

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



SEGURANÇA



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

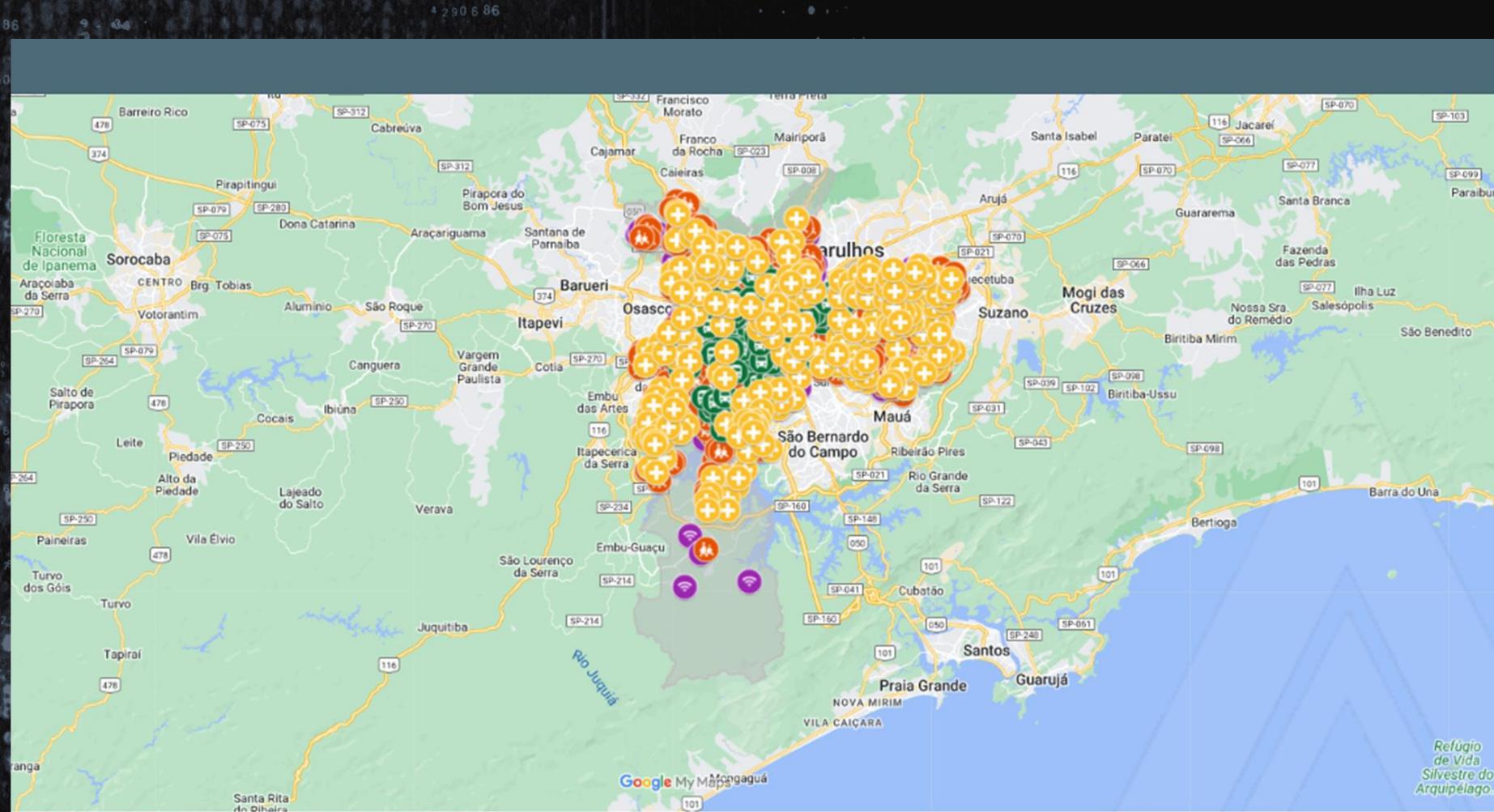
INTERNET PARA QUEM MAIS PRECISA
MAIS DE 300 LOCALIDADES EM
REGIÕES DE VULNERABILIDADE SOCIAL

