

Utilizando Hardware Hacking para coleta de credenciais

O foco em “experiência do usuário” acima de tudo tem proporcionando uma maior insegurança online. Muitas empresas deixam a segurança em segundo plano para que seus usuários tenham uma boa experiência em seus produtos e serviços.

Um atacante pode explorar este cenário.



Usabilidade versus Segurança



Comportamento dos usuários



Exemplo de Ataque



Material da Apresentação

Quem sou eu?

**LEONARDO LA ROSA**

Leonardo La Rosa

[/leonardolarosa](https://www.linkedin.com/in/leonardolarosa)

Bio

LEONARDO LA ROSA

Mais de 20 Anos de Experiência nas áreas de TI, incluindo Infraestrutura e Cibersegurança, com atuação em diversos setores de mercado, sendo a maior parte Instituições Financeiras.

Tecnólogo em Processamento de Dados pela UNIBAN
MBA em Gestão de Tecnologia da Informação pela FIAP

• CISCU • NISF • CIND • CIEH • ECIH • CIASE Java • CIEI • ICSICNSS • Lead Implementer ISO 27701 • CCSE • CSA • CTIA

- Infrastructure e Cyber Security Manager na ACADI-TI
- Instrutor das certificações EC-COUNCIL
- Instrutor de treinamentos próprios na ACADI-TI
- Docente do Curso de Pós Graduação em Cibersegurança Ofensiva - ACADI-TI
- Digital Influencer sobre temas relacionados a Cibersegurança

Fácil de usar... mas e a segurança?

EXPERIÊNCIA DO USUÁRIO



SECURITY



Aumento de Internet Pública



Projetos em Grandes Cidades

wifi LIVRESP
SÃO PAULO, CIDADE INTELIGENTE E HUMANA

EXPANSÃO DA REDE
WI-FI MAIS PERTO DE VOCÊ

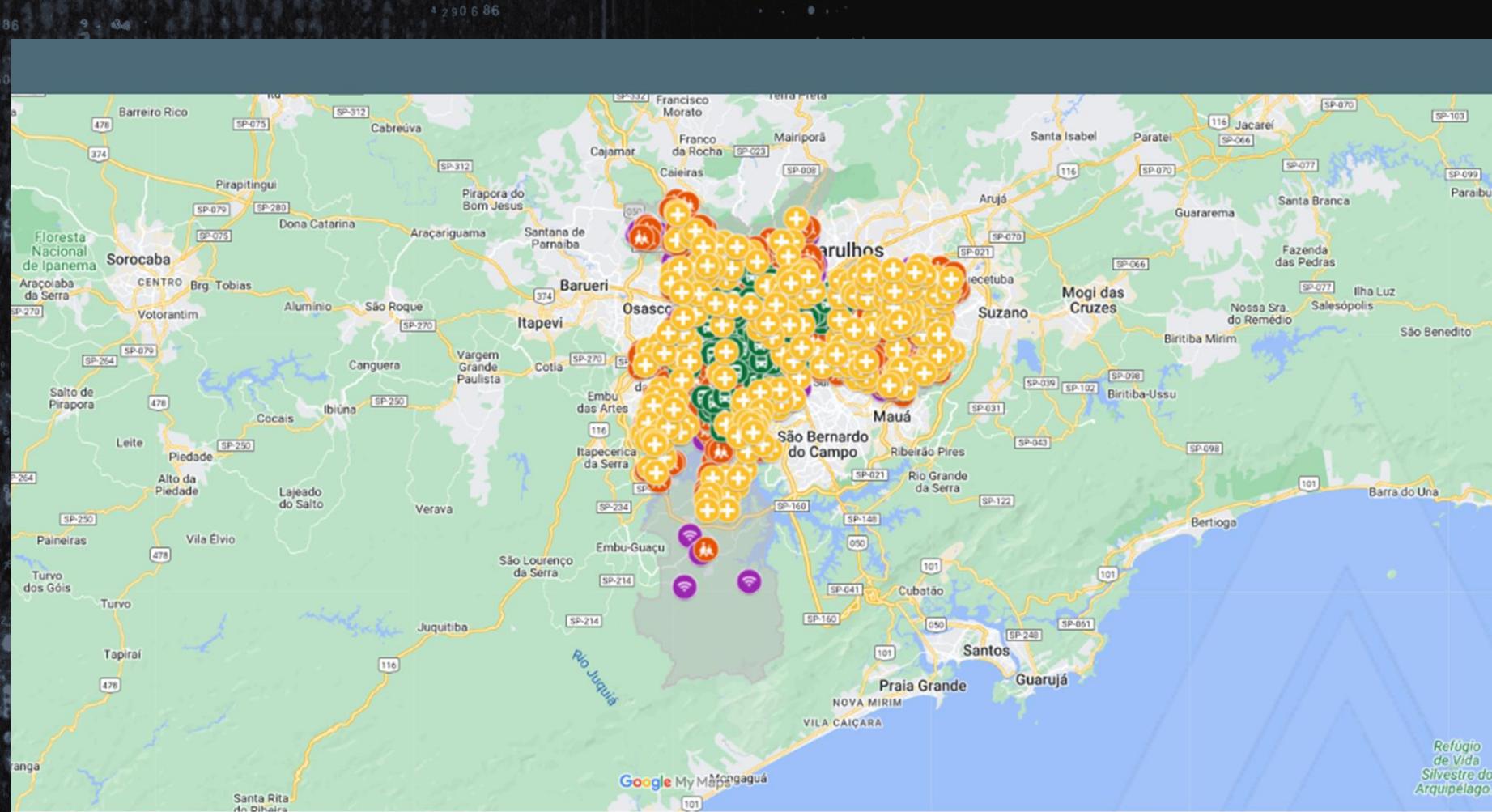
INTERNET PARA QUEM MAIS PRECISA
MAIS DE 300 LOCALIDADES EM
REGIÕES DE VULNERABILIDADE SOCIAL

**EQUIPAMENTOS PÚBLICOS
CONECTADOS**
PONTOS DE ACESSO EM LOCAIS COMO
UBS, BIBLIOTECAS, CEUS, CENTROS
CULTURAIS E DESPORTIVOS

LOCK icon
CLOUD icon
GEAR icon

<https://www.wifilivre.sp.gov.br/>

Centenas de pontos de Acesso em São Paulo



<https://www.gov.br/mcom/pt-br/acesso-a-information/acoes-e-programas/wi-fi-brasil>

Programa Wi-Fi Brasil

Programa Wi-Fi Brasil

Programa de Governo Eletrônico - Serviço de Atendimento ao Cidadão (GESAC)

Publicado em 30/06/2022 18h54 | Atualizado em 16/08/2022 19h20

Compartilhe:   

O Programa de Governo Eletrônico — Serviço de Atendimento ao Cidadão (GESAC), criado pela Portaria MC nº 256, de 13 de março de 2002, é gerido pelo Ministério das Comunicações (MCom) e oferece o acesso a serviços de conexão à internet, com o objetivo de promover a inclusão digital e social, bem como para incentivar ações de governo eletrônico para a população.

