2015 CEE-SEC(R)
Software Engineering
Conference in Russia

Why Security Testing Is More Important Than Ever

Slavy Slavov
slavy.slavov@equafy.com

www.equafy.com

equafy

About me

Managed Experian Global QA for UK, Monaco, Malaysia and Bulgaria

Managed the teams developing some of the world's largest online stores

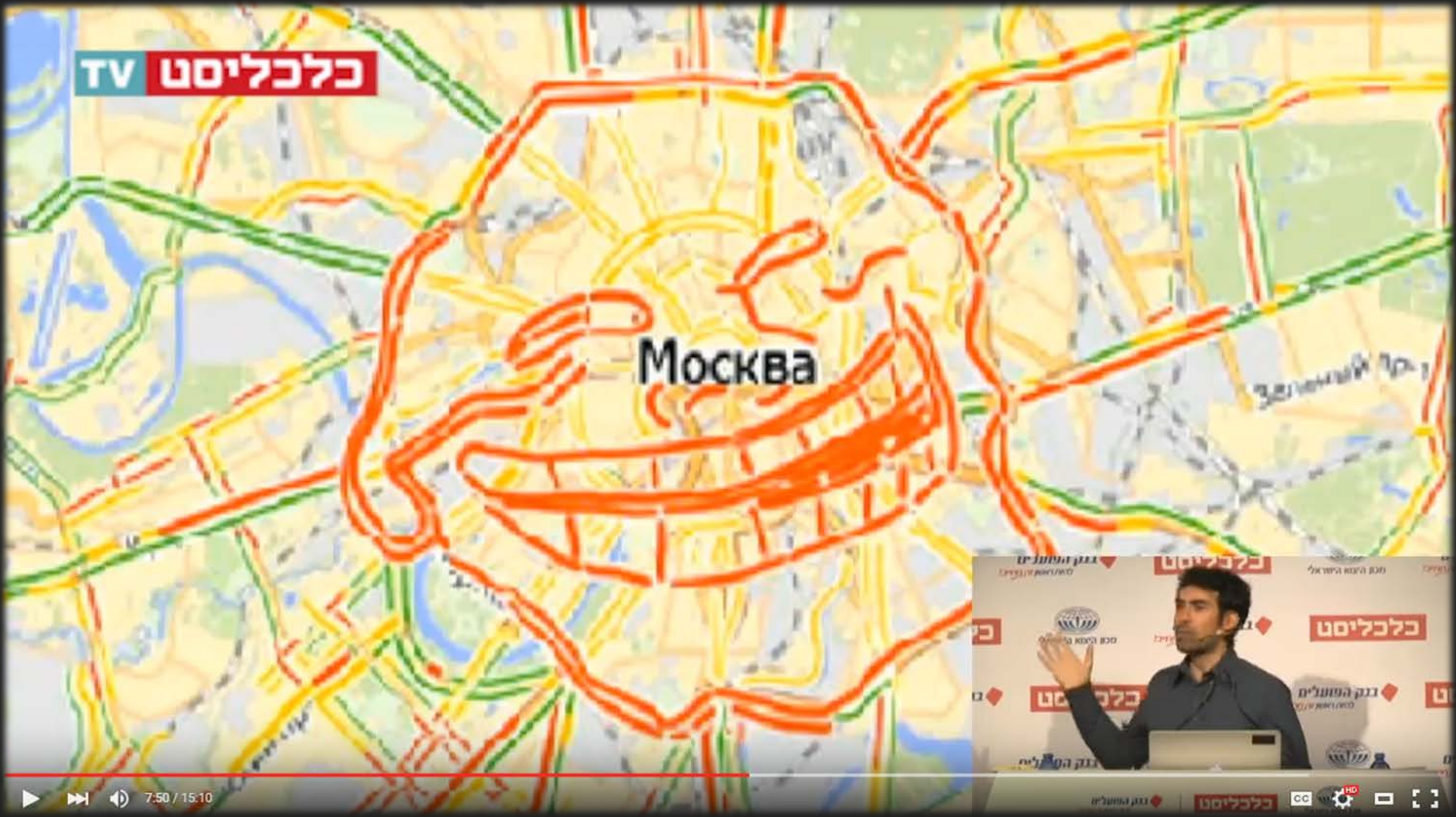
Founder of Equafy - Cross Browser Testing SaaS

Indeed 471,000 of them…

equafy

Ooops…the wrong person?

