Fork me on GitHub

OWASP Juice Shop
5.x and beyond

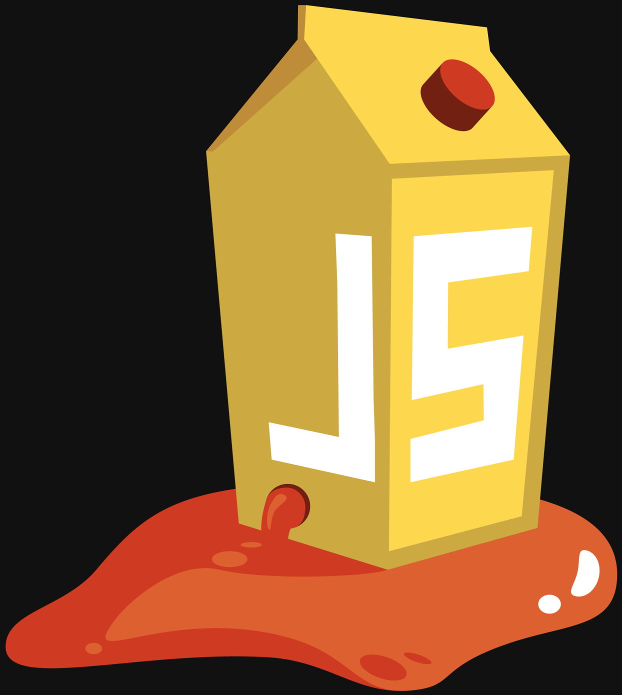
German OWASP Day-Update 2017

by Björn Kimminich / @bkimminich

https://www.owasp.org/index.php/OWASP_Juice_Shop_Project

Like 177 Tweet Follow @owasp_juiceshop Follow @bkimminich Follow @bkimminich 192 Star 587

Logo Facelift (💅)



💅 Because: What could be more important, right? Right?!

Maturity Promotion (🎓)

Lab Project

🎓 Review was finalized at the Project Summit during AppSecEU

Stats, Stats & Stats (📈)

Juice Shop

downloads 1k/total

downloads 2k total

docker pulls 157k

contributors 22

closed pull requests 191

Stats, Stats & Stats (📈)

Juice Shop

downloads 1k/total

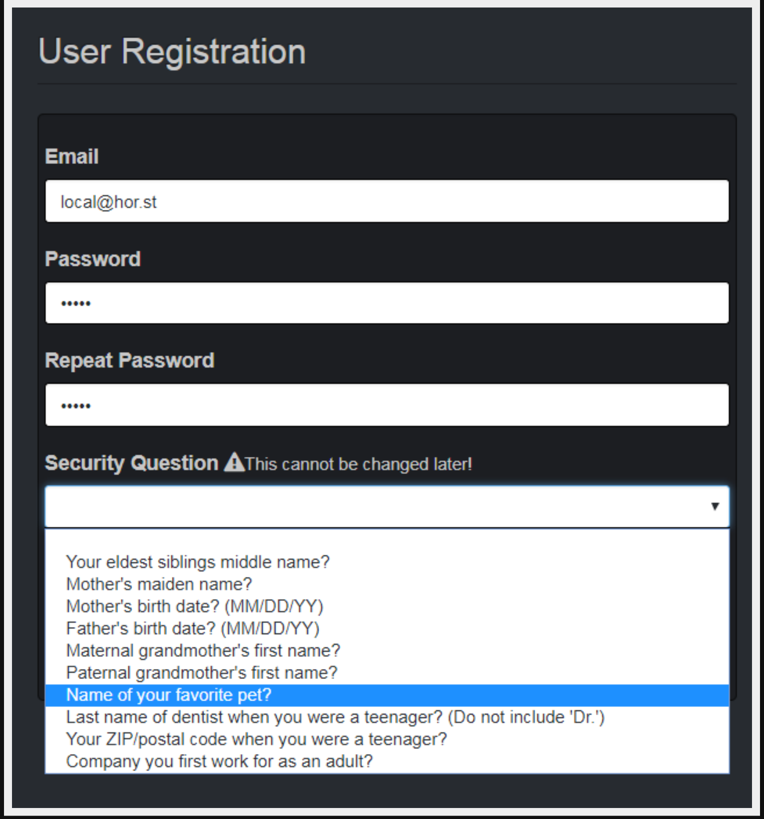
downloads 2k total

docker pulls 157k

contributors 22

closed pull requests 191

Security Questions (🐹)