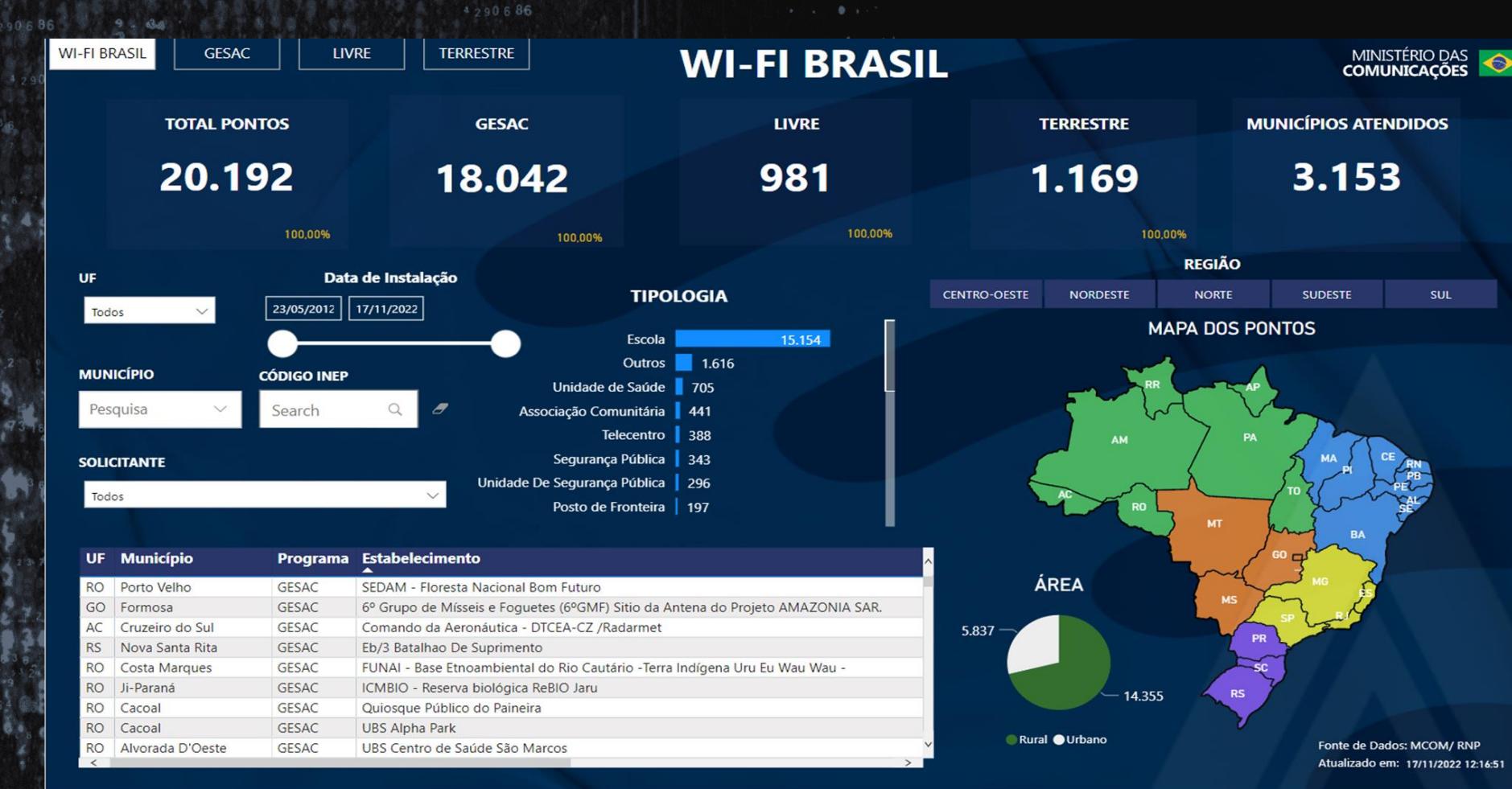
OBJETIVOS

O Programa GESAC tem os seguintes objetivos:

- i. a promoção da inclusão digital, por meio do fornecimento de conexão à internet em banda larga, inclusive naquelas localidades onde inexista oferta adequada de conexão à Internet;
- ii. o apoio a comunidades em estado de vulnerabilidade social, localizadas em áreas rurais, remotas e nas periferias urbanas, oferecendo acesso a serviços de conexão à internet, promovendo a inclusão digital e social e incentivando as ações de governo eletrônico;
- iii. a ampliação do provimento de acesso à internet em banda larga para instituições públicas, com prioridade para regiões remotas e de fronteira;
- iv. o apoio a órgãos governamentais em ações de governo eletrônico; e
- v. a contribuição para a ampliação do acesso à internet em consonância com outros programas de governo.

<https://www.gov.br/mcom/pt-br/acesso-a-informacao/acoes-e-programas/wi-fi-brasil>

Mais de 20.000 pontos de acesso



<https://app.powerbi.com/view?r=eyJrljoiYTM3NzkwZjYtNTVjYi00YTY5LWExOGUtYzNiZTMzMjY2ZDVmlividCI6ImExMTlwMGVkLTNhYTctNDFhMy05M2UxLtcwYWU4ZmMxZWMxYSJ9&pageName=ReportSection2bdd6a5c141f7bb78457>

Comportamento dos usuários



11%

das organizações usam MFA, em geral.



73%

Das contas online usam senhas duplicadas.



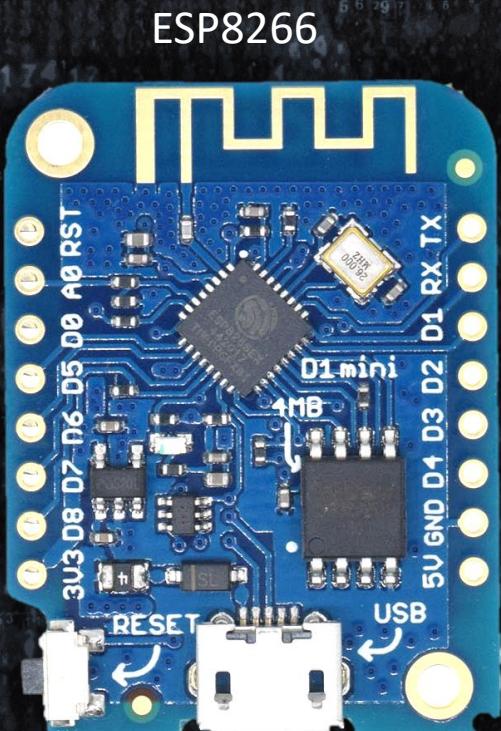
58%

Dos brasileiros acreditam que suas informações pessoais estão seguras ao usar uma rede Wi-Fi pública

E se um atacante tiver explorar este cenário?



