UNIVERSITAT DE BARCELONA

Treball de Fi de Grau

GRAU D'ENGINYERIA INFORMÀTICA

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

PLATAFORMES DE SIMULACIÓ D'ATACS DE PHISHING

Abdelkarim Azzouguagh Ouniri

Director: Raül Roca Cànovas
Realitzat a: Departament de
Matemàtiques i Informàtica

Barcelona, 20 de juny de 2021

Resum

Avui dia, no és cap notícia que, tant usuaris com empreses, rebem gran quantitat de correus electrònics diàriament amb promocions, propagandes, informació de subscripcions... Aquest fet ha provocat que els ciberdelinqüents s'interessin per aquest medi com a porta d'entrada per a llançar els seus atacs a les víctimes.

Això també ha provocat un augment del 33% dels ciberatacs, segons un informe publicat per l'empresa Atlas VPN (1), on es comentat que aquest augment ha demostrat que moltes empreses o administracions governamentals no estan preparades per a gestionar amenaces de ciberseguretat i que cada cop més gent cau víctima dels ciberdelinqüents.

Per aquest motiu, en aquest Treball de Final de Grau té com a objectiu tractar una de les metodologies d'atacs més comunes, el Phishing, creant una plataforma capaç de crear i llançar campanyes d'atacs de phishing per tal de prova la seguretat que prenen els usuaris en rebre un correu electrònic, que en un principi sembla innocent.

Resumen

Hoy en día, no es ninguna noticia que, tanto usuarios como empresa, recibimos una gran cantidad de correos electrónicos diariamente con promociones, propagandas, información de suscripciones... Este hecho ha provocado que los ciberdelincuentes se interesen por este medio como Puerta de entrada para lanzar sus ataques a las víctimas.

Esto también ha provocado un aumento del 33% de ciberataques, según un informe publicado por la empresa AtlasVPN (1), donde se comenta que este aumento ha demostrado que muchas empresa o administraciones gubernamentales no están preparadas para gestionar amenazas de ciberseguridad y que cada vez, más gente cae víctima de los ciberdelincuentes.

Por este motivo, este Trabajo de Final de Grado, tiene como objetivo tratar una de las metodologías de ataques más comunes, el Phishing, creado una plataforma capaz de crear y lanzar campañas de ataques de phishing con la finalidad de probar la seguridad que toman los usuarios al recibir un correo electrónico, que en un principio es inofensivo.

Abstract

Nowadays, it is no news that both users and companies receive many e-mails every day with promotions, advertisements, subscription information... This fact has led cybercriminals to becoming interested in this medium as a gateway to launch their attacks on victims.

This has also led to a 33% increase in cyberattacks, according to a report published by the company AtlasVPN (1), which commented that this increase has shown that many companies or governmental administrations are not prepared to manage cybersecurity threats and that mor and more people are falling victims to cybercriminals.

For this reason, this Final Degree Project aims to address one of the most common attack methodologies, Phishing, by creating a platform capable of creating and launching phishing attack campaigns in order to test the security that users take when they receive an email, which at first seems harmless.

Índex

1. Introducció i motivació

Avui en dia internet està present en quasi totes les activitats diàries de les persones, cosa que ha suposat un gran avanç per a la societat. No obstant això, també ha portat els seus inconvenients, com es la ciberdelinqüència i els ciberatacs. Una de les metodologies de ciberatacs més freqüents al llarg de la història són els de Phishing [9.1].

El primer cop que es va sentir a parlar sobre el Phishing va ser en 1987 en una conferència, on Jerry Felix i Chris Hauck van fer referència a aquest terme a causa d'un document titulat "Sistema de Seguridad: La perspectiva del Hacker", on es comentava la possibilitat que una persona es fes passar per una entitat o organisme de confiança. Però no es fins al gener de 1996, a la companyia AOL, una empresa proveïdora de serveis d'internet amb seu a Nova York, on es fa servir aquest terme oficialment. El fet que milions de persones es connectessin a aquesta xarxa, a causa de la seva popularitat en aquells moments, va cridar l'atenció dels atacants, els quals ho van aprofitar fent-se passar per empleats d'aquesta empresa per a enganyar a víctimes potencials. Aquest va ser el començament dels atacs de phishing, Abans de l'any 1995 era molt senzilla l'obertura d'un compte en la companya AOL mitjançant algoritmes que generaven números de compte totalment aleatoris i falsos. Això va portar com a conseqüència una gran pèrdua econòmica per a AOL. L'empresa en adonar-se d'aquesta situació, va prendre mesures dràstiques, arribant a crear AOHell una eina per a la lluita contra aquest tipus d'estafes.

Segons informa un estudi de la INTERPOL (2), els ciberatacs han augmentat amb la declaració mundial de la pandèmia COVID-19. Això és degut al fet que els ciberdelinqüents, han vist en la pandèmia una oportunitat per augmentar les probabilitats d'èxit, enviant correus electrònics sobre la COVID-19, fent-se passar per autoritats governamentals i sanitàries i incitant a les víctimes a facilitar les seves dades personals.

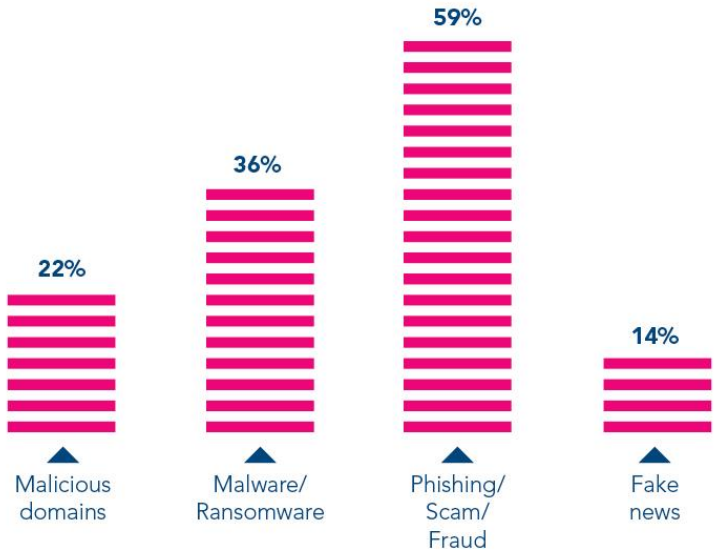


Fig. 1 Proporció de les principals ciberamenaçes relacionades amb la COVID-19, calculades a partir d'informació donada pels països membres de la INTERPOL (Font: INTERPOL)

En el gràfic anterior, Fig. 1, es pot observar els percentatges de les principals ciberamenaçes relacionades amb la COVID-19 i es pot veure com, clarament, un gran nombre de les amenaces son de tipus phishing.

La realització d'aquest treball ha estat motivada per la repercussió que ha tingut el phishing en l'última dècada i el fet que aquests atacs segueixin tenint una gran taxa d'èxit, cosa que fa dubtar de les precaucions que prenen les empreses i els seus empleats. Un altre aspecte que m'ha motivat a tractar aquest tema ha estat la possibilitat d'aplicar els coneixements adquirits en ciberseguretat, posar-me en la pell de l'atacant i crear una web capaç de llançar atacs de phishing però sense el mateix objectiu que els ciberdelinqüents, sinó per a testejar la seguretat de les empreses.

2. Objectius

L'objectiu principal d'aquest treball és crear una web que permeti als responsables de seguretat de les empreses fer una avaluació de les precaucions que prenen els seus empleats, mitjançant campanyes de phishing. Un altre dels principals objectius és aplicar els coneixements adquirits durant el grau.

Aquests objectius es podrien englobar en els següents:

- Dissenyar la web esmentada, la qual l'he anomenat PHSHNG.
- Fer que aquesta web sigui el més responsive [9.1] possible perquè es pugui accedir a ella des de qualsevol dispositiu.
- Aplicar metodologies Agile en la planificació i desenvolupament de la web.
- Aplicar les tecnologies apreses durant el grau.

2.1 Planificació

Per a planificar d'aquest treball, s'ha seguit un procés molt semblant a Scrum, un tipus de metodologia Agile.

Scrum és un model basat en un sistema de desenvolupament per iteracions en el que es pretén maximitzar la productivitat de les hores dedicades a un projecte, basat en la comunicació constant entre els integrants d'un equip. Donat que aquest projecte es fa individualment, s'ha fet servir Scrum només per la part de planificar i organitzar les hores de treball, sense tenir en compte aspectes com el Daily Scrum, Burdown Chart o els diferents rols que es fan servir en aquesta metodologia. [9.1]

Una de les primeres coses que es va fer, va ser establir un seguit d'històries d'usuari amb les diferents funcionalitats que havia de tenir la web a desenvolupar, i afegir-les a un Product Backlog [9.1] (3). En la taula de la figura, Fig. 2, es poden observar aquestes històries d'usuari.

User story	Descripció
US-1	Com a usuari, vull fer el log-in per a poder accedir al meu compte.
US-2	Com a usuari, vull fer log-out per sortir del meu compte.
US-3	Com a usuari no registrar, vull registrar-me a la web per a tenir un compte.
US-4	Com a usuari, vull afegir una empresa per a poder crear una campanya amb aquesta.
US-5	Com a usuari, vull eliminar una empresa per deixar de tenir-la en el meu compte.
US-6	Com a usuari, vull afegir empleats per a poder crear una campanya amb aquests.
US-7	Com a usuari, vull eliminar els empleats de "x" empresa per deixar de tenir-los en el meu compte.
US-8	Com a usuari, vull afegir una campanya per a poder llançar-la.
US-9	Com a usuari, vull eliminar una campanya per a deixar de tenir-la en el meu compte.
US-10	Com a usuari, vull afegir una plantilla de correu per tal d'enviar correus mitjançant d'aquest.
US-11	Com a usuari, vull eliminar una plantilla de correu per a deixar de tenir-lo en el meu compte.
US-12	Com a usuari, vull veure la llista de campanyes per tal de saber quines tinc registrades.
US-13	Com a usuari, vull veure la llista d'empreses per tal de saber quines tinc registrades.
US-14	Com a usuari, vull veure la llista de plantilles de correu per al de saber quins tinc registrats.
US-15	Com a usuari, vull veure les estadístiques d'una campanya per a saber quins empleats han caigut en ella.
US-16	Com a usuari, vull poder canviar la meva contrasenya per tal de assegurar millor el meu compte.
US-17	Com a usuari, vull veure les estadístiques d'una empresa per a saber quins empleats han caigut en alguna campanya.
US-18	Com a usuari, vull llaçar una campanya per tal de comprovar la seguretat dels meus empleats.
US-19	Com a usuari, vull poder veure el meu perfil.
US-20	Com a usuari, tant registrat com no, vull poder acceptar o rebutjar les cookies.
US-21	Com a usuari, vull veure els detalls de les meves campanyes per tal de saber com han estat configurades.
US-22	Com a usuari, vull veure els detalls de les meves empreses per tal de saber com han estat configurades.
US-23	Com a usuari, vull poder descarregar la llista d'empreses registrades en el meu compte
US-24	Com a usuari administrador, vull veure els comptes que registrats en la web, per tal de tenir un registre d'aquests.
US-25	Com a usuari administrador, vull poder eliminar un compte en el cas de que es produeixi un mal us de la web.
US-26	Com a usuari, vull eliminar el meu compte per tal de deixar d'estar en el registre de la web.

Fig. 2 Fragment figura A1, històries d'usuari amb les diferents funcionalitats de la web (Font: Pròpia)

Un cop establertes aquestes històries d'usuari i una certa prioritat per a cada una d'aquestes(Story Points [9.1]), el que es va fer va ser distribuir-les entre els diferents Sprints en el que s'ha dividit el projecte. Un Sprint és un període de temps que oscil·la entre dues setmanes i un més, amb l'objectiu d'aconseguir un increment de valor en el producte final.

En el meu cas, els Sprint s'ha distribuït en períodes de 2 setmanes, ja que segons el temps disponible i la complicitat del treball a realitzar vaig pensar que era la millor opció. Es per això que s'han fet un total de 6 Sprints on en cada un d'aquest s'ha realitzat una part del projecte. Donat que en alguns dels Sprints no s'ha aconseguit desenvolupar alguna història d'usuari completament, o simplement, s'ha hagut de fer alguna petita modificació, en la taula de la figura Fig. 3, aquesta apareixerà al llarg de més d'un Sprint, com es el cas de la US-8 US-10, etcètera.

Així doncs, una idea genèrica del que és la principal funcionalitat de la web seria la següent: Dissenyar una web que permeti a l'usuari crear campanyes de phishing per tal de testejar la seguretat de la seva empresa.

User story	Sprint 1	Sprint 2	Sprint 3	Sprint 4	Sprint 5	Sprint 6
US-1						
US-3						
US-4						
US-6						
US-2						
US-8						
US-10						
US-11						
US-12						
US-14						
US-5						
US-7						
US-13						
US-18						
US-21						
US-22						
US-9						
US-15						
US-16						
US-17						
US-19						
US-20						
US-23						
US-24						
US-25						
US-26						

Fig. 3 Diagrama de Gantt amb la distribució de les històries d'usuari, ordenades temporalment, entre els diferents Sprint (Font: Pròpia)

3. Anàlisis

3.1 Anàlisis de competència

Per tal de poder establir els requisits de la web, el que s'ha fet en un principi ha sigut analitzar altres plataformes de simulació d'atacs, ja sigui de phishing com qualsevol antre tipus d'atac. Algunes de les plataformes analitzades han sigut les següents:

- Gophish. (4) És un software de codi obert que permet crear campanyes de correu electrònic de phishing.
- Infection Monkey: (5) Es tracta d'una eina de simulació de violació i atacs, de codi obert que permet avaluar la seguretat en la xarxa, ja sigui pública com privada.
- CALDERA: (6) És un sistema automatitzat de codi obert que permet fer simulacions de bretxes de seguretat i executar comportaments o accions posteriors al compromís d'un atac dins de les xarxes corporatives.
- PICUS. (7) És una plataforma de simulació d'atacs i violacions que avalua contínuament el nivell de preparació dels controls de seguretat i operacions rellevants d'una empresa, utilitzant la seva biblioteca de mostres de tècniques i amenaces
- LUCY. (8) Es tracta d'una plataforma que permet a les organitzacions assumir el paper d'atacant per a descobrir les debilitats existents tant en la infraestructura tècnica com en el coneixement de personal i eliminar-les a través d'un programa d'aprenentatge virtual.

Donat que Gophish era la que més s'assimilava a la web que es volia dissenyar, es va fer una anàlisi més detallada.

3.1.1 Gophish

Gophish és una plataforma gratuïta i de codi obert dissenyada especialment per facilitar la formació de terceres persones pel que fa a la seguretat. Gràcies a aquesta eina, es poden llançar campanyes de phishing simulades i monitoritzar i analitzar els resultats segons aquelles que hagin tingut èxit i les que no.

Una dels avantatges que té aquesta eina és la simplicitat amb la qual es pot gestionar i el fet que qualsevol persona la pot aprendre a usar molt fàcilment. Aquesta funciona de la següent manera:

1. Un cop descarregada, gratuïtament, s'executen els binaris.
2. Ens connectem des del navegador a localhost a través del port 3333 i s'introdueixen les credencials: Usuari: admin i contrasenya: hash creat al executar els binaris.
3. Ja estem dins del panell d'administrador de Gophish.

Un cop aquí, si es vol crea qualsevol campanya, l'únic que s'ha de fer es crear un grup d'usuaris al que anirà dirigida aquesta, dissenyar el correu electrònic i ja es podrà llançar aquesta. Arribats d'aquí només quedarà esperar que es comenci a registrar activitat segons les persones que hagin caigut o no en aquesta campanya.

3.2 Grups d'usuaris

Un altra cosa a tenir en compte a l'hora de crear una plataforma d'aquest tipus, es el fet que qualsevol persona pot fer un mal ús d'aquesta. Es per aquest motiu pel qual en aquesta plataforma s'han distingit tres tipus de rols, un d'usuari per defecte no registrat, un d'usuari registrat i un altre d'usuari administrador.

El rol que té menys funcionalitats disponibles es el d'usuari per defecte no registrat, el qual només podrà accedir a la pàgina principal de la web o crear un compte. Quant als altres dos rols, a part de les funcionalitats de les quals disposa l'usuari no registrat, tenen les següents disponibles:

- Eliminar compte propi.
- Crear/Eliminar campanya.
- Crear/Eliminar empreses.
- Crear/Eliminar plantilla de correu electrònic.
- Editar perfil.

L'única funcionalitat que diferencia els dos rols comentats anteriorment amb el d'administrador, és el fet de aquest usuari tindrà un registre amb totes les comptes de la plataforma i en cas que algun compte amb rol d'usuari normal faci ún mal us de la plataforma, aquest podrà eliminar el compte.