Google Maps getting data…



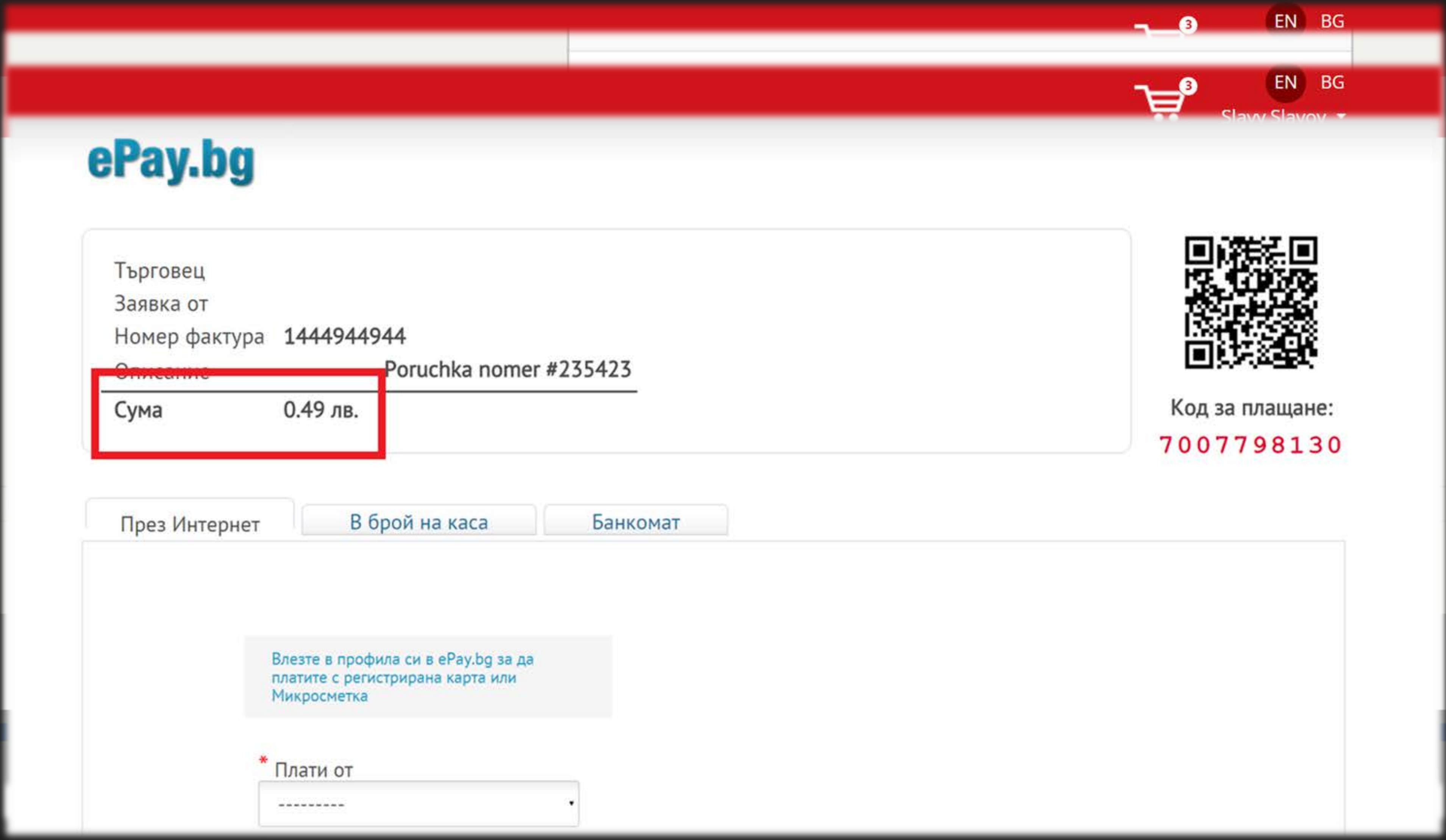
Old school

New generation

equafy

What’s next?