E se um atacante tiver explorar este cenário?



ESP8266



Leitor SD

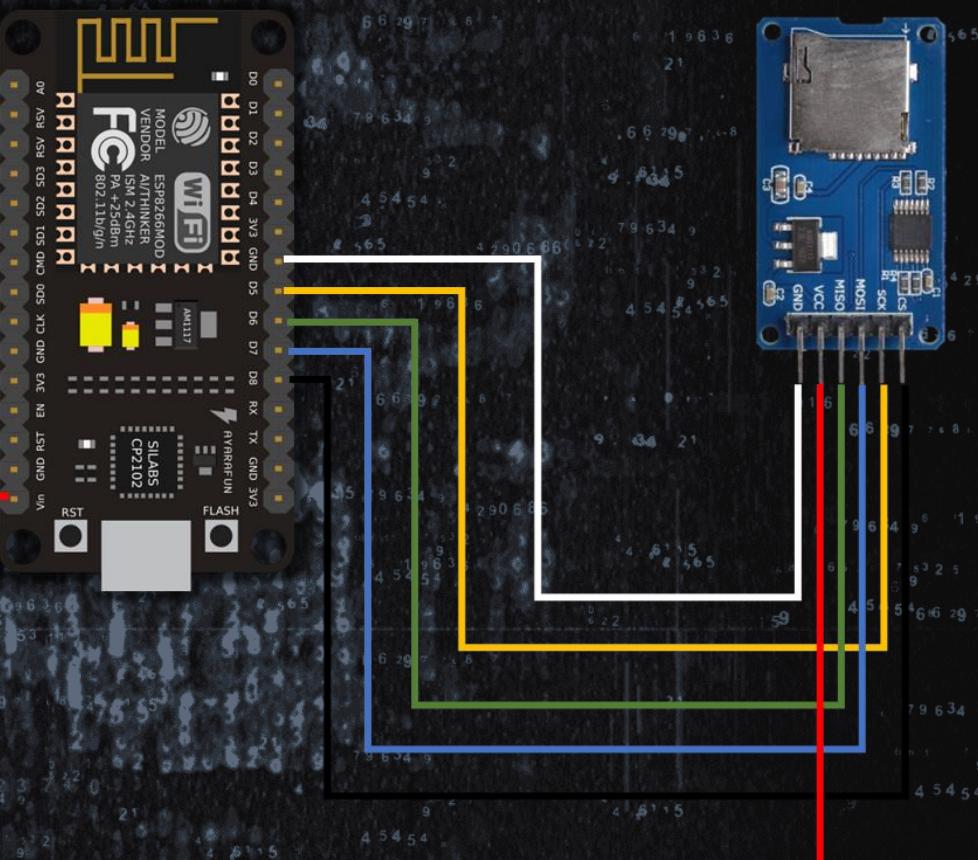


Display Oled

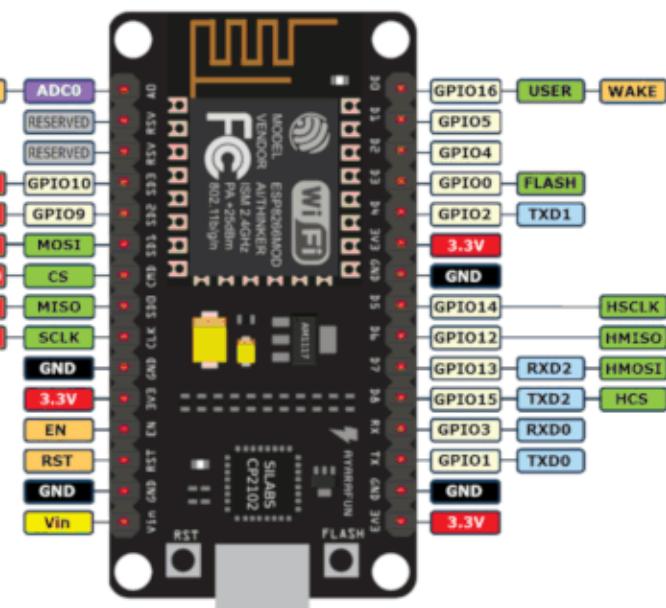
R\$120,00

E se um atacante tiver explorar este cenário?

V1.0

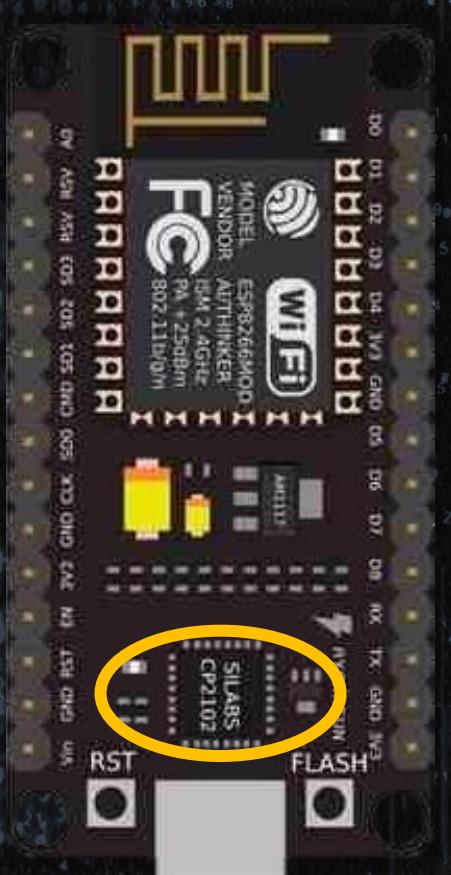


**NodeMCU Devkit V1.0
aka NodeMCU V2**

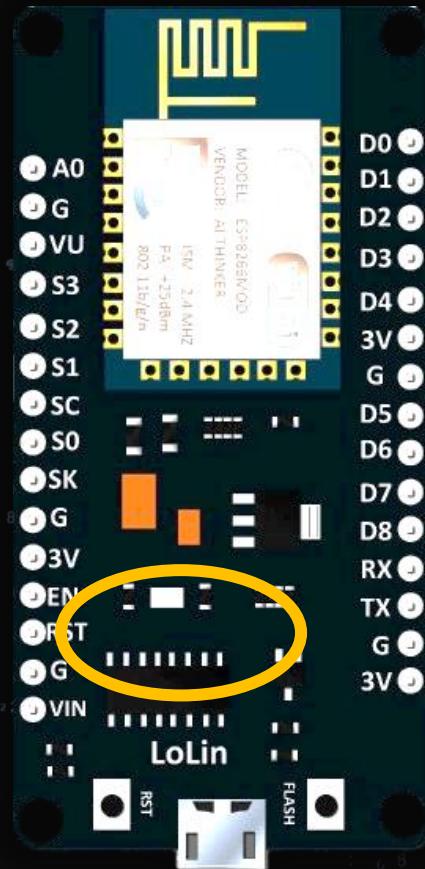


Página 13 de

E se um atacante tiver explorar este cenário?

