How we successfully built an AppSec team from scratch

Tiago Mendo
March 2, 2023

me

me

- 2004 Developer / security engineer at Portugal Telecom
- 2008 Master in Information Security - Carnegie Mellon / FCUL
- 2010 Builder of the SAPO security team at Portugal Telecom
- 2016 Lead pentester at Cobalt
- 2017 **Co-founder and CTO at Probely**
- 2022 **OWASP Lisboa chapter co-leader**

me

2004 Devel

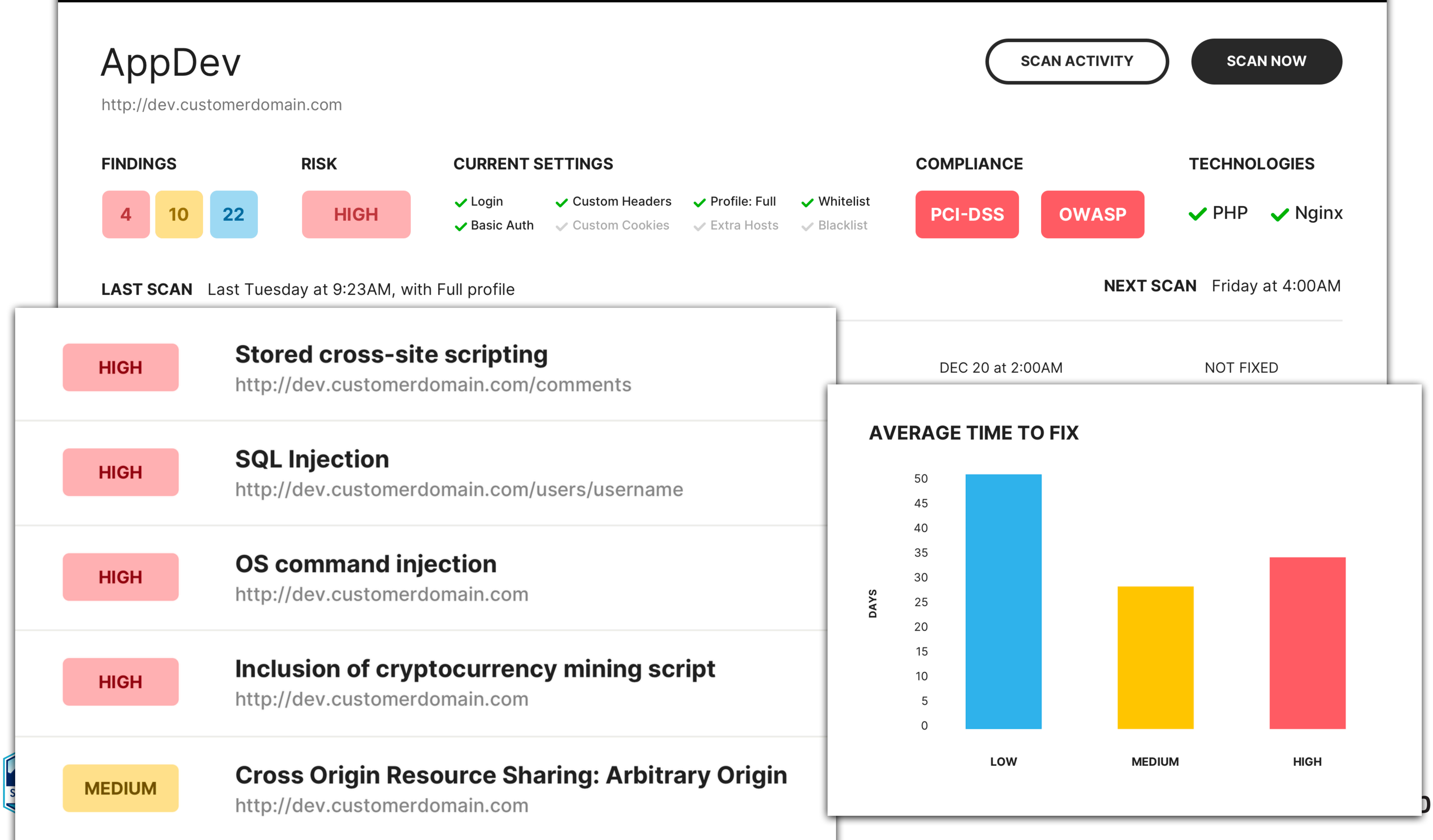
2008 Maste

2010 Builde

2016 Lead p

2017 **Co-fou**

2022 **OWAS**



AppDev

http://dev.customerdomain.com

FINDINGS 4 10 22

RISK HIGH

CURRENT SETTINGS

✓ Login
✓ Basic Auth
✓ Custom Headers
✓ Custom Cookies
✓ Profile: Full
✓ Extra Hosts
✓ Whitelist
✓ Blacklist

COMPLIANCE PCI-DSS OWASP

TECHNOLOGIES ✓ PHP ✓ Nginx

LAST SCAN Last Tuesday at 9:23AM, with Full profile

NEXT SCAN Friday at 4:00AM

DEC 20 at 2:00AM NOT FIXED

HIGH **Stored cross-site scripting**
http://dev.customerdomain.com/comments

HIGH **SQL Injection**
http://dev.customerdomain.com/users/username

HIGH **OS command injection**
http://dev.customerdomain.com

HIGH **Inclusion of cryptocurrency mining script**
http://dev.customerdomain.com

MEDIUM **Cross Origin Resource Sharing: Arbitrary Origin**
http://dev.customerdomain.com

AVERAGE TIME TO FIX

me

2004

2008

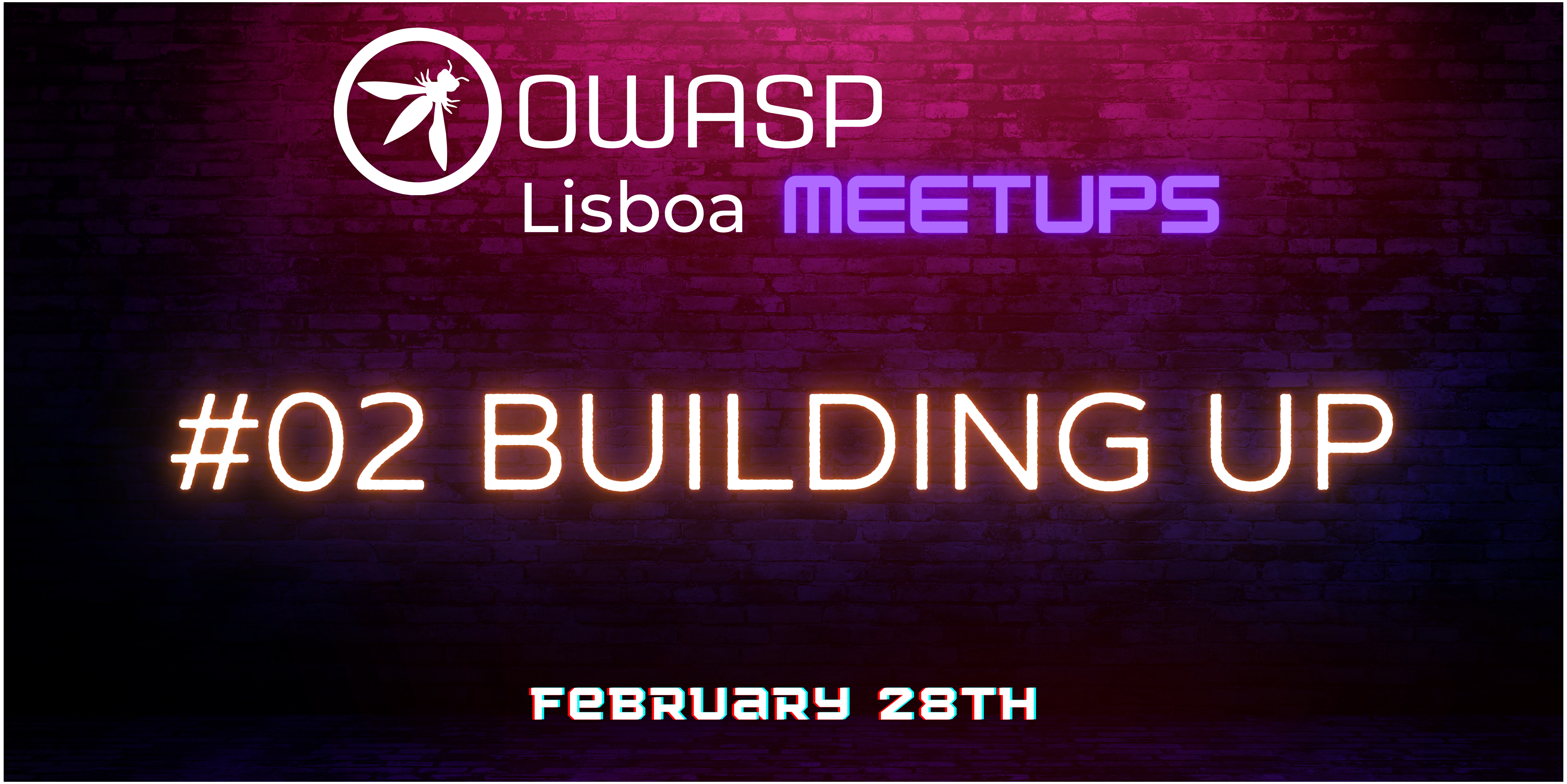
2010

2016

2017

2022 **OWASP Lisboa chapter co-leader**

me



OWASP
SUMMIT
2011
LISBON
PORTUGAL
FEB 8-11

© Ofer Maor

12-16 JUNE 2017
WOBURN FOREST CENTER PARCS

Welcome to OWASP Summit 2017!

#OWASPSummit

Why this talk?

Why

- **Why this talk?**
  - Share the experience, the good and the bad parts
  - Help others creating their app sec teams

The context

Context

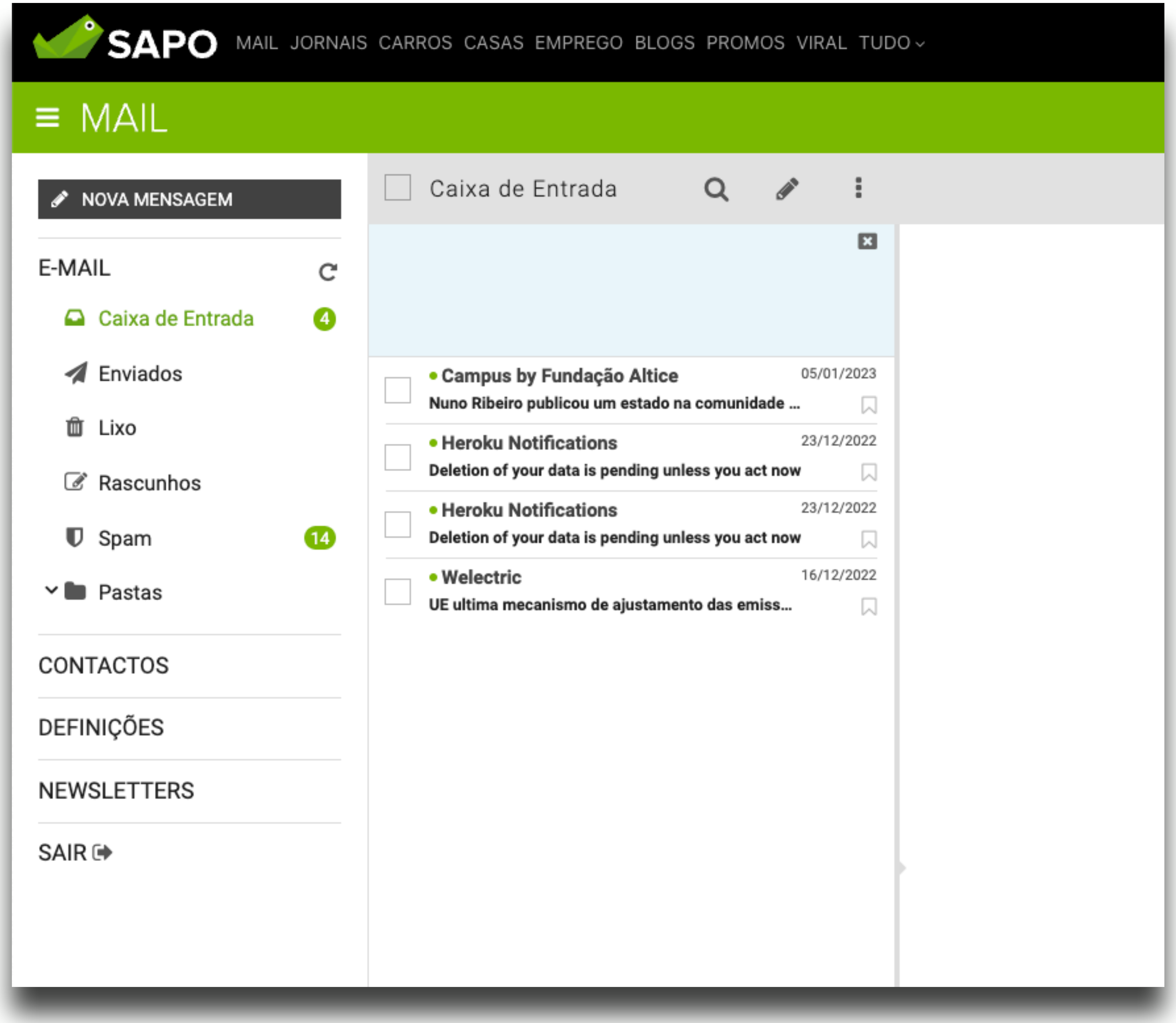
SAPO, the Internet division of Portugal Telecom