3.3 Requeriments

Des d'un principi es va establir l'objectiu de la plataforma fos capaç de simular atacs de phishing i es per això que aquesta havia de tenir certs requeriments/funcionalitats. Alguns d'aquests ja s'han comentat en l'apartat anterior, tot i això ara es detallaran més a fons. Depenent del rol, els requeriments s'estructuren en els següents:

- Usuari no registrat:
    - Accedir a la pàgina principal: La web permetrà que qualsevol usuari pugui accedir a la web principal sense haver de fer cap registre.
    - Crear un compte: La web ha de permetre l'usuari no registrat, crear-se un compte.
- Usuari registrat:
    - Eliminar compte propi: La web ha de permetre a l'usuari eliminar el seu propi compte.
    - Entrar o sortir en el seu propi compte: La web ha de permetre a l'usuari fer log-in o log-out en el seu propi compte.
    - Crear/Eliminar una empresa: La web ha de permetre a l'usuari crear o eliminar una empresa per tal de poder llançar una campanya a aquesta.
    - Crear/Eliminar una plantilla de correu electrònic: La web ha de permetre a l'usuari crear o eliminar una plantilla per tal de poder enviar correus de phishing mitjançant aquesta.
    - Crear/Eliminar campanya: La web ha de permetre a l'usuari crear o eliminar una campanya per tal de poder llançar-la.

- Veure estadístiques d'una empresa: La web ha de permetre a l'usuari veure les estadístiques d'una empresa per tal de poder visualitzar si els empleats pertanyents a aquesta empresa han caigut en alguna de les campanyes de phishing que s'hagin llançat.
- Veure estadístiques d'una campanya: La web ha de permetre a l'usuari veure les estadístiques d'una campanya per tal de poder visualitzar quins empleats han caigut en ella i quins no.
- Editar el perfil: La web ha de permetre a l'usuari modificar el seu perfil, com per exemple la contrasenya.

Quant al rol d'administrador, aquest té permeses totes les funcionalitats de les quals disposa el rol d'usuari normal, ja sigui per poder llançar ell també campanyes com per assegurar-se del funcionament de la plataforma.

- Usuari administrador:
  - Eliminar qualsevol compte: Per tal d'evitar un mal ús de la web, aquesta haurà de permetre, únicament a l'usuari amb rol d'administrador, eliminar qualsevol compte.

Segons els requeriments comentats anteriorment, s'ha generat un petit diagrama de casos d'ús, Fig. 4, en el que es mostra un resum de la funcionalitat de la web. També es poden observar els casos d'ús individuals més detalladament en els annexos. (

Figura A2: Casos d'ús)

Fig. 4 Diagrama de casos d'ús de la web (Font: Pròpia)

4. Disseny

4.1 Diagrama de classes

Per tal de decidir com s'havia d'estructura la web, el que es va fer en un primer moment va ser dissenyar un diagrama de classes. En la figura, Fig. 5, es poden observar les classes principals de la web encarregada de llançar les campanyes juntament amb els seus atributs i en la figura, Fig. 6, les de la web trampa.

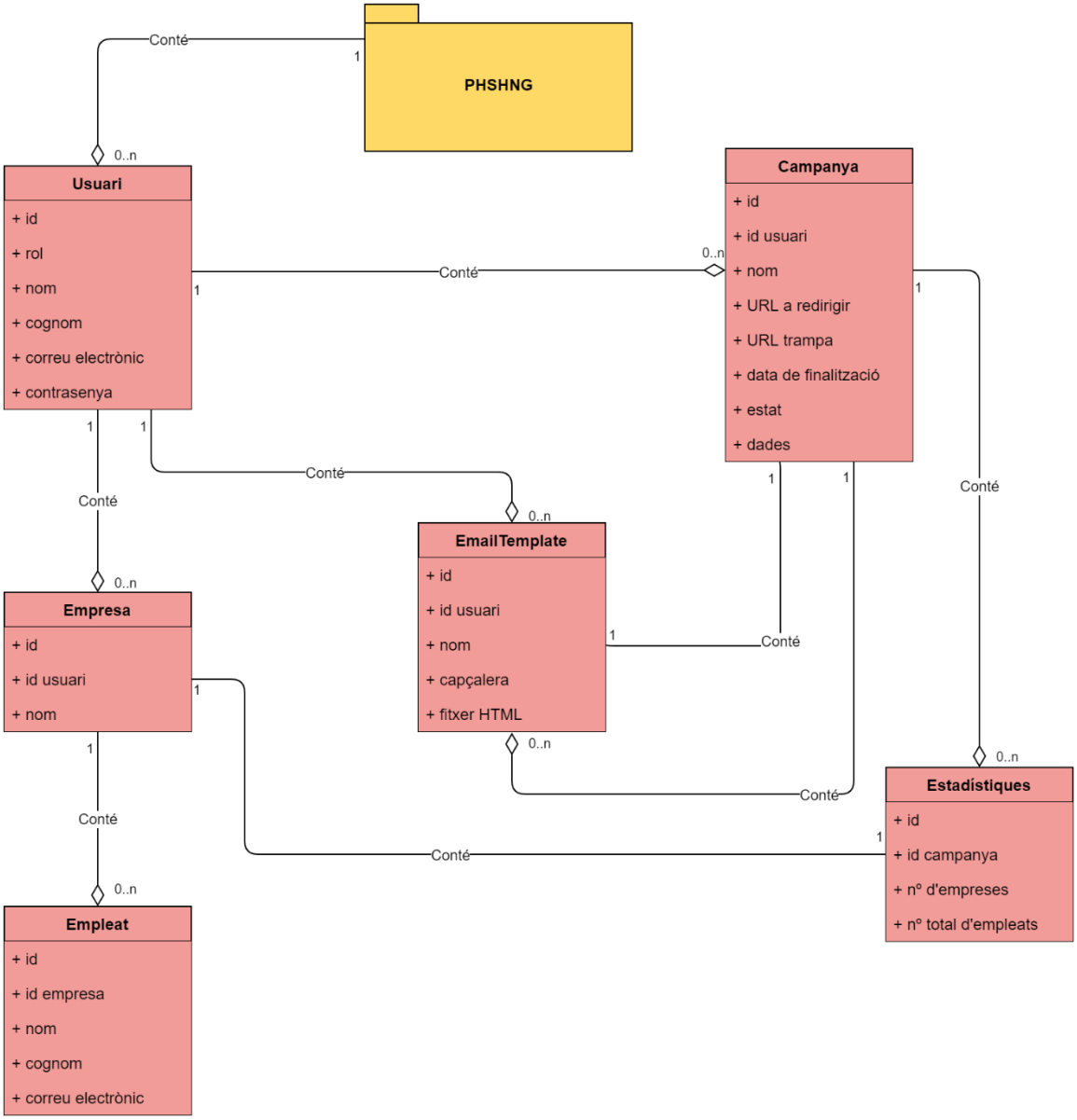


Fig. 5 Diagrama de classes de la web principal (Font: Pròpia)

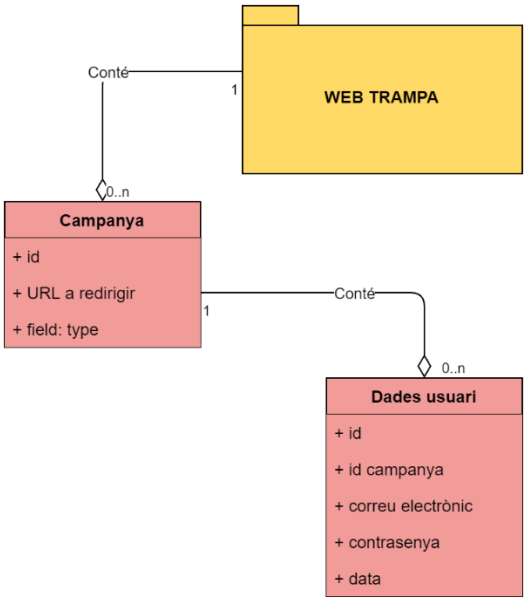


Fig. 6 Diagrama de classes de la web trampa (Font: Pròpia)

Arribats a aquest punt, procedirem a explicar que és el que emmagatzema cada una de les classes que es poden observar en les figures anteriors.

PHSHNG:

- Usuari: És l'encarregada d'emmagatzemar els comptes de cada un dels usuaris, aquesta, tal com es pot observar en el primer diagrama, contindrà una instància de campanyes, empreses i plantilles de correu electrònic.
- Campanya: Aquesta serà l'encarregada d'emmagatzemar les dades referents a cada una de les campanyes. Aquesta també contindrà una plantilla de correu electrònic, una o més empreses i les respectives estadístiques.
- Empresa: En aquesta s'emmagatzemarà la informació de cada una de les empreses, juntament amb els seus respectius empleats i estadístiques.
- Empleat: Encarregada d'emmagatzemar la informació de cada empleat, la qual es farà servir per a enviar els correus electrònics.
- Estàtiques: Serà l'encarregada d'emmagatzemar les estadístiques de les campanyes.

WEB TRAMPA:

- Campanya: En aquesta classe s'emmagatzemarà la informació relacionada amb la web trampa a la qual la víctima serà redirigida des del correu electrònic.
- Dades de l'usuari: En aquesta classe s'hi emmagatzemaran les dades de l'usuari en cas que caigui en la campanya de phishing.

4.2 Estructura de la base de dades

Seguit el diagrama de les figures, Fig. 5 i Fig. 6, s'ha dissenyat la base utilitzant SQLAlchemy [9.1], una base de dades tipus SQLite i mitjançant l'eina DB *Browser for SQLite* [9.1] (9) s'han extret les taules d'aquestes bases de dades. A continuació es podem veure aquestes taules, tant les de la web PHSHNG com la web trampa.

PHSHNG:

Nombre	Tipo	Esquema
account		CREATE TABLE account (id INTEGER NOT NULL, rol INTEGER NOT NULL, name VARCHAR(30) NOT NULL, lastname VARCHAR(30) NOT NULL, email VARCHAR(30) NOT NULL, password VARCHAR NOT NULL, PRIMARY KEY (id), UNIQUE (id))
id	INTEGER	"id" INTEGER NOT NULL
rol	INTEGER	"rol" INTEGER NOT NULL
name	VARCHAR(30)	"name" VARCHAR(30) NOT NULL
lastname	VARCHAR(30)	"lastname" VARCHAR(30) NOT NULL
email	VARCHAR(30)	"email" VARCHAR(30) NOT NULL
password	VARCHAR	"password" VARCHAR NOT NULL

Fig. 7 Taula de comptes (Font: DB Browser for SQLite)

Nombre	Tipo	Esquema
campaign		CREATE TABLE campaign (id INTEGER NOT NULL, id_user INTEGER NOT NULL, name VARCHAR(30) NOT NULL, redirect_url VARCHAR NOT NULL, cheat_url VARCHAR NOT NULL, finish_date VARCHAR NOT NULL, state INTEGER NOT NULL, get_data_url VARCHAR NOT NULL, PRIMARY KEY (id), FOREIGN KEY(id_user) REFERENCES account (id), UNIQUE (id))
id	INTEGER	"id" INTEGER NOT NULL
id_user	INTEGER	"id_user" INTEGER NOT NULL
name	VARCHAR(30)	"name" VARCHAR(30) NOT NULL
redirect_url	VARCHAR	"redirect_url" VARCHAR NOT NULL
cheat_url	VARCHAR	"cheat_url" VARCHAR NOT NULL
finish_date	VARCHAR	"finish_date" VARCHAR NOT NULL
state	INTEGER	"state" INTEGER NOT NULL
get_data_url	VARCHAR	"get_data_url" VARCHAR NOT NULL

Fig. 8 Taula de campanyes (Font: DB Browser for SQLite)

Nombre	Tipo	Esquema
company		CREATE TABLE company (id INTEGER NOT NULL, id_user INTEGER NOT NULL, name VARCHAR(30) NOT NULL, PRIMARY KEY (id), FOREIGN KEY(id_user) REFERENCES account (id), UNIQUE (id))
id	INTEGER	"id" INTEGER NOT NULL
id_user	INTEGER	"id_user" INTEGER NOT NULL
name	VARCHAR(30)	"name" VARCHAR(30) NOT NULL

Fig. 9 Taula de empreses (Font: DB Browser for SQLite)

Nombre	Tipo	Esquema
emailtemplate		CREATE TABLE emailtemplate (id INTEGER NOT NULL, id_user INTEGER NOT NULL, name VARCHAR(30) NOT NULL, header VARCHAR NOT NULL, html_file VARCHAR, PRIMARY KEY (id), FOREIGN KEY(id_user) REFERENCES account (id))
id	INTEGER	"id" INTEGER NOT NULL
id_user	INTEGER	"id_user" INTEGER NOT NULL
name	VARCHAR(30)	"name" VARCHAR(30) NOT NULL
header	VARCHAR	"header" VARCHAR NOT NULL
html_file	VARCHAR	"html_file" VARCHAR

Fig. 10 Taula de correus electrònics (Font: DB Browser for SQLite)

Nombre	Tipo	Esquema
employee		CREATE TABLE employee (id INTEGER NOT NULL, id_company INTEGER NOT NULL, name VARCHAR(30) NOT NULL, lastname VARCHAR(30) NOT NULL, email VARCHAR(30) NOT NULL, PRIMARY KEY (id), FOREIGN KEY(id_company) REFERENCES company (id), UNIQUE (id))
id	INTEGER	"id" INTEGER NOT NULL
id_company	INTEGER	"id_company" INTEGER NOT NULL
name	VARCHAR(30)	"name" VARCHAR(30) NOT NULL
lastname	VARCHAR(30)	"lastname" VARCHAR(30) NOT NULL
email	VARCHAR(30)	"email" VARCHAR(30) NOT NULL

Fig. 11 Taula d'empleats (Font: DB Browser for SQLite)

Nombre	Tipo	Esquema
statistics		CREATE TABLE statistics (id INTEGER NOT NULL, id_campaign INTEGER NOT NULL, num_companies INTEGER NOT NULL, num_total_employees INTEGER NOT NULL, PRIMARY KEY (id), FOREIGN KEY(id_campaign) REFERENCES campaign (id), UNIQUE (id))
id	INTEGER	"id" INTEGER NOT NULL
id_campaign	INTEGER	"id_campaign" INTEGER NOT NULL
num_companies	INTEGER	"num_companies" INTEGER NOT NULL
num_total_employees	INTEGER	"num_total_employees" INTEGER NOT NULL

Fig. 12 Taula d'estadístiques (Font: DB Browser for SQLite)

Nombre	Tipo	Esquema
tags1		CREATE TABLE tags1 (campaigns_id INTEGER, companies_id INTEGER, FOREIGN KEY(campaigns_id) REFERENCES campaign (id), FOREIGN KEY(companies_id) REFERENCES company (id))
campaigns_id	INTEGER	"campaigns_id" INTEGER
companies_id	INTEGER	"companies_id" INTEGER

Fig. 13 Taula de relació entre les taules campanyes i empreses (Font: DB Browser for SQLite)

Nombre	Tipo	Esquema
tags2		CREATE TABLE tags2 (campaigns_id INTEGER, emailtemplate_id INTEGER, FOREIGN KEY(campaigns_id) REFERENCES campaign (id), FOREIGN KEY(emailtemplate_id) REFERENCES emailtemplate (id))
campaigns_id	INTEGER	"campaigns_id" INTEGER
emailtemplate_id	INTEGER	"emailtemplate_id" INTEGER

Fig. 14 Taula de relació entre les taules campanyes i plantilles de correu electrònic (Font: DB Browser for SQLite)

Nombre	Tipo	Esquema
tags3		CREATE TABLE tags3 (employee_id INTEGER, campaign_id INTEGER, FOREIGN KEY(campaign_id) REFERENCES campaign (id), FOREIGN KEY(employee_id) REFERENCES employee (id))
employee_id	INTEGER	"employee_id" INTEGER
campaign_id	INTEGER	"campaign_id" INTEGER

Fig. 15 Taula de relació entre les taules empleats i empreses (Font: DB Browser for SQLite)

WEB TRAMPA:

Nombre	Tipo	Esquema
campaign		CREATE TABLE campaign (id INTEGER NOT NULL, redirect_url VARCHAR NOT NULL, PRIMARY KEY (id), UNIQUE (id))
id	INTEGER	"id" INTEGER NOT NULL
redirect_url	VARCHAR	"redirect_url" VARCHAR NOT NULL

Fig. 16 Taula de campanyes (Font: DB Browser for SQLite)

Nombre	Tipo	Esquema
dataUser		CREATE TABLE "dataUser" (id INTEGER NOT NULL, id_campaign INTEGER NOT NULL, email VARCHAR NOT NULL, password VARCHAR NOT NULL, date VARCHAR NOT NULL, PRIMARY KEY (id), FOREIGN KEY(id_campaign) REFERENCES campaign (id), UNIQUE (id))
id	INTEGER	"id" INTEGER NOT NULL
id_campaign	INTEGER	"id_campaign" INTEGER NOT NULL
email	VARCHAR	"email" VARCHAR NOT NULL
password	VARCHAR	"password" VARCHAR NOT NULL
date	VARCHAR	"date" VARCHAR NOT NULL

Fig. 17 Taula de dades de la víctima (Font: DB Browser for SQLite)

En figures anteriors, es poden observar les taules de les bases de dades esmentades, també hi ha algunes d'elles anomenades tagsN les quals serveixen com a taula de relacions entre les taules principals.