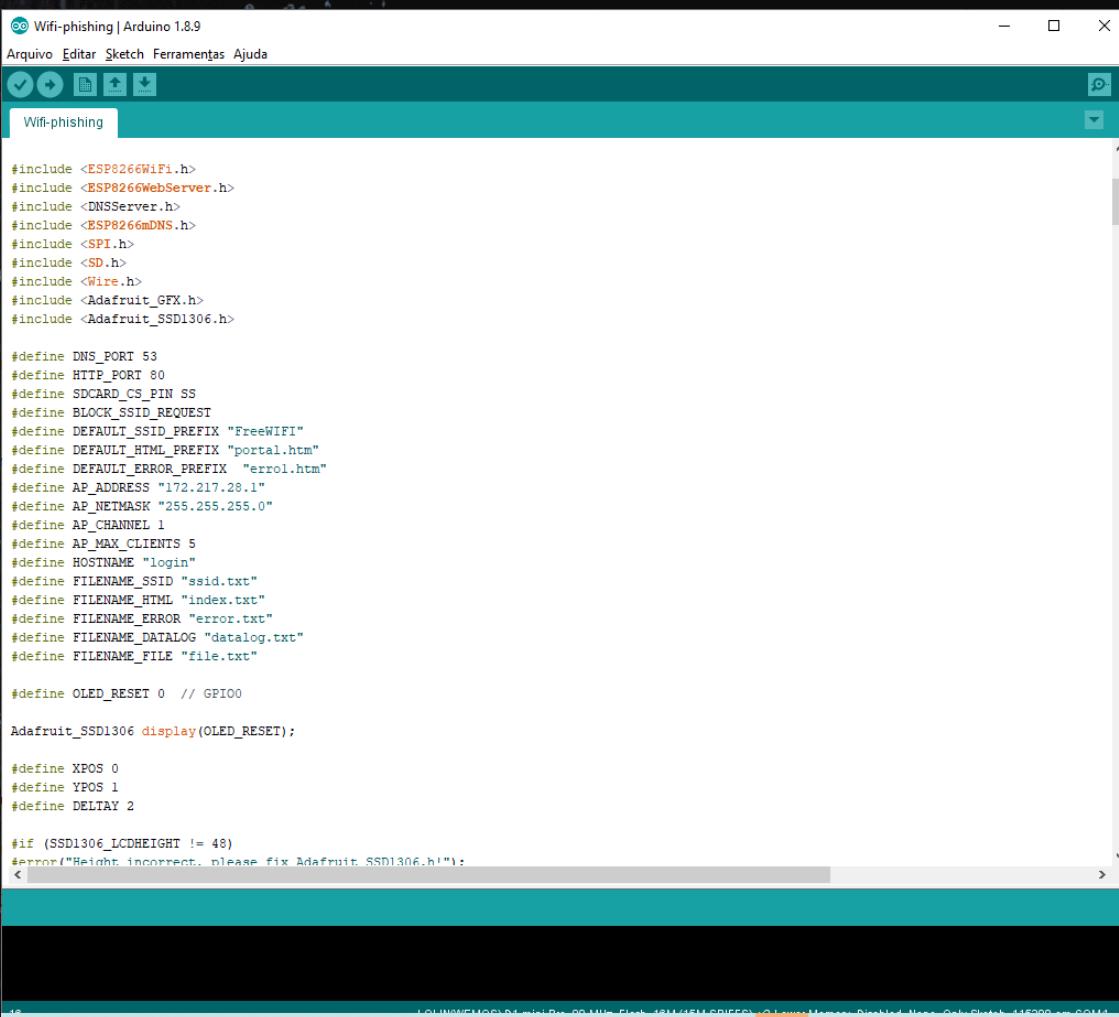


CP2102



CH34X

E se um atacante tiver explorar este cenário?