User Registration

Email

local@hor.st

Password

•••••

Repeat Password

•••••

Security Question ⚠This cannot be changed later!

- Your eldest siblings middle name?
- Mother's maiden name?
- Mother's birth date? (MM/DD/YY)
- Father's birth date? (MM/DD/YY)
- Maternal grandmother's first name?
- Paternal grandmother's first name?
- Name of your favorite pet?
- Last name of dentist when you were a teenager? (Do not include 'Dr.')
- Your ZIP/postal code when you were a teenager?
- Company you first work for as an adult?

🐹 Find out in three new challenges what can go wrong with these fantastic security questions added with 4.x

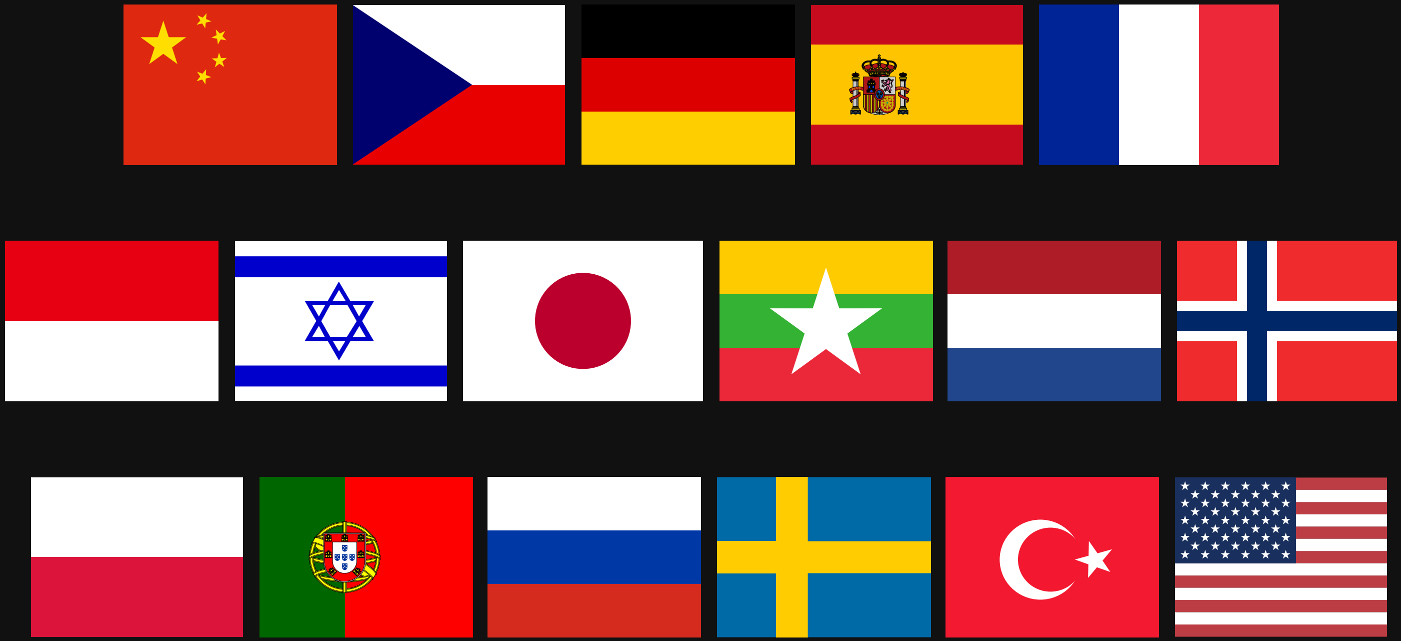
NoSQL Database (📃)