Aquestes relacions són les anomenades many-to-many i es troben quan una o més files d'una entitat o classe s'associen a més d'una fila d'una altra entitat. Per exemple, en la taula tags1, ens trobem en la situació en la qual una empresa pot estar relacionada a una o més campanyes.

5. Implementació

5.1 Tecnologies utilitzades

Com tot projecte de software, aquest web té un Frontend i un Backend. En aquest apartat parlarem de les tecnologies usades en cada un d'aquests i com s'han estructurat les diferents webs creades, ja que hem de recordar que s'han creat dues webs, una encarregada de crear i llançar la campanya i una altra encarregada de simular la web trampa en la qual la víctima pot o no caure.

Per a la creació d'ambdós webs s'ha usat l'eina PyCharm. PyCharm és un IDE *(Integrated Development Enviroment*), es a dir no només és un editor de codi sinó que també té un depurador, un intèrpret i altres eines que ajuden a crear i exportar qualsevol programa. Aquest també conté un editor de codi que ajuda a detectar possibles errors de codi en temps real, cosa que ha fet que Python i PyCharm siguin escollits per molts usuaris com a IDE per defecte en els projectes en el que s'utilitza Python com a llenguatge de programació.

Fig. 18 PyCharm

5.1.1 Backend

5.1.1.1 Flask

Quant al Backend, en ambdós webs s'ha fet servir diversos frameworks [9.1], el principal, Flask (10). Flask és un "micro" Framework escrit en Python i creat per a facilitar el desenvolupament d'aplicacions web sota el patró Model-Vista-Controlador. El fet d'haver utilitzat aquest framework es perquè s'ha utilitzat en tant en l'assignatura de Software Distribuït com la d'Enginyeria del Software i ja tenia certs coneixements d'aquest.

Fig. 19 Flask Framework

El patró Model-Vista-Controlador és una manera o forma de treballar que permet diferenciar i separar el que es la representació de les dades que gestiona el sistema, la lògica i els mecanismes de persistència (Model), les interfícies d'usuari que componen la informació que s'enviarà al client i els mecanismes d'interacció amb aquesta (Vista) i l'intermediari entre Model i Vista (Controlador), que gestiona el flux d'informació entre ells i les transformacions per adaptar les dades a les necessitats de cada una de les parts. En la següent figura, Fig. 20, es pot observar l'estructura de la part de Backend en el que podem observar la part de model i la part de controlador només, ja que la part de vista la tenim en el Frontend.

En la carpeta models tenim el que són les classes i la representació de les dades les quals serien l'equivalent al part de Model i la resta; carpeta de recursos (resources), útils i tots els altres fitxers .py que són els que comprendrien la part del Controlador. Destacar el fitxer app.py, que es tracta del fitxer encarregat de tota la lògica de la web i de les crides als diferents End-Points [9.1].

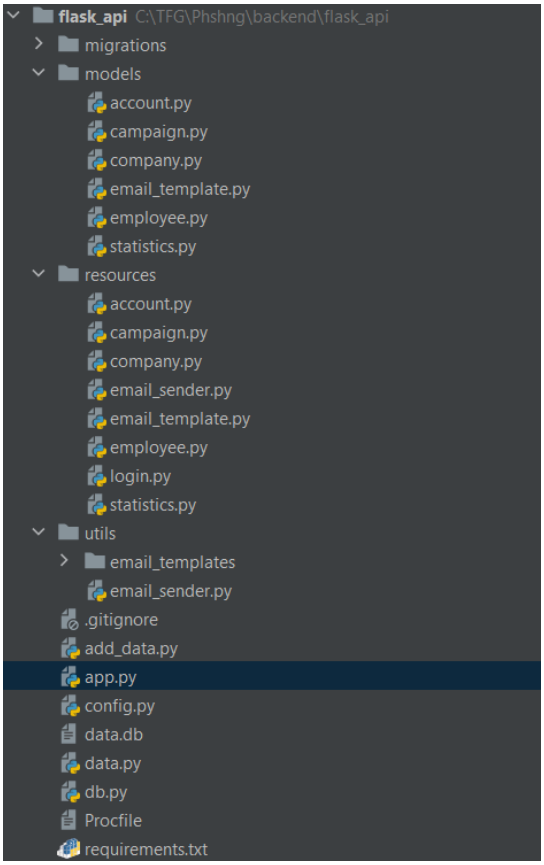


Fig. 20 Estructura del Backend de la web (Font: PyCharm)

Quan ens referim al framework de Flask amb la paraula micro no ens referim al fet que sigui un projecte petit o que només ens permeti crear pàgines web petites, sinó que en instal·lar Flask tenim les eines necessàries per a crear una aplicació web funcional, però si en algun moment es necessita una nova funcionalitat, aquest framework té un ampli conjunt d'extensions (pluguins) que ens permeten dotar-lo de més funcionalitats. A continuació es mostraran les extensions utilitzades en la nostra web.

- Flask-RESTful (11): Es tracta d'una extensió de Flask que afegeix suport per a construir ràpidament una API REST. És una abstracció lleugera que funciona amb biblioteques/llibreries existents. Una API REST (Representational State Transfer), és una aplicació web creada tenint en compte un conjunt de restriccions especificades per Roy Fielding, pare de les especificacions HTTP, en la seva tesi en l'any 2000. Algunes d'aquestes són: seguir una estructura Client-Servidor, que les peticions siguin independents entre elles, que se segueixi un sistema de capes per a una millor escalabilitat, etc. En aquest projecte s'han seguit aquestes directrius, on, per un costat tenim el client que serien els usuaris de la web els quals realitzaren peticions HTTP, i el servidor Flask encarregat de proveir amb les dades que se li van demanant.
  En la següent figura es poden observar alguns dels mètodes més importants d'una API REST, els quals s'han fet servir en les webs creades. (Figura A3: Llista d'End-Points)

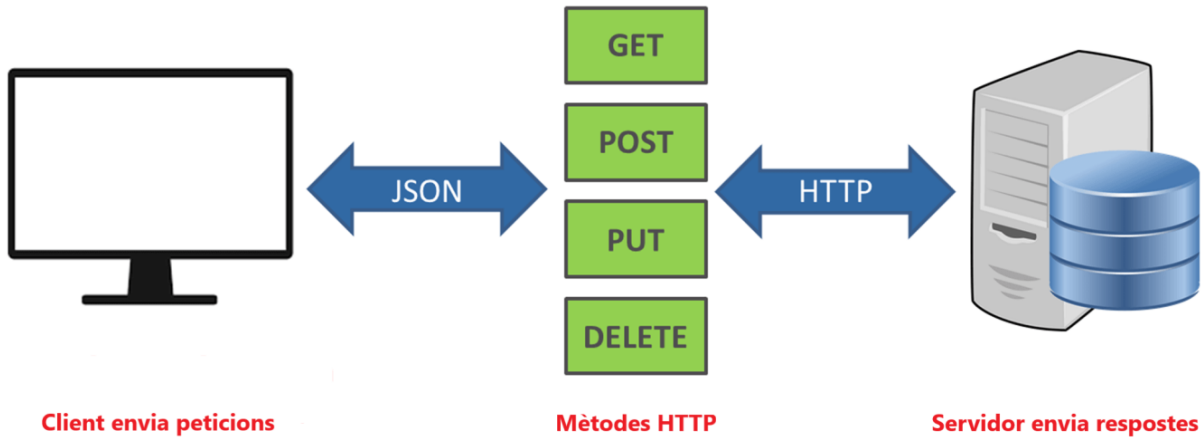


Fig. 21 Estructura Client-Servidor (Font pròpia)

- Flask-SQLAlchemy (12): Es tracta d'una extensió de Flask que dòna suport a ORM (Object-Relational Mapper), un conjunt d'eines que ens ajuda a treballar amb les taules de la base de dades com si fossin objectes, de manera que cada taula es mapeja com una classe i cada columna com un camp d'aquesta classe. A part, també permet mapejar les relacions entre les taules com a relacions entre els objectes.

  No obstant, una de les característiques més importants d'aquests ORMs es el fet que permeten fer canvis en la base de dades sense modificar gaire codi. D'aquesta forma es pot programa una aplicació web sense preocupar-se gaire en el tipus de base de dades a usar. En el nostre cas, tal com s'ha comentat en la secció, Estructura de la base de dades, s'ha fet servir SQLite.

Fig. 22 SQLite

- Flask-Migrate (13): Es tracta d'una altra extensió de Flask que ens permet menejar la migració de la base de dades SQLAlchemy per a les aplicacions Flask. Això fa possible el fet de poder operar amb les dades de la base de dades a través de la interfície de línia de comandes de Flask o Flask-Scripts.
- Flask-CORS (14): Es tracta d'una extensió de Flask que permet tractar l'intercanvi de recursos amb origen creuat. Amb això el que aconseguíem, en aquest projecte, es poder fer crides de recursos des de fora de lorigen, en altres paraules, ens permet fer crides des del Frontend als End-Points de les peticions HTTP

- Flask-mail (15): Aquest és un altre recurs de Flask el qual ens proporciona una interfície simple per a configurar SMTP [9.1] amb una aplicació Flask. Aquesta eina és la que em permet enviar correus a les possibles víctimes de les campanyes creades en la web.

```
app.config['MAIL_SERVER'] = 'smtp.mail.yahoo.com'
app.config['MAIL_PORT'] = 587
app.config['MAIL_USE_TLS'] = True
app.config['MAIL_USE_SSL'] = False
app.config['MAIL_USERNAME'] = "noreply.supio@yahoo.com"
app.config['MAIL_PASSWORD'] = "lvewhncidrglzotf"
app.config['MAIL_DEFAULT_SENDER'] = ["", "noreply.supio@yahoo.com"]
```

Fig. 23 Configuració del servidor SMTP utilitzant Yahoo Mail

En la figura anterior es pot observar que s'ha utilitzat un SMTP de Yahoo, cosa que no va ser així en un principi. En començar, per a enviar correus a les víctimes s'utilitzava un SMTP de Gmail, però com que Gmail va bloquejar l'enviament de correus amb l'enllaç de la pàgina trampa, ja que la detectava com a pàgina fraudulenta, es va haver de canviar a un SMTP de Yahoo.

Per tal de disfressar la direcció d'on procedien aquests correus electrònics amb l'enllaç de la pàgina trampa, el correu que es va utilitzar va ser el següent: noreply.supio@yahoo.com

5.1.2 Frontend

5.1.2.1 Vue

Pel que fa a la part de Frontend, tant la web principal com la web trampa s'ha utilitzat Vue (16). Vue és un framework de codi obert de JavaScript (JS) amb una corba d'aprenentatge baixa que permet a l'usuari crear interfícies d'usuari de forma molt senzilla. Així com en la part de Backend, en Frontend s'ha utilitzat el framework de Vue pel mateix motiu, ja que s'havia tractat en assignatures del grau.

Fig. 24 Framework Vue

Aquest framework, al contrari que Angular, un altre framework de JavaScript, és completament modular, ja que només ofereix les funcionalitats més bàsiques i en el cas de voler afegir-ne alguna de nova, aquest dóna la possibilitat i facilitat d'instal·lar-les posteriorment. Un altre aspecte a descartar d'aquest framework és la seva capacitat de crear vistes reactives, ja que permet actualitzar aquestes vistes, quan les dades són modificades, sense la necessitat que el programador hagi de propagar aquests canvis de forma manual en cada una de les pàgines on es visualitzen aquestes dades.

Seguint amb el patró Model-Vista-Controlador, hem vist que en la part de Backend es trobaven el Model i el Controlador. Vue pertany a la família de frameworks que se centren en la part de la Vista. En la figura següent podem observar l'estructura d'aquesta vista en el projecte, on es poden distingir les diferents pantalles de la web.

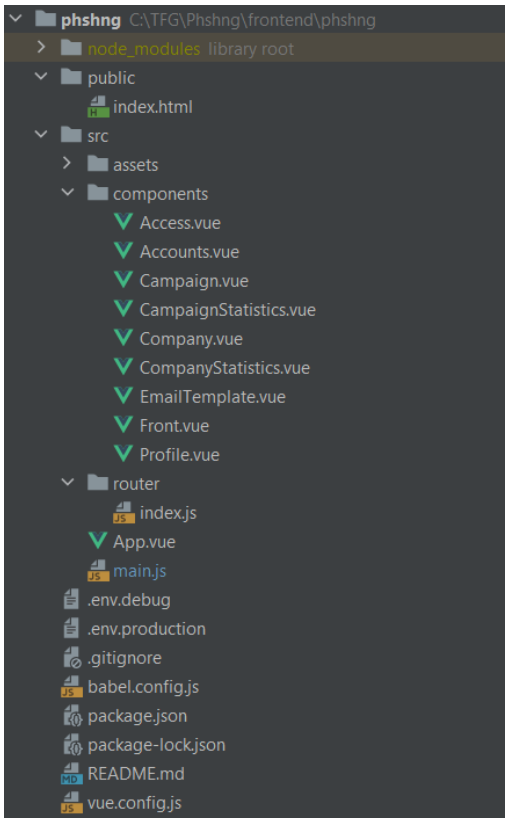


Fig. 25 Estructura del Frontend de la web (Font: PyCharm)

Una de les característiques més importants de Vue és el fet que treballa amb components web (exemple: Fig. 25). Un component web és una part d'una web que pot ser reutilitzada i que normalment té estils i funcionalitats aïllades. Dins d'aquests components es troben les etiquetes HTML, estils de CSS i codi JavaScript.

```
<template>
<h1 class="text-center"> Hola Cody </h1>
</template>

<script>
</script>

<style>
</style>
```

Fig. 26 Component web (Font: (17))

L'ecosistema de Vue està format per varies parts, on cada una du a terme una tasca concreta. Aquestes parts són les següents:

- Vue: El nucli del framework Vue, on es troben les seves funcions principals.
- Vue CLI: Assistent per a crear i administrar projectes de Vue des d'una terminal o un entorn gràfic.
- Vue Router: Sistema per a crear i gestionar rutes URL des del navegador en una aplicació Vue.
- Vuex: Gestor d'estats per a aplicacions SPA de Vue.
- Vue Test Utils: Api per a realitzar test sobre les aplicacions Vue.

Per ajudar al desenvolupament de tota la part gràfica de la web s'ha utilitzat altres frameworks i eines. Aquestes es detallen a continuació:

- BootstrapVue (18): Aquesta és una eina que ens permet utilitzar el Framework de Bootstrap integrat en el de Vue. Bootstrap utilitza un framework HTML & CSS cosa que facilita la seva integració en Vue. Aquest ajuda al programador aportant una sèrie de scripts de JavaScript i estils CSS molt ben elaborats que permeten afegir a la pàgina molts components, tan component simples com podrien ser botons o inputs com més complexos com per exemple menús desplegables, simplement copiant el

codi disponible en la documentació de la pàgina web oficial (19). Aquesta documentació està estructurada i separada per seccions, d'aquesta forma permet buscar fàcilment qualsevol classe de característica que es vulgui afegir en el mateix disseny i veure diferents exemples.

Fig. 27 BootstrapVue

Un dels aspectes pel qual més destaca aquest framework és que ofereix un disseny en concret per a les seves pàgines que facilita la inclusió dels elements HTML en qualsevol part. Normalment aquesta acció de col·locar elements en segons quins llocs és una tasca tediosa per al programador, sobre tot vigilant que no es descol·loqui cap altre element. En aquest sentit, aquest framework és de tipus responsive, cosa que permet que el contingut que s'afegeixi al disseny s'adapti a la mida del dispositiu on s'està visualitzant d'una manera còmoda i accessible.

- VueApexchart (20): Es tracta d'un component contenidor que permet fer la integració de ApexCharts (21) en Vue, permetent així crear tota mena de gràfics de dades. Així com Bootstrap, ApexCharts és responsive, cosa que permet una bona visualització en qualsevol dispositiu.

Fig. 28 ApexCharts + Vue

- VueCookies (22): Es tracta d'un complement simple de Vue que permet treballar amb les galetes del navegador. Aquesta eina s'ha fet servir per a mantenir la sessió d'un usuari durant 1 hora encara que tanqui la finestra del navegador.

```
this.$cookies.set( keyName: "logindata", data, expireTimes: {
  expire: '1h',
  path: '/',
  domain: '',
  secure: '',
  sameSite: '',
})
```

Fig. 29 Configuració de les galetes (Font: PyCharm)

Donat que Vue utilitza JS, també s'ha hagut d'utilitzar l'eina Nodejs, un entorn d'execució de JS en temps real que inclou tot el que es necessita per a executar programes en JavaScript.

5.1.3 Altres tecnologies

A continuació es descriuen altes tecnologies utilitzades en el desenvolupament del projecte però que no estant tan relacionades amb el Frontend o Backend en concret.