The screenshot shows the Arduino IDE interface with a sketch named "Wifi-phishing". The code is written in C++ and includes various libraries for WiFi, WebServer, and Adafruit SSD1306. It defines constants for WiFi port, HTTP port, SD card pin, and various file names. It also includes definitions for hostnames, file paths, and error messages. The code is intended to run on an ESP8266 board connected to an Adafruit SSD1306 display.

```
#include <ESP8266WiFi.h>
#include <ESP8266WebServer.h>
#include <DNSServer.h>
#include <ESP8266mDNS.h>
#include <SPI.h>
#include <SD.h>
#include <Wire.h>
#include <Adafruit_GFX.h>
#include <Adafruit_SSD1306.h>

#define DNS_PORT 53
#define HTTP_PORT 80
#define SDCARD_CS_PIN SS
#define BLOCK_SSID_REQUEST
#define DEFAULT_SSID_PREFIX "FreeWIFI"
#define DEFAULT_HTML_PREFIX "portal.htm"
#define DEFAULT_ERROR_PREFIX "errol.htm"
#define AP_ADDRESS "172.217.28.1"
#define AP_NETMASK "255.255.255.0"
#define AP_CHANNEL 1
#define AP_MAX_CLIENTS 5
#define HOSTNAME "login"
#define FILENAME_SSID "ssid.txt"
#define FILENAME_HTML "index.txt"
#define FILENAME_ERROR "error.txt"
#define FILENAME_DATALOG "datalog.txt"
#define FILENAME_FILE "file.txt"

#define OLED_RESET 0 // GPIO0

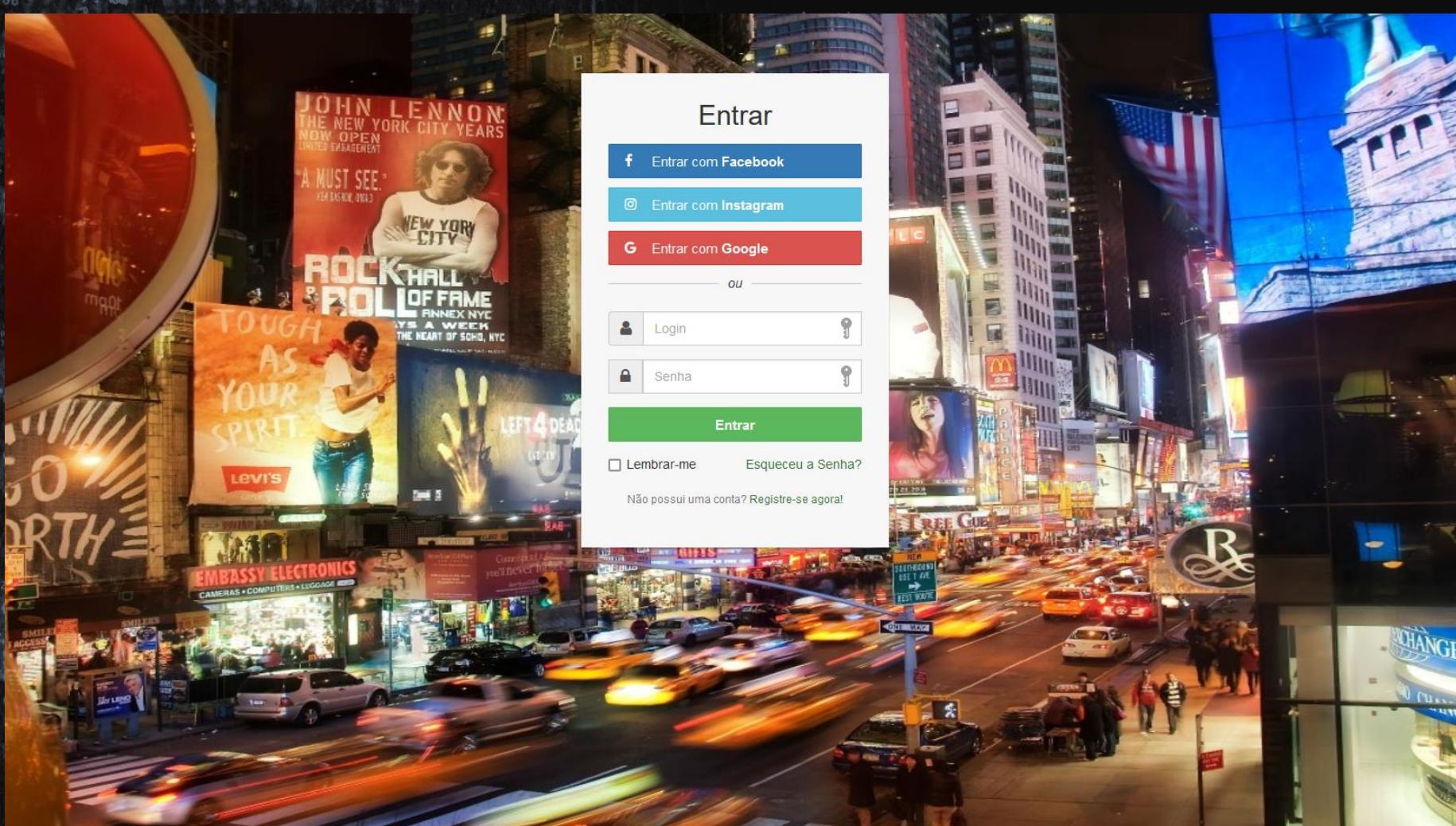
Adafruit_SSD1306 display(OLED_RESET);

#define XPOS 0
#define YPOS 1
#define DELTAY 2

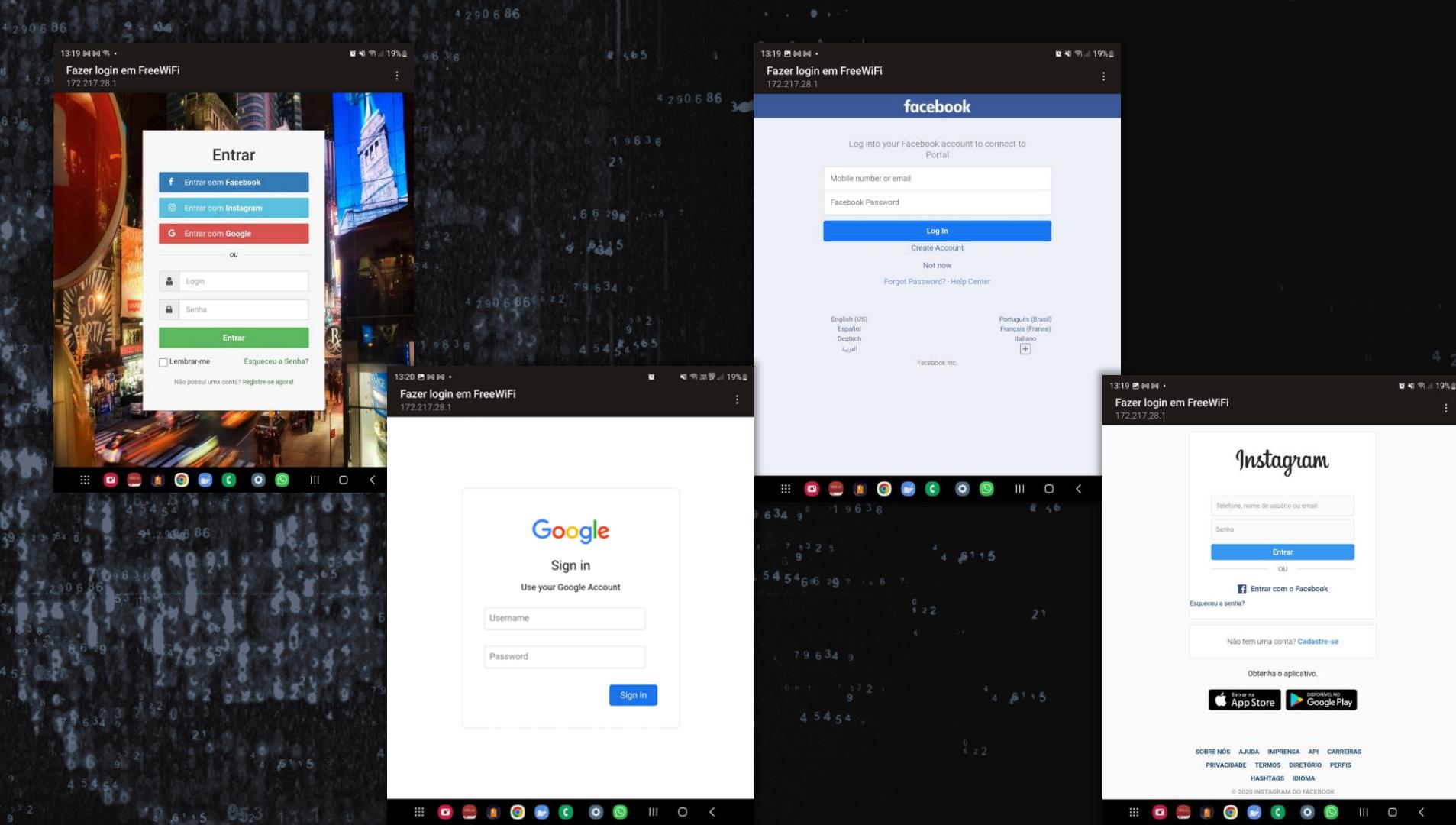
#if (SSD1306_LCDHEIGHT != 48)
#error("Height incorrect, please fix Adafruit_SSD1306.h!")