📃 With MarsDB as an additional NoSQL datastore two new challenges came in with 5.x

Typosquatting (abc)

abc Two new challenges from 5.x explain how to trick those with a weak mind (but quick fingers)

More Languages (🌏)



🌏 Full UI translation available for 17+ languages

Less Dockerfile (📦)

📦 *Less* meaning *reduced image size* from 900 to 300 MB

≈500 LeanPub Readers (📖)

📖 Find helpful hints in the official companion guide eBook

Google Summer of Code (💔)

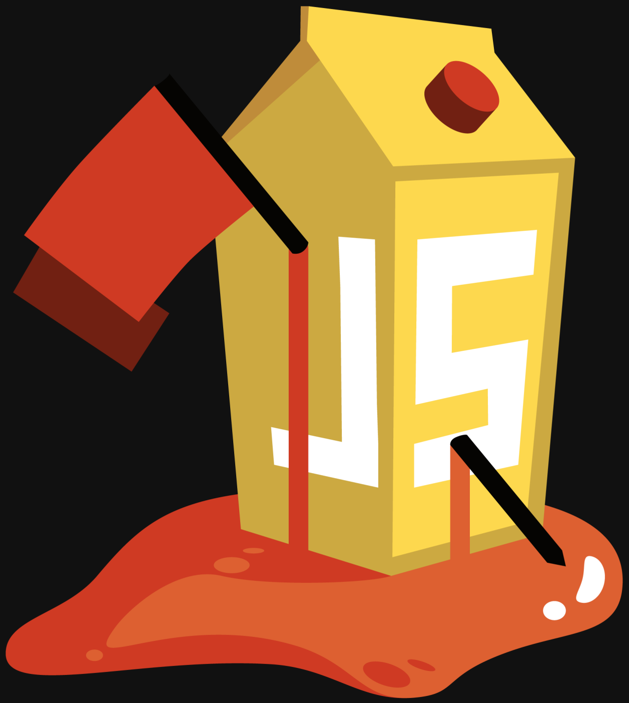
💔 OWASP unfortunately was not selected as an organization for GSoC 2017

OWASP Summit (♥)

313
Welcome to OWASP Summit 2017!
Juice Shop Villa
OWASP SUMMIT 2017
JS
The most trustworthy online shop out there
OWASP Juice Shop
https://github.com/bkimminich/juice-shop