5.1.3.1 Trello

Fig. 30 Software d'administració de projectes Trello

Aquest és un software que no és essencial per al desenvolupament del projecte, però molt útil si l'usuari el fa servir. Trello (23) és una aplicació molt utilitzada a tant en l'àmbit professional com personal, la qual permet la gestió de qualsevol projecte. Aquesta permet crear diferents estats en el que es poden trobar certes tasques (pendent, en procés, acabada...). També permet crear targetes, equivalents a una tasca o història d'usuari, establint un títol, descripció, prioritat, criteris d'acceptació, subtasques... D'aquesta forma es pot obtenir, de forma molt ràpida i visual, l'estat en que es troba el projecte i cada una de les tasques que fan referència a aquest.

Com bé s'ha comentat anteriorment, el projecte es pot realitzar sense usar aquesta eina, però el fet d'utilitzar-se pot ajudar a que el desenvolupador no s'oblidi de cap punt durant el transcurs del projecte.

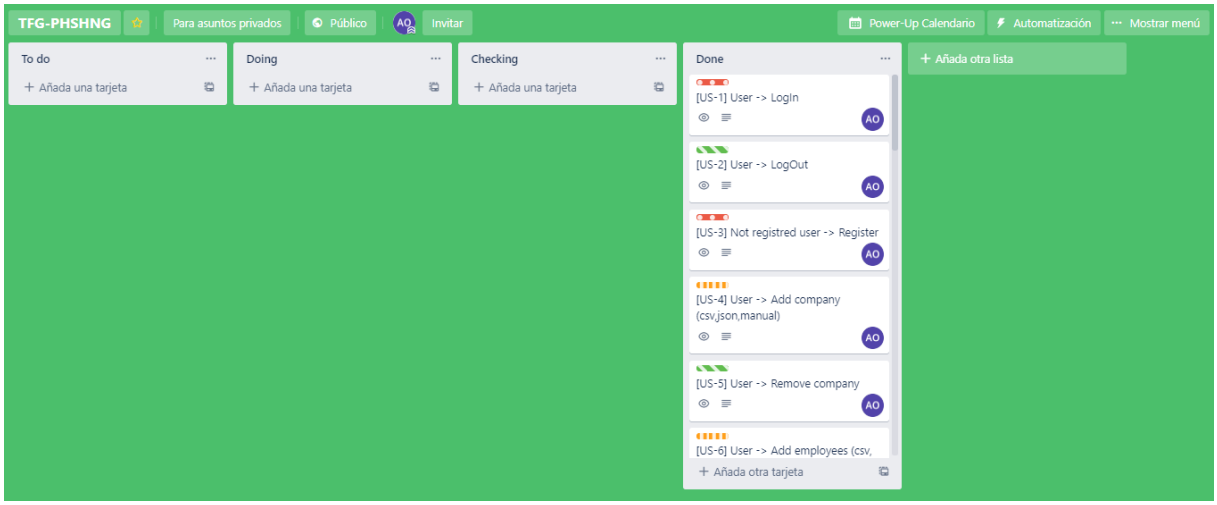


Fig. 31 Trello TFG-PHSHING (Font: Pròpia, Trello)

5.1.3.2 Git, GitHub i GitHub Project Boards

Fig. 32 Control de versions Git i Servei public de control de versoins Github

Fins fa un parell d'anys, en el desenvolupament web, s'ha treballat de forma més directa, ja que per a realitzar qualsevol modificació en els fitxers d'una web, simplement es modificaven localment i mitjançant qualsevol client FTP [9.1] es pujaven aquests fitxers modificats al servidor. Però aquesta forma de treballar té un inconvenient, ja que si en algun moment sorgeix un problema, no es tenia un historial dels canvis que s'havien anat fent cosa que complicava el fet de recuperar l'última versió funcional. Aquí es on entra Git (24) i GitHub (25).

Git és un control de versions, una eina que facilita un lloc on pujar el projecte, anomenats repositori, i una sèrie de funcionalitats. Aquí, un cop es vol pujar una modificació del projecte, s'han de realitzar unes accions anomenades *commits* que són bàsicament una forma d'etiquetatge que permeten portar un seguiment de les modificacions que es van fent en el transcurs del desenvolupament del projecte. Aquests *commits*, només es fan localment, fins que es fa la crida a *push*, que consisteix en pujar els diferents *commits* al repositori.

L'avantatge de treballar amb aquesta eina és que fa possible tornar a un estat/*commit* anterior molt fàcilment, simplement revocant els canvis de forma automàtica. També permet el treball en barques, cosa que fa possible generar una còpia de l'estat en el qual es troba el projecte en certa branca i evitar modificar el codi original o codi funcional que es té en aquell moment. Un cop s'han fet les modificacions que es desitgin en certa branca, aquesta es pot unir a la branca principal (branca *master* o branca *main*) que és on es troba el codi original.

En el nostre cas, s'ha fet servir Git per a evitar els problemes comentats anteriorment com tenir una versió funcional del projecte en cada moment emmagatzemada en la branca principal i GitHub com a plataforma on es troben els repositoris que fan servir Git.

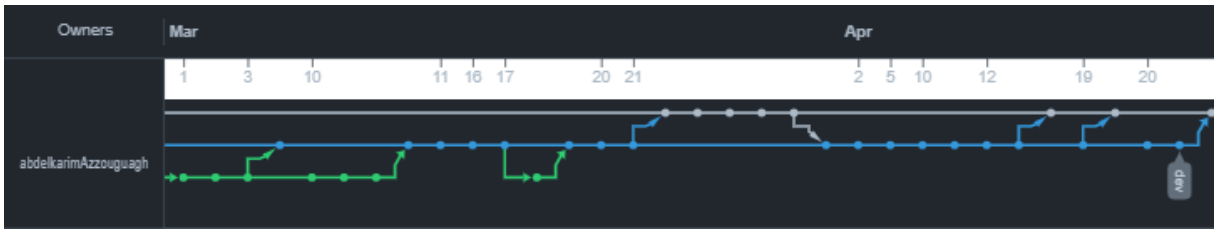


Fig. 33 Registre de versions PHSHNG Març-Abril (Font: Pròpia, Github)

Entrant en detall en la plataforma de GitHub, també s'ha usat l'eina de Project Boards, la qual és semblant a Trello, però en aquest cas, a part de tenir-hi les tasques en les quals se subdivideixen les històries d'usuari, també s'hi tenen problemes que han anat sorgint durant el desenvolupament, tasques per a buscar informació sobre alguna nova tecnologia a afegir al projecte... Aquestes tasques s'anomenen *issuess*, les quals tenen dos estats, obertes (pendent o en procés) o

tancades (finalitzades). Aquests *issues*, es tanquen un cop es fa un *commit* a la branca principal amb la funcionalitat que descriu, implementada.

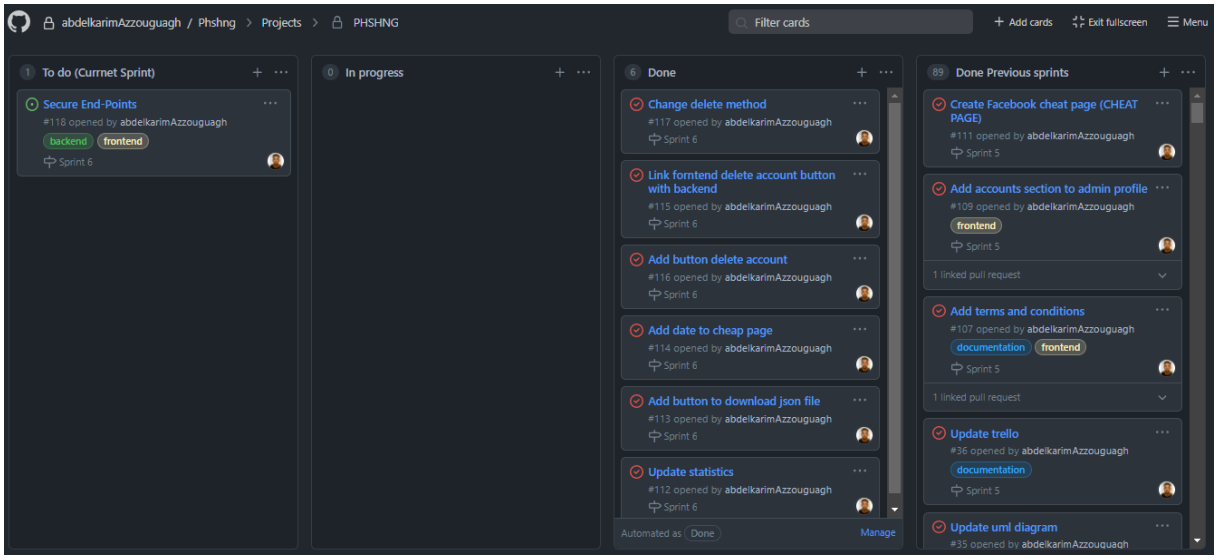


Fig. 34 GitHub Project Board PHSHNG (Font: Propia, Github)

5.1.3.3 Heroku

Fig. 35 PaaS Heroku

Per al desenvolupament d'aplicacions web, s'ha de ser conscient de l'impacte que hi ha quan es comencen a tenir certa quantitat d'usuaris, per això és molt important llançar aplicacions web sense tenir complicacions d'infraestructures, administracions de servei, bases de dades i la seguretat que aquests han de tenir.

Heroku (26) és una PaaS (Platform as a Service) [9.1] que suporta una gran quantitat de llenguatges de programació, entre ells Python o Java. També té suport per molts tipus de bases de dades, com en el nostre cas SQL. Heroku és una de les PaaS més utilitzades en l'actualitat i gira entorn a l'àmbit empresarial pel seu enfocament en resoldre el desplegament d'aplicacions.

Cal destacar que és una plataforma en el núvol, el que significa que els desenvolupadors no s'han de preocupar per la infraestructura, sinó que solament

s'han de centrar en el desenvolupament de la web/aplicació, el que evita tots els problemes que pugui suposar portar la idea a un servidor. Només cal indicar quin llenguatge s'està fent servir en el Backend, en el nostre cas Python, i quina base de dades es vol utilitzar, en aquest cas PostgreSQL, i Heroku s'encarregarà de fer la resta.

Per a poder executar el codi de la web mitjançant Heroku, aquesta fa servir el que s'anomenen *Dynos*, aquests són contenidors gestionats en temps d'execució basats en Contenidors Linux. Aquests estan aïllats de la resta, cosa que fa que les comandes que s'executen i els fitxers que es guarden en un Dynos no afecten els altres.

Aquesta plataforma ha permès fer un Deployment [9.1] fàcil i ràpid de les dues webs que s'han creat, PHSHNG i web trampa. També comentar un problema que ha tingut fer servir aquesta plataforma usant els Dynos per defecte gratuïts és el fet que aquests si no reben peticions durant un període de 30 minuts es desconnecten cosa que fa que al tornat a rebre alguna petició, aquests s'hagin de reiniciar. Això provoca que tota la informació que hi havia emmagatzemada en aquests Dynos, l'equivalent a la informació emmagatzemada en la web, com comptes dels usuaris o qualsevol altre fitxer guardat per "x" usuari, es perdi, i al accedir a la web aquesta es trobi en el mateix estat en el qual es trobava en l'últim Deployment.

5.1.3.4 Travis Ci

Fig. 36 Eina d'integració continua Travis Ci

Tots hem tingut algun cop problemes a l'hora d'ajuntar el nostre codi amb el d'algun altre desenvolupador i ens hem trobat en el punt en el qual trobem conflictes entre aquests codis, ja que ambdós hem modificat el mateix tros de codi. Aquí és on entre en joc el terme d'integració contínua.

Quan parlem d'integració contínua ens referim al fet que el codi de tots els integrants d'un projecte es puja al repositori compartit freqüentment. D'aquesta forma es manté una versió del codi estable i amb l'última versió des d'on qualsevol dels integrants pot començar a treballar en algun canvi sense trepitjar el treball dels altres desenvolupadors. En aquest cas es té totalment automatitzada la construcció del projecte, llançar els diferents testos, revisió de la qualitat del codi, entre d'altes.

Una eina que ens permet per aquesta integració continua és Travis Ci (27). La qual s'ha fet servir per a que cada cop que es puja el codi a la branca principal del projecta al GitHub, aquest faci el Deployment de la web a Heroku automàticament.

```yaml
language: python
python:
- 3.8.6
cache: npm
install:
- npm install newman
script:
- cd frontend/phshng
- npm install
- npm run production
before_deploy:
- cd ../../backend/flask_api
on:
  repo: abdelkarimAzzouguagh/Phshng
branches:
  only:
  - main
deploy:
  provider: heroku
  skip_cleanup: true
  api_key:
    secure: ggeggDYc6zx2QFiqJwmXysOQLizUPYgEy8ga4fxD...
  app:
    main: phshng
```

Fig. 37 Configuració del fitxer .travis.yml de la web PHSHNG (Font: Pròpia, GitHub)

5.1.3.5 NameCheap

Fig. 38 Servidor de hosting i dominis Namecheap

Tot i que Heroku en crear una web et facilita un commini acabat amb “herokuapp.com” es va decidir comprar-ne un per a donar més estètica a la web. Per a fer això, es va fer servir Meancheap (28). Aquesta és una base de dades distribuïda, amb informació que es fa servir per a traduir els noms de domini mitjançant el protocol d’internat IP, que és la forma en la qual les màquines es poden trobar en internet.

Nom de domini comprat: http://www.phshng.com

5.1.3.6 Postman

Fig. 39 Postman

Quant a la part de Backend, concretament l’API REST, per tal de comprovar que tots els End-Points retornaven el que se’ls demanava o demanaven les dades necessàries en cas que l’usuari no es proporcionés, s’ha fet servir Postman (29). Aquesta és una eina que, bàsicament, s’encarrega de la part de *testing* de les APIs REST. Aquesta eina també té altres funcionalitats com monitoritzar aquests tests, escriure proves automatitzades per a aquestes apis, documentar-les, entre d’altes.

5.1.3.7 Pomodoro

Fig. 40 Aplicació Pomodoro (30)

Aquesta és una altra eina que no és essencial per al desenvolupament del projecte, però el fet d'utilitzar-la ha permès portar una millor organització del temps a l'hora de treballar en el projecte.

La tècnica pomodoro consisteix en un temporitzador que divideix el treball en blocs de temps en els que el desenvolupador està completament enfocat en el treball, sense cap distracció. Aquests períodes de temps normalment oscil·len entre 25-30 minuts. Entre aquests blocs de temps, el programador té 5 minuts per a descansar i després de 4 blocs de temps es fa un descans més llars, normalment 20-30 minuts.

Els beneficis d'aquesta tècnica provenen dels descansos freqüents, ja que ajuden al fet que la ment es mantingui fresca. Els blocs de temps enfocats també obliguen al desenvolupador a complir amb els límits establerts, ja que animen a completar la tasca més ràpidament o en el cas de ser una tasca més llarga, estendre-la en diversos pomodoros.

5.2 Pantalles de la web i funcionament

Arribats a aquest punt, només ens falta explicar com s'estructuren les diferents pantalles de les quals consta la web, tant en dispositius mòbils com ordinadors i quines són les transicions que s'han de fer per a poder crear i llançar una campanya.
En la següent figura, Fig. 41, es pot observar el diagrama de transicions entre les diferents pantalles de la web. Un aspecte a destacar d'aquest diagrama és que un cop l'usuari ja està registrat en la web, es pot moure per les diferents pantalles de gestió de les campanyes, com són la pàgina de campanyes, la d'empreses, la de plantilles de correu electrònic i la de perfil.