```

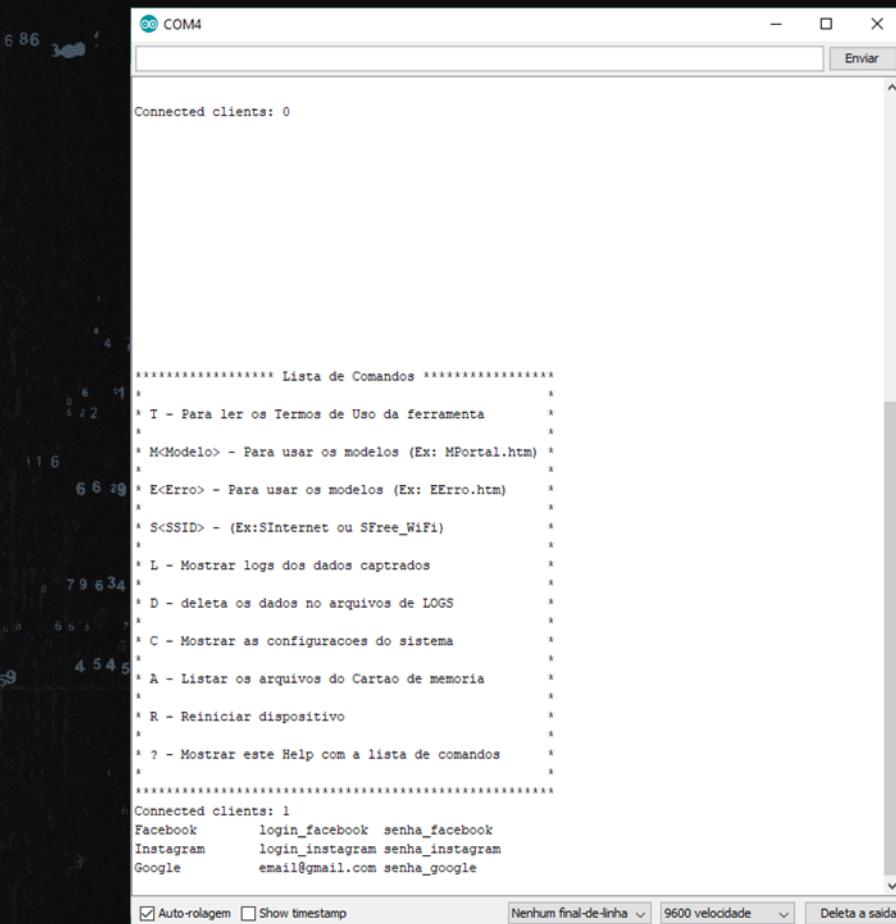
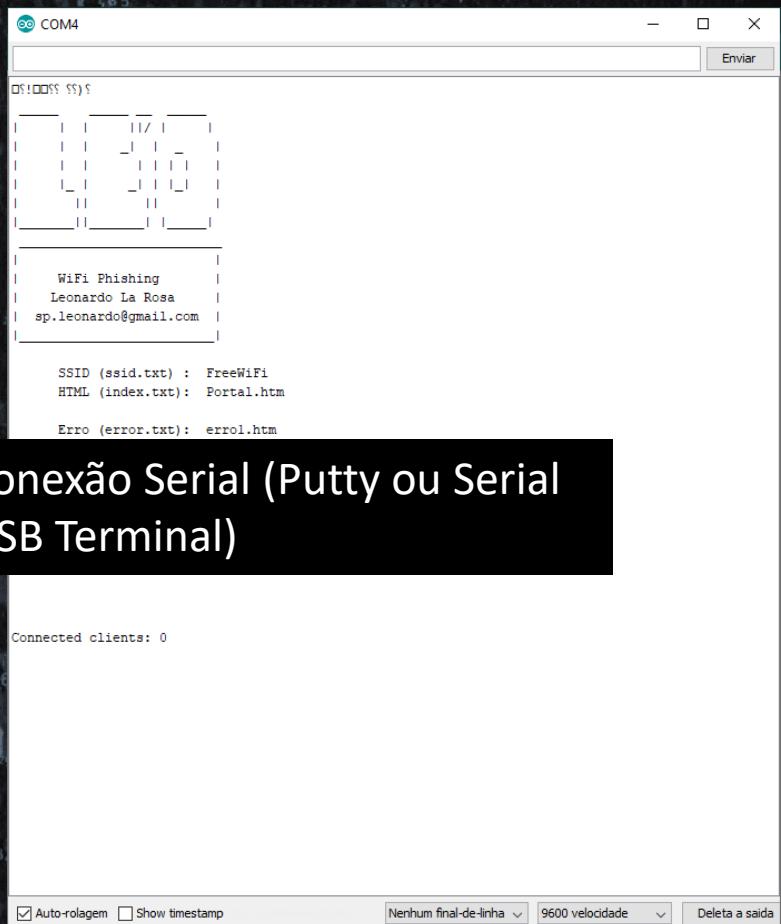
E se um atacante tiver explorar este cenário?



Vários templates para uso



Gerenciamento realizado via SERIAL (conexão USB)



Ou via Wi-Fi

The screenshot shows a web browser window with the URL <http://172.217.28.1/admin.htm>. The page title is "WiFi Phishing Admin". It features a logo of a person with a beard and glasses. The interface includes several input fields and dropdown menus:

- SSID:** Free_WIFI
- MODELO:** Portal.htm (selected from a dropdown menu which also includes Bhack.htm, Portal.htm, model01.htm, facebook.htm, and insta.htm)
- RETORNO:** erro1.htm (selected from a dropdown menu which also includes bhack.htm, errfb.htm, errgo.htm, erro1.htm, and err404.htm)
- DADOS:** A table with three rows:

Facebook	login_facebook senha_facebook
Instagram	login_instagram senha_instagram
Google	email@gmail.com senha_google
- Salvar** button at the bottom right.