- Portugal Telecom (now Altice)
    - 11000 employees, the largest telecom in Portugal

- SAPO (sapo.pt)
    - created in 1995, as a search engine
    - similar to Yahoo / Google
    - Internet Service Provider
    - Ads-based business

SAPO

Context



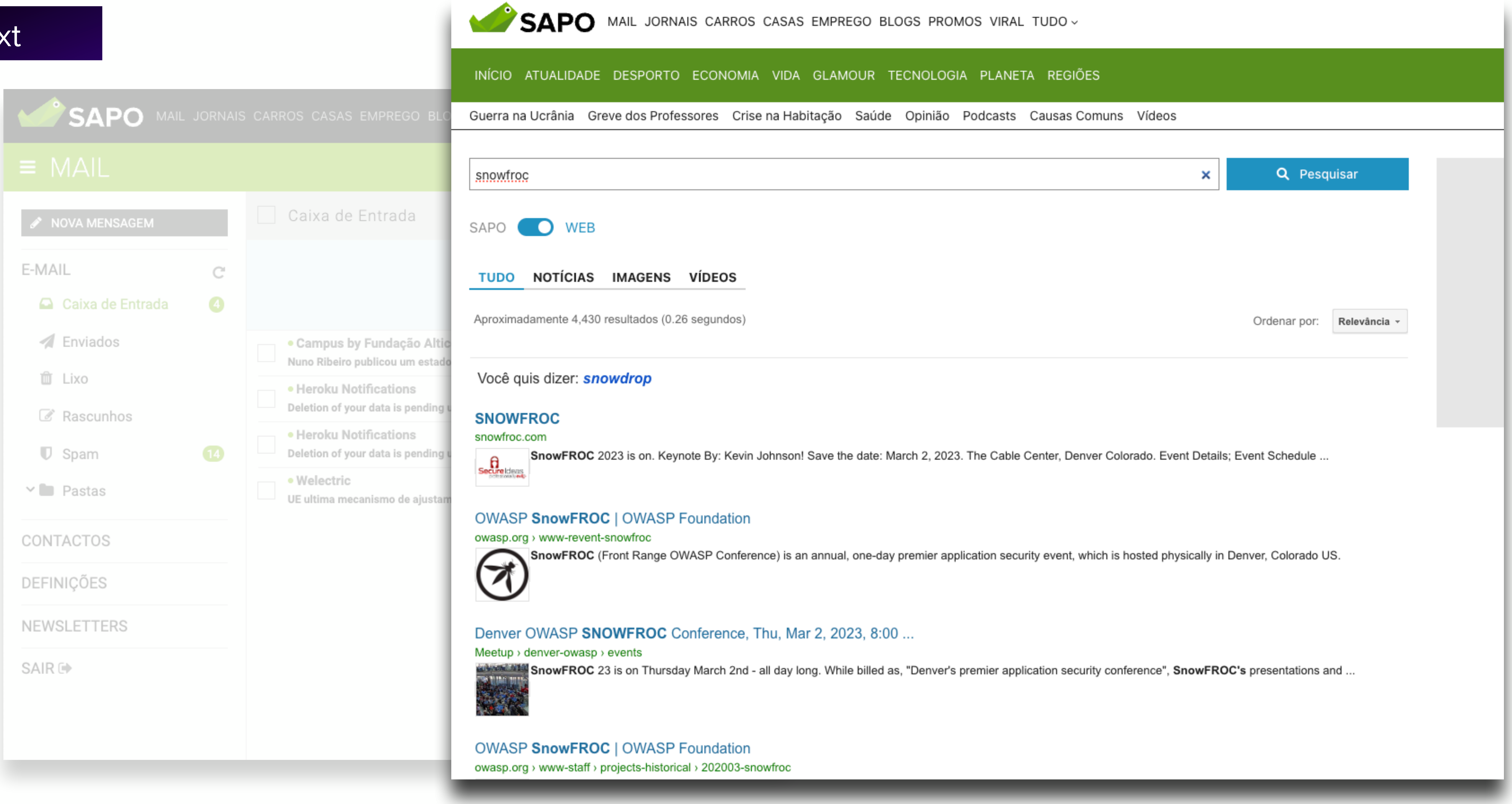
Campus by Fundação Altice 05/01/2023
Nuno Ribeiro publicou um estado na comunidade ...

Heroku Notifications 23/12/2022
Deletion of your data is pending unless you act now

Heroku Notifications 23/12/2022
Deletion of your data is pending unless you act now

Welectric 16/12/2022
UE ultima mecanismo de ajustamento das emiss...

Context



SAPO
MAIL JORNAIS CARROS CASAS EMPREGO BL
MAIL
NOVA MENSAGEM
E-MAIL
Caixa de Entrada 4
Enviados
Lixo
Rascunhos
Spam 14
Pastas
CONTACTOS
DEFINIÇÕES
NEWSLETTERS
SAIR

Caixa de Entrada

- Campus by Fundação Altic
  Nuno Ribeiro publicou um estado
- Heroku Notifications
  Deletion of your data is pending
- Heroku Notifications
  Deletion of your data is pending
- Welectric
  UE ultima mecanismo de ajustam

SAPO
MAIL JORNAIS CARROS CASAS EMPREGO BLOGS PROMOS VIRAL TUDO
INÍCIO ATUALIDADE DESPORTO ECONOMIA VIDA GLAMOUR TECNOLOGIA PLANETA REGIÕES
Guerra na Ucrânia Greve dos Professores Crise na Habitação Saúde Opinião Podcasts Causas Comuns Vídeos
Pesquisar
SAPO WEB
TUDO NOTÍCIAS IMAGENS VÍDEOS
Ordenar por: Relevância

snowfroc

Aproximadamente 4,430 resultados (0.26 segundos)

Você quis dizer: ***snowdrop***

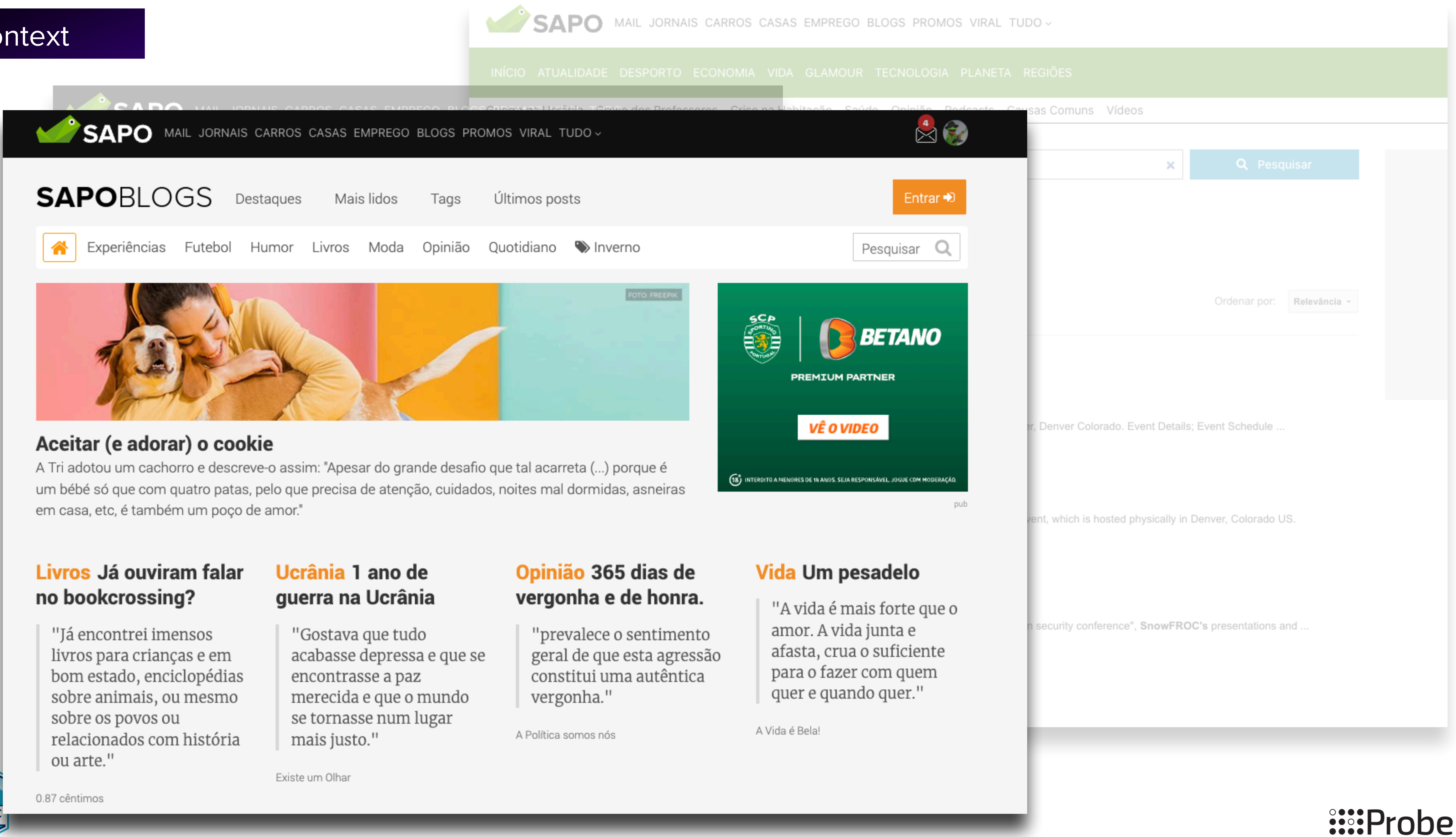
SNOWFROC
snowfroc.com
SnowFROC 2023 is on. Keynote By: Kevin Johnson! Save the date: March 2, 2023. The Cable Center, Denver Colorado. Event Details; Event Schedule ...

OWASP **SnowFROC** | OWASP Foundation
owasp.org › www-revent-snowfroc
SnowFROC (Front Range OWASP Conference) is an annual, one-day premier application security event, which is hosted physically in Denver, Colorado US.

Denver OWASP **SNOWFROC** Conference, Thu, Mar 2, 2023, 8:00 ...
Meetup › denver-owasp › events
SnowFROC 23 is on Thursday March 2nd - all day long. While billed as, "Denver's premier application security conference", **SnowFROC's** presentations and ...

OWASP **SnowFROC** | OWASP Foundation
owasp.org › www-staff › projects-historical › 202003-snowfroc

Context



r, Denver Colorado. Event Details; Event Schedule ...

ent, which is hosted physically in Denver, Colorado US.

n security conference", **SnowFROC's** presentations and ...

