

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**

Fácil de usar... mas e a segurança?

EXPERIÊNCIA DO USUÁRIO



SECURITY



Aumento de Internet Pública

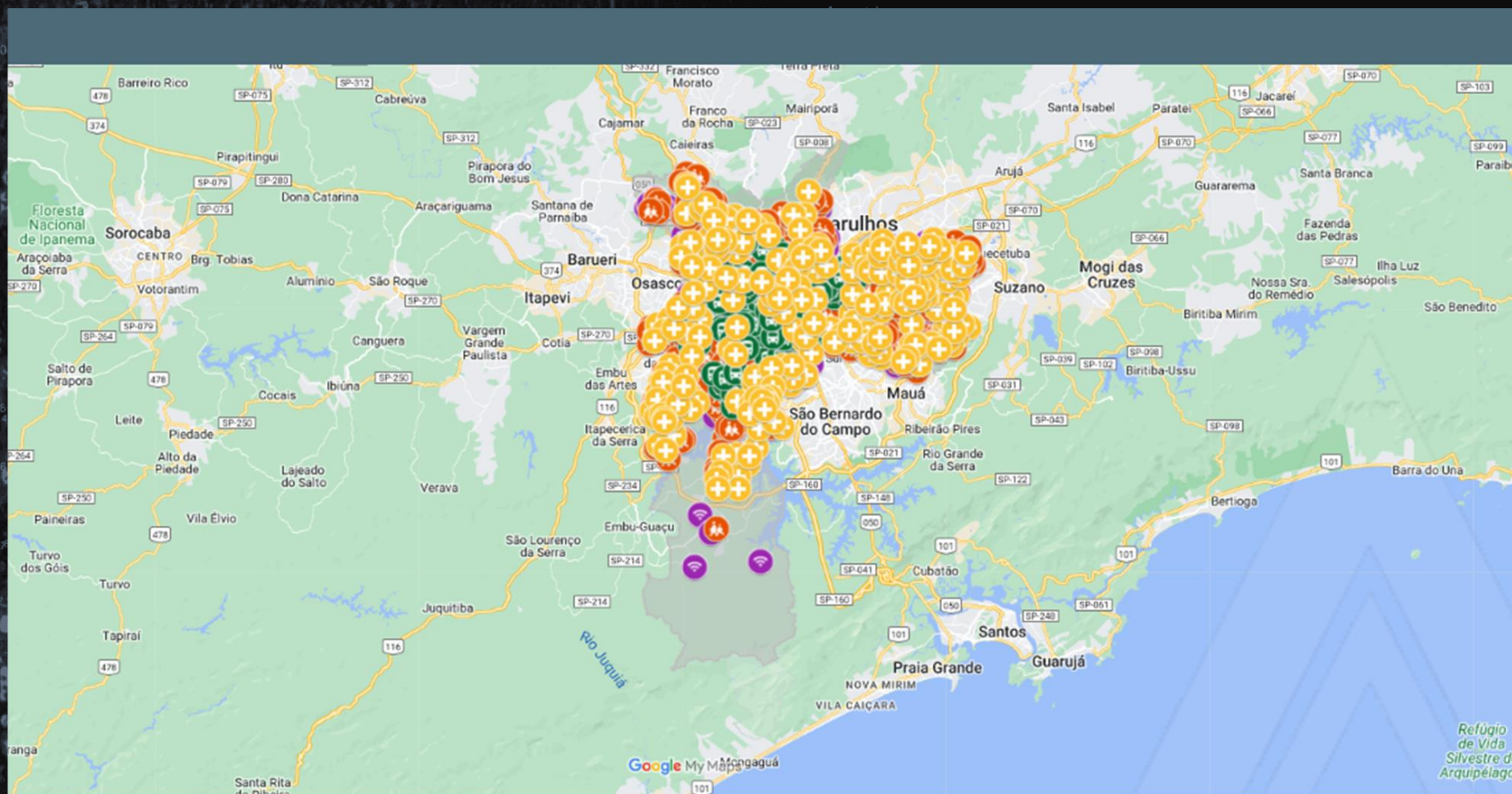


Projetos em Grandes Cidades



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

Centenas de pontos de Acesso em São Paulo



<https://www.gov.br/mcom/pt-br/aceso-a-informacao/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: [f](#) [t](#) [g](#)

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.