É possível criar um novo rede em segundos

The screenshot shows a web-based configuration interface for a WiFi Phishing attack. At the top, there's a logo of a person with a beard and glasses, followed by the text "WiFi Phishing Admin". Below this are four input fields with associated text boxes:

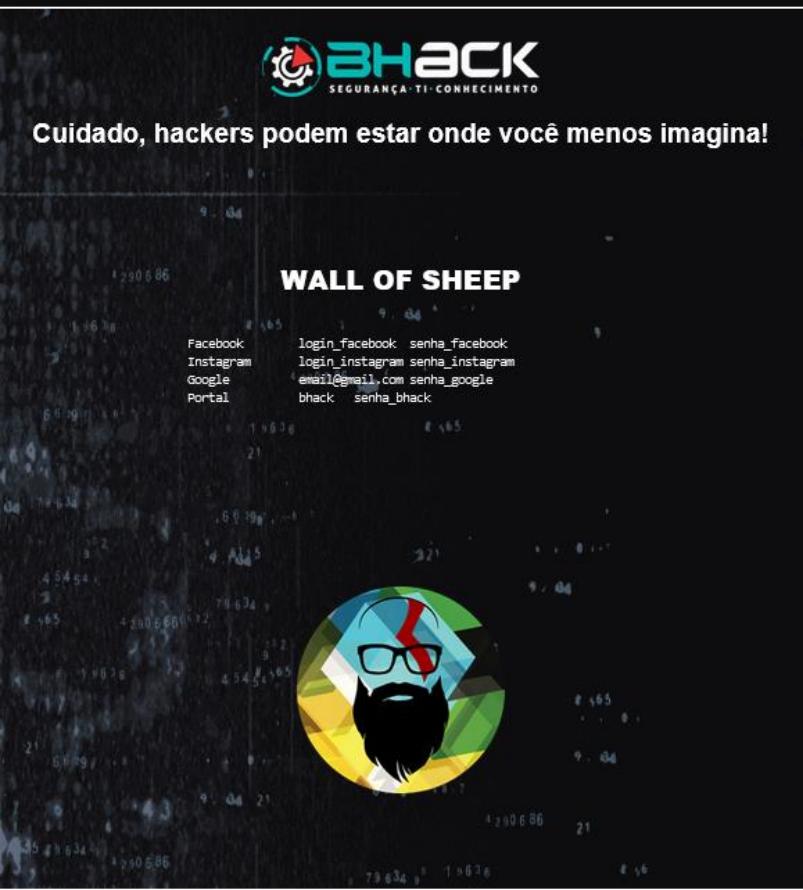
- SSID:** A text input field containing "Free_WIFI" with the label "Define o nome do SSID" to its right.
- MODELO:** A dropdown menu set to "Portal.htm" with the label "Define a página do Ataque" to its right. The dropdown also lists "Bhack.htm", "Portal.htm", "model01.htm", "facebook.htm", and "insta.htm".
- RETORNO:** A dropdown menu set to "erro1.htm" with the label "Define a página do Erro" to its right. The dropdown also lists "bhack.htm", "errfb.htm", "errgo.htm", "erro1.htm", "erro404.htm", and others.
- DADOS:** A table showing captured data from users:

Facebook	Instagram	Google
login_facebook senha_facebook	login_instagram senha_instagram	email@gmail.com senha_google

At the bottom center is a green "Salvar" (Save) button.

A black box highlights the URL in the browser address bar: **http://172.217.28.1/admin.htm**.

BHACK Edition



Página 21 de

Como criar novos arquivos

The screenshot shows the identification registration page of the Magalu website. At the top, there is a navigation bar with links to 'Nossas lojas', 'Tenha sua loja', 'Regulamentos', 'Acessibilidade', 'Guia de segurança', 'Atendimento', 'Compre pelo tel: 0800 773 3838', and 'Meus pedidos'. Below the navigation bar, there is a search bar with the placeholder 'Busca no Magalu' and a 'Bem-vindo :)' message with a link to 'Entre ou cadastre-se'. There are also icons for location, heart, and a shopping bag with a '0'.

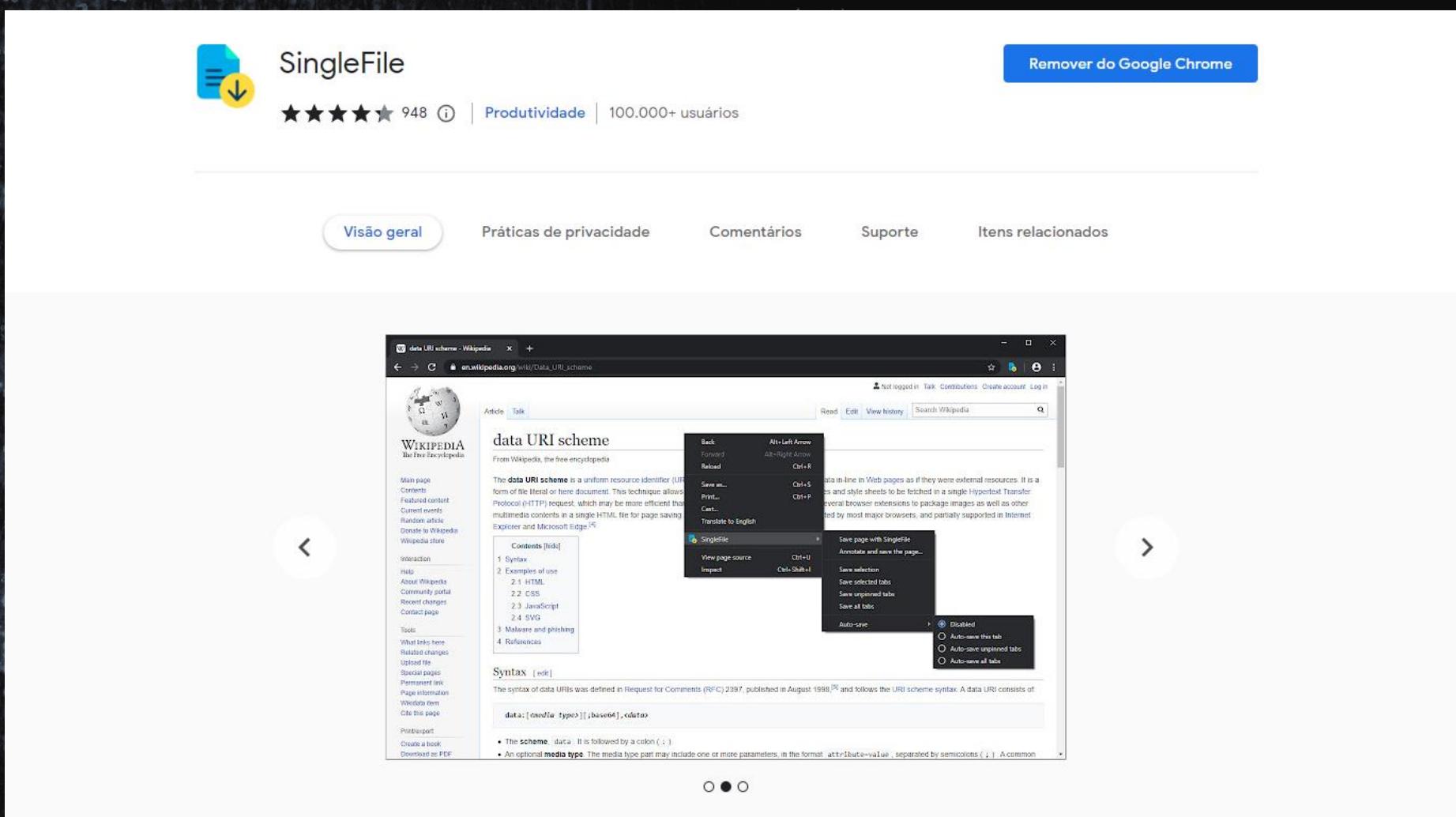
The main content area is titled 'Identificação' and contains two sections: 'Quero criar uma conta' and 'Já sou cliente'. Both sections have input fields for 'E-mail' or 'E-mail, CPF ou CNPJ' and a 'Continuar' button. Below each input field is a key icon. Under the 'Quero criar uma conta' section, there is a link 'Dúvidas? [fale conosco](#)'. Under the 'Já sou cliente' section, there is a link 'Esqueci minha senha'.