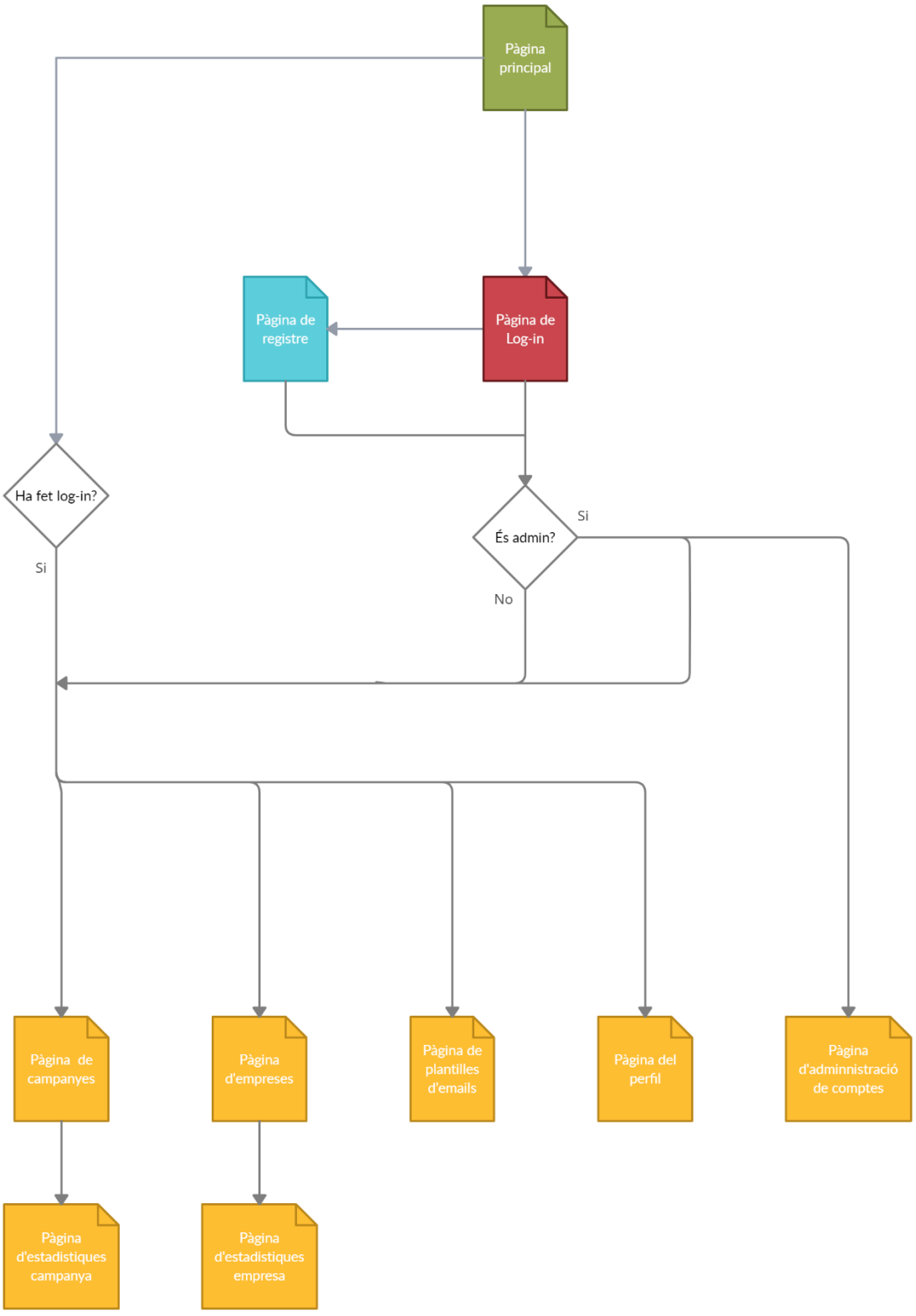


Fig. 41 Diagrama de transicions de la web PHSHNG (Font: Pròpia)

Tal i com es pot observar en la figura anterior, la web consta de les següents pantalles:

5.2.1 Pantalla principal

Aquesta és només la primera vista que tindrà l'usuari al accedir a la web. En aquesta primera vista, també, serà on se li mostrarà un missatge a l'usuari per a que accepti l'ús de les galetes.

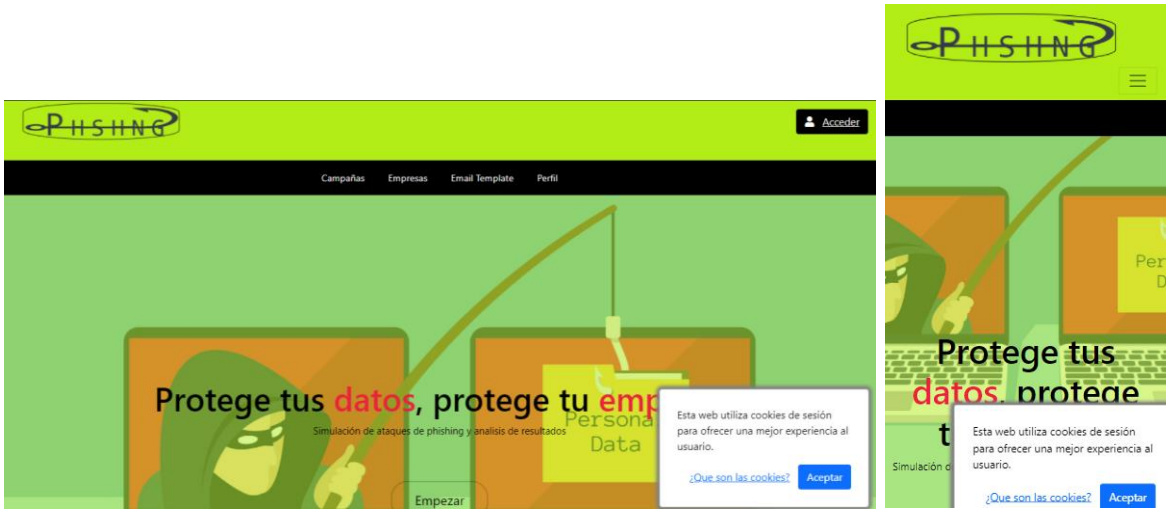


Fig. 42 Disseny responsive de la pantalla principal (Font: Pròpia)

En aquesta pantalla l'usuari només es podrà dirigir a la pantalla de Log-in, ja que si intenta accedir a algun dels apartats del menú, se li mostrarà un missatge indicant-li que primer de tot ha d'iniciar sessió.

5.2.2 Pantalla de Log-in

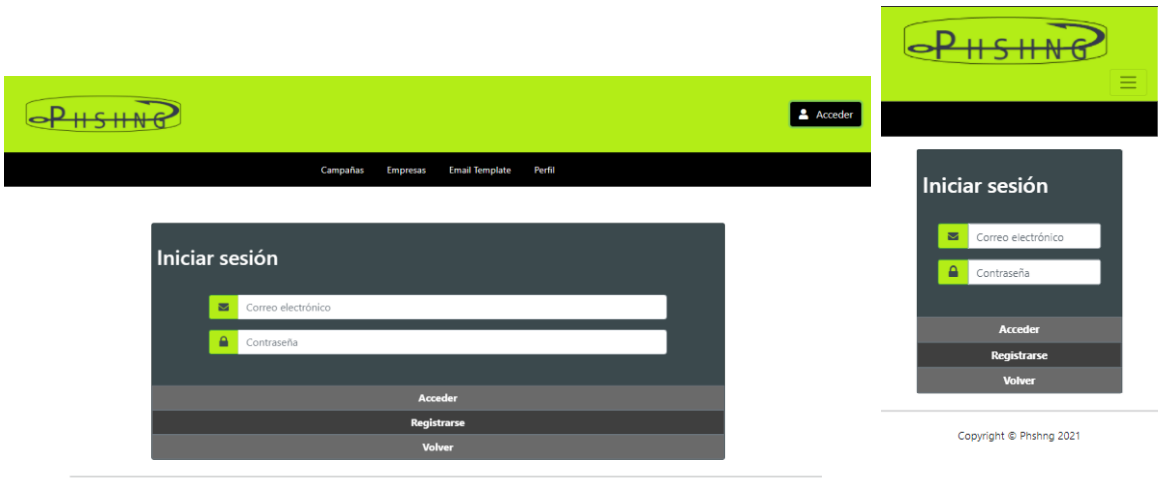


Fig. 43 Disseny responsive de la pantalla de Log-in (Font: Pròpia)

En aquesta pantalla, l'usuari podrà accedir al seu compte. En cas d'estar registrat, només haurà d'indicar el seu correu electrònic i la contrasenya i automàticament el sistema recorrerà la taula de comptes de la base de dades i en cas d'existir el compte que s'ha indicat, aquest serà redirigit a la pantalla principal i sinó es mostrarà un missatge d'error.

L'usuari també tindrà l'opció de navegar entre les pantalles principals i de registre mitjançant els botons que es poden veure en la part de sota del formulari de la figura Fig. 43.

5.2.3 Pantalla de registre

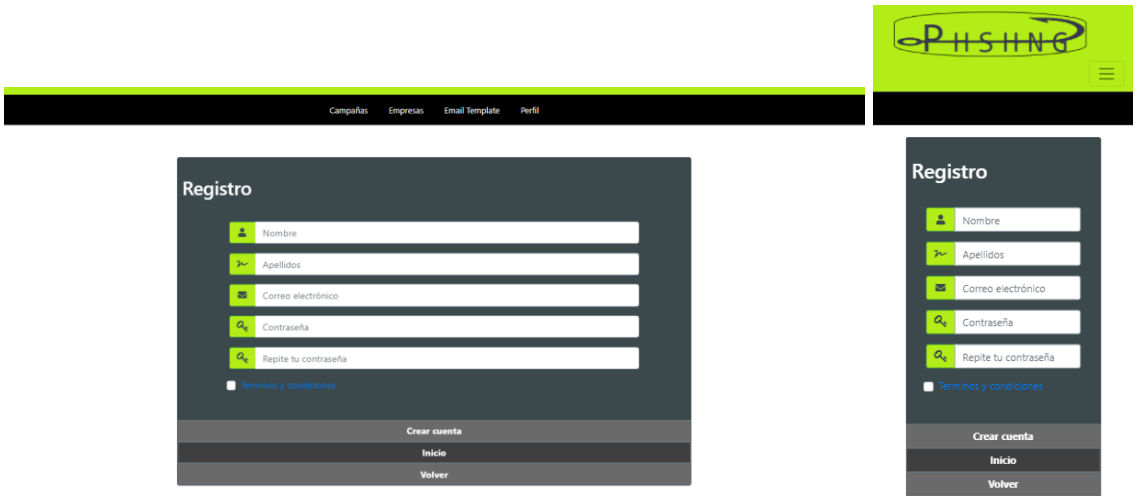


Fig. 44 Disseny responsive de la pantalla de registre (Font: Pròpia)

Amb un disseny semblant al de la pantalla de Log-in, la pantalla de registre fa la mateixa funcionalitat. En aquesta, es demanaran el nom, cognom, correu electrònic, contrasenya i acceptar els termes i condicions de la web (PDF al que pot accedir fent clic sobre del text de la casella de secció), i en cas que el correu electrònic no estigui ja registrat en la web, es farà un registre d'aquest compte a la base de dades i automàticament es farà el Log-in d'aquest usuari a la web, redirigint-lo a la pantalla principal.

Així com en el cas de la pantalla anterior, l'usuari podrà navegar cap a la pantalla de Log-in fent servir el menú que hi ha sota del formulari.

5.2.4 Pantalla d'empreses

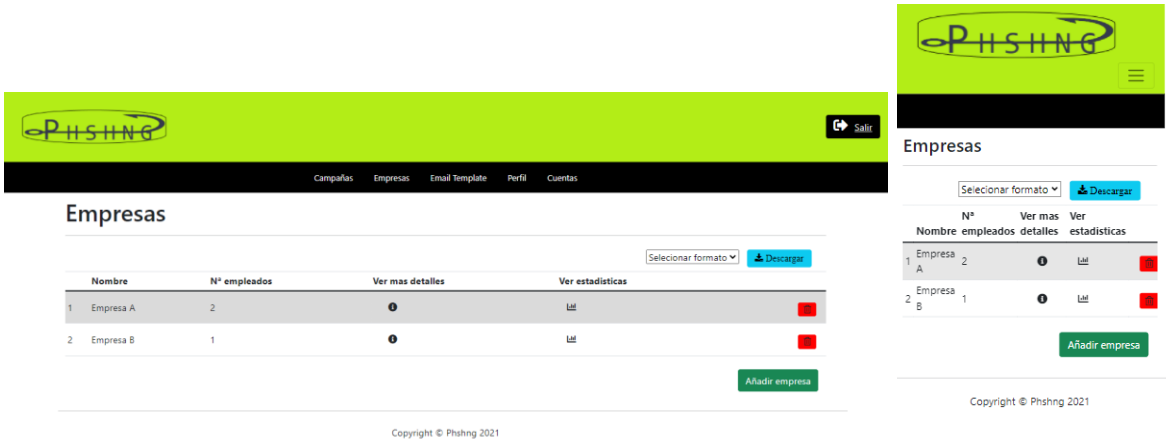


Fig. 45 Disseny responsive de la pantalla d'empreses (Font: Pròpia)

En aquesta pantalla, l'usuari tindrà una llista de totes les empreses registrades en el seu compte i podrà descarregar la llista d'aquestes empreses tant en format csv com json. Mitjançant els botons disponibles en la llista, es podran fer les següents accions:

- Veure més detalla de l'empresa: S'obre una finestra emergent on es mostren els empleats d'aquesta.
- Veure estadístiques: L'usuari serà redirigit a la pantalla d'estadístiques de l'empresa en concret, on podrà observar una llista de tots els usuaris d'aquesta empresa i el número de campanyes en les quals aquest ha caigut aquest.
- Eliminar empresa: S'obre una finestra emergent per a confirmar o rebutjar l'eliminació de l'empresa.

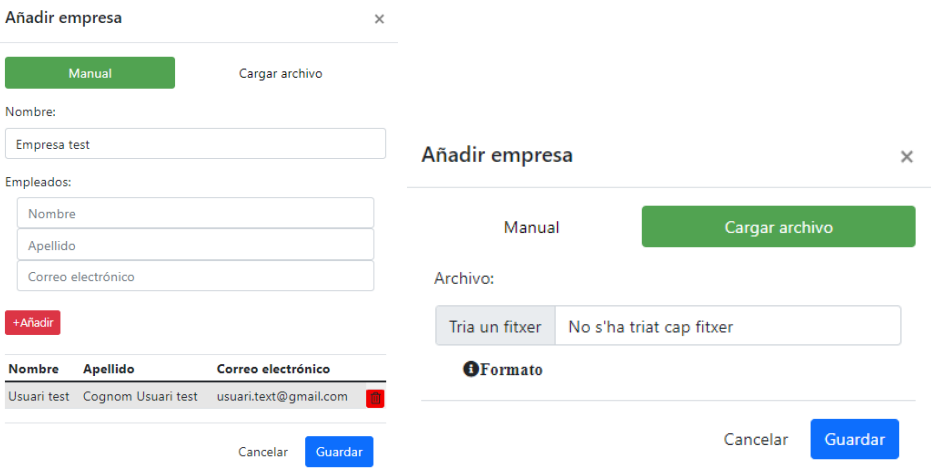


Fig. 46 Finestres emergent per a afegir empresa (Font: Pròpia)

Tal com s'ha pogut observar en la taula d'històries d'usuari, en aquesta pantalla es podran afegir noves empreses tant manualment com en format csv o json. Això es podrà fer a mitjançant el botó verd de sota que es pot observar en la figura anterior, mitjançant el qual s'obrirà una finestra emergent per a afegir l'empresa. Veure figura, Fig. 46.

- Manualment: Es demana el nom de l'empresa i a continuació es poden afegir tants empleats com es desitgin, tot indicant nom, cognom i correu electrònic.
- Mitjançant fitxer json o csv: Seleccionant el fitxer des del mateix ordinador. Aquest fitxer haurà d'estar estructurant idènticament al format que es demana. Format que es pot veure accedint a l'enllaç (Botó amb l'etiqueta "Formato") que hi ha sota l'input demanat.

5.2.5 Pantalla de plantilles de correus electrònics

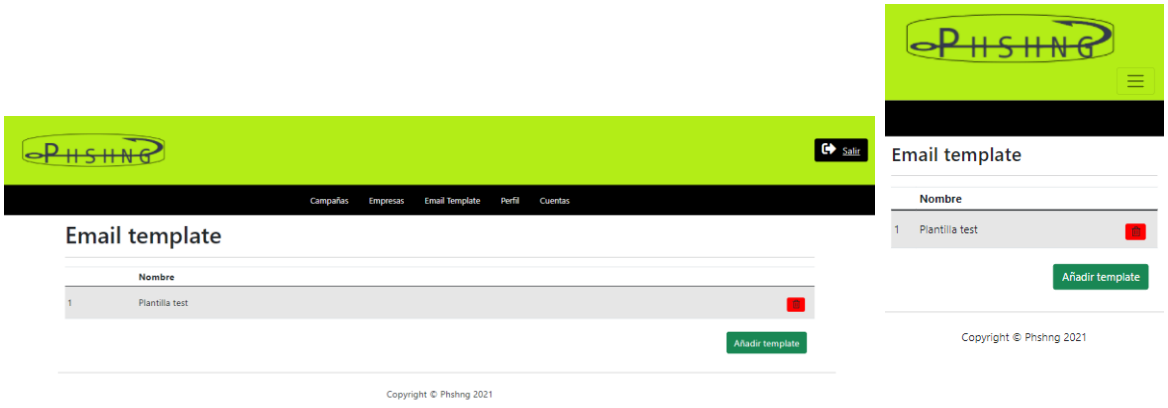


Fig. 47 Disseny responsive de la pantalla de plantilles de correu electrònic (Font: Pròpia)

Seguint amb el disseny de l'anterior pantalla, en aquesta l'usuari podrà veure totes les plantilles de correu electrònic de les que disposa, eliminar-ne alguna o afegir-ne alguna de nova mitjançant el botó inferior de la llista.