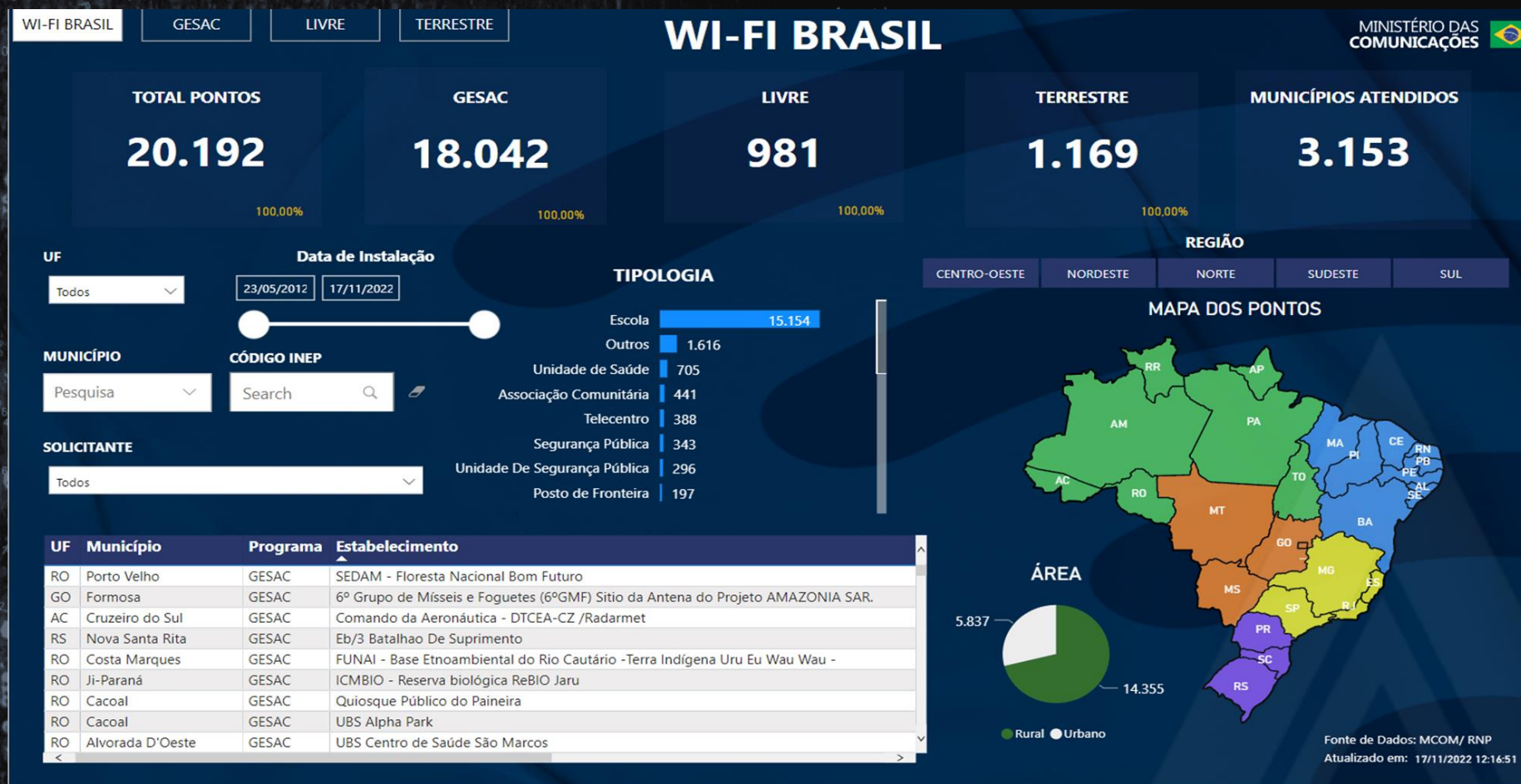
OBJETIVOS

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 inexistia 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=eyJrIjoiTUM3NzkwZjYtNTVjYi00YTU5LWExOGUtYzNiZTMzMjY2ZDVmliwidCI6ImExMTIwMGVhLTNhYTctNDZhMy05M2UxLTcwYWU4ZmMxZWMyYSJ9&pageName=ReportSection2bdd6a5c141f7bb78457>

Comportamento dos usuários



11%

das organizações usam MFA, em geral.