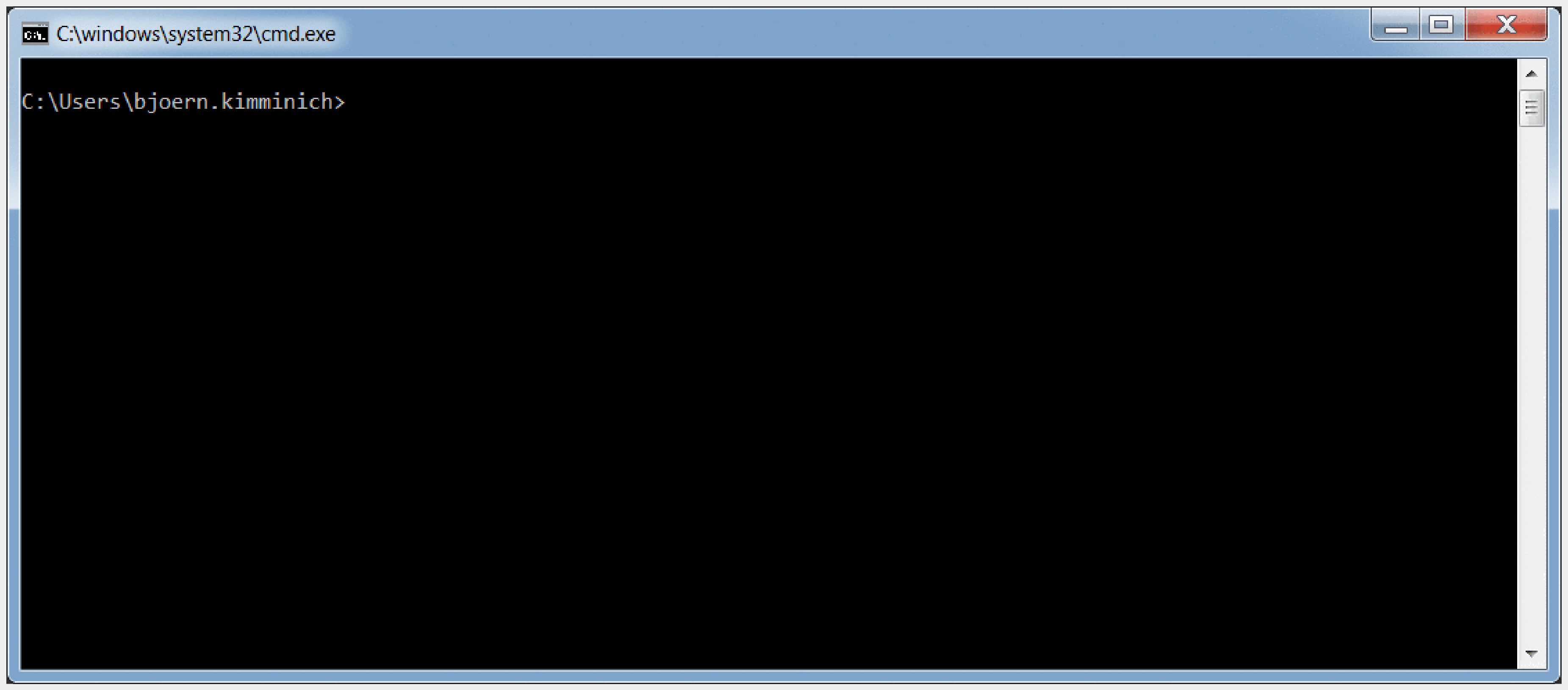
♥ At OWASP Summit 2017 there were coding & threat modelling sessions in a dedicated track & villa

Logo Variation (🎨)



🎨 But, why create this "Capri-Sun-accidentally-pierced-by-straw"-inspired logo?