Donate to Unicef



ePay.bg

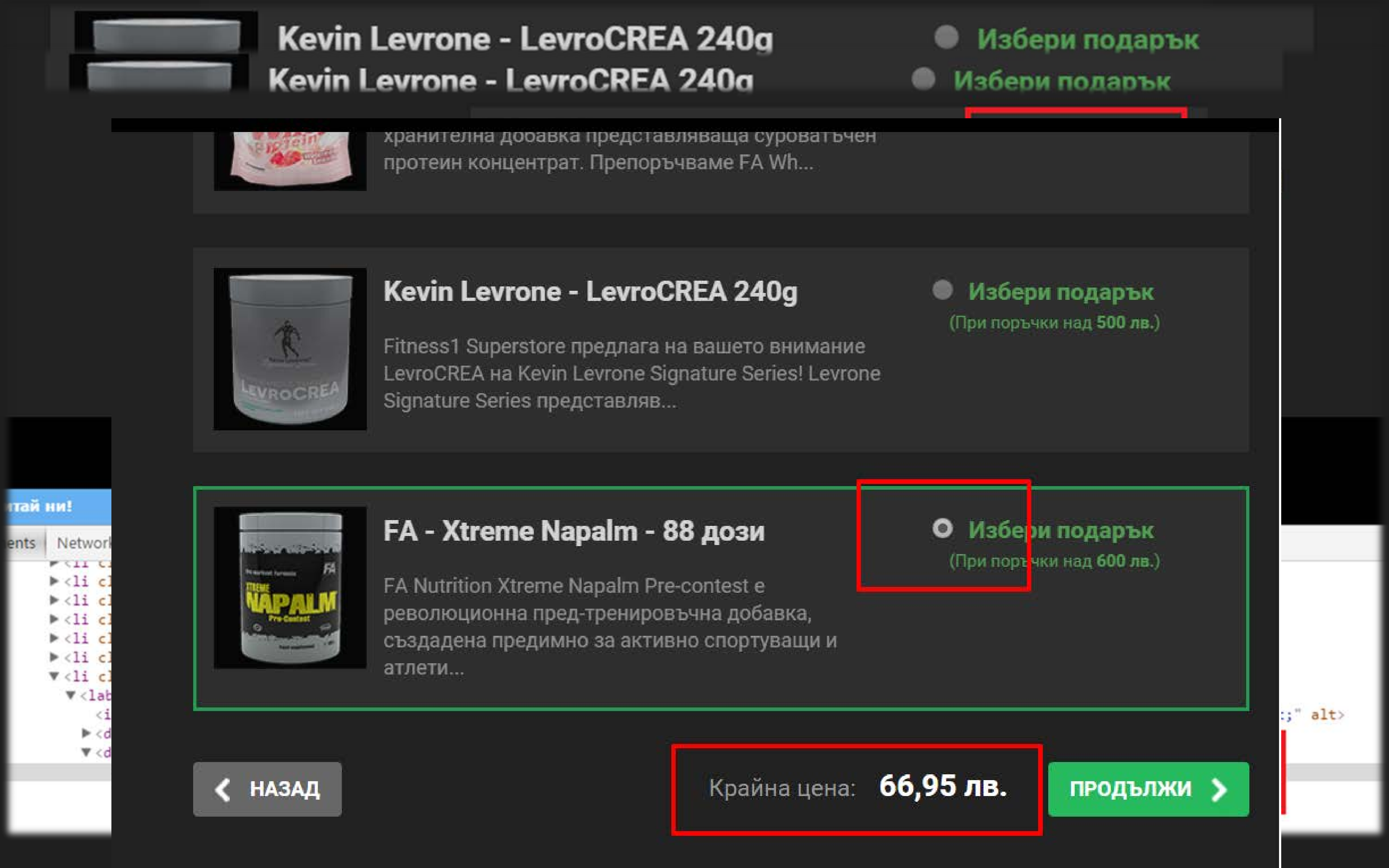
Търговец
Заявка от
Номер фактура 1444944944
Описание Poruchka nomer #235423
Сума 0.49 лв.

Код за плащане:
7007798130

Влезте в профила си в ePay.bg за да платите с регистрирана карта или Микросметка

* Плати от

Nice present!



Kevin Levrone - LevroCREA 240g ○ Избери подарък

Kevin Levrone - LevroCREA 240g ○ Избери подарък

хранителна добавка представляваща суроватъчен протеин концентрат. Препоръчваме FA Wh...

Kevin Levrone - LevroCREA 240g ○ Избери подарък (При поръчки над 500 лв.)

Fitness1 Superstore предлага на вашето внимание LevroCREA на Kevin Levrone Signature Series! Levrone Signature Series представляв...

FA - Xtreme Napalm - 88 дози ◉ Избери подарък (При поръчки над 600 лв.)