**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.

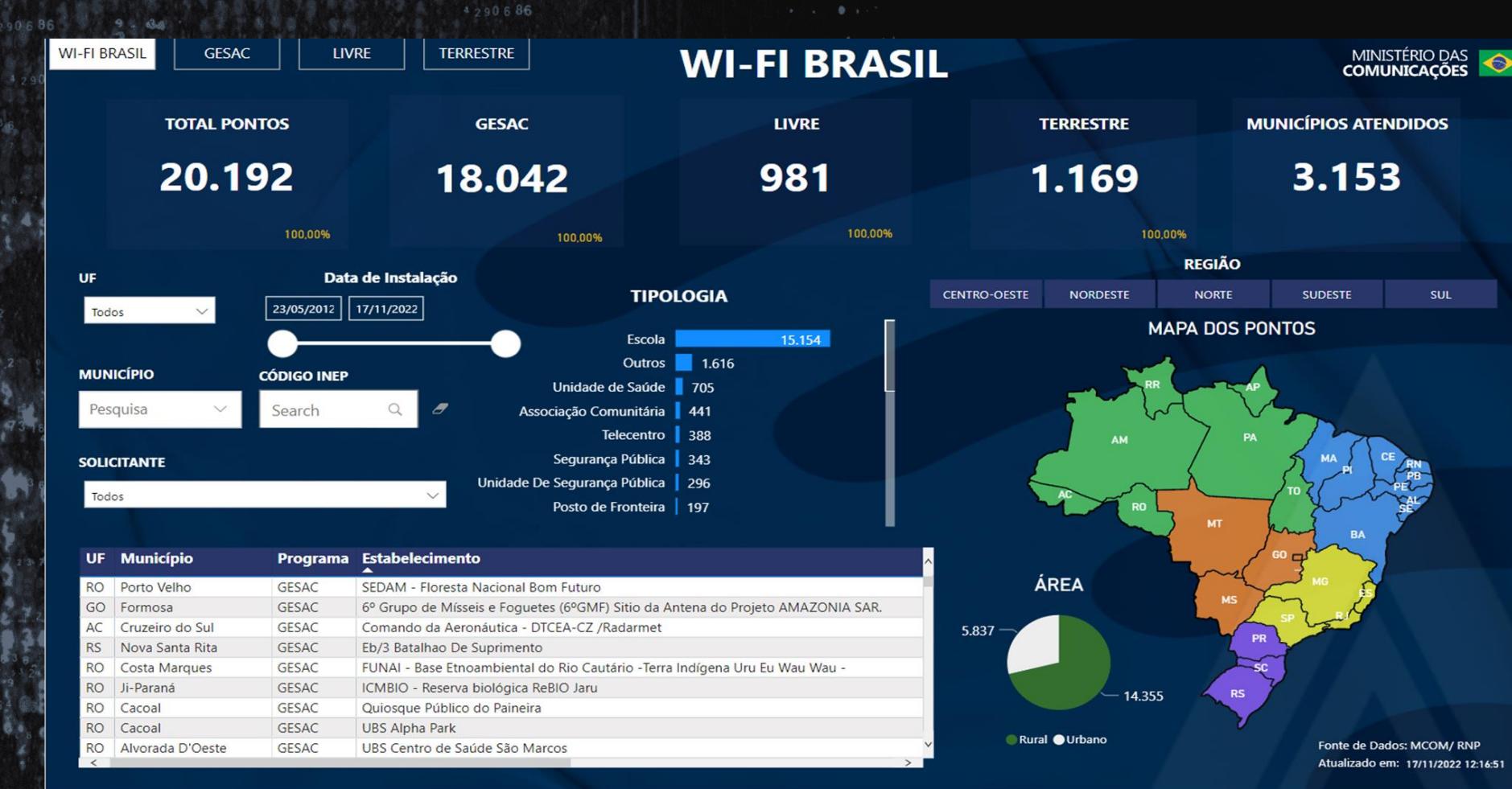
OBJETIVOS

O Programa GESAC tem os seguintes objetivos:

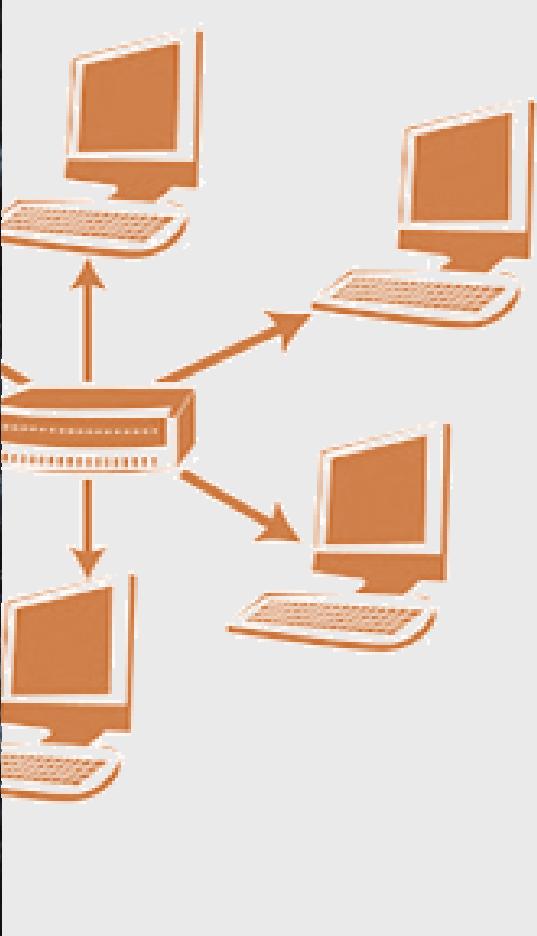
- i. a promoção da inclusão digital, por meio do fornecimento de conexão à internet em banda larga, inclusive naquelas localidades onde inexista oferta adequada de conexão à Internet;
- ii. o apoio a comunidades em estado de vulnerabilidade social, localizadas em áreas rurais, remotas e nas periferias 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



Os perigos do WiFi Público



**Os dispositivos em uma mesma rede
comunicam-se entre si.**

**O fomento de criação de Redes
Públicas criam nos usuários uma
falsa sensação de segurança.**

Os perigos do WiFi Público

**Quando acreditamos que estamos seguros,
deixamos de tomar certos cuidados**



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

Aviso!!

