corporate History & Policy". A large block of placeholder text (Lorem ipsum) follows.

You successfully solved a challenge: Access a confidential document.

About Us Corporate History & Policy

*Placeholder text (Lorem ipsum) follows.*

# ADVANCED DISASTER RECOVERY

Restore your hacking progress - like a kid of the 80's

Find the hidden easter egg.	★★	solved
Apply some advanced cryptanalysis to find <i>the real</i> easter egg.	★★★	unsolved
Forge a coupon code that gives you a discount of at least 80%.	★★★	unsolved
Travel back in time to the golden era of web design.	★★	unsolved
Order the Christmas special offer of 2014.	★	unsolved
Upload a file larger than 100 KB.	★★	unsolved
Upload a file that has no .pdf extension.	★★	unsolved
Retrieve the language file that never made it into production.	★	solved
Give a devastating zero-star feedback to the store.	★	unsolved

 Your current continue code: A6IXDW1KxgpevZBP0m59GbRdantEF0sofRfkVn8a3kAyLNojz7rOYEQJqM49 

**Continue Code** (Enter continue code here to restore previous challenge progress.)

 **Restore Progress**

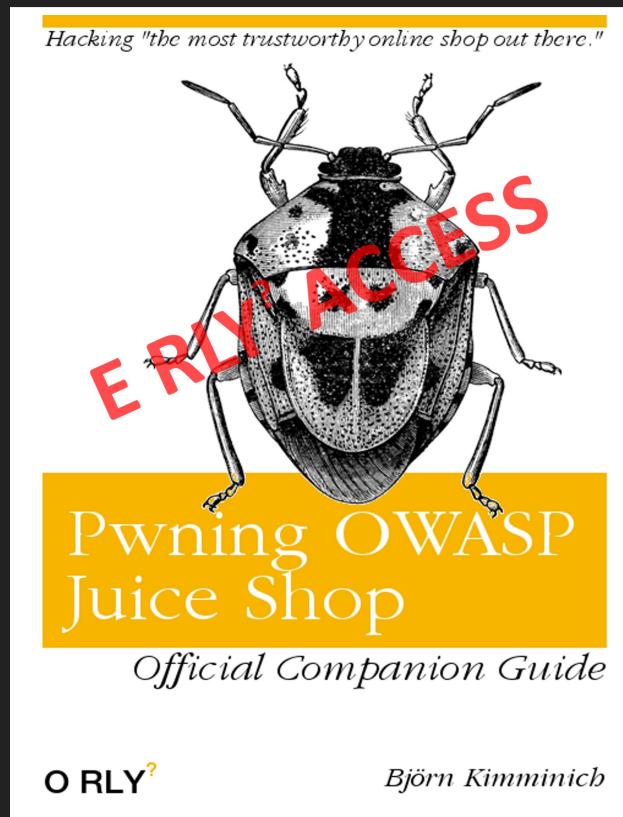
# MORE DISASTERS

Juice Shop now sports 30+7 tracked challenges!

Upload a file larger than 100 KB.	★★★	unsolved
Upload a file that has no .pdf extension.	★★★	unsolved
Retrieve the language file that never made it into production.	★★★★	unsolved
Give a devastating zero-star feedback to the store.	★	unsolved
Fake a continue code that solves only (the non-existent) challenge #99.	★★★★★	unsolved
Log in with Bjoern's user account <i>without</i> previously changing his password, applying SQL Injection, or hacking his Google account.	★★★	unsolved
Exploit OAuth 2.0 to log in with the Chief Information Security Officer's user account.	★★★★	unsolved

# MORE DOCUMENTATION

The official companion guide for the aspiring hacker!



# WHAT'S UP NEXT?

# ROADMAP

- Continually adding more challenges to the application
- Lab Project status on OWASP (*project review ongoing*)
- Technical Evolution (*Angular, Sequelize, Jasmine/Frisby*)
- CTF-Server for classrooms & group training setups
- Finish and publish the Pwning OWASP Juice Shop eBook



Timeline? When it's done!

# MEDIA COVERAGE

# JUICE SHOP ON 7 MINUTE SECURITY

5 dedicated episodes hacking all challenges (up to that date)

## 7 MINUTE SECURITY

[www.7ms.us](http://www.7ms.us)

"Regurgitating what I'm  
learning about infosec -  
in seven minute chunks!"