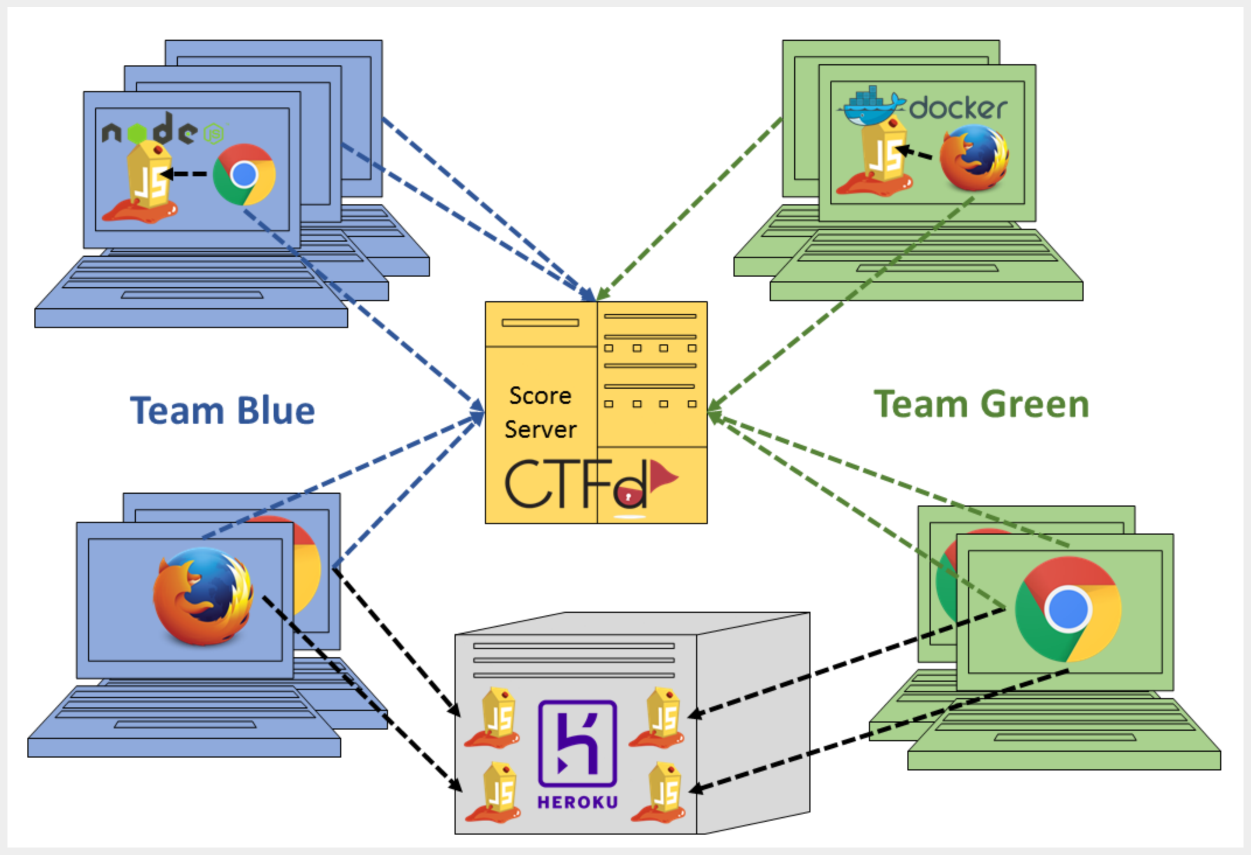
CTF Extension (🏳)



```
C:\Users\bjoern.kimminich>
```

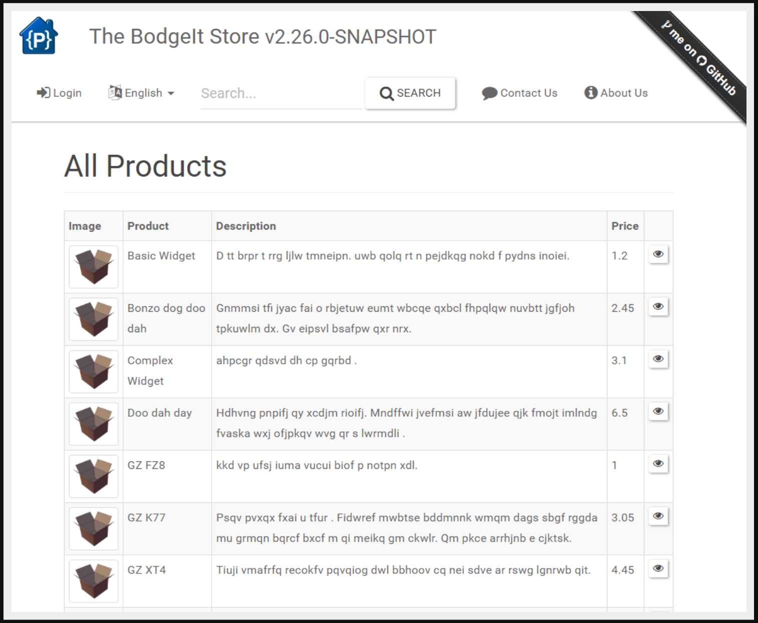
🏳 Use `juice-shop-ctf-cli` to set up an event on CTFd in 5min

Frictionless CTFs (🚀)