Aceitar (e adorar) o cookie

A Tri adotou um cachorro e descreve-o assim: "Apesar do grande desafio que tal acarreta (...) porque é um bébé só que com quatro patas, pelo que precisa de atenção, cuidados, noites mal dormidas, asneiras em casa, etc, é também um poço de amor."

Livros Já ouviram falar no bookcrossing?

> "Já encontrei imensos livros para crianças e em bom estado, enciclopédias sobre animais, ou mesmo sobre os povos ou relacionados com história ou arte."

0.87 cêntimos

Ucrânia 1 ano de guerra na Ucrânia

> "Gostava que tudo acabasse depressa e que se encontrasse a paz merecida e que o mundo se tornasse num lugar mais justo."

Existe um Olhar

Opinião 365 dias de vergonha e de honra.

> "prevalece o sentimento geral de que esta agressão constitui uma autêntica vergonha."

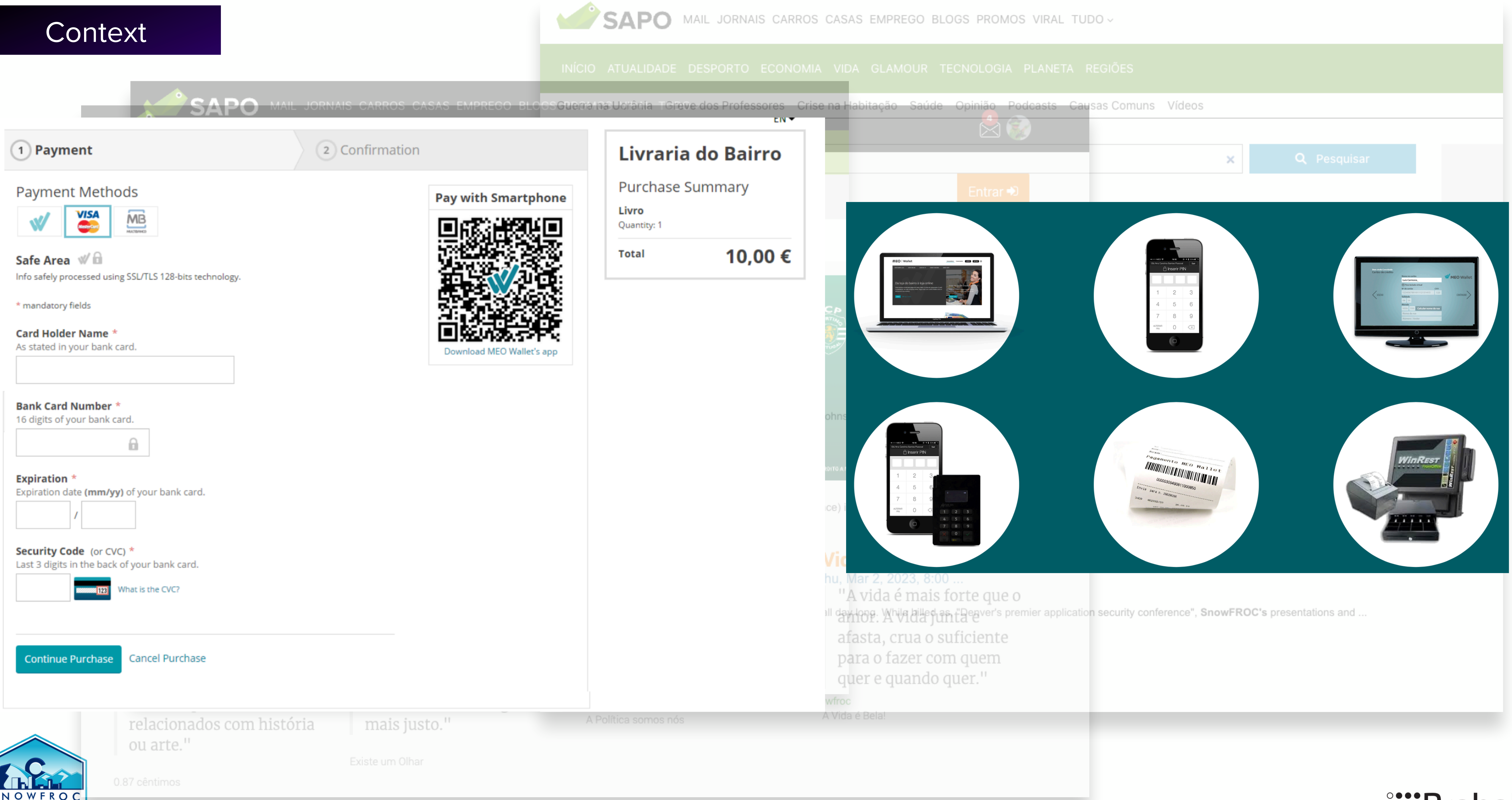
A Política somos nós

Vida Um pesadelo

> "A vida é mais forte que o amor. A vida junta e afasta, crua o suficiente para o fazer com quem quer e quando quer."

A Vida é Bela!

Context



1 **Payment** 2 Confirmation

Payment Methods

Safe Area

Info safely processed using SSL/TLS 128-bits technology.

* mandatory fields

Card Holder Name *
As stated in your bank card.

Bank Card Number *
16 digits of your bank card.

Expiration *
Expiration date **(mm/yy)** of your bank card.

Security Code (or CVC) *
Last 3 digits in the back of your bank card.

What is the CVC?

