eScore

HackYeah 2024

Team **Mniejsza Dawka Development**

- Adam Piaseczny
- Tymoteusz Jagła
- Mateusz Karłowski
- Maciej Kaszkowiak

Defining the Problem

- More **trustworthy looking fakes** thanks to AI

- Harder to judge by first glance

- **E-commerce** gets hit especially hard because of sheer **fraud** potential

- CERT stats from 2023 report over **34,000** online fraud cases (only reported ones count, imagine **how many could there be in the wild?**)

How could we combat this?

- **Automation of client-facing fraud detection mechanisms**

- **Easy to digest fraud evaluations** using varying metrics to guarantee validity

- Harnessing expert knowledge **beyond the optics**
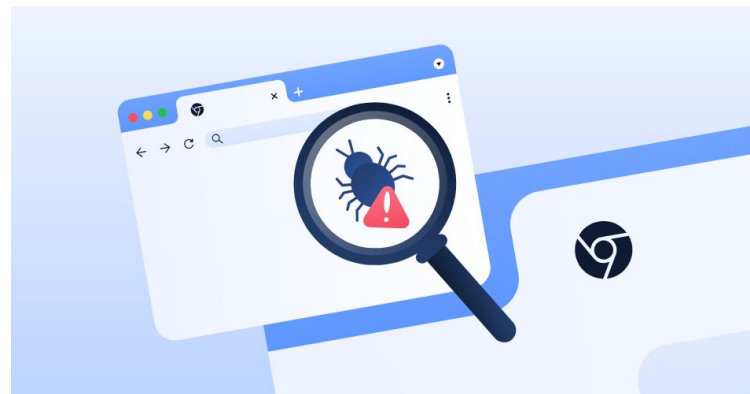
Our Solution

eScore

WOW!!! Cheap Ray-Bans
Wait… is this site legit?

TIME TO ESCORE
Using the extension or
a dedicated website

76.25%
Security Score

Tech standards:	70%
Reviews:	95%
Phising:	100%
Social:	40%

Damn, it really is a crazy deal
Easy to digest scores

Evaluation categories

Tech

HSTS, MX, SPF, DMARC, robots.txt, CERT

Reviews

Reviews from Trustpilot, Facebook, Google Maps, etc.

Social

IP Abuse Lists, Contact, Social Media

Phishing

Domain comparison against similar well-known sites
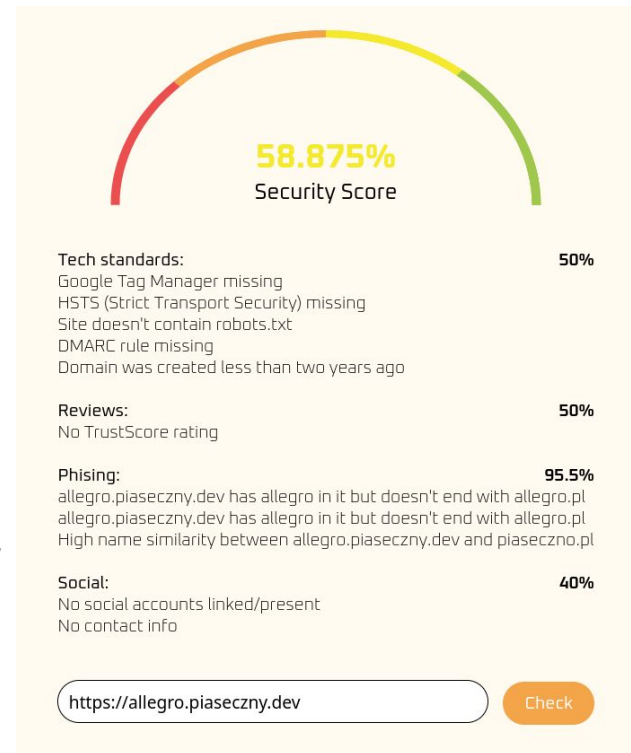
eScore

Why not just an extension - Rake Analogy

Problems with extension code:

- **Cannot reliably check DNS/IP Abuse** records
- It's easy for the attacker **to know that they are being evaluated**
- **You shouldn't need to step on the rake to know that it's there!** The same applies to the website! Extensions require that you are on the website - **We don't - we also have a checker website**
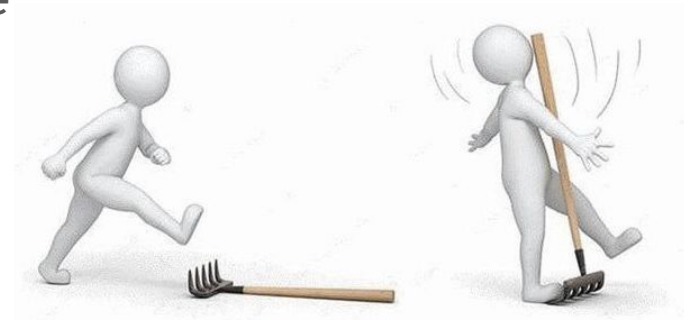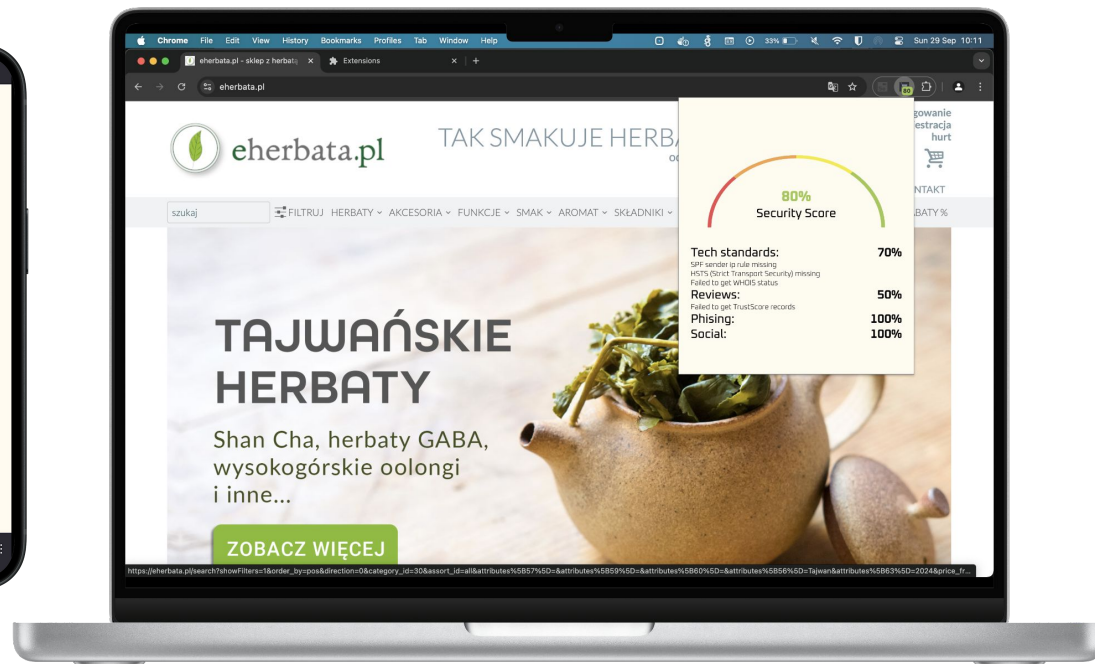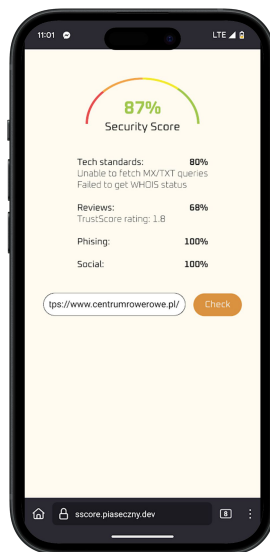
Evaluation server advantages

- We can share evaluations between users - **now everyone is safe and requests can be rerouted (block lists)**
- By having a evaluation database, **we can gather statistics about new fraud tactics** and respond appropriately
- We can chain abusers by **tracking their origin (IP chain abuse)**
- We can monetize data - **Ray-Ban would definitely want to know that a new fake shop with their products appeared** (legal action)

eScore

58.875%
Security Score

Tech standards: 50%
Google Tag Manager missing
HSTS (Strict Transport Security) missing
Site doesn't contain robots.txt
DMARC rule missing
Domain was created less than two years ago

Reviews: 50%
No TrustScore rating

Phising: 95.5%
allegro.piaseczny.dev has allegro in it but doesn't end with allegro.pl
allegro.piaseczny.dev has allegro in it but doesn't end with allegro.pl
High name similarity between allegro.piaseczny.dev and piaseczno.pl

Social: 40%
No social accounts linked/present
No contact info

https://allegro.piaseczny.dev   Check

Demo

A website **demo** is **patiently waiting** for you at sscore.piaseczny.dev

Expanding further

- Introducing **more review-based checkers** since they are the **most reliable** when it comes to shops
- Providing paid **guidance to e-commerce shop owners** to increase their score and security
- Integrations with **CERT, Abuse Databases** and other **Open Source Security (OSS)** tools

Roadmap

eScore

We are here!

User driven solution. Report fake page feature by users.

Analyze aggregate data from frauds, detect similarities, AI

Price based detection - doesn't require TrustScores

Exploring monetization options or further integrations with OSS