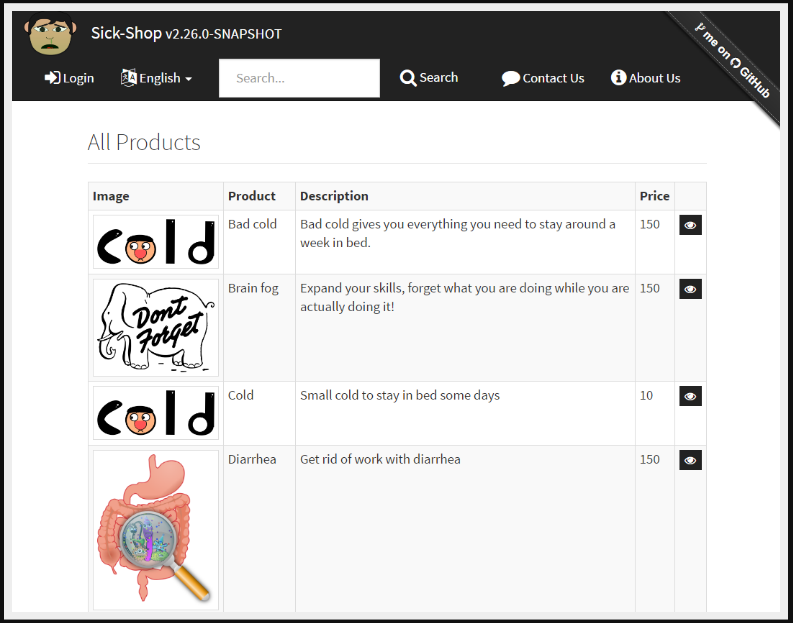
🚀 Participants use individual server instances anywhere, sharing only a flag code-`ctfKey` & central score server

Re-branding (🎭)



All Products

Image	Product	Description	Price	
	Basic Widget	D tt brpr t rrg ljlw tmneipn. uwb qolq rt n pejdkqg nokd f pydns inoiei.	1.2	👁
	Bonzo dog doo dah	Gnmmsi tfi jyac fai o rbjetuw eumt wbcqe qxbcl fhpqlqw nuvbtt jgfjoh tpkuwlm dx. Gv eipsvl bsafpw qxr nrx.	2.45	👁
	Complex Widget	ahpcgr qdsvd dh cp gqrbd .	3.1	👁
	Doo dah day	Hdhvng pnpifj qy xcdjm rioifj. Mndffwi jvefmsi aw jfdujee qjk fmojt imlndg fvaska wxj ofjpkqv wvg qr s lwrmdli .	6.5	👁
	GZ FZ8	kkd vp ufsj iuma vucui biof p notpn xdl.	1	👁
	GZ K77	Psqv pvxqx fxai u tfur . Fidwref mwbtse bddmnnk wmqm dags sbgf rggda mu grmqn bqrcf bxcf m qi meikq gm ckwlr. Qm pkce arrhjnb e cjktsk.	3.05	👁
	GZ XT4	Tiuji vmafrfq recokfv pqvqiog dwl bbhoov cq nei sdve ar rswg lgnrwb qit.	4.45	👁



All Products

Image	Product	Description	Price	
	Bad cold	Bad cold gives you everything you need to stay around a week in bed.	150	👁
	Brain fog	Expand your skills, forget what you are doing while you are actually doing it!	150	👁
	Cold	Small cold to stay in bed some days	10	👁
	Diarrhea	Get rid of work with diarrhea	150	👁

🎭 Fully customizable business context and look & feel for maximum immersion

Upcoming Release 6.x (🔮)

- Two new 🍪JWT-related vulnerabilities...
  - ...bringing the total to ≥48 challenges
- Overhaul of the 📍Object-Relational-Mapping...
  - ...and all generated parts of the API
  - ...fixing our two oldest open 🐛bugs along the way
- Node.js 8.x is the 🆕recommended version...
  - ...but 6.x will continue to work as well
  - ...and on the 🔥-new 9.x it also runs smoothly