73%

Das contas online usam senhas duplicadas.



58%

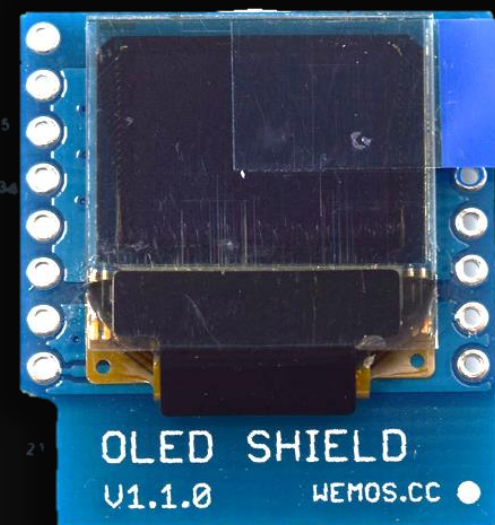
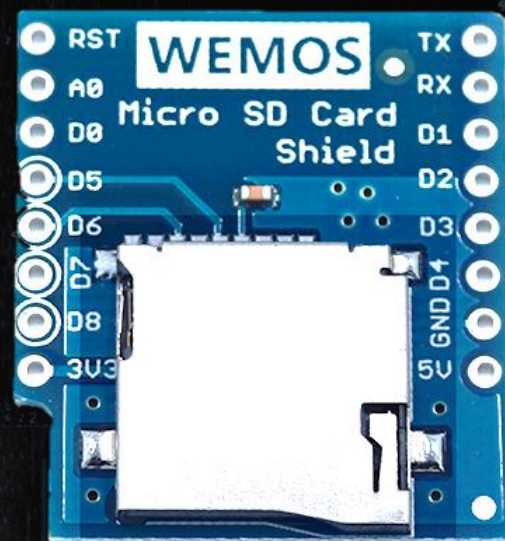
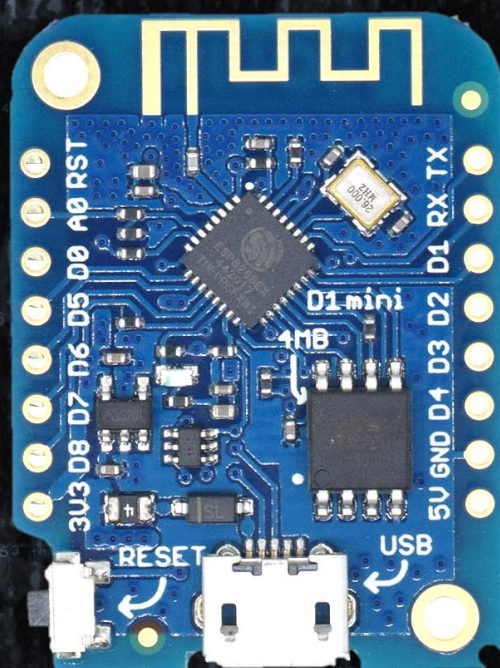
Dos brasileiros acreditam que suas informações pessoais estão seguras ao usar uma rede Wi-Fi pública

<https://webinarcare.com/best-multi-factor-authentication-software/multi-factor-authentication-statistics/#1>

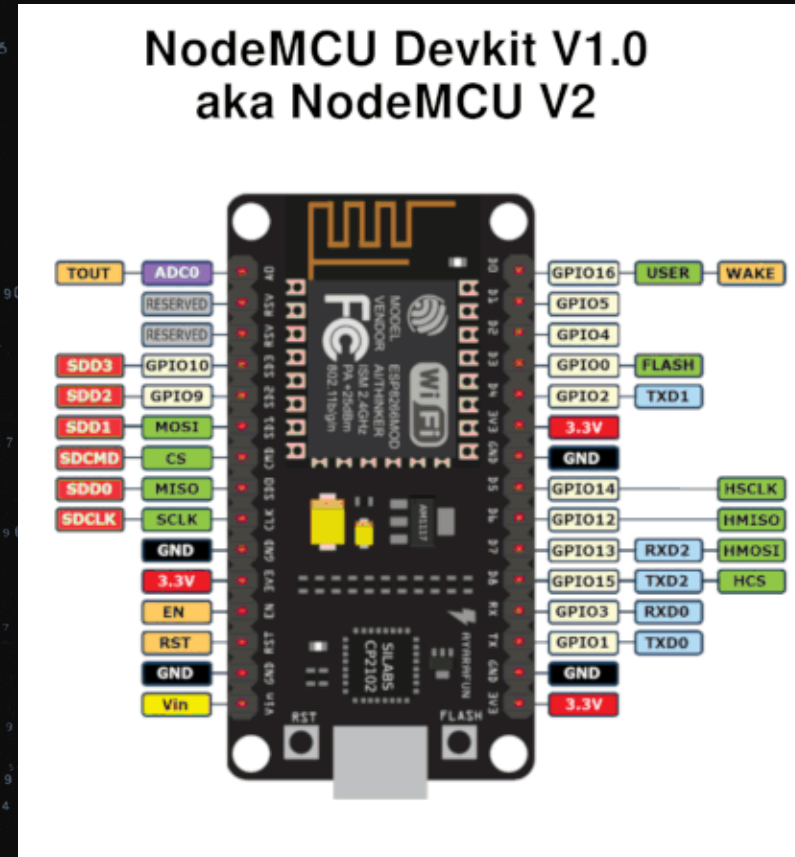
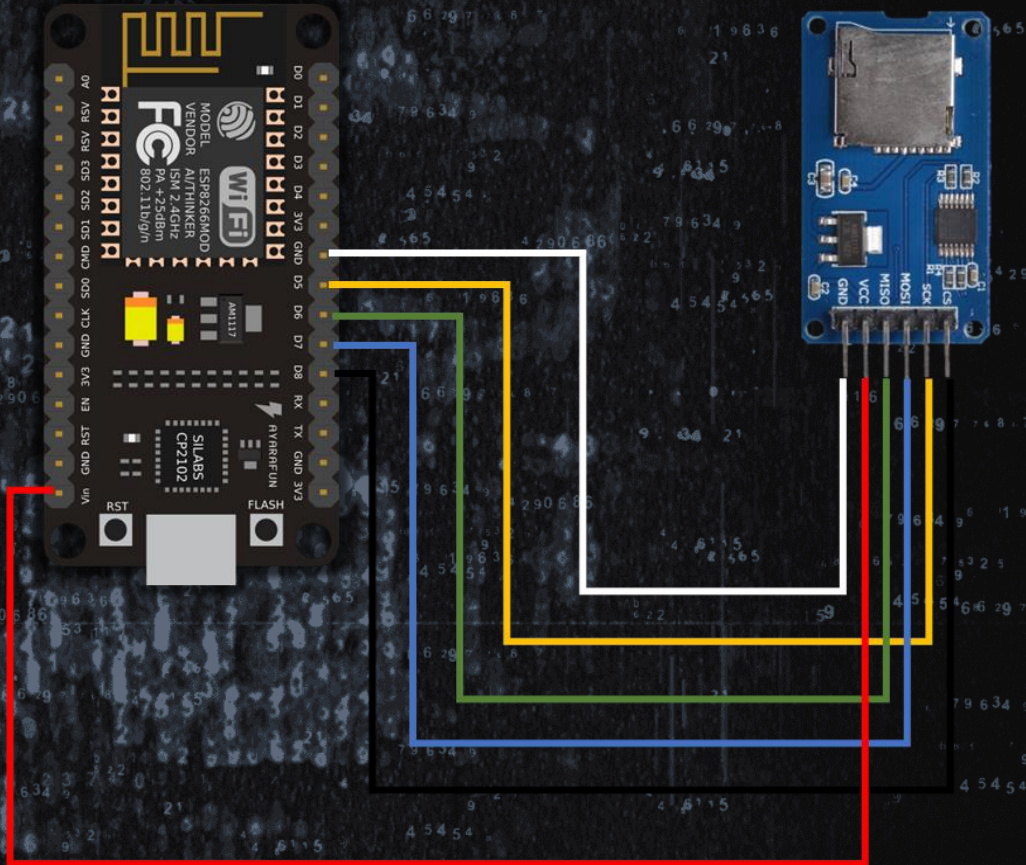
E se um atacante tiver explorar este cenário?



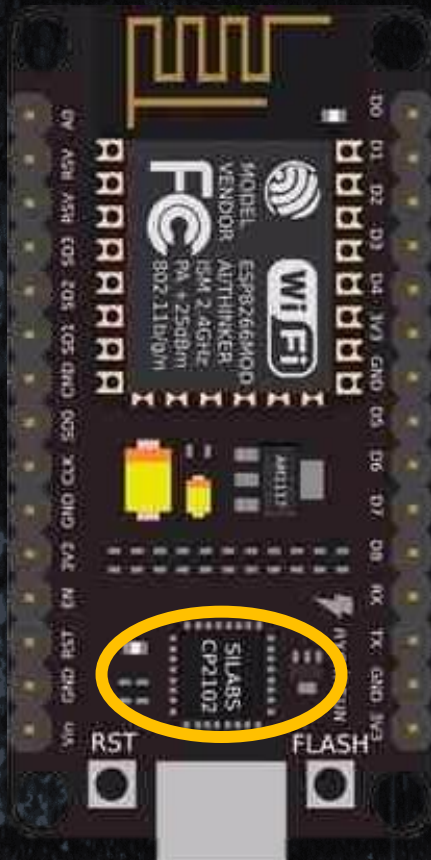
E se um atacante tiver explorar este cenário?



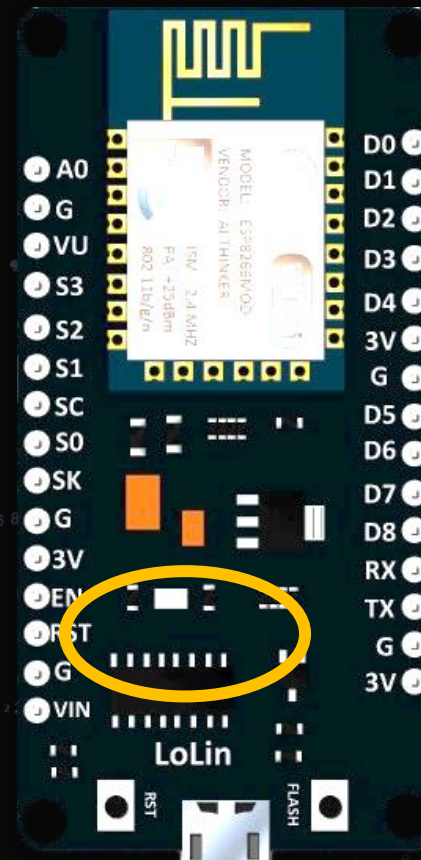
E se um atacante tiver explorar este cenário?



E se um atacante tiver explorar este cenário?