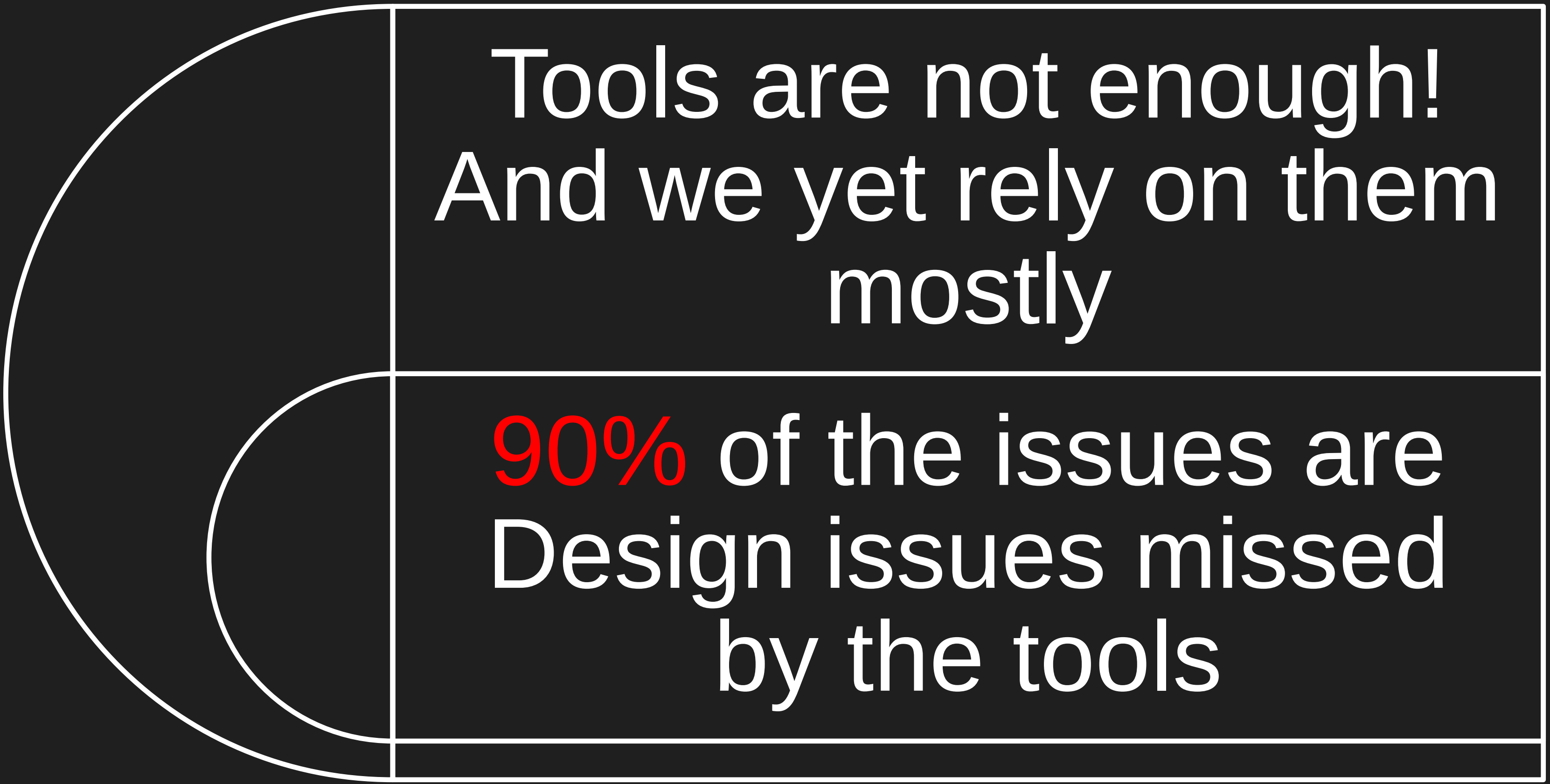
FA Nutrition Xtreme Napalm Pre-contest е революционна пред-тренировъчна добавка, създадена предимно за активно спортуващи и атлети...

< НАЗАД

Крайна цена: 66,95 лв.

ПРОДЪЛЖИ >

80% of shops are very weak



Tools are not enough!
And we yet rely on them mostly

90% of the issues are Design issues missed by the tools

Most common issues

- ✗ No server side checks
- ✗ Too much POST data
- ✗ Caching sensitive info
- ✗ Ability to guess repetitive data (fuzzy matching)
- ✗ Predictable IDs and weak access control
- ✗ Neglected XSS (steal personal data)
- ✗ Inject code
- ✗ Stupidity

Best process practices

- ✓ Rely on common platforms (they resolved 95% of the issues already)
- ✓ Combine architecture review with tools
- ✓ Monitor & Analyze data flow and traffic
- ✓ Implement CI Security tests
- ✓ Runtime tools/plugins
- ✓ Act wild – I learned a lot from my 2 years old son
- ✓ Know your stuff…architecture is key

Best technical practices

- ✓ Isolate environments and layers
- ✓ Use cookies securely
- ✓ Do not store plain text sensitive data
- ✓ Have detailed audit log
- ✓ Validate empty, large or fake data input
- ✓ Do not cache user data (embedded)
- ✓ Use complex object IDs
- ✓ Cross fingers to not be a target ☺

equafy

Thank You!

Q & A

slavy.slavov@equafy.com

@sslavov

equafy