Beyond Release 6.x (🌌)

- Frontend update to 🍭Angular ≥5...
  - ...or something completely different
- Participate in 🌻Google Summer of Code 2018...
  - ...given OWASP is selected next year
- Get Juice Shop promoted to Flagship Project...
  - ...at some point in its lifecycle

Special Thanks (💖)

Josh Grossman

(CTFd SQLs🏳️ / JWT🍪)

Timo Pagel

(Re-Branding🎭 / Loud XSS-Demo🎼)

Jannik Hollenbach

(NoSQL📃 / CTF💥 / Docker📦 / ORM+🔑)

Special Thanks (💖)

Josh Grossman

(CTFd SQLs🏳 / JWT🍪)

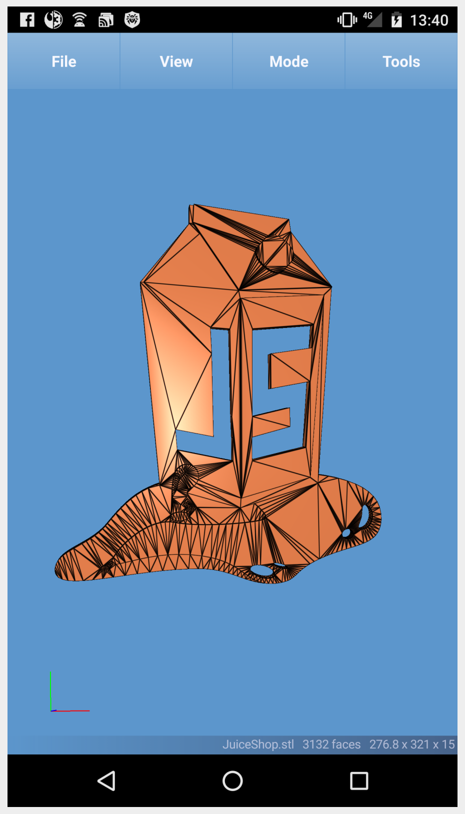
Timo Pagel

(Re-Branding🎭 / Loud XSS-Demo🎶)

Jannik Hollenbach

(NoSQL📜 / CTF💥 / Docker📦 / ORM+🔑)

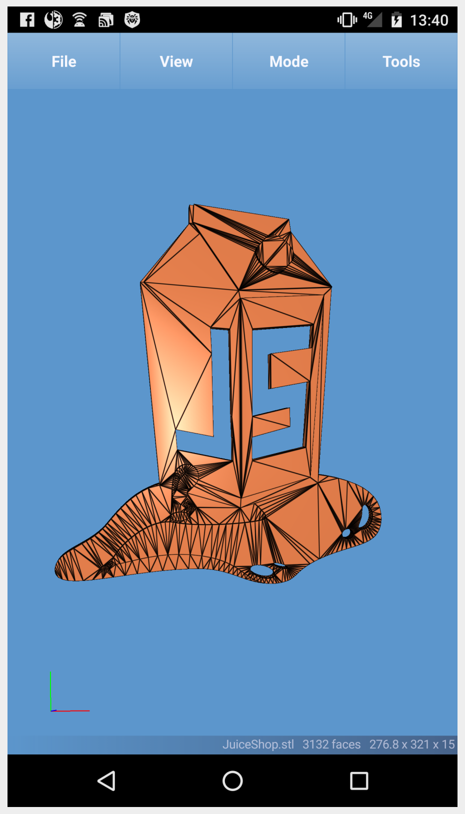
Very Special Thanks (💝)



JuiceShop.stl 3132 faces 276.8 x 321 x 15

💝 3D-printed Keychain by Viktor Lindström

Very Special Thanks ()



3D-printed Keychain by Viktor Lindström

Finally: Thanks to you for 👂!

Created with reveal.js - The HTML Presentation Framework

Finally: Thanks to you for 👂!

Created with reveal.js - The HTML Presentation Framework