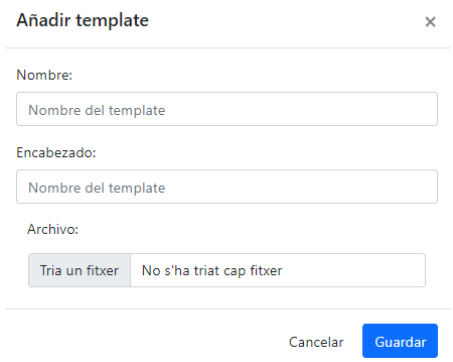


Fig. 48 Finestra emergent per a afegir plantilla (Font : Pròpia)

En cas de voler afegir alguna nova plantilla, s'obrirà la finestra emergent com la que es pot observar en la figura anterior, en la qual haurà d'indicar, el nom amb el qual la vol distingir, l'encapçalat que portarà el correu quan s'enviï i finalment haurà de seleccionar el fitxer HTML a fer servir.

5.2.6 Pantalla de campanyes

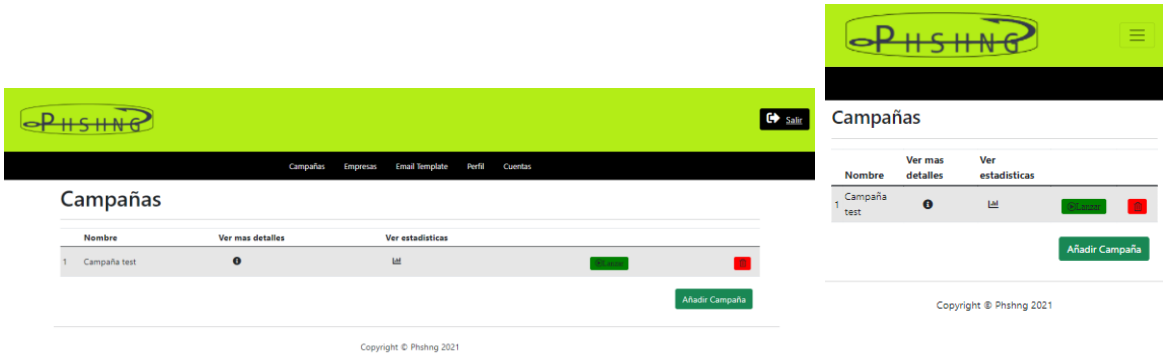


Fig. 49 Disseny responsive de la pantalla de campanyes (Font: Pròpia)

Amb un disseny igual a les altres pantalles, aquí l'usuari podrà crear les campanyes que desitja i veure les que ja té creades. Seguint també amb el funcionament de les altres pantalles, l'usuari podrà fer les següents accions a partir dels botons disponibles en la llista:

- Veure més detalls: S'obre una finestra emergent on es poden veure amb detall les característiques d'aquesta campanya, com empreses afectades, URL a redirigir, data de finalització, etc.

- Accedir a la pantalla d'estadístiques de la campanya: L'usuari serà redirigit a aquesta pantalla. Aquesta acció només estarà disponible en el cas que la campanya s'hagi llançat, en cas contrari, s'informarà mitjançant un missatge per pantalla.
- Llançar la campanya: La campanya serà llançada. Aquesta acció trigar més temps que les altres, ja que s'hauran d'enviar correus a tots els empleats de les empreses per les quals s'ha creat aquesta campanya.
- Eliminar la campanya: S'obre una finestra emergent per a confirmar o rebutjar l'eliminació de la campanya.

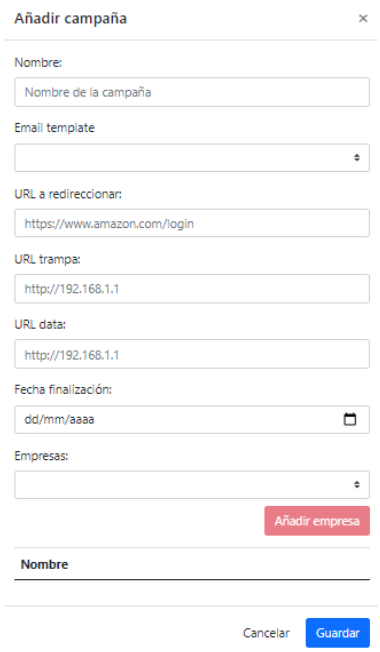


Fig. 50 Finestra emergent per a afegir campanya (Font : Pròpia)

Per tal d'afegir una nova campanya, es mostrarà la finestra emergent de la figura, Fig. 50. Aquí l'usuari haurà d'indicar el nom de la campanya, seleccionar una plantilla de correu electrònic a fer servir, URL a redirigir, URL de la pàgina trampa, URL des d'on s'extrauran les dades de la pàgina trampa, data de finalització de la campanya i finalment indicar les empreses a les quals s'enviarà aquesta campanya.

Un aspecte a destacar és que en cas de no disposar de cap plantilla o cap empresa registrada, no es podran crear noves campanyes.

5.2.7 Pantalla d'estadístiques d'una campanya

Fig. 51 Disseny responsive de la pantalla de plantilles d'estadístiques d'una campanya (Font: Pròpia)

En aquesta pantalla, l'usuari podrà monitoritzar les campanyes llançades. Com es pot veure en la figura superior, es mostra un gràfic de dònut on s'hi distingeixen la part pertanyent a totes les víctimes a les quals s'ha llançat la campanya i no han caigut i la part pertanyent a les víctimes de cada una de les empreses a les quals s'ha llançat aquesta campanya. Sota d'aquest gràfic, s'ha afegit una nota informativa juntament amb un botó, el qual permet redimensionar el gràfic perquè sigui visible a qualsevol dispositiu.

Finalment, a la part de sota de tot, es mostra una llista de les víctimes que han anat caient en la campanya, amb el seu nom, cognom, correu electrònic, contrasenya i data en la qual ha caigut.

5.2.8 Pantalla del perfil

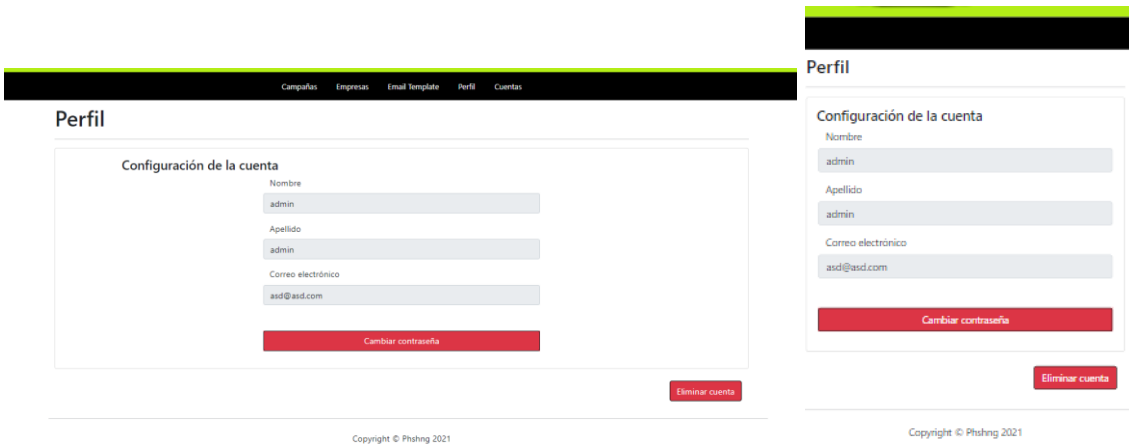


Fig. 52 Disseny responsive de la pantalla de plantilles del perfil(Font: Pròpia)

En aquesta pantalla, l'usuari podrà veure les dades respectives al seu compte, eliminar aquest compte o canviar la contrasenya a través del botó de sota del formulari (Fig. 53) per tal de millorar la seguretat d'aquest.

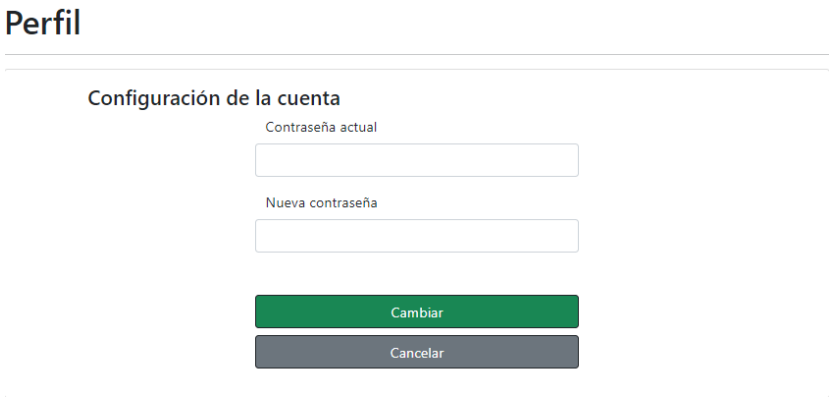


Fig. 53 Configuració de canvi de contrasenya (Font: Pròpia)

5.2.9 Pantalla d'administració de comptes

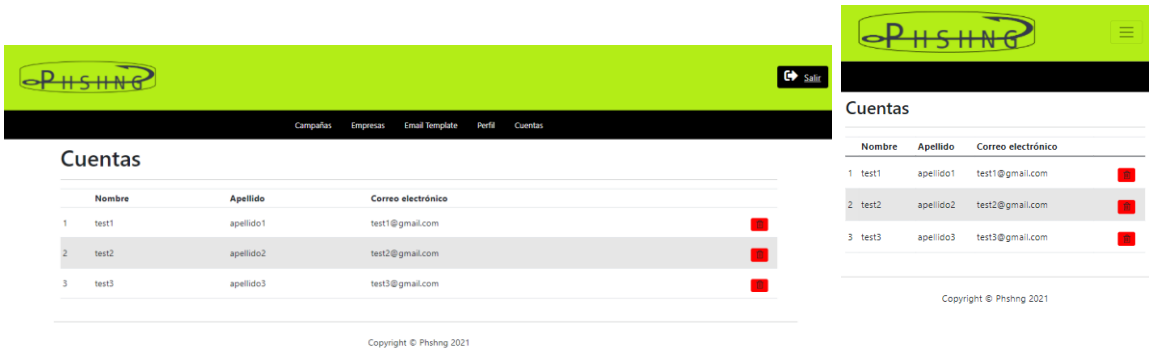


Fig. 54 Disseny responsive de la pantalla d'administració de comptes (Font: Pròpia)

Com s'ha comentat anteriorment, a aquesta pantalla comes hi tindran accés els usuaris amb rol d'administrador, ja que en aquesta es podran eliminar qualsevol dels comptes registrats en la web. El funcionament és senzill, es té una llista amb tots els comptes i un botó per a eliminar. En pressionar aquest botó, sobre una finestra emergent en la qual es confirma o cancel·la aquesta acció.

6 Proves

Per tal de poder visualitzar un exemple d'una campanya, s'ha creat una intentant imitar el que seria la pàgina d'inici de sessió de Netflix i fent servir víctimes fictícies. En aquest apartat es veuran alguns dels aspectes més representatius d'aquesta.

6.1 Campanya Netflix

Quant a la pantalla d'imitació a la d'inici de sessió de Netflix, s'ha creat una nova pàgina fent servir les mateixes tecnologies que les esmentades en l'apartat de, 5.1 Tecnologies utilitzades. Aquesta serà l'encarregada de recollir les dades de les víctimes i guardar-les en la seva base de dades per a posteriorment ser recollides per la web PHSHNG. En la figura següent es pot observar una visualització d'aquesta.

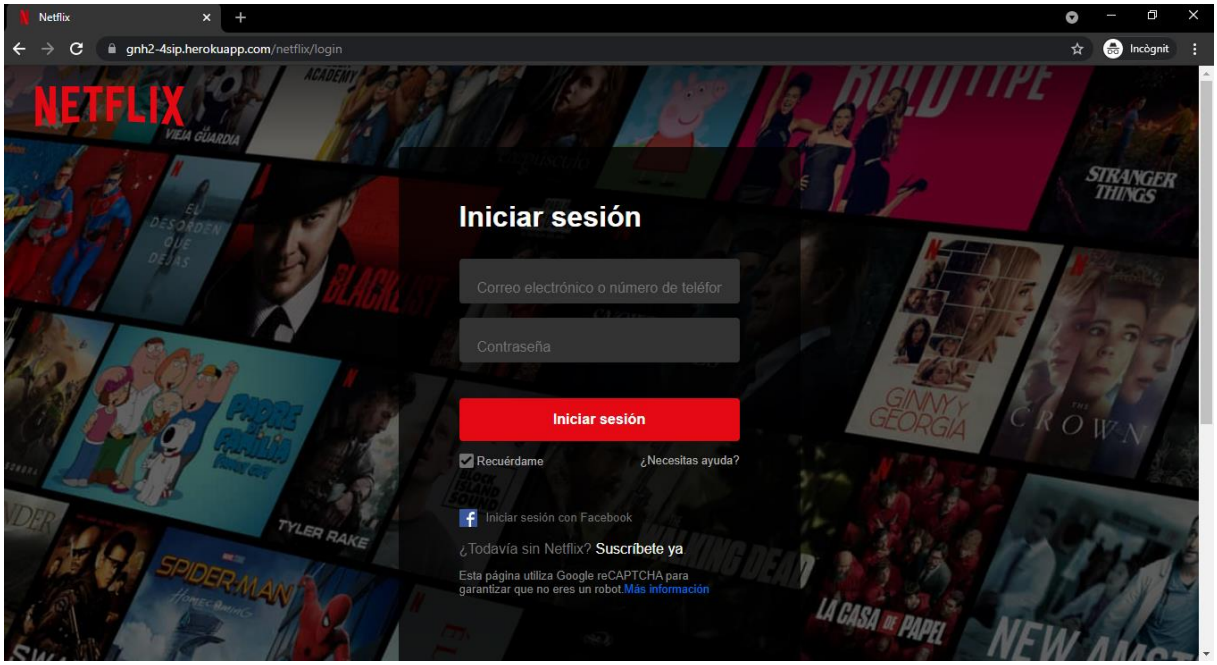


Fig. 55 Pantalla d'inici de sessió a Netflix de la web trampa (Font: Pròpia)

Com s'ha comentat anteriorment, ha arribat un moment en el qual Chrome ja detecta aquesta pàgina com a maliciosa i al intentar accedir a ella amb la configuració de Navegació segura activada et dóna un avís que s'està intentant accedir a un lloc web enganyós.

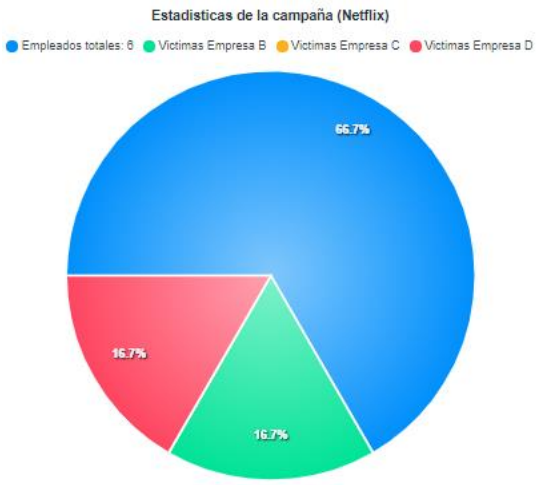
Un altre aspecte a comentar és l'URL que s'ha fet servir. Per defecte, s'ha fet servir el domini que dóna Heroku en fer el Deployment d'una web, però per tal de maquillar una mica més aquest domini i que no sembli el d'una pàgina maliciosa, s'ha afegit "/netflix/login/".

Pel que fa al correu electrònic a enviar a les víctimes, s'ha aprofitat un HTML d'una campanya de phishing comentada per Luis Lubeck en un dels seus documents (31).

Fig. 56 Correu electrònic enviat (Font: Gmail)

En la figura superior, es pot observar el correu electrònic enviat a les víctimes. Aquestes un cop facin clic sobre el botó “Actualizar datos” seran redirigits a la pàgina trampa i un cop hagin introduït les seves credencials tornaran a ser redirigits a la pàgina oficial d’inici de sessió de Netflix. I arribats a aquest punt només ens queda tornar a la web PHSHNG i esperar que les víctimes caiguin en la campanya.

Si ens redirigim a les estadístiques de la campanya, podrem observar totes les víctimes que han anat caient en la campanya i les seves credencials.