- by Brian Johnson

# OFFICIAL YOUTUBE PLAYLIST

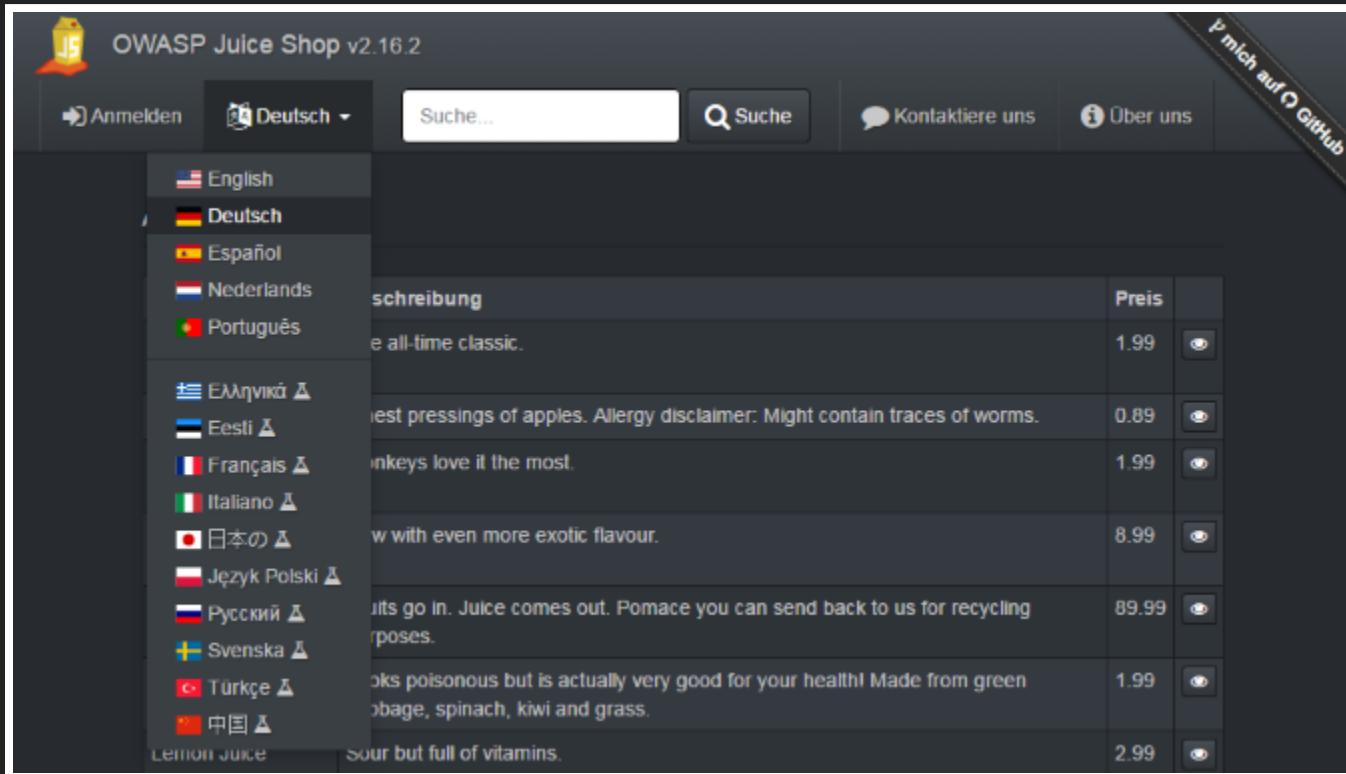
All you need for a romantic hacker-movie night!



CALL FOR  
CONTRIBUTIONS

# HELP WITH TRANSLATIONS

I18N is managed via [CrowdIn](#), but [GitHub PRs](#) also work fine



The screenshot shows the OWASP Juice Shop v2.16.2 website. The top navigation bar includes a logo, a login button, a language dropdown set to "Deutsch", a search bar, and links for "Kontaktiere uns" and "Über uns". A GitHub integration link "mich auf GitHub" is visible in the top right. The sidebar on the left lists language options with their flags: English (selected), Deutsch, Español, Nederlands, Português, Greek, Estonian, French, Italian, Japanese, Polish, Russian, Swedish, Turkish, and Chinese. The main content area displays a table of juice products:

	schreibung	Preis	
	the all-time classic.	1.99	<input type="button" value=""/>
	atest pressings of apples. Allergy disclaimer: Might contain traces of worms.	0.89	<input type="button" value=""/>
	monkeys love it the most.	1.99	<input type="button" value=""/>
	with even more exotic flavour.	8.99	<input type="button" value=""/>
	uits go in. Juice comes out. Pomace you can send back to us for recycling purposes.	89.99	<input type="button" value=""/>
	looks poisonous but is actually very good for your health! Made from green cabbage, spinach, kiwi and grass.	1.99	<input type="button" value=""/>
Lemon Juice	Sour but full of vitamins.	2.99	<input type="button" value=""/>

# HELP WITH DEVELOPMENT

Our [contribution guideline](#) will help you send PRs in no-time



help wanted

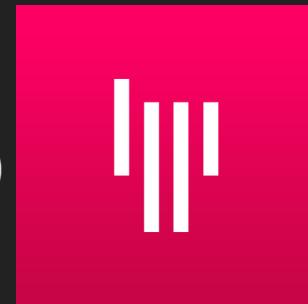
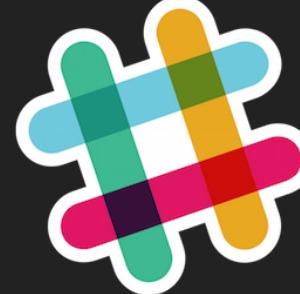
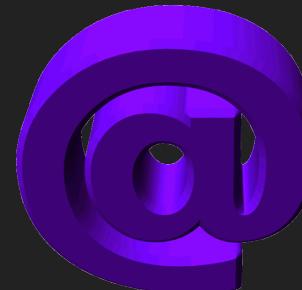
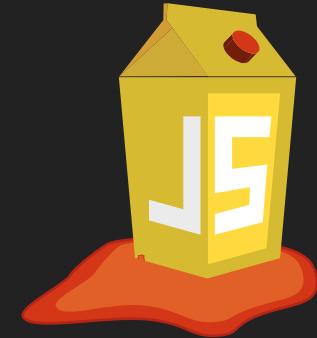
THANKS FOR !



TALK:



IN



COPYRIGHT (C) 2014-2016 **BJÖRN KIMMINICH**

Licensed under the **MIT** license.