At the bottom of the page, there is a section titled 'Use sua rede social para se conectar*' with buttons for 'Facebook' and 'Google'. Below this, there is a note about data privacy and a link to the 'política de privacidade'. There is also a note about service availability for physical persons and a link to the 'Central de atendimento'.

Formas de pagamento



Utilizando a extensão Single File



Modificando arquivo html gerado

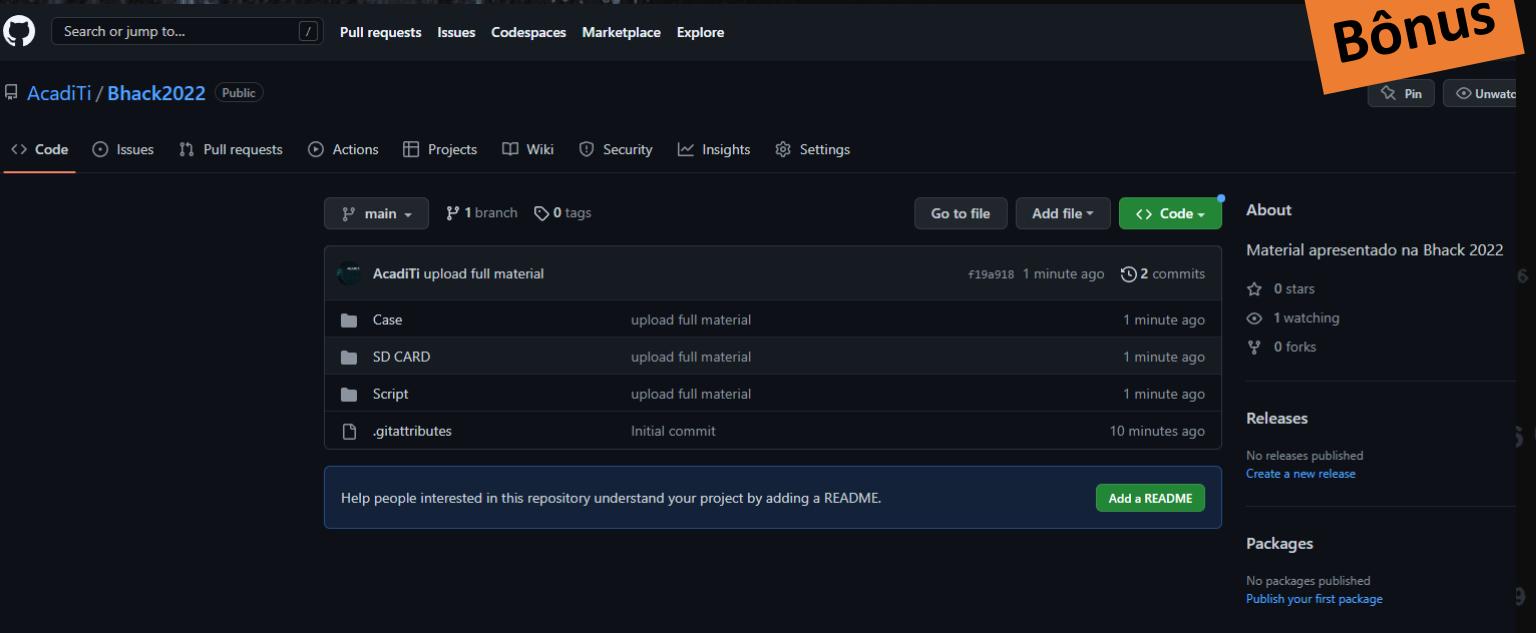
```
<input type="text" class="form-control" id="usr" name="usr" placeholder="Login required value">  
<input type="password" class="form-control" id="pwd" name="pwd" placeholder="Senha required value">  
<input type="hidden" name="svc" value="Portal " />
```



Código Fonte e apresentação

<https://github.com/AcadiTi/Bhack2022>

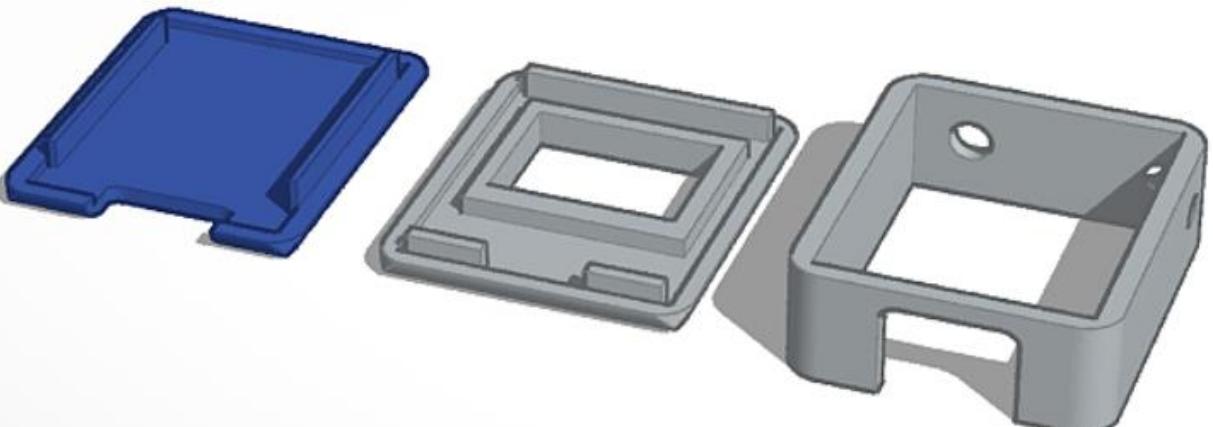
Bônus



Código Fonte e apresentação

<https://github.com/AcadiTi/Bhack2022>

Bônus



Utilizando Hardware Hacking para coleta de credenciais



Obrigado!



/leonardolarosa



/school/acaditi



/academiainovadora



/acaditi_oficial



@ACADITI