Não seja mané... Utilize o conteúdo aprendido aqui de forma consciente e com ética.

“Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

(...)

§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.

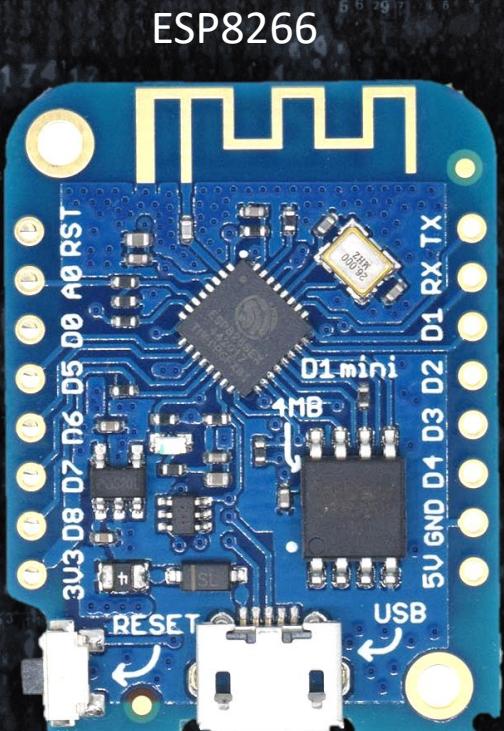
§ 3º (...)

Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

E se um atacante tiver explorar este cenário?



E se um atacante tiver explorar este cenário?



ESP8266



Leitor SD

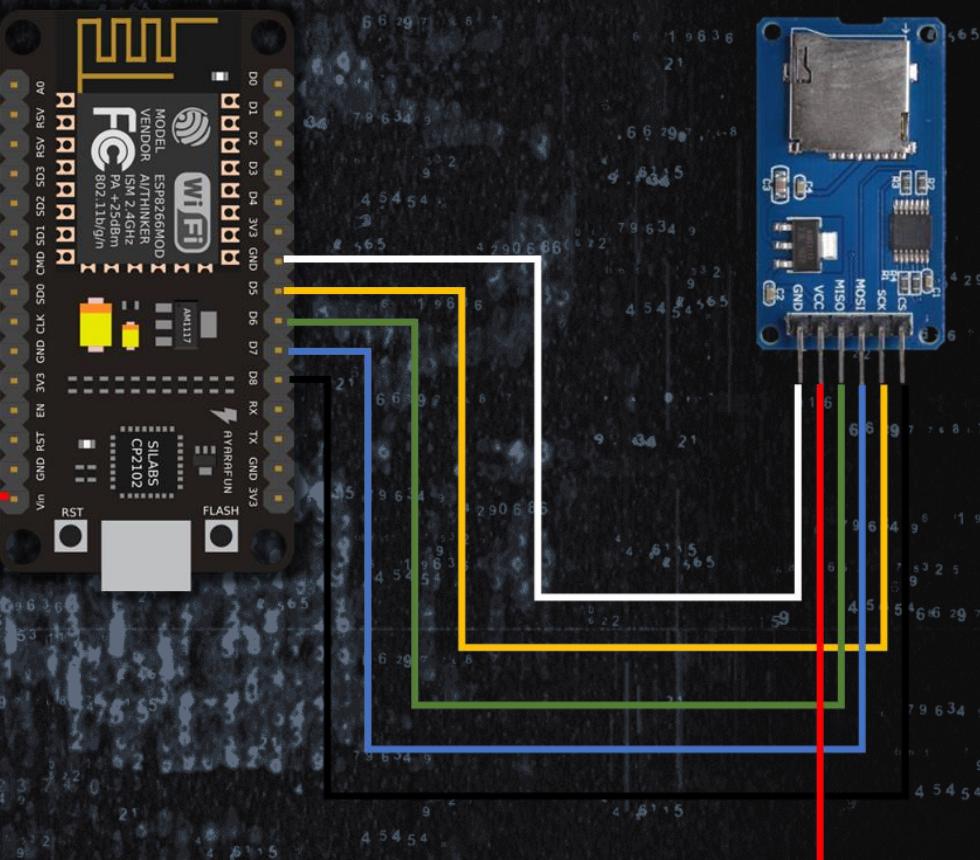


Display Oled

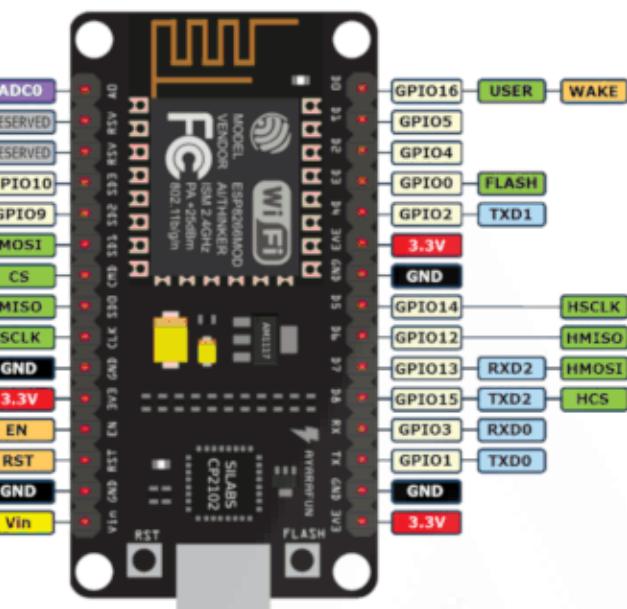
R\$120,00

E se um atacante tiver explorar este cenário?