Continue Purchase Cancel Purchase

Pay with Smartphone

Download MEO Wallet's app

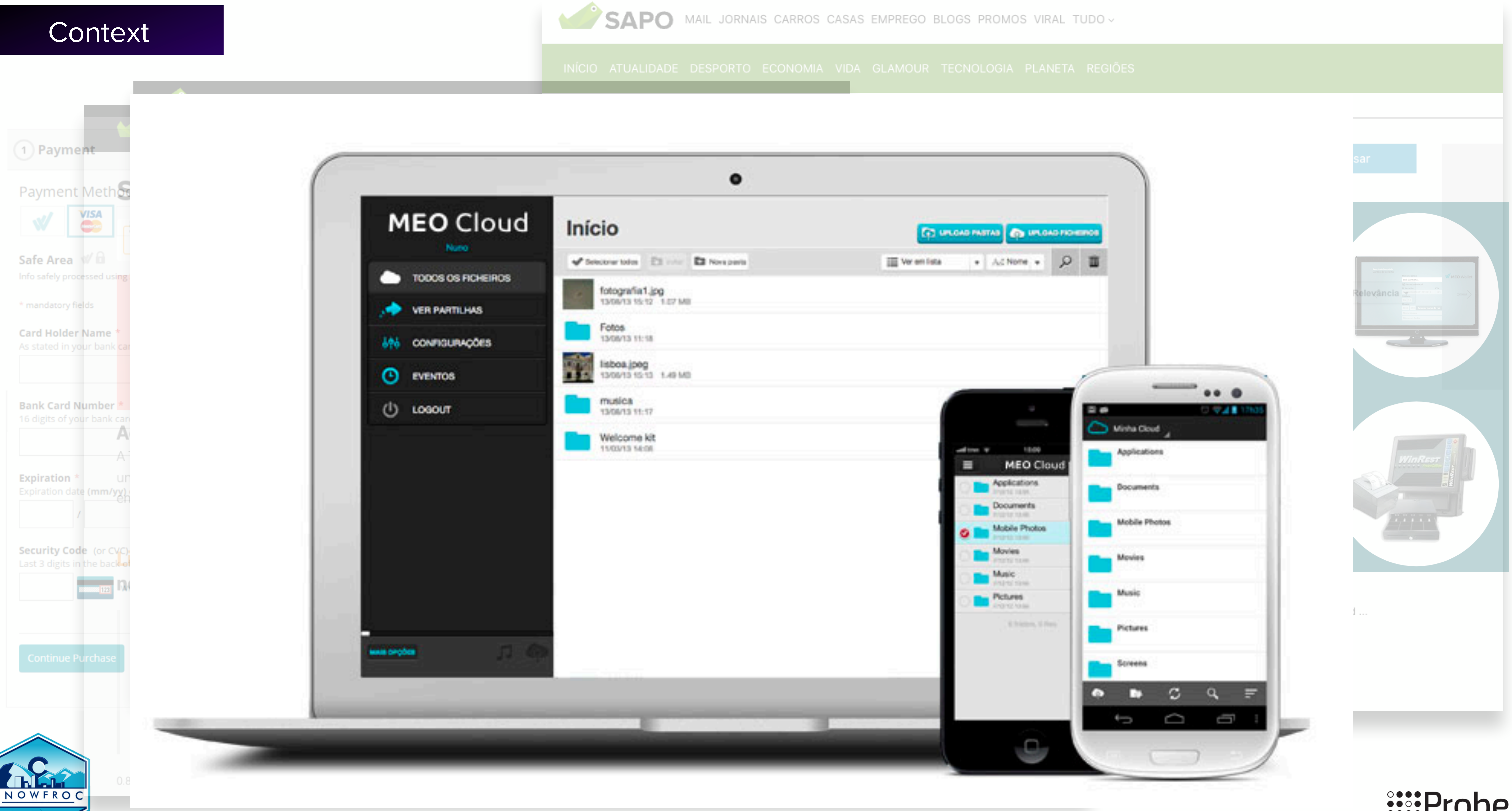
Livraria do Bairro

Purchase Summary

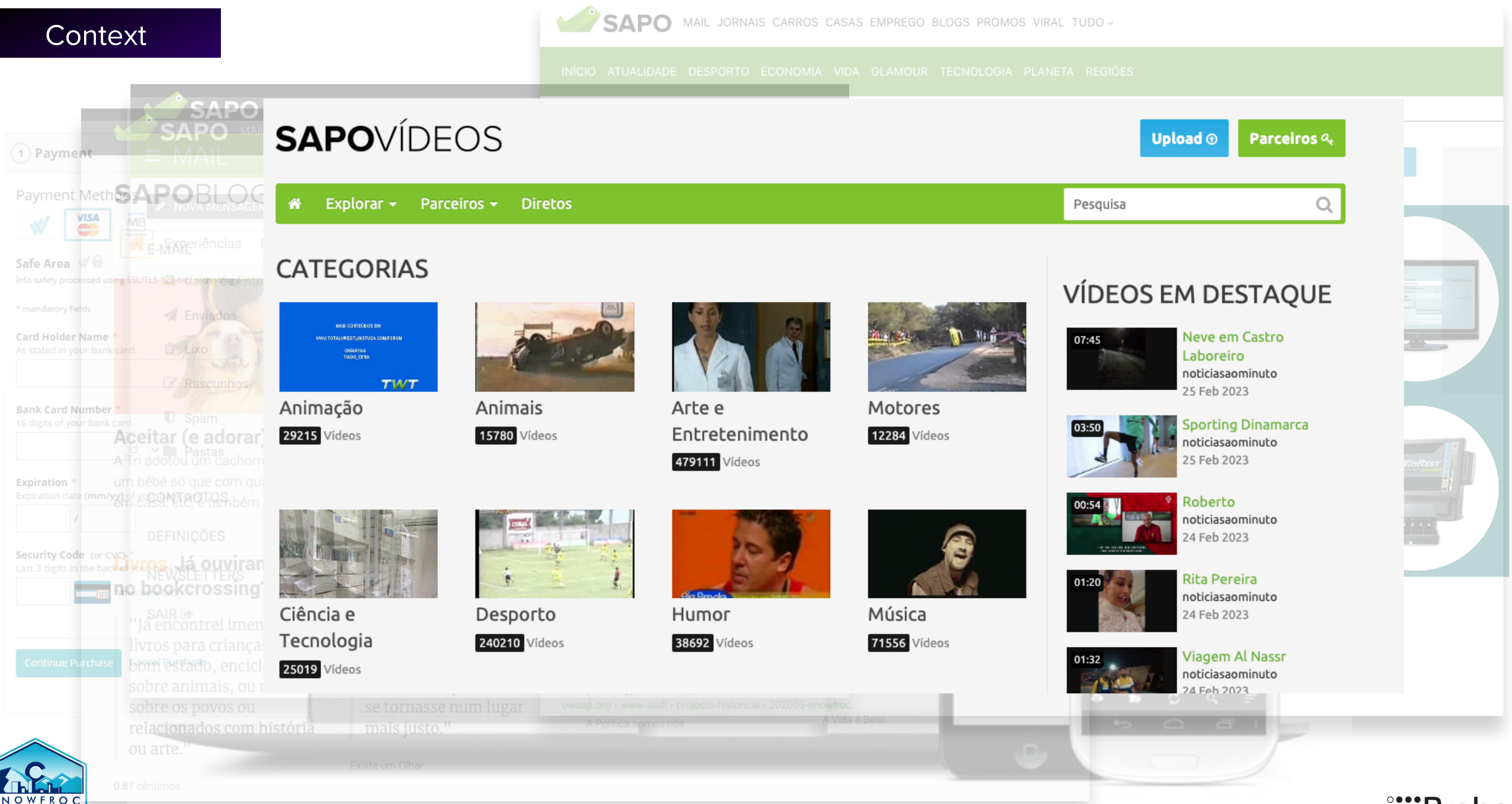
Livro Quantity: 1	
Total	**10,00 €**

SAPO
MAIL JORNAIS CARROS CASAS EMPREGO BLOGS PROMOS VIRAL TUDO
INÍCIO ATUALIDADE DESPORTO ECONOMIA VIDA GLAMOUR TECNOLOGIA PLANETA REGIÕES
Guerra na Ucrânia Greve dos Professores Crise na Habitação Saúde Opinião Podcasts Causas Comuns Vídeos
Pesquisar
Entrar
EN
"A vida é mais forte que o amor. A vida junta e afasta, crua o suficiente para o fazer com quem quer e quando quer."
...ll day long. While billed as "Denver's premier application security conference", SnowFROC's presentations and ...
relacionados com história ou arte."
mais justo."
A Política somos nós
A Vida é Bela!
Existe um Olhar
0,87 cêntimos
Pagamento MEO Wallet
WinRest

Context


SAPO
MAIL JORNAIS CARROS CASAS EMPREGO BLOGS PROMOS VIRAL TUDO
INÍCIO ATUALIDADE DESPORTO ECONOMIA VIDA GLAMOUR TECNOLOGIA PLANETA REGIÕES
1 Payment
Payment Method
Safe Area
Info safely processed using
* mandatory fields
Card Holder Name *
As stated in your bank card
Bank Card Number *
16 digits of your bank card
Expiration *
Expiration date (mm/yy)
Security Code (or CVC)
Last 3 digits in the back of
Continue Purchase
MEO Cloud
TODOS OS FICHEIROS
VER PARTILHAS
CONFIGURAÇÕES
EVENTOS
LOGOUT
Início
UPLOAD PASTAS
UPLOAD FICHEIROS
Selecionar todos
Nova pasta
Ver em lista
Nome
fotografia1.jpg
Fotos
lisboa.jpeg
musica
Welcome kit
Minha Cloud
Applications
Documents
Mobile Photos
Movies
Music
Pictures
Screens
Relevância

Context



Payment Methods

Safe Area

Info safely processed using SSL/TLS 128-bit technology

* mandatory fields

Card Holder Name *
As stated in your bank card.

Bank Card Number *
16 digits of your bank card.

Expiration *
Expiration date (mm/yy) of your bank card.

Security Code (or CVC) *
Last 3 digits in the back of your bank card.

Aceitar (e adorar)
A Tri adotou um cachorro... um bebé só que com qua... em casa, etc, e também...

Livros. Já ouviram ... no bookcrossing?

"Já encontrei imen... livros para crianças... bom estado, encicl... sobre animais, ou l... sobre os povos ou relacionados com história ou arte."

se tornasse num lugar mais justo."

CATEGORIAS

Animação 29215 Vídeos	Animais 15780 Vídeos	Arte e Entretenimento 479111 Vídeos	Motores 12284 Vídeos
Ciência e Tecnologia 25019 Vídeos	Desporto 240210 Vídeos	Humor 38692 Vídeos	Música 71556 Vídeos

VÍDEOS EM DESTAQUE

07:45	Neve em Castro Laboreiro	noticiasaominuto	25 Feb 2023
03:50	Sporting Dinamarca	noticiasaominuto	25 Feb 2023
00:54	Roberto	noticiasaominuto	24 Feb 2023
01:20	Rita Pereira	noticiasaominuto	24 Feb 2023
01:32	Viagem Al Nassr	noticiasaominuto	24 Feb 2023

owasp.org › www-staff › projects-historical › 202003-snowfroc

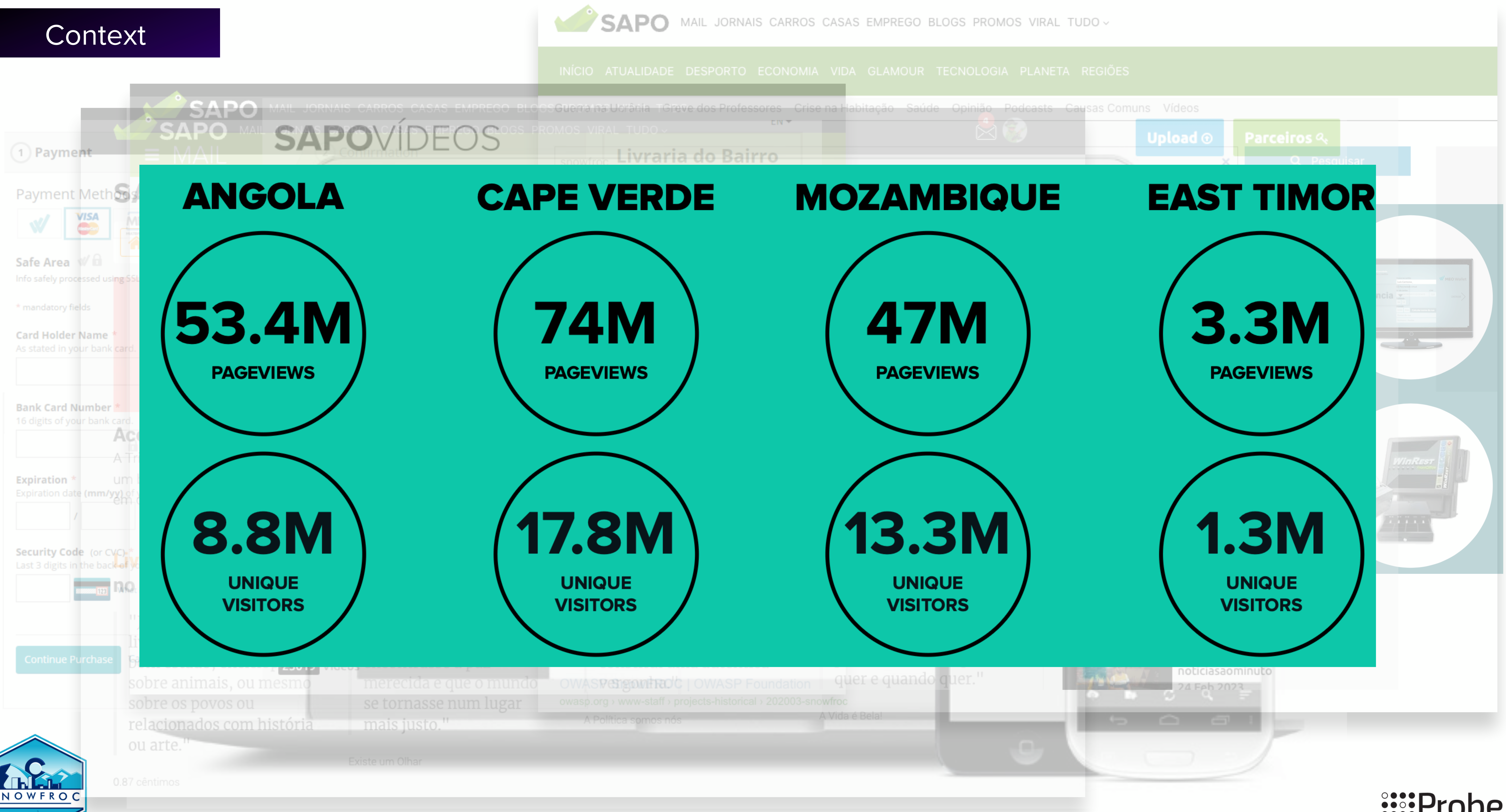
A Política somos nós

A Vida é Bela!

Existe um Olhar

0.87 cêntimos

Context

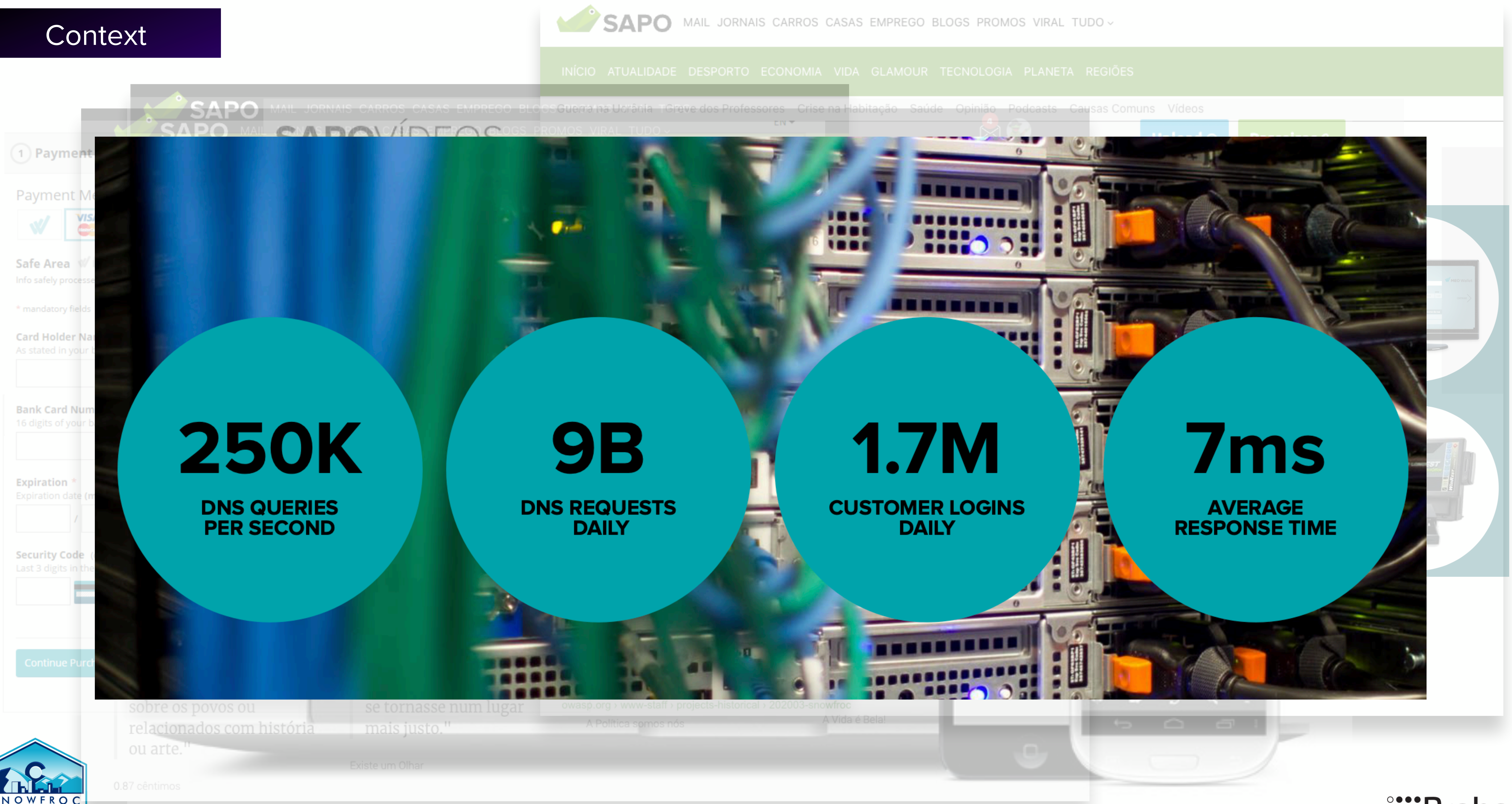

SAPO
MAIL JORNAIS CARROS CASAS EMPREGO BLOGS PROMOS VIRAL TUDO
INÍCIO ATUALIDADE DESPORTO ECONOMIA VIDA GLAMOUR TECNOLOGIA PLANETA REGIÕES
SAPO VÍDEOS
Upload
Parceiros
Payment
Continue Purchase