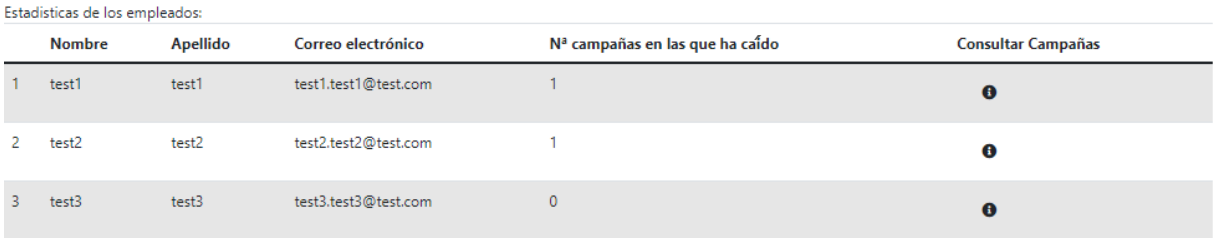


Victimas:

Nombre	Apellido	Email	Contraseña	Fecha
test	test	phshng.suport@gmail.com	contraseñatest	06/15/2021 - 11:34:20
test1	test1	test1.test1@test.com	contraseñatest1	06/15/2021 - 11:35:20
test2	test2	test2.test2@test.com	contraseñatest2	06/15/2021 - 11:35:50
test4	test4	test4.test4@test.com	contraseñatest4	06/15/2021 - 11:36:07

Fig. 57 Estadística de la campanya creada (Font: Pròpia)

I si ens dirigim cap a les estadístiques d'una empresa, podem observar les estadístiques de cada un dels empleats d'aquesta juntament amb les campanyes en les quals ha sigut víctima.


Estadisticas de los empleados:

	Nombre	Apellido	Correo electrónico	Nª campañas en las que ha caído	Consultar Campañas
1	test1	test1	test1.test1@test.com	1	
2	test2	test2	test2.test2@test.com	1	
3	test3	test3	test3.test3@test.com	0	

Fig. 58 Estadístiques d'una empresa (Font: Pròpia)

Tant les URLs com la plantilla que s'han fet servir per a llançar aquesta campanya de prova es poden trobar en els annexos, juntament amb altres per a fer-ne d'altres. (Documentació per al testing)

7 Conclusions i millores.

Tot i que aquest projecte compleix amb l'objectiu principal, plantejat al començament, de crear una web que sigui capaç de llançar i monitoritzar una campanya de phishing, també hi ha aspectes en el que es pot millorar alguna cosa per tal de tenir una millor web de cara a projectes futurs. Alguns d'aquests són els següents:

- **Base de dades més persistent**: Aquest és un dels aspectes més destacats a millorar, ja que, com s'ha comentat en la secció Heroku, tal com està creada actualment la web, en cas de no rebre alguna petició durant un període de 30 minuts, la base de dades es reinicialitza. És per això, que de cara a un projecte futur, una idea podria ser fer servir un servidor local [9.1] on emmagatzemar les dades o fer servir altres plataformes PaaS més persistents a canvis com per exemple S3 d'Amazon (32).
- **Correu electrònic de contacte**: Per tal d'obtenir feedback dels usuaris, una idea seria facilitar un correu electrònic de contacte per a aquests i crear una secció dins de la web perquè aquests enviïn les seves opinions o denunciïn un mal ús de la web.
- **Monitoritzar campanyes**: Tot i que la versió actual monitoritza les víctimes de les campanyes, es podria afegir noves gràfiques en l'apartat d'estadístiques per tal d'observar quins són els empleats que han obert el correu electrònic enviat o quins han accedit a la pàgina trampa, però no han facilitat les seves credencials.
- **Correu electrònic de prova**: Per tal de provar el coreu electrònic que s'enviarà a les possibles víctimes, permetre que l'usuari pugui provar aquest correu enviant-se'l a si mateix.
- **Noves pàgines trampa**: Tal com s'ha creat aquest projecte, no es permeten crear campanyes des de la web principal (PHSHNG) sinó que s'ha de crear a part i passar-li les URLs a aquesta. És per aquest motiu que seria una millora bastant important permetre crear pàgines trampa des de la mateixa web, facilitant així la feina als usuaris.

Durant la realització del projecte, també han sorgit certs problemes que han fet alentir el desenvolupament. Aquests són els més destacats:

- Que al cap d'un temps la SMTP (Gmail) que s'estava fent servir per a enviar els correus electrònics deixes de funcionar. En un començament no es va entendre que estava passant, però després de dies cercant informació es va observar que el motiu era que s'havia detectat la URL com a enganyosa i Gmail no permetia enviar correus on hi constes aquesta URL.
- Que les dades s'eliminessin de la base de dades al cap d'un temps: Com s'ha comentat anteriorment, això va ser degut a la plataforma PaaS que s'estava fent servir i el fet que no s'hagués fet el Deployment molt més abans, va provocar que no donés tems a migrar aquest Deployment a una altra plataforma PaaS, ja que en un principi era inconscient d'aquest inconvenient de Heroku.
- Aconseguir una web totalment responsive.

Tot i això, la realització d'aquest projecte ha suposat la consolidació de coneixements, habilitats adquirides i eines utilitzades en les diferents assignatures cursades durant el grau. També s'han après noves tècniques orientades a la programació d'aplicacions web, ja que el fet d'haver de crear una web sense cap referència i sense unes pautes concretes a seguir quant al disseny, han donat una facilitat quant a la decisió de quina forma o no s'havia de realitzar cada funcionalitat.

Finalment, agrair tant al meu tutor, Raül Roca Cànovas, pels consells que m'ha donat tant en aquest projecte com en les seves assignatures, com a tots els altres professors del grau pels coneixements que m'han brindat els darrers anys. També agrair a tots els meus companys, amics, i família per haver estat sempre al meu costat i haver-me donat suport en totes les meves decisions.

8 Referències

1 Sword, W. (2021). *AtlasVPN*. Recollit de https://atlasvpn.com/blog/cyberattacks-surge-by-33-in-a-year

2 INTERPOL. (2020). *INTERPOL*. Retrieved from https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

3 Ouniri, A. A. (2021). *Trello*. Recollit de https://trello.com/b/idj9ooeA/tfg-phshng

4 Wright, J. (2012). *Gophish*. Recollit de https://getgophish.com/documentation/

5 Gurvich, P. (2018). *Infection Monkey*. Recollit de https://www.guardicore.com/infectionmonkey/

6 MITRE. (2020). *CALDERA*. Recollit de https://github.com/mitre/caldera

7 Picus Security. (2013). *Picus Security*. Recollit de https://www.picussecurity.com/

8 *Lucy Security*. (2015). Recollit de https://lucysecurity.com/es/simulaciones-de-ataques/

9 Piacentini, M. (2003). *sqlitebrowser*. Recollit de https://sqlitebrowser.org/

10 Ronacher, A. (2004). *Flask*. Recollit de https://flask.palletsprojects.com/en/2.0.x/

11 Burey, K., Conroy, K., Stratton, F., & Binet, G. (2012). *Flask-RESTful*. Recollit de https://flask-restful.readthedocs.io/en/latest/

12 Bayer, M. (2006). *Flask-SQLAlchemy*. Recollit de https://flask-sqlalchemy.palletsprojects.com/en/2.x/

13 Grinberg, M. (2013). *Flask-Migrate*. Recollit de https://flask-migrate.readthedocs.io/en/latest/

14 Dolphin, C. (2014). *Flask-CORS*. Recollit de https://flask-cors.readthedocs.io/en/latest/

15 Wright, M., Jacob, D., & DuPlain, R. (2010). *Flask-mail*. Recollit de https://pythonhosted.org/Flask-Mail/

16 You, E. (2014). *Vue.js*. Recollit de https://es.vuejs.org/

17 Pérez, E. I. (2019). *Códigofacilito*. Recollit de https://codigofacilito.com/articulos/que-es-vue

18 Megan, A., Müler, J., Mosin, V., & Morehous, T. (2016). *BootstrapVue*. Recollit de https://bootstrap-vue.org/

19 Otto, M., & Thornton, J. (2011). *Bootstrap Documentation*. Recollit de https://getbootstrap.com/docs/5.0/getting-started/introduction/

20 Apexcharts. (2018). *Vue Charts*. Recollit de https://apexcharts.com/docs/vue-charts/

21 ApexCharts. (2017). *ApexCharts*. Recollit de https://apexcharts.com/docs/installation/

22 @cmp-cc. (2016). *Vue-cookies*. Recollit de https://www.npmjs.com/package/vue-cookies

23 Spolsky, A. J. (2010). *Trello*. Recollit de https://trello.com/es

24 Torvalds, L. (2007). *Git*. Recollit de https://git-scm.com/
25 Wanstrath, C., Heytt, P., Preston Werner, T., & Chacon, S. (2007). *GitHub*. Recollit de https://github.com/
26 Lindenbaum, J., Henry, O., & Wiggins, A. (2007). *Heroku*. Recollit de https://www.heroku.com/
27 Travis Ci community. (2011). *Travis Ci*. Recollit de https://travis-ci.com/
28 Kirkendall, R. (2000). *Namecheap*. Recollit de https://www.namecheap.com/
29 Asthana, A., Sobti, A., & Kane, A. (2014). *Postman*. Recollit de https://www.postman.com/
30 Drmic, S. (2020). *Pomodor*. Recollit de https://pomodor.app/timer
31 Lubeck, L. (2020). *Welivesecurity*. Recollit de https://www.welivesecurity.com/la-es/2020/08/17/phishing-netflix-intenta-hacer-creer-cuenta-suspendida/
32 Amazon. (2014). *AWS*. Recollit de https://aws.amazon.com/es/s3/
33 C0r0n1con Congreso. (2020). Youtube. Recollit de https://www.youtube.com/watch?v=7SRucfPPiHo
34 Belcic, I. (2020). *Avast*. Recollit de https://www.avast.com/es-es/c-phishing
35 Gophish. (2012). *Github*. Recollit de https://github.com/gophish/gophish
36 Pankaj. (2019). *JournalDev.* Recollit de https://www.journaldev.com/16774/sql-data-types
37 Garza. G. (2020) *StackOverflow*. Recollit de https://es.stackoverflow.com/questions/371647/por-qu%C3%A9-heroku-elimina-las-im%C3%A1genes-que-subo-en-mi-aplicaci%C3%B3n
38 *Wikipedia*. Recollit de https://es.wikipedia.org/wiki/Phishing
39 *Vue.js Examples.* Recollit de https://vuejsexamples.com/
40 Printed, P. (2019). *Youtube.* Recollit de https://www.youtube.com/watch?v=48Eb8JuFuUI

9 Annex

9.1 Glossari

- Phishing: Estafa que té com a objectiu obtenir a través d'internet dades privades dels usuaris, especialment per accedir a comptes o dades bancàries.
- Disseny Responsive: Tècnica de disseny web que busca la correcta visualització d'una mateixa pàgina en diferents dispositius.
- Daily Scrum: Reunions diàries portades a terme pels integrants d'un equip en les que es responen les següents preguntes: Que s'ha fet ahir? Que es farà avui? Ha sorgit algun problema?
- Burdown Chart: Aquest és un gràfic que mostra el treball pendent per a acabar totes les tasques del sprint, en funció dels dies que queden per a l'entrega d'aquest.
- Històries d'usuari: Les històries d'usuari són petites descripcions de tots els requeriments que ha de complir el projecte final i que són especificades pel client
- Product Backlog: Taula on es troben presents totes les històries d'usuari del projecte en concret.
- Story Points : Sistema de puntuació segons la dificultat de les històries d'usuari, que pot prendre valors de la sèrie de Fibonacci.
- SQLAlchemy: Llibreria utilitzada per a crear bases de dades i manipular les dades d'aquestes sense la necessitat d'usar SQL.
- DB Browser for SQLite: Aplicació gratuïta de codi obert dissenyada per facilitar la creació i administració de les bases de dades amb SQLite.
- Framework: Es tracta d'una eina que ens dóna un esquema de treball i una sèrie d'utilitats i funcions que ens facilita la construcció de pàgines webs dinàmiques.
- End-Points: Es tracta de les URLs d'una API o un Backend que responen a les peticions del client. Aquests mateixos End-Points, han d'anar acompanyats d'un altre End-Points per a existir.

- SMTP (Simple Mail Transfer Protocol): Protocol que permet que els correus electrònics viatgin a través d'internat, és a dir, enviar un correu des d'un servidor d'origen o servidor sortint, a un servidor destí o servidor entrant.
- Client FTP: Aplicació o programa que permet pujar fitxers mitjançant el protocol FTP(File Transfer Protocol).
- PaaS (Platafor as a Service): Servei en el núvol a través del qual el proveïdor proporciona al client un entorn de desenvolupament, així com les eines necessàries per al desenvolupament de noves aplicacions.
- Deployment: Fa referència a l'acció de portar el codi a producció. En altres paraules, en el cas de voler visualitzar una web a tothom, aquesta s'haurà de fer un deploy a un servidor en el núvol.
- Servidor local: Computadora encarregada de respondre a les peticions que se li fan a la qual es pot accedir mitjançant l'URL localhost o 127.0.0.1.

9.2 Figures

Figura A1: Product Backlog

User story	Descripció	Prioritat	Dificultat	Hores estimades
US-1	Com a usuari, vull fer el log-in per a poder accedir al meu compte.	Alta	2	4
US-2	Com a usuari, vull fer log-out per sortir del meu compte.	Baixa	1	2
US-3	Com a usuari no registrar, vull registrar-me a la web per a tenir un compte.	Alta	3	6
US-4	Com a usuari, vull afegir una empresa per a poder crear una campanya amb aquesta.	Mitja	3	3
US-5	Com a usuari, vull eliminar una empresa per deixar de tenir-la en el meu compte.	Baixa	1	1
US-6	Com a usuari, vull afegir empleats per a poder crear una campanya amb aquests.	Mitja	2	2
US-7	Com a usuari, vull eliminar els empleats de "x" empresa per deixar de tenir-los en el meu compte.	Baixa	1	1
US-8	Com a usuari, vull afegir una campanya per a poder llançar-la.	Mitja	8	8
US-9	Com a usuari, vull eliminar una campanya per a deixar de tenir-la en el meu compte.	Baixa	2	2
US-10	Com a usuari, vull afegir un plantilla de correu electrònic per tal d'enviar correus mitjançant d'aquest.	Mitja	2	2
US-11	Com a usuari, vull eliminar un plantilla de correu electronic per a deixar de tenir-lo en el meu compte.	Baixa	1	1
US-12	Com a usuari, vull veure la llista de campanyes per tal de saber quines tinc registrades.	Baixa	1	1
US-13	Com a usuari, vull veure la llista d'empreses per tal de saber quines tinc registrades.	Baixa	1	1
US-14	Com a usuari, vull veure la llista de plantilles de correu electrònic per al de saber quins tinc registrats.	Baixa	1	1
US-15	Com a usuari, vull veure les estadístiques d'una campanya per a saber quins empleats han caigut en ella.	Alta	21	30
US-16	Com a usuari, vull poder canviar la meva contrasenya per tal de assegurar millor el meu compte.	Mitja	3	2
US-17	Com a usuari, vull veure les estadístiques d'una empresa per a saber quins empleats han caigut en alguna campanya.	Alta	5	6

US-18	Com a usuari, vull llaçar una campanya per tal de comprovar la seguretat dels meus empleats.	Alta	13	15
US-19	Com a usuari, vull poder veure el meu perfil.	Mitja	5	4
US-20	Com a usuari, tant registrat com no, vull poder acceptar o rebutjar les cookies.	Baixa	3	3
US-21	Com a usuari, vull veure els detalls de les meves campanyes per tal de saber com han estat configurades.	Baixa	2	2
US-22	Com a usuari, vull veure els detalls de les meves empreses per tal de saber com han estat configurades.	Baixa	2	2
US-23	Com a usuari, vull poder descarregar la llista d'empreses registrades en el meu compte	Mitja	5	3
US-24	Com a usuari administrador, vull veure els comptes que registrats en la web, per tal de tenir un registre d'aquests.	Baixa	3	3
US-25	Com a usuari administrador, vull poder eliminar un compte en el cas de que es produeixi un mal us de la web.	Baixa	1	1
US-26	Com a usuari, vull eliminar el meu compte per tal de deixar d'estar en el registre de la web.	Baixa	2	3
User Story al que pertany	**Descripció**	**Prioritat**	**Dificultat**	**Hores estimades**
X	Implementació de la vista de la pagina principal	Baixa	3	5
US-1-2-3	Implementació de les vistes de registre i accés a la web	Mitja	5	6
US-4-5	Implementació de la vista de la pagina d'empreses	Mitja	3	4
US-8-9-18	Implementació de la vista de la pagina de campanyes	Alta	5	8
US-10-11	Implementació de la vista de la pagina de les plantilles de correu electrònic	Mitja	3	4
US-17	Implementació de la vista d'estadístiques d'una empresa	Mitja	3	4
US-15	Implementació de la vista d'estadístiques d'una campanya	Alta	13	10
US-16-19	Implementació de la vista del perfil	Mitja	3	5
X	Integració continua del treball utilitzant Travis.com	Alta	5	6
X	Documentació	Alta	X	100
X	Memòria	Alta	X	100

Figura A2: Casos d'ús

Cas d'us	1
Actores	Administrador, Usuari no registrat, Usuari registrat.
Descripció	Accedir a la pàgina principal.
Pre-condicions	N/A
Flux principal	1. Usuari: Accedeix a la pagina principal mitjançant la URL. 2. Sistema: Processa petició. 3. Usuari: Navega per la pàgina principal.
Flux alternatiu	2.1 La pagina no esta disponible, mostrar missatge.