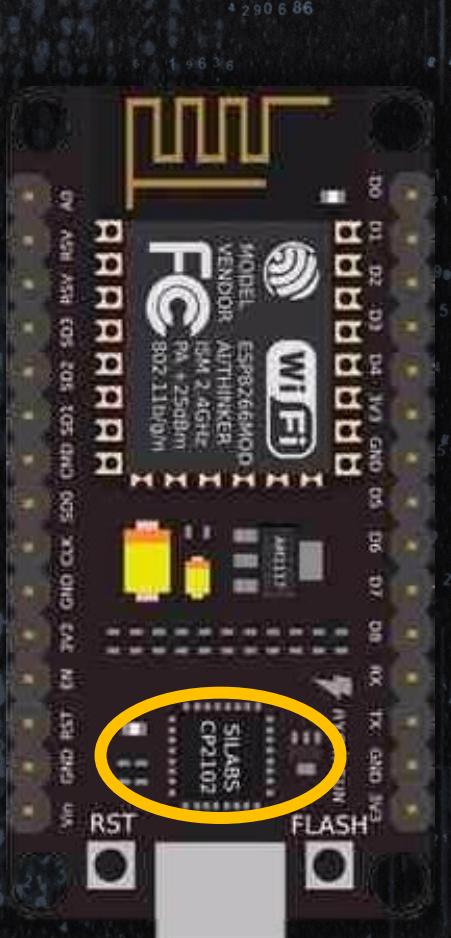
V1.0



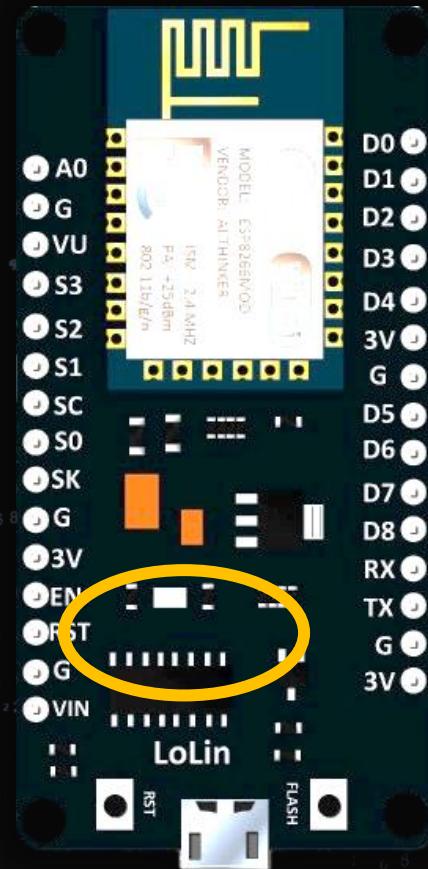
**NodeMCU Devkit V1.0
aka NodeMCU V2**



E se um atacante tiver explorar este cenário?

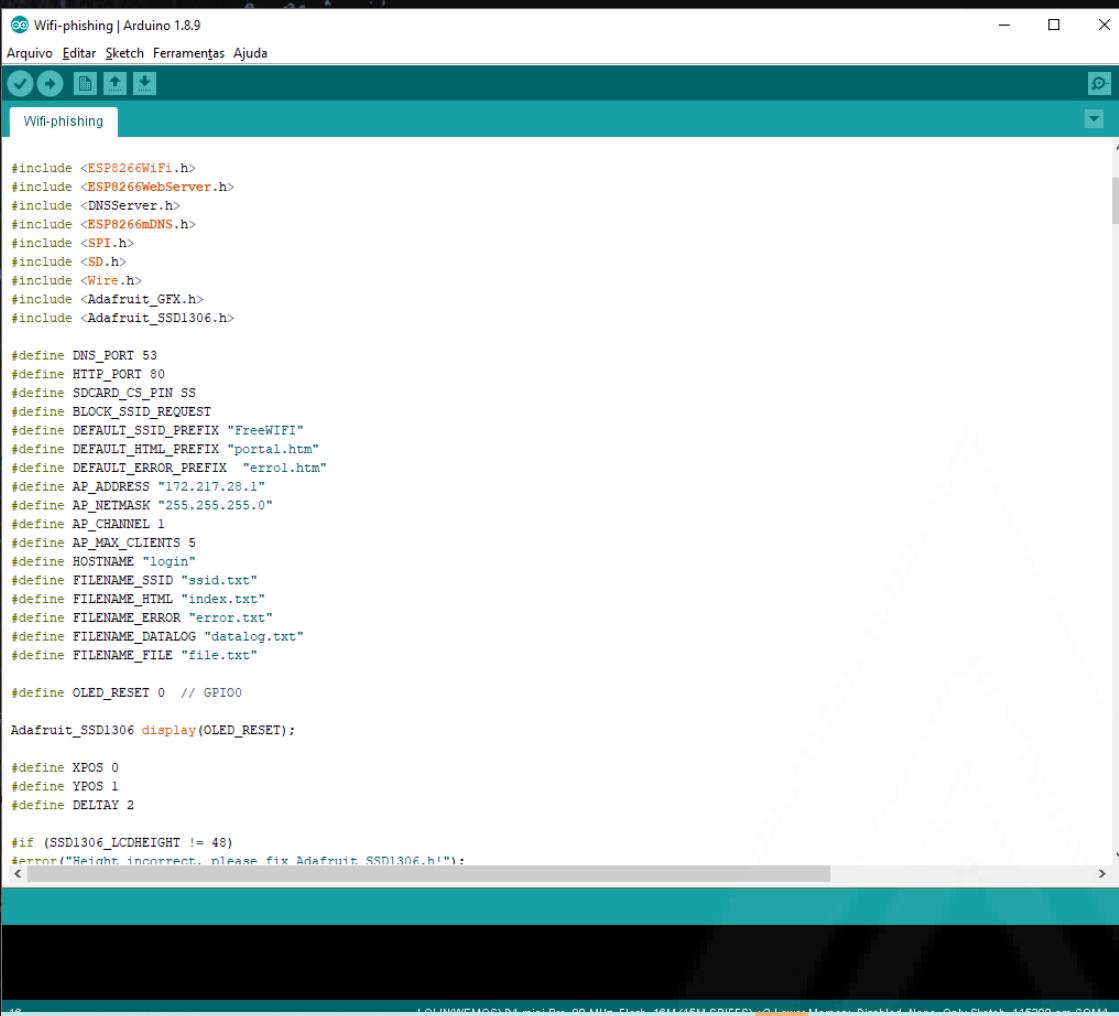


CP2102



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. The code 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 be run on an ESP8266 board connected to an 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

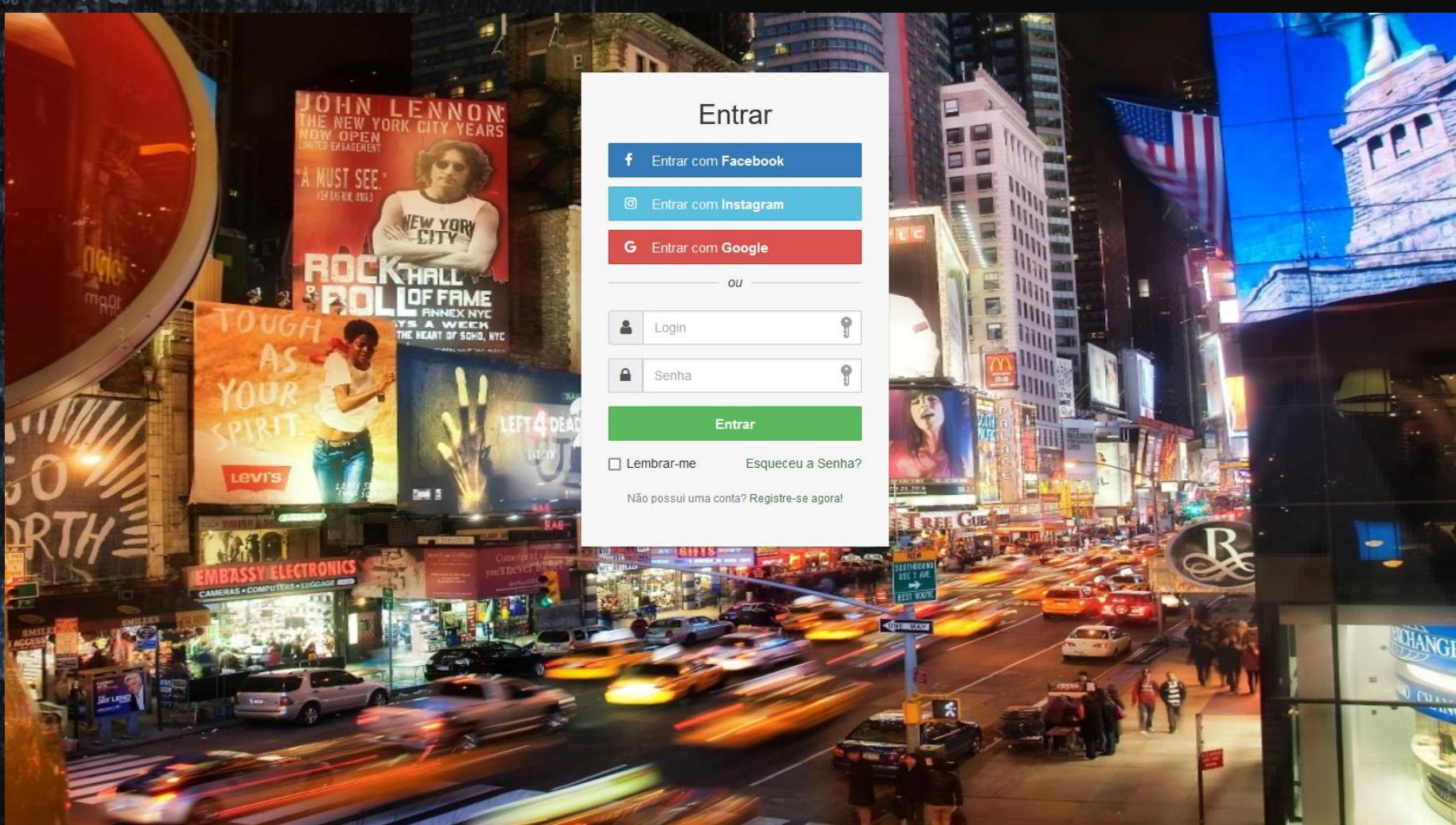
Adafruit_SSD1306 display(OLED_RESET);

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

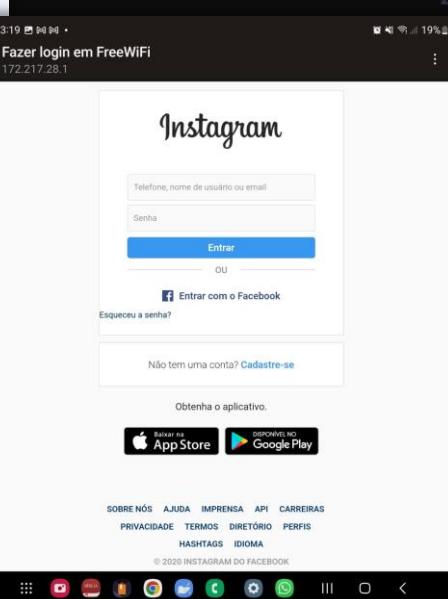
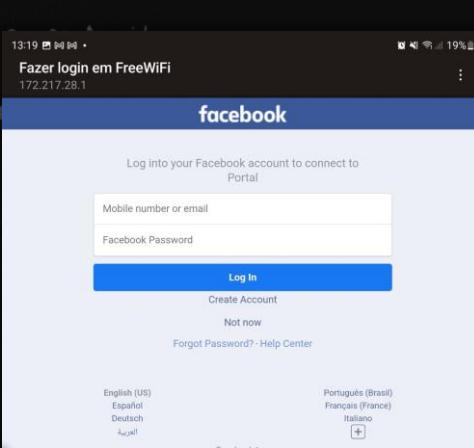
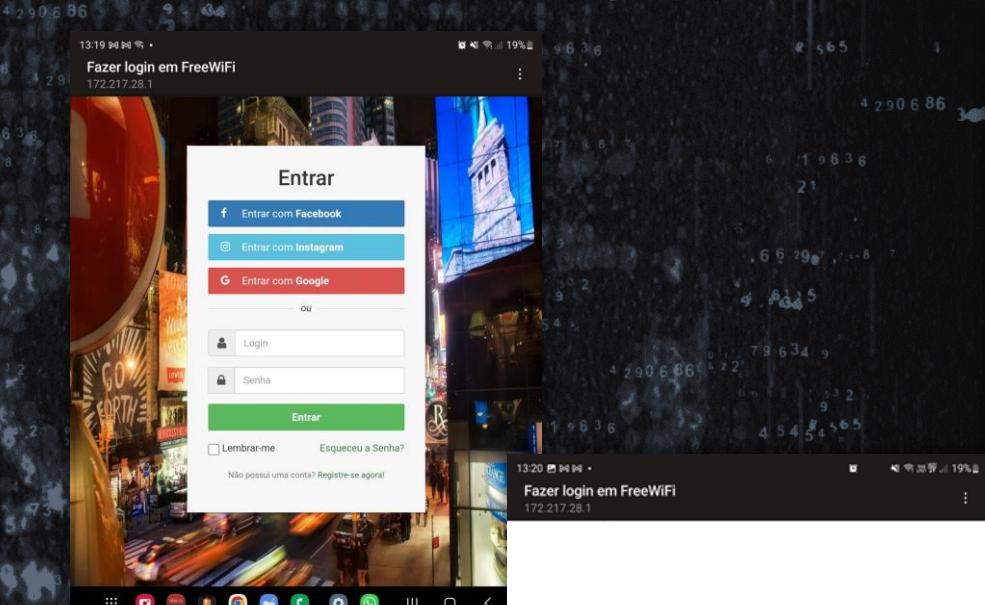
#if (SSD1306_LCDHEIGHT != 48)
#error("Height incorrect, please fix Adafruit_SSD1306.h!")

```

E se um atacante tiver explorar este cenário?



Vários templates para uso



Gerenciamento realizado via SERIAL (conexão USB)

```
WiFi Phishing
Leonardo La Rosa
sp.leonardo@gmail.com

SSID (ssid.txt) : FreeWiFi
HTML (index.htm) : Portal.htm

Erro (error.htm) : error.htm
```

Conexão Serial (Putty ou Serial USB Terminal)

```
Connected clients: 0

*****
* T - Para ler os Termos de Uso da ferramenta
* M<Modelo> - Para usar os modelos (Ex: MPortal.htm)
* E<Erro> - Para usar os modelos (Ex: EError.htm)
* S<SSID> - (Ex:SInternet ou SFree_WiFi)
* L - Mostrar logs dos dados capturados
* D - deleta os dados no arquivos de LOGS
* C - Mostrar as configurações do sistema
* A - Listar os arquivos do Cartão de memória
* R - Reiniciar dispositivo
* ? - Mostrar este Help com a lista de comandos
*****

Connected clients: 1
Facebook login_facebook senha_facebook
Instagram login_instagram senha_instagram
Google email@gmail.com senha_google

 Auto-rolagem  Show timestamp Nenhum final-de-linha 9600 velocidade Deleta a saída
```

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 columns for "Facebook", "Instagram", and "Google". The "Facebook" row contains "login_facebook senha_facebook". The "Instagram" row contains "login_instagram senha_instagram". The "Google" row contains "email@gmail.com senha_google".
- Salvar:** A green button at the bottom left.

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 the logo are four input fields with dropdown menus:

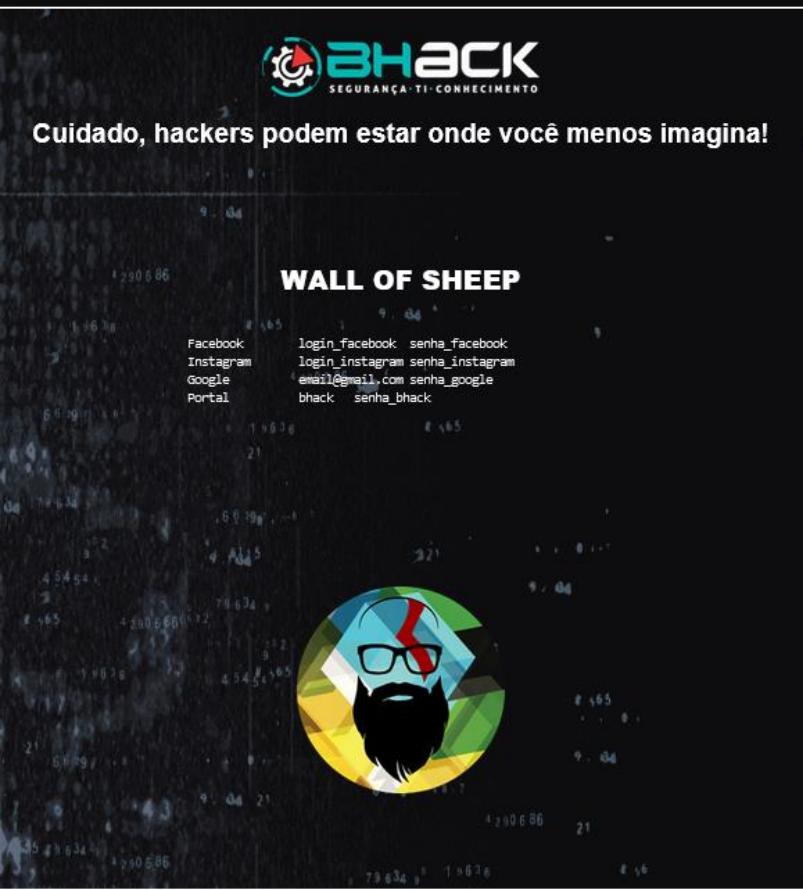
- SSID:** A text input field containing "Free_WIFI". A callout box to its right says "Define o nome do SSID".
- MODELO:** A dropdown menu set to "Portal.htm". A callout box to its right says "Define a página do Ataque".
- RETORNO:** A dropdown menu set to "erro1.htm". A callout box to its right says "Define a página do Erro".
- DADOS:** A table showing captured data from users:

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

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

A large black box on the left side of the interface contains the URL **http://172.217.28.1/admin.htm**.

BHACK Edition



Como criar novos arquivos

The screenshot shows the identification registration page of the Magalu website. The page is titled "Identificação" (Identification) and offers two options: "Quero criar uma conta" (I want to create an account) and "Já sou cliente" (I am a customer). Both sections require an email address and a password. There is also a link to connect via social media (Facebook and Google). A note at the bottom states that personal data will be handled according to the privacy policy.

Nossas lojas | Tenha sua loja | Regulamentos | Acessibilidade | Guia de segurança | Atendimento | Compre pelo tel: 0800 773 3838 | Meus pedidos

magalu Busca no Magalu

Bem-vindo :) Entre ou cadastre-se | Ver ofertas para minha região | Coração | Carrinho 0

Todos os departamentos | Ofertas do Dia | Celulares | Móveis | Eletrodomésticos | TV e Vídeo | Informática | Saldão | Black das Blackas | Cartão Magalu | Smartphoniza

Identificação

Quero criar uma conta

E-mail Continuar

Dúvidas? [fale conosco](#)

Já sou cliente

E-mail, CPF ou CNPJ Senha Continuar

[Esqueci minha senha](#)

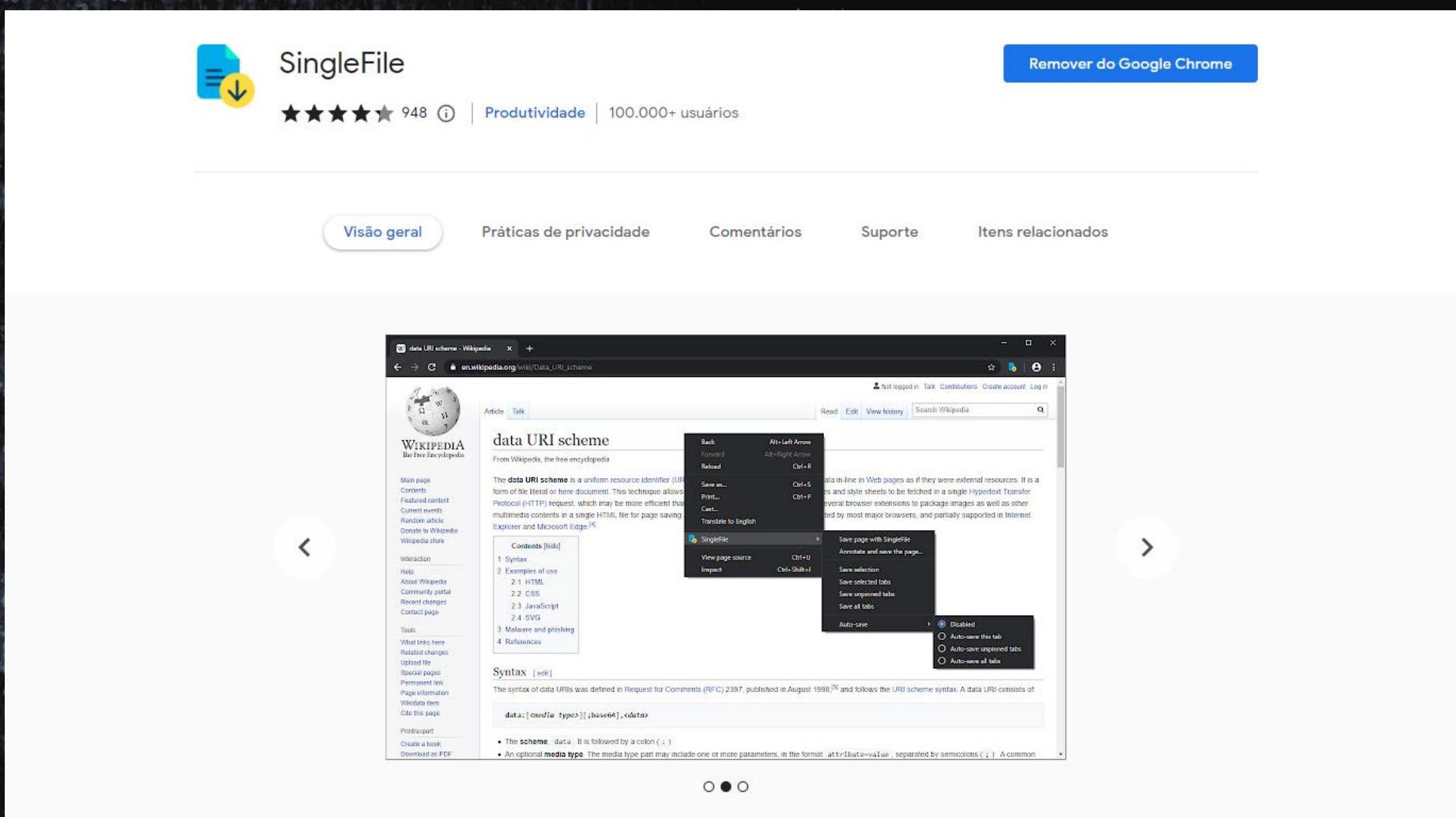
Use sua rede social para se conectar* [Facebook](#) [Google](#)

Seus dados pessoais serão respeitados de acordo com a nossa [política de privacidade](#). *Nada será publicado em sua timeline. Serviço válido somente para pessoas físicas.
Em caso de dúvidas, acesse nossa 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

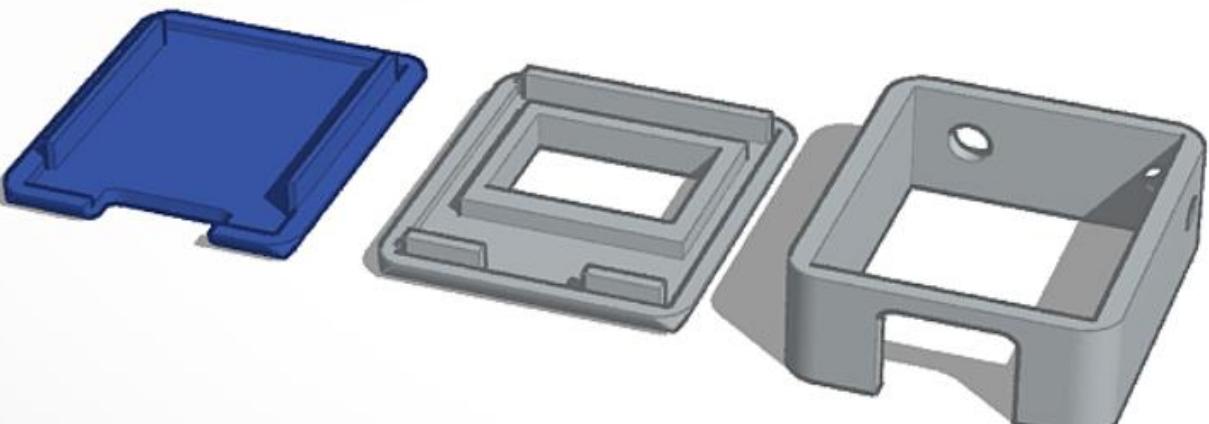
<https://github.com/AcadiTi/Bhack2022>

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