ANGOLA	CAPE VERDE	MOZAMBIQUE	EAST TIMOR
53.4M PAGEVIEWS	74M PAGEVIEWS	47M PAGEVIEWS	3.3M PAGEVIEWS
8.8M UNIQUE VISITORS	17.8M UNIQUE VISITORS	13.3M UNIQUE VISITORS	1.3M UNIQUE VISITORS

SNOWFROC

Probely

Context


SAPO
MAIL JORNAIS CARROS CASAS EMPREGO BLOGS PROMOS VIRAL TUDO
INÍCIO ATUALIDADE DESPORTO ECONOMIA VIDA GLAMOUR TECNOLOGIA PLANETA REGIÕES
Guerra na Ucrânia Greve dos Professores Crise na Habitação Saúde Opinião Podcasts Causas Comuns Vídeos
SAPO VÍDEOS
Payment
Payment M
Safe Area
Card Holder Na
Bank Card Num
Expiration
Security Code
Continue Purc

250K
DNS QUERIES PER SECOND

9B
DNS REQUESTS DAILY

1.7M
CUSTOMER LOGINS DAILY

7ms
AVERAGE RESPONSE TIME

Context

500M
pageviews

5.3M
users in Portugal

1400
servers

350
employees

200
in engineering

- 300 applications
  - web/mobile, responsive, native iOS/Android/Windows
  - set top boxes, LG/Samsung TV apps
  - OS X/Windows/Linux desktop apps
  - payment terminals

Why a security team?

Why

- Protect the company
- Protect the brand
- Protect customers (data)
- Follow legal and contractual requirements
- Avoid fines

Why

- Protect the company
- Protect the brand
- Protect customers (data)
- Follow legal and contractual requirements
- Avoid fines

<insert headlines of companies being attacked, leaked, fined>

Team objectives

Team objectives

Most app sec teams have common set of objectives

Ours were clear

- Educate technical, product, sales, and management teams in security and guide them through best practices
- Audit all applications
- Prevent emerging threats

Team objectives

Most app sec teams have common set of objectives

Ours were clear

- Educate technical, product, sales, and management teams in security and guide them through best practices
- Audit all applications
- Prevent emerging threats
- Handle incident response
- Ensure compliance

Building an AppSec team - Day 0

Day 0

- Be humble
- Listen
- Understand

Day 0

I'M A
CYBER SECURITY
SPECIALIST
TO SAVE TIME LET'S
JUST ASSUME I'M
ALWAYS RIGHT

DON'T ARGUE
with the
CYBER SECURITY
SPECIALIST

Day 0

- Be humble
- Listen
- Understand
- Do not try to immediately fix stuff

Day 0

Meet the teams

- What do you do?
- How do you do it?
  - people, processes, and tools
- What concerns you?
- Are there any obvious security issues?

- Let them know you are here to help

First processes

- Focus on new applications first
  - easier to influence, to fix
  - mandatory pentest before publication
  - publication requires an OK from the security team

  - Piggyback on the QA and UX teams

First processes

- Mandatory training
  - 4/5h sessions, small groups of 10/15
  - 1st developers, 2nd other tech roles, 3rd non tech roles
  - targeted at the audience

- 2 objectives

Awareness & How to Write Secure Code

Training Table of Contents (part of)

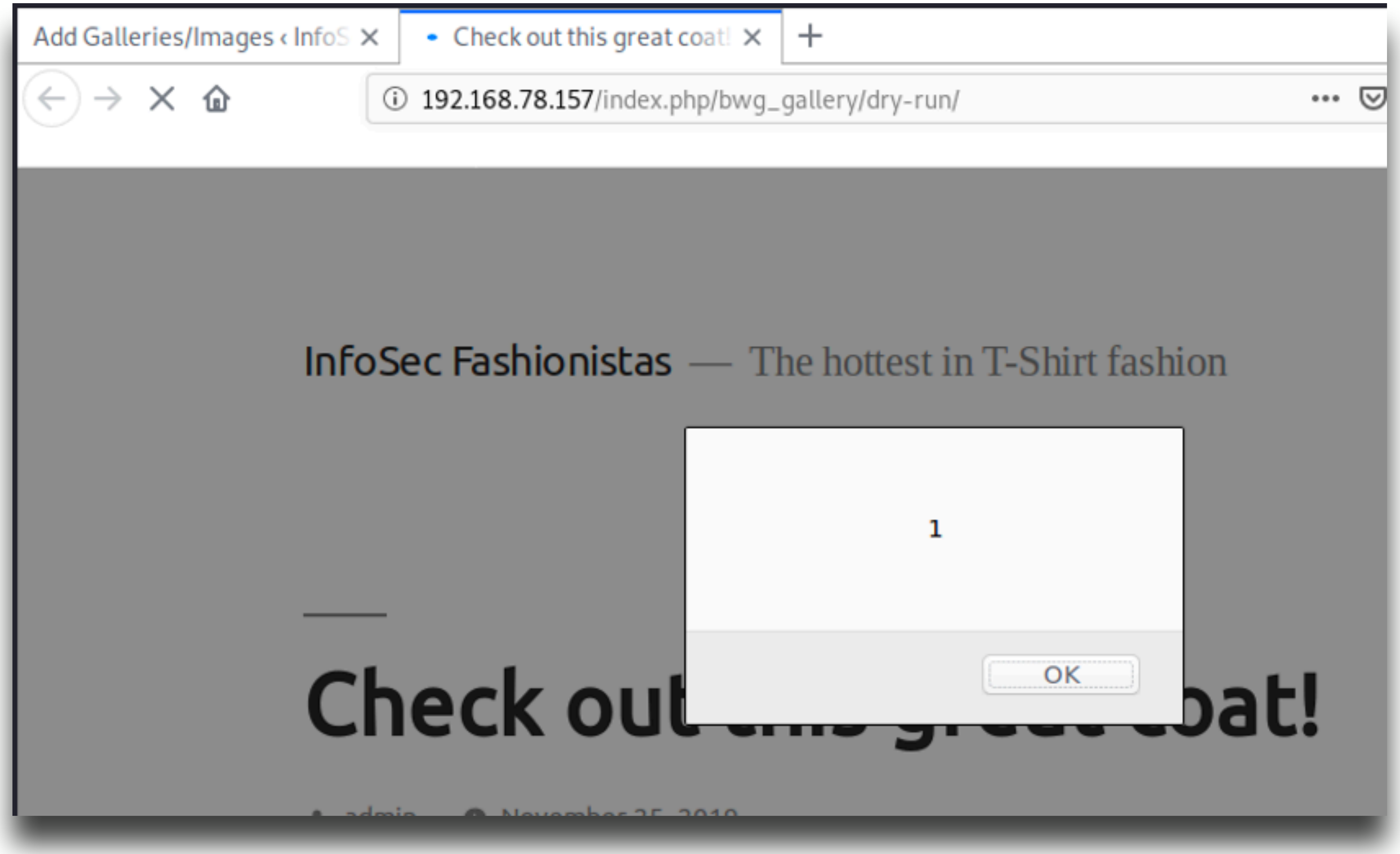
- OWASP Top10 Application Security Risks
- General Principles
- Error Handling and Logging
- Cryptography
- Authentication & Session Management
- Anti-Abuse
- Open Redirects
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- SQL Injections
- File Handling

First processes

- Mandatory training
  - **Focus on the impact, ease of exploitation, and using our own vulns**
    - PoC all the things

    - CSRF -> switched private profile to public
    - SQLi -> dumped the DB with sqlmap
    - XSS -> injected a malicious login form

Day 0



Add Galleries/Images ‹ InfoS
Check out this great coat!
192.168.78.157/index.php/bwg_gallery/dry-run/

InfoSec Fashionistas — The hottest in T-Shirt fashion

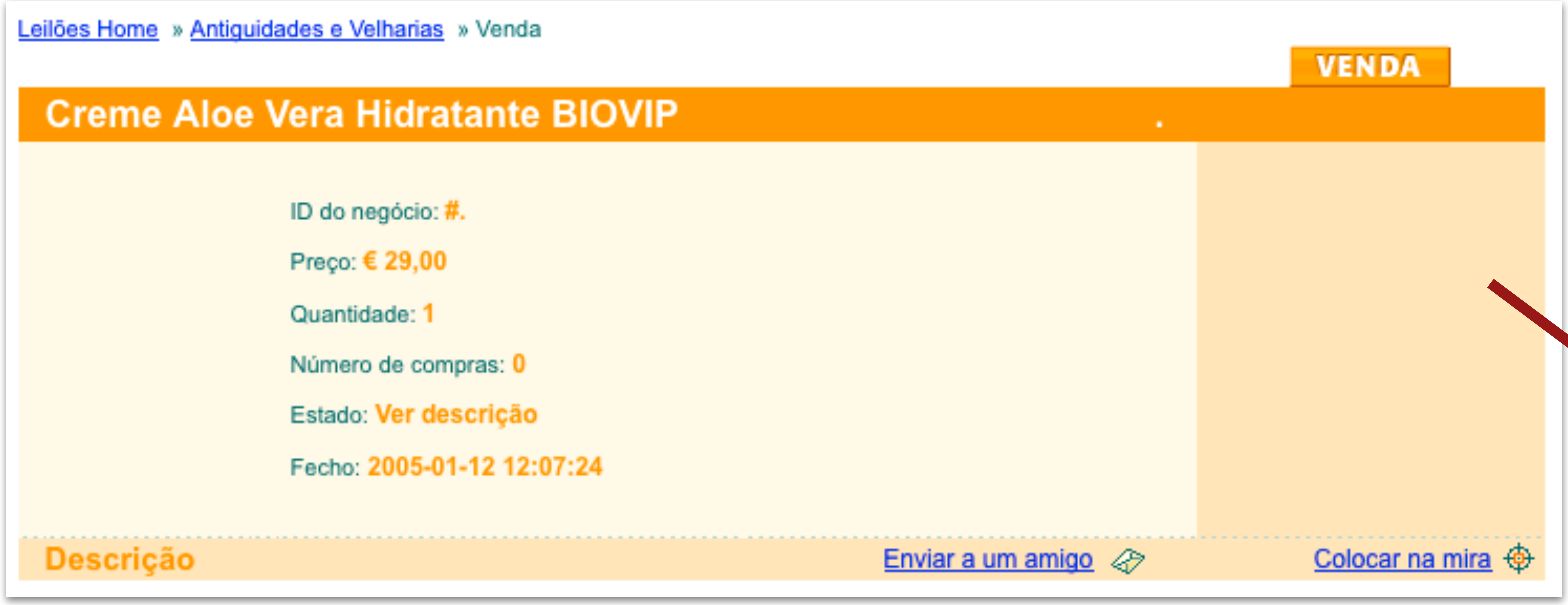
1

OK

Check out this great coat!

admin November 25, 2019

Day 0



Leilões Home » Antiguidades e Velharias » Venda

VENDA

Creme Aloe Vera Hidratante BIOVIP .

ID do negócio: #.

Preço: € 29,00

Quantidade: 1

Número de compras: 0

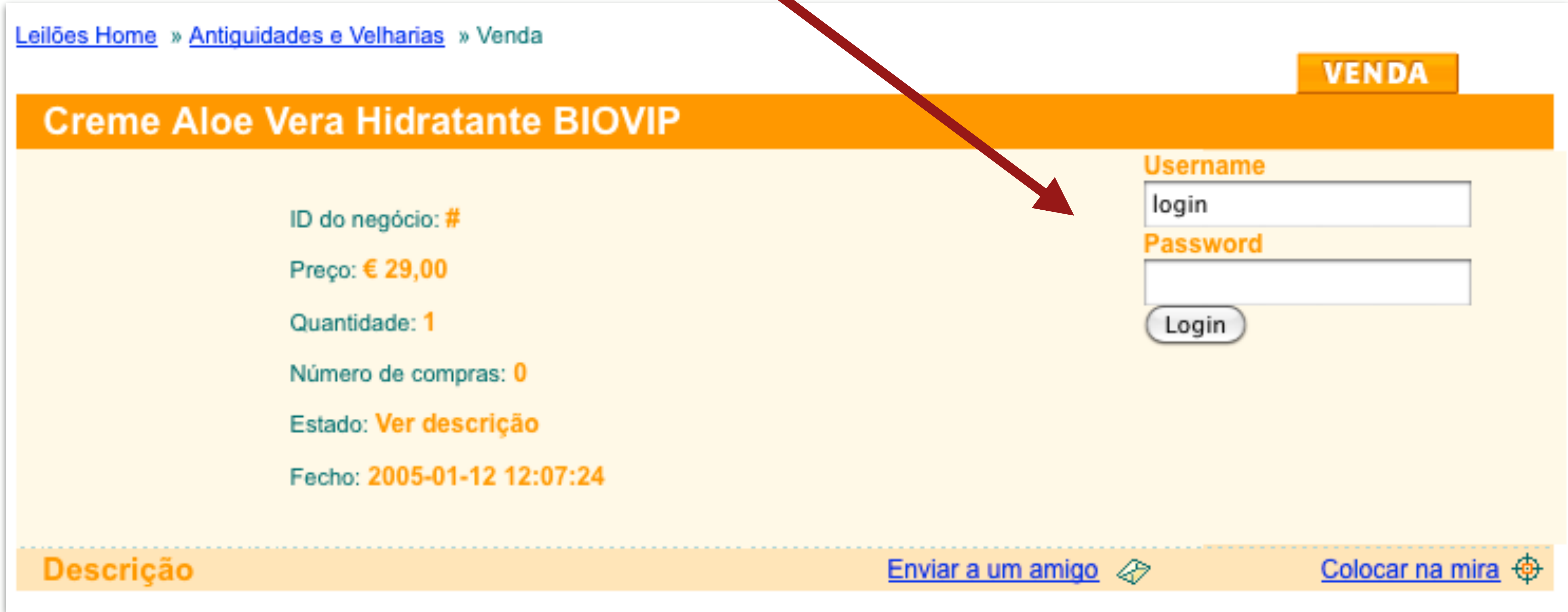
Estado: Ver descrição

Fecho: 2005-01-12 12:07:24

Descrição

Enviar a um amigo

Colocar na mira



Leilões Home » Antiguidades e Velharias » Venda

VENDA

Creme Aloe Vera Hidratante BIOVIP

Username: login

Password:

Login

ID do negócio: #

Preço: € 29,00

Quantidade: 1

Número de compras: 0

Estado: Ver descrição

Fecho: 2005-01-12 12:07:24

Descrição

Enviar a um amigo

Colocar na mira

First processes - summary

- Know the *status quo*
- Focus on new applications first
- Require approval for new applications
- Piggyback on existing teams/processes (QA/UX)
- Mandatory training

Going deeper

Eventually we increased our reach, and you should too

- Mobile and embedded apps
- Involvement in the project planning phase
- Infrastructure
- Legacy

Mobile and embedded apps

- Very time consuming to test
  - platform specific vulnerabilities (e.g. credential store, isolation)
  - good coverage might require using a remote
  - usually less documented API
  - fragile
- Requires specific knowledge

Mobile and embedded apps

- Very time consuming to test
  - platform specific vulnerabilities (e.g. credential store, isolation)
  - good coverage might require using a remote
  - usually less documented API
  - fragile
- Requires specific knowledge

Deeper

Involvement in the project planning phase

- Create really good relationships with the product teams
- Presence in product meetings
- Make it official

Involvement in the project planning phase

- Create really good relationships with the product teams
- Presence in product meetings
- Make it official

- Success: product managers/owners queueing to talk with us

Deeper

Infrastructure

- Security Champions
  - someone from the infrastructure team
  - hands on, pragmatic and with a security conscious
  - still a member of the infra team, but present in the security team daily life

Legacy

- Really challenging
- Requires a clear identification of the problems
- Prioritization, clear solutions, avoid half-measures
- Clearly stated in the infrastructure team roadmap

Legacy

- Really challenging
- Requires a clear identification of the problems
- Prioritization, clear solutions, avoid half-measures
- Clearly stated in the infrastructure team roadmap

Legacy

- Fixing legacy means questioning stuff that was “always done it this way”

Tools

Your basic toolset

- Your own (Virtual) Machine
- A vulnerability management tool (e.g. DefectDojo)
- Your intranet page with contacts, how to’s

Your basic toolset

- Your own (Virtual) Machine
- A vulnerability management tool (e.g. DefectDojo)
- Your intranet page with contacts, how to’s

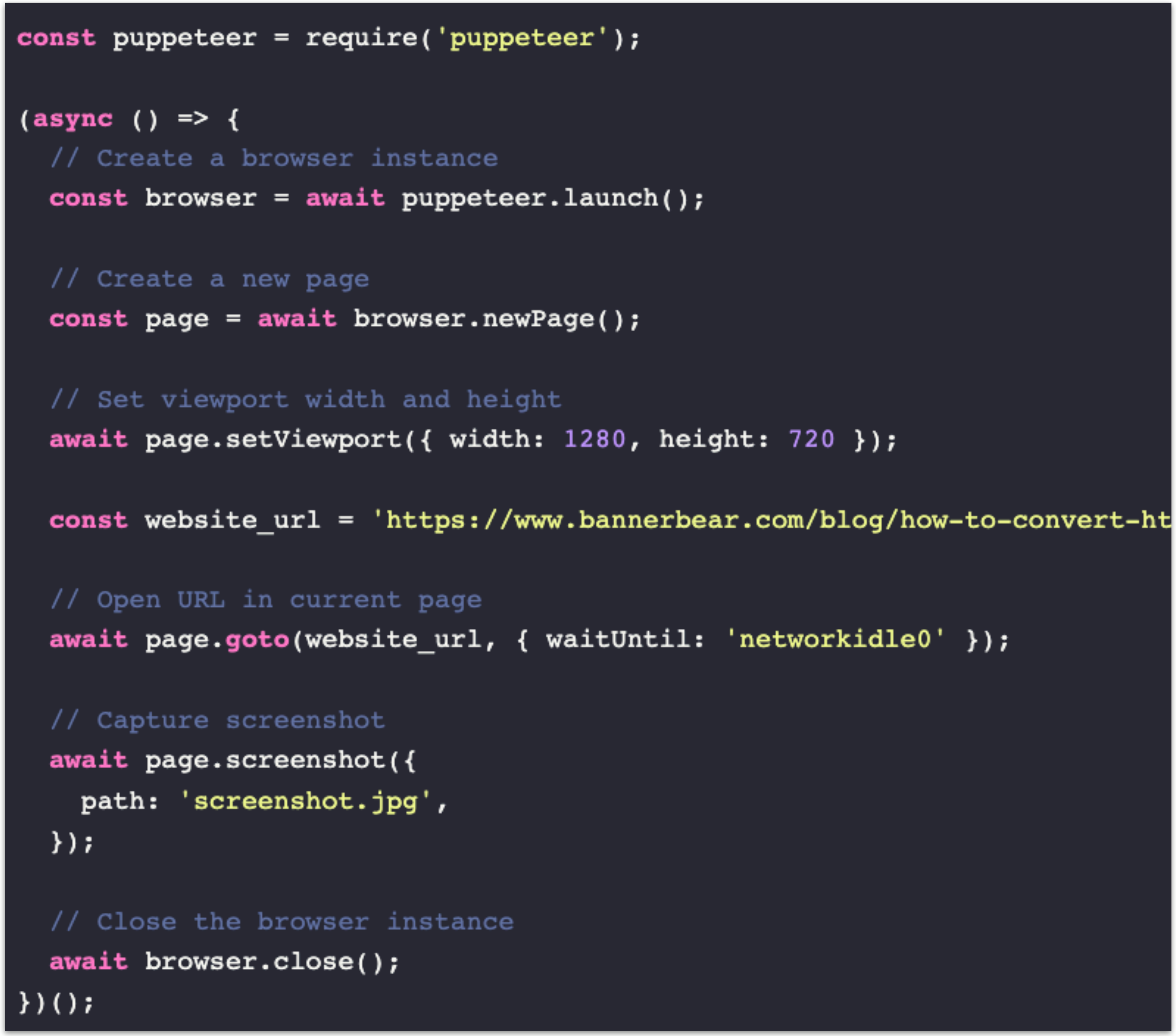
- Start by reporting vulnerabilities **on the teams issue trackers**
  - instead of adding another system to their life

Increase your visibility

- Will make you feel even more outnumbered

- Know your attack surface
  - get eyes on the DNS with post-commit hooks or zone transfer
  - screenshot everything

Tools



```
const puppeteer = require('puppeteer');

(async () => {
  // Create a browser instance
  const browser = await puppeteer.launch();

  // Create a new page
  const page = await browser.newPage();

  // Set viewport width and height
  await page.setViewport({ width: 1280, height: 720 });

  const website_url = 'https://www.bannerbear.com/blog/how-to-convert-ht

  // Open URL in current page
  await page.goto(website_url, { waitUntil: 'networkidle0' });

  // Capture screenshot
  await page.screenshot({
    path: 'screenshot.jpg',
  });

  // Close the browser instance
  await browser.close();
})();
```

Increase your visibility

- Know your attack surface
  - use broad scanner such as Shodan, BinaryEdge, etc
  - follow the company social networks

Increase your visibility

- Know your attack surface
  - scan everything all the time
  - but slowly
    - low requests/second
    - only GET
    - unauthenticated
    - only one vulnerability type, e.g. SQLi

Increase your visibility

- Know your attack surface
  - scan everything all the time
  - but slowly
    - low requests/second
    - only GET
    - unauthenticated
    - only one vulnerability type, e.g. SQLi

Team

First hires

- While the team is small, experience is a requirement
  - pentester(s)
    - good soft skills and ability to evaluate risk
    - ensures your team is not a bottleneck
  - developer
    - backend profile
    - automate scans, integrate with issue trackers

First hires

- Give you pentesters a break from pen testing
  - time to automate
  - time to try tools
  - to investigate targets or weird vulnerabilities
  - follow white rabbits

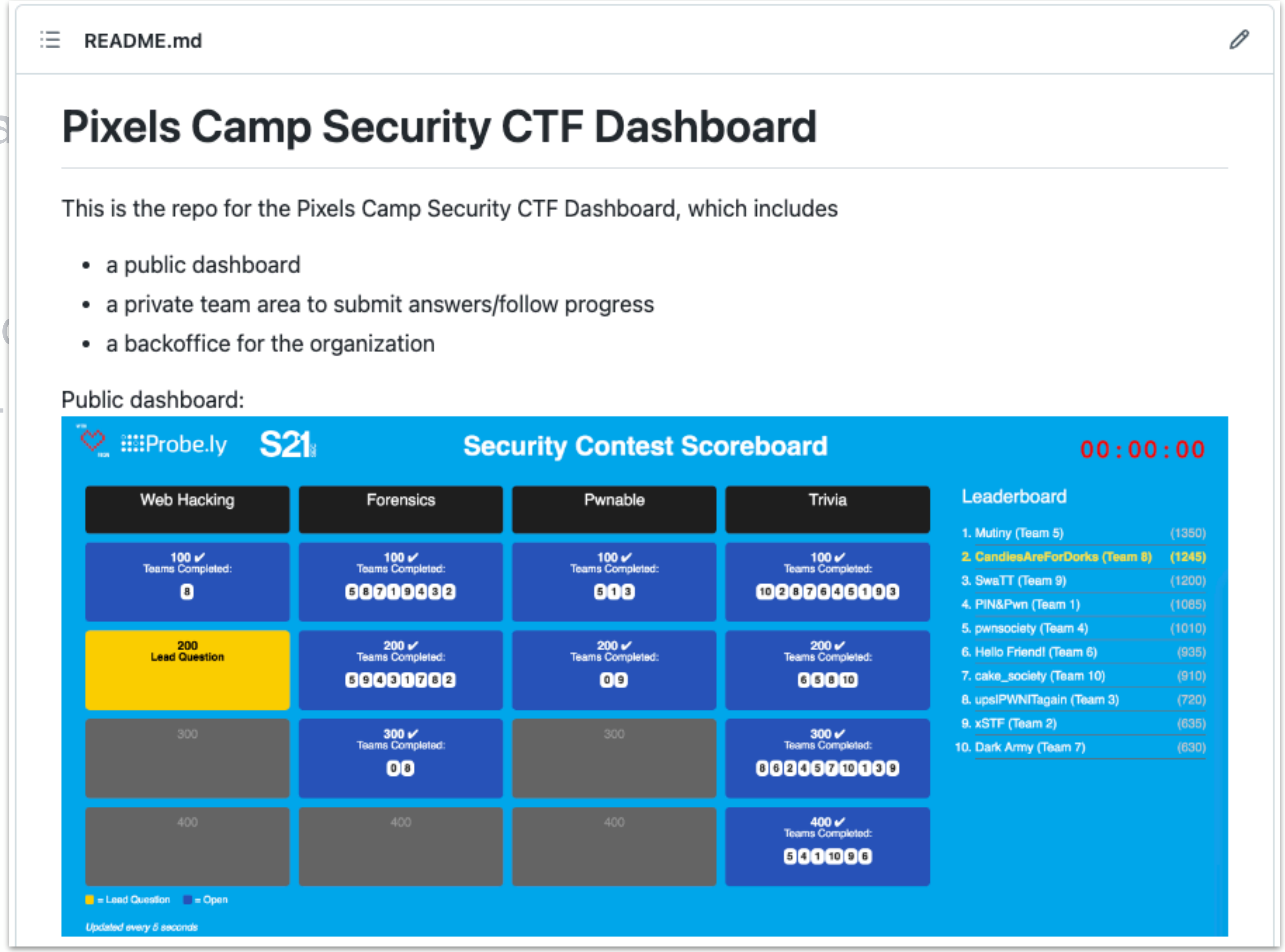
Growing the team

- An expected source of candidates: CTFs
  - Capture The Flag security competition

Team

Growing the tea

- An expecte
  - Capture T



README.md

Pixels Camp Security CTF Dashboard

This is the repo for the Pixels Camp Security CTF Dashboard, which includes

- a public dashboard
- a private team area to submit answers/follow progress
- a backoffice for the organization

Public dashboard:

Security Contest Scoreboard

00:00:00

Web Hacking	Forensics	Pwnable	Trivia
100 ✓ Teams Completed: 8	100 ✓ Teams Completed: 5 8 7 1 9 4 3 2	100 ✓ Teams Completed: 5 1 3	100 ✓ Teams Completed: 10 2 8 7 6 4 5 1 9 3
200 Lead Question	200 ✓ Teams Completed: 5 9 4 3 1 7 8 2	200 ✓ Teams Completed: 0 9	200 ✓ Teams Completed: 6 5 8 10
300	300 ✓ Teams Completed: 0 8	300	300 ✓ Teams Completed: 8 6 2 4 5 7 10 1 3 9
400	400	400	400 ✓ Teams Completed: 5 4 1 10 9 6

🟨 = Lead Question 🟦 = Open

Updated every 5 seconds

Leaderboard

1. Mutiny (Team 5)	(1350)
2. CandiesAreForDorks (Team 8)	(1245)
3. SwaTT (Team 9)	(1200)
4. PIN&Pwn (Team 1)	(1085)
5. pwnsociety (Team 4)	(1010)
6. Hello Friend! (Team 6)	(935)
7. cake_society (Team 10)	(910)
8. upsIPWNITagain (Team 3)	(720)
9. xSTF (Team 2)	(635)
10. Dark Army (Team 7)	(630)

Growing the team

- Security Champions
  - identify people that like security
  - pragmatic
  - respected by their teams

- Eventually some moved to our team

Team

Areas of expertise / roles

- Network
- Infrastructure
- Compliance
- Development
- IDP / SSO

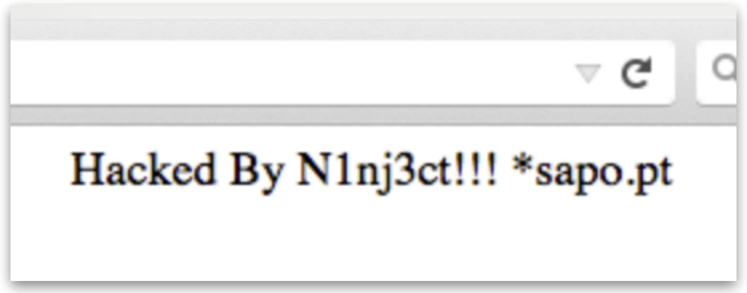
Having fun

Fun

Eventually you will get hacked.

Fun

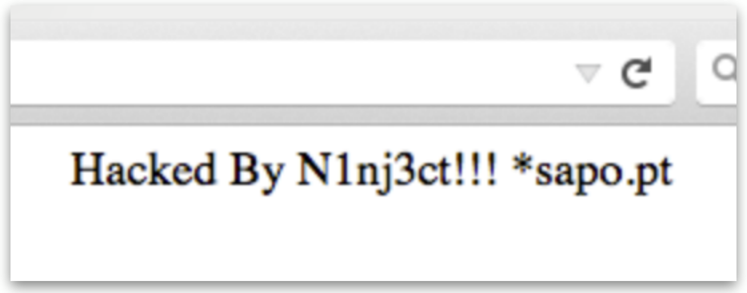
Eventually you will get hacked.



Hacked By N1nj3ct!!! *sapo.pt

Fun

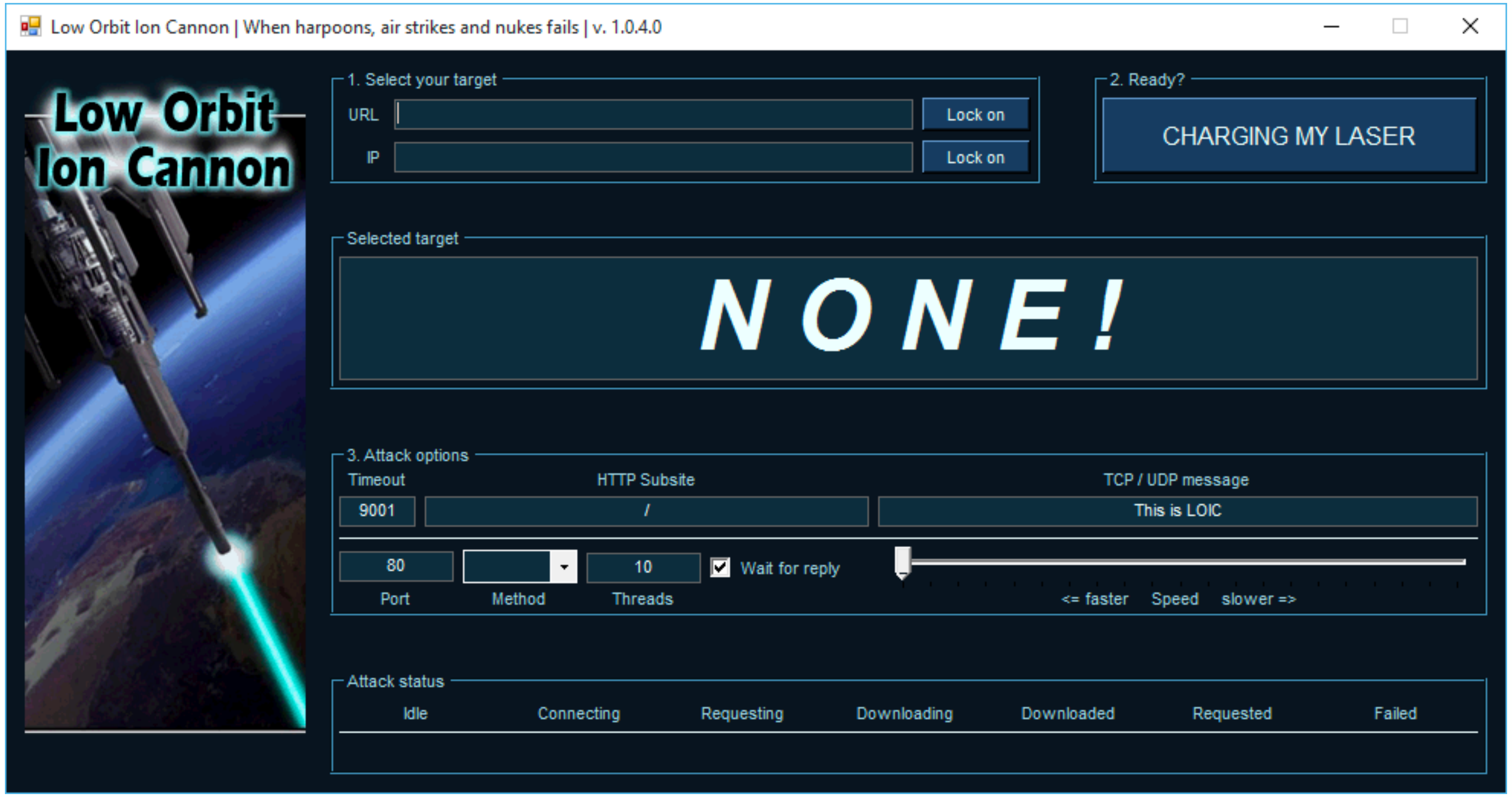
Eventually you will get hacked.



Hacked By N1nj3ct!!! *sapo.pt

```
Linux playground 5.15.0-56-generic #62-Ubuntu SMP Tue Nov 22 19:54:14 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
```

Fun



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.4.0

1. Select your target

URL | Lock on

IP | Lock on

2. Ready?

CHARGING MY LASER

Selected target

N O N E !

3. Attack options

Timeout: 9001

HTTP Subsite: /

TCP / UDP message: This is LOIC

Port: 80

Method:

Threads: 10

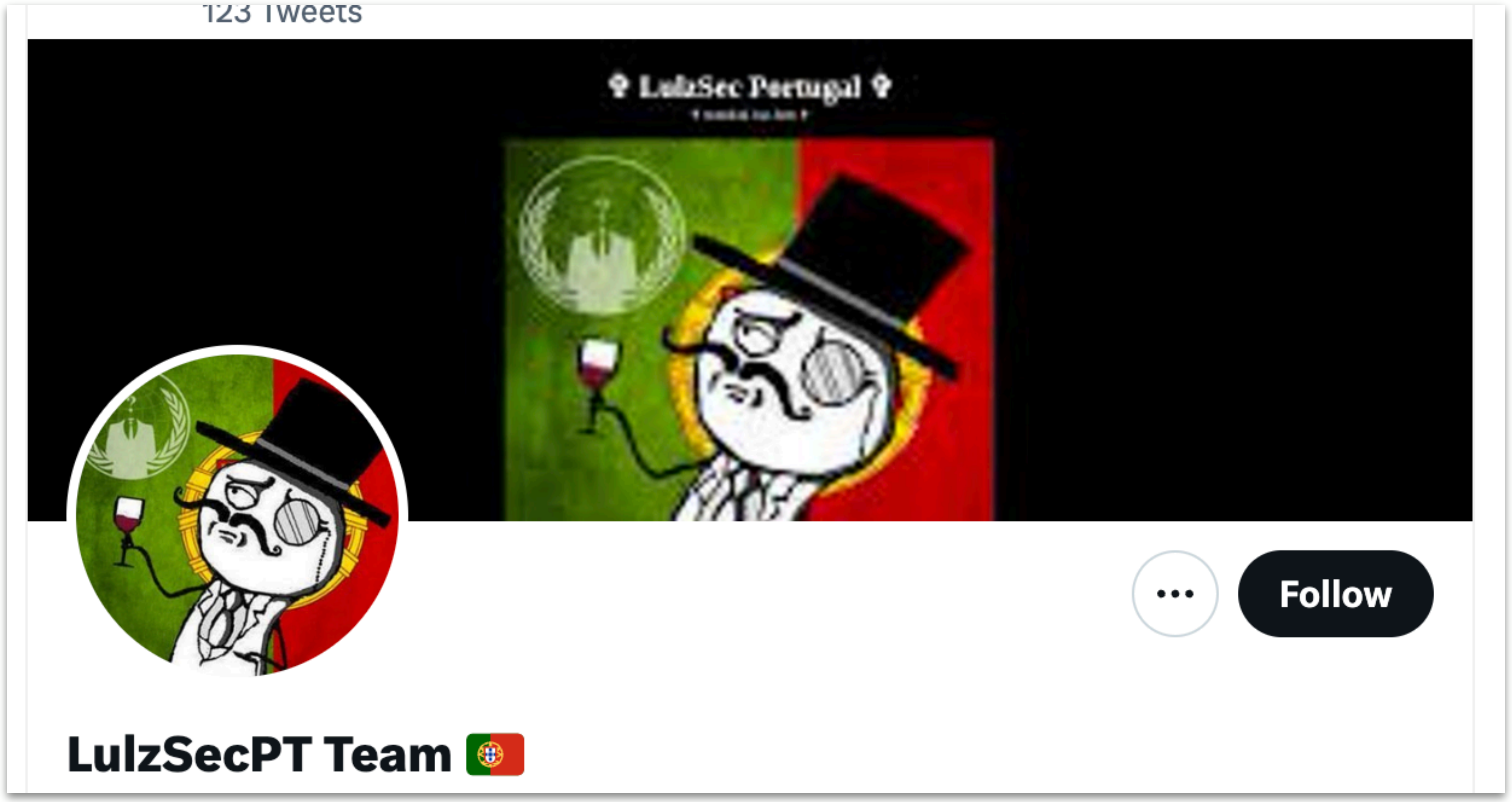
☑ Wait for reply

<= faster Speed slower =>

Attack status

Idle Connecting Requesting Downloading Downloaded Requested Failed

Fun



123 Tweets

LulzSecPT Team 🇵🇹

Eventually you will get hacked.

- Be prepared. Easier said than done
  - identify a few attack scenarios
  - define what to do when the attack is detected
  - define what to do after

We could have been better prepared

- Kick or talk to the attacker?
- Takedown attack vector, i.e. the vulnerable application?
- Reinstall the application, the whole server?

Active monitoring

- pastebin keyword monitoring
- Twitter / Facebook / IRC

Fun

As the team succeeds, the fun increases

- card cloning
- usb drops
- phishing emails

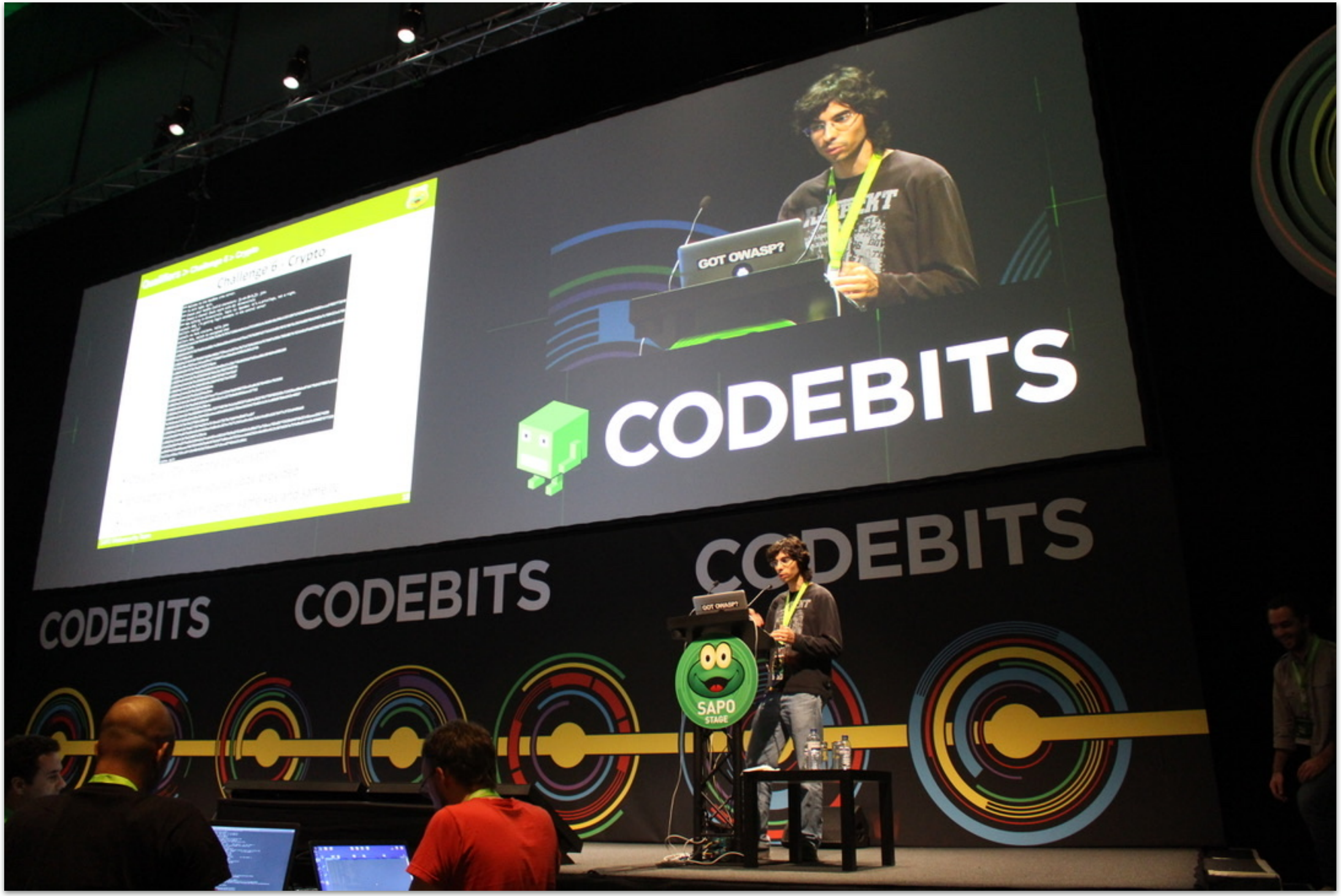
Community

Giving back to the community == more awareness

- “Internal” technical sessions (e.g. TLS, SQLi, Password management)
- Present at community meetups and events
- Support meetups (venue, recording, streaming)
- Organize CTFs

- Eventually led to the OWASP chapter rebirth

Community



Community

Community

STAGE 4
PIXELS
Camp

WORKSHOPS
PIXELS
Camp
brpx Bright Pixel
WORKSHOPS

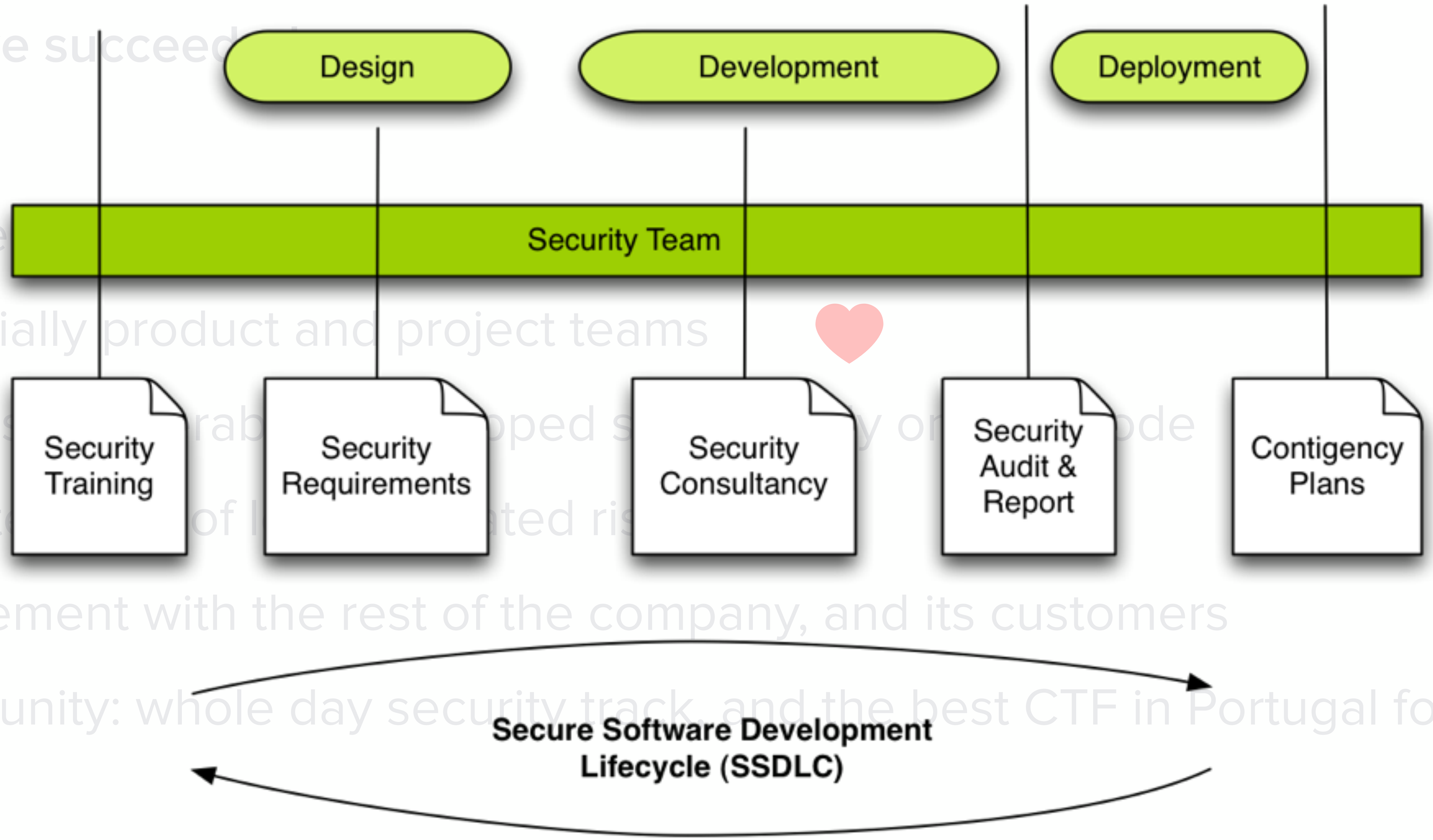
Conclusions

Conclusions

I believe we succeeded

- People would come to us at project planning & design phase
    - specially product and project teams ❤️
- High-risk vulnerabilities dropped significantly on new code
- Mitigated a lot of legacy related risks
- Involvement with the rest of the company, and its customers
- Community: whole day security track, and the best CTF in Portugal for 10 years

Conclusions



I believe we succeed

- People
  - specially product and project teams
- High-ris rab oped s y or ode
- Mitigat of l ated ris
- Involvement with the rest of the company, and its customers
- Community: whole day security track, and the best CTF in Portugal for 10 years

Conclusions

I believe we succeeded

- People would come to us at project planning & design phase
  - specially product and project teams ❤
- High-risk vulnerabilities dropped significantly on new code
- Mitigated a lot of legacy related risks
- Involvement with the rest of the company, and its customers
- Community: whole day security track, and the best CTF in Portugal for 10 years

Conclusions

Times are harder

- More awareness, more demand for your team
- More regulation, higher risk of fines
- More visibility and peer pressure (security ratings, headlines, public disclosures)

- Use these on your favor

Conclusions

General guidance

- Training: use real vulnerabilities, real attacks, real consequences
- Piggyback on QA teams
- Listen, understand the teams, processes, and business
- Weigh risks
- **Management empowerment**

Questions?

Tiago Mendo
mendo@probely.com