Cas d'us	2
Actores	Administrador, Usuari no registrat.
Descripció	Crear compte.
Pre-condicions	1. No estar registrat. 2. Estar en la pantalla de registre
Flux principal	1. Usuari: Accedeix a la pantalla de registre a través de la de Log-in. 2. Sistema: Processa petició. 3. Usuari: Introdueix les dades demanades. 4. Usuari: Fa clic en el botó de registrar. 5. Sistema: Processa la petició. 6. Sistema: Redirigeix a la pàgina d'inici, iniciant sessió al compte de l'usuari.
Flux alternatiu	5.1 Les contrasenyes introduïdes per l'usuari son diferents. 5.2 Es mostra un missatge d'error. 5.1 L'usuari es deixa alguna altre dada per introduir. 5.2 Es mostra un missatge d'error.

Cas d'us	3
Actores	Administrador, Usuari registrat.
Descripció	Eliminar el propi compte.
Pre-condicions	1. Estar registrat. 2. Estar en la pantalla del perfil.
Flux principal	1. Usuari: Accedeix a la pantalla del perfil. 2. Sistema: Processa petició. 3. Usuari: Fa clic en el botó d'eliminar compte. 4. Sistema: Processa la petició i mostra un finestra emergent demanant confirmació. 5. Usuari: Fa clic en el botó d'acceptar. 6. Sistema: Processa la petició. 7. Sistema: Redirigeix a la pagina d'inici, havent eliminat el compte de l'usuari.
Flux alternatiu	6.1 Es produeix qualsevol error. 6.2 Es mostra el missatge d'error i no s'elimina el compte.

Cas d'us	4
Actores	Administrador, Usuari registrat.
Descripció	Accedir al compte (Log-in).

Pre-condicions	1. Estar registrat. 2. Estar en la pantalla de Log-in.
Flux principal	1. Usuari: Fa clic en el boto d'identificar-se. 2. Sistema: Processa petició. 3. Sistema: Redirigeix a l'usuari a la pantalla de Log-in. 4. Usuari: Introdueix el coreu electrònic i la contrasenya. 5. Sistema: Processa la petició. 6. Sistema: Redirigeix a la pagina d'inici, iniciant sessió al compte de l'usuari.
Flux alternatiu	5.1 L'usuari introdueix un correu electrònic o contrasenya incorrecta. 5.2 Es mostra el missatge d'error mostrant el motiu d'aquest.

Cas d'us	5
Actores	Administrador, Usuari registrat.
Descripció	Sortir del compte (Log-out).
Pre-condicions	1. Estar registrat.
Flux principal	1. Usuari: Fa clic en el boto Sortir. 2. Sistema: Processa petició. 3. Sistema: Redirigeix a la pagina d'inici, sortir del compte de l'usuari.
Flux alternatiu	2.1 Es produeix qualsevol error en la petició 2.2 Es mostra el missatge d'error mostrant el motiu d'aquest i es manté la sessió iniciada.

Cas d'us	6
Actores	Administrador, Usuari registrat.
Descripció	Afegir una empresa
Pre-condicions	1. Estar registrat. 2. Estar en la pantalla d'empreses.
Flux principal	1. Usuari: Fa clic en el boto d'afegir empresa. 2. Sistema: Processa petició i mostra la finestra emergent per introduir les dades. 3. Usuari: Introdueix les dades sol·licitades. 4. Usuari: Fa clic en el boto d'afegir. 5. Sistema: Processa la petició. 6. Sistema: Afegeix la empresa a la llista d'empreses i les mostra.
Flux alternatiu	Afegir empresa manualment: 5.1 Si l'usuari no ha introduït alguna dada respecte al nom de l'empresa o dades dels empleats. 5.2 Tanca la finestra emergent i mostra el missatge d'error. Afegir empresa a traves d'un fitxer csv o json: 5.1 L'usuari introdueix un fitxer que no segueix amb el format establert. 5.2 Es mostra un missatge d'error.

Cas d'us	7
Actores	Administrador, Usuari registrat.
Descripció	Eliminar una empresa.

Pre-condicions	1. Estar registrat. 2. Estar en la pantalla d'empreses.
Flux principal	1. Usuari: Fa clic en el boto disponible per eliminar una certa empresa. 2. Sistema: Processa petició i mostra la finestra emergent demanant confirmació. 3. Usuari: Fa clic en el boto de confirmar. 4. Sistema: Processa la petició. 5. Sistema: Mostra la llista d'empreses actualitzada
Flux alternatiu	4.1 Si es produeix algun error. 4.2 Mostrar el missatge d'error i no s'elimina la empresa.

Cas d'us	8
Actores	Administrador, Usuari registrat.
Descripció	Afegir una plantilla de correu electrònic.
Pre-condicions	1. Estar registrat. 2. Estar en la pantalla de plantilles de correu electrònic.
Flux principal	1. Usuari: Fa clic en el boto d'afegir plantilla. 2. Sistema: Processa petició i mostra la finestra emergent per introduir les dades. 3. Usuari: Introdueix les dades sol·licitades. 4. Usuari: Fa clic en el boto d'afegir. 5. Sistema: Processa la petició. 6. Sistema: Afegeix la plantilla a la llista de plantilles i les mostra.
Flux alternatiu	5.1 Si l'usuari no ha introduït alguna dada. 5.2 Tanca la finestra emergent i mostra el missatge d'error.

Cas d'us	9
Actores	Administrador, Usuari registrat.
Descripció	Eliminar una plantilla de correu electrònic.
Pre-condicions	1. Estar registrat. 2. Estar en la pantalla de plantilles de correu electrònic.
Flux principal	1. Usuari: Fa clic en el boto disponible per eliminar una certa plantilla. 2. Sistema: Processa petició i mostra la finestra emergent demanant confirmació. 3. Usuari: Fa clic en el boto de confirmar. 4. Sistema: Processa la petició. 5. Sistema: Mostra la llista d'empreses actualitzada
Flux alternatiu	4.1 Si es produeix algun error. 4.2 Mostrar el missatge d'error i no s'elimina la plantilla.

Cas d'us	10
Actores	Administrador, Usuari registrat.
Descripció	Afegir una campanya.
Pre-condicions	1. Estar registrat. 2. Estar en la pantalla de campanyes.

	3. Tenir registrades al menys alguna empresa i una plantilla de correu electrònic.
Flux principal	1. Usuari: Fa clic en el boto d'afegir campanya. 2. Sistema: Processa petició i mostra la finestra emergent per introduir les dades. 3. Usuari: Introdueix les dades sol·licitades. 4. Usuari: Fa clic en el boto d'afegir. 5. Sistema: Processa la petició. 6. Sistema: Afegeix la plantilla a la llista de plantilles i les mostra.
Flux alternatiu	5.1 Si l'usuari no ha introduït alguna dada. 5.2 Tanca la finestra emergent i mostra el missatge d'error.

Cas d'us	11
Actores	Administrador, Usuari registrat.
Descripció	Eliminar una campanya.
Pre-condicions	3. Estar registrat. 4. Estar en la pantalla de campanyes.
Flux principal	6. Usuari: Fa clic en el boto disponible per eliminar una certa campanya. 7. Sistema: Processa petició i mostra la finestra emergent demanant confirmació. 8. Usuari: Fa clic en el boto de confirmar. 9. Sistema: Processa la petició. 10. Sistema: Mostra la llista d'empreses actualitzada
Flux alternatiu	4.1 Si es produeix algun error. 4.2 Mostrar el missatge d'error i no s'elimina la campanya.

Cas d'us	12
Actores	Administrador, Usuari registrat.
Descripció	Veure estadístiques d'una empresa.
Pre-condicions	1. Estar registrat. 2. Estar en la pantalla d'empreses. 3. Tenir registrada al menys alguna empresa.
Flux principal	1. Usuari: Fa clic en el boto per veure les estadístiques, disponible en cada una de les empreses. 2. Sistema: Processa petició 3. Sistema: Redirigeix a un altre pantalla amb les estadístiques.
Flux alternatiu	2.1 Si es produeix qualsevol error en la petició. 2.2 Mostra el missatge d'error i roman en la pantalla d'empreses.

Cas d'us	13
Actores	Administrador, Usuari registrat.
Descripció	Veure estadístiques d'una campanya.
Pre-condicions	1. Estar registrat. 2. Estar en la pantalla de campanyes. 3. Tenir registrada al menys alguna empresa. 4. Haver iniciat aquesta campanya.

Flux principal	1. Usuari: Fa clic en el boto per veure les estadístiques, disponible en cada una de les campanyes. 2. Sistema: Processa petició 3. Sistema: Redirigeix a la pantalla d'estadístiques.
Flux alternatiu	2.1 Si es produeix qualsevol error en la petició. 2.2 Mostra el missatge d'error per pantalla.

Cas d'us	14
Actores	Administrador, Usuari registrat.
Descripció	Editar el perfil.(Contrasenya)
Pre-condicions	1. Estar registrat. 2. Estar en la pantalla de perfil.
Flux principal	1. Usuari: Fa clic en el boto per editar la contrasenya. 2. Sistema: Processa petició 3. Sistema: Mostra un formulari per introduir les dades. 4. Usuari: Introdueix les dades demanades. 5. Sistema: Processa la petició 6. Sistema: Redirigeix a la pantalla de perfil amb la contrasenya actualitzada.
Flux alternatiu	5.1 Si l'usuari no ha introduït alguna dada. 5.2 Tanca la finestra emergent i mostra el missatge d'error.

Cas d'us	15
Actores	Administrador.
Descripció	Eliminar qualsevol compte.
Pre-condicions	3. Estar registrat. 4. Estar en la pantalla de comptes.
Flux principal	8. Usuari: Accedeix a la pantalla de comptes. 9. Sistema: Processa petició. 10. Usuari: Fa clic en el botó d'eliminar compte. 11. Sistema: Processa la petició i mostra un finestra emergent demanant confirmació. 12. Usuari: Fa clic en el botó d'acceptar. 13. Sistema: Processa la petició. 14. Sistema: Mostra la llista de comptes actualitzada.
Flux alternatiu	6.1 Es produeix qualsevol error. 6.2 Es mostra el missatge d'error i no s'elimina el compte.

Figura A3: Llista d'End-Points

Mètode	End-Point	Descripció
POST	/login	Permet fer el log-in a la web.
POST	/account	Permet afegir un nou compte.
GET	/account/<int:id>	Permet obtenir les dades d'un compte.
PUT	/account/<int:id>	Permet modificar les dades d'un compte.
DELETE	/account/<int:id>	Permet eliminar un compte.
GET	/accounts	Permet obtenir una llista de tots els comptes.
PUT	/account/<int:id>/change_password	Permet modificar la contrasenya.
GET	/account/<int:id>/company_list	Permet obtenir una llista de les empreses.
GET	/account/<int:id>/email_template_list	Permet obtenir una llista de les plantilles de correu electrònic.
GET	/account/<int:id>/campaign_list	Permet obtenir una llista de les campanyes.
GET	/company/<int:id>	Permet obtenir les dades d'una empresa.
POST	/company/<int:id>	Permet afegir una nova empresa
PUT	/company/<int:id>	Permet modificar una empresa.
DELETE	/company/<int:id>	Permet eliminar una empresa.
GET	/company/<int:id>/employees_list	Permet obtenir una llista dels empleats d'una empresa.
GET	/employee/<int:id>	Permet obtenir les dades d'un empleat.
POST	/employee/<int:id>	Permet afegir un nou empleat.
PUT	/employee/<int:id>	Permet modificar un empleat.
DELETE	/employee/<int:id>	Permet eliminar un empleat.
POST	/AddFallenCampaign/<int:id_employee>/<int:id_campaign>	Permet afegir un empleat a la llista de víctimes d'una campanya.
GET	/email_template/<int:id>	Permet obtenir les dades d'una plantilla de correu electrònic.
POST	/email_template/<int:id>	Permet afegir una nova plantilla de correu electrònic.
PUT	/email_template/<int:id>	Permet modificar una plantilla de correu electrònic.
DELETE	/email_template/<int:id>	Permet eliminar una plantilla de correu electrònic.
GET	/campaign/<int:id>	Permet obtenir les dades d'una campanya.
POST	/campaign/<int:id>	Permet afegir una nova campanya.
PUT	/campaign/<int:id>	Permet modificar una campanya.
DELETE	/campaign/<int:id>	Permet eliminar una campanya.
GET	/statistics/<int:id>	Permet obtenir les estadístiques d'una campanya.
POST	/statistics/<int:id>	Permet afegir noves estadístiques.
GET	/getData/<int:id>	Permet obtenir mes dades d'una campanya.
PUT	/changeState/<int:id>	Permet canviar l'estat en el que es troba una campanya.
POST	/startCampaign/<int:id>	Permet llançar una campanya.

9.3 Documentació per al testing

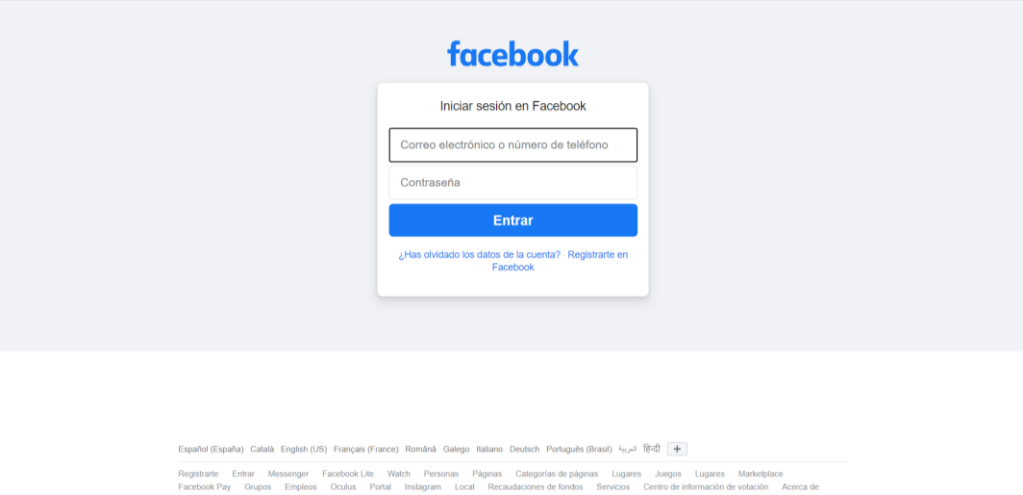
URLs fets servir per a la campanya de prova Netflix:

- URL a redirigir: https://www.netflix.com/es/Login
- URL dades: https://gnh2-4sip.herokuapp.com/data/2
- URL trampa: https://gnh2-4sip.herokuapp.com/netflix/login

Altres URLs d'altres campanyes de prova:

Fabeook:

- URL a redirigir: https://es-es.facebook.com/login/web/
- URL dades: https://gnh2-4sip.herokuapp.com/data/3
- URL trampa: https://gnh2-4sip.herokuapp.com/facebook/login

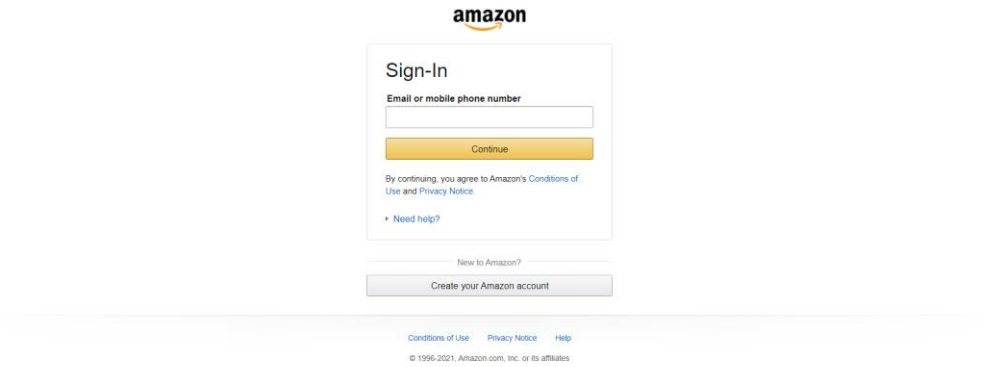


Web trampa Facebook

Amazon:

- URL a redirigir: https://www.amazon.com/ap/signin?openid.pape.max_auth_age=0&openid.return_to=https%3A%2F%2Fwww.amazon.com%2Flog%2Fs%2F%3F_encoding%3DUTF8%26k%3Dlog%2520in%26ref_%3Dnav_ya_signin&openid.identity=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.assoc_handle=usflex&openid.mode=checkid_setup&openid.claimed_id=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0&
- URL dades: https://gnh2-4sip.herokuapp.com/data/1

- URL trampa: https://gnh2-4sip.herokuapp.com/amazon/login



Web trampa Amazon

En el següent enllaç, es poden trobar els fitxers HTML fets servir en la campanya Netfilx de prova i altre campanyes, juntament amb fitxers per a afegir alguna empresa amb el format correcte.

- https://drive.google.com/drive/folders/1t2YuIfmdps80FlLt4BQxgUTFEJ0BTL93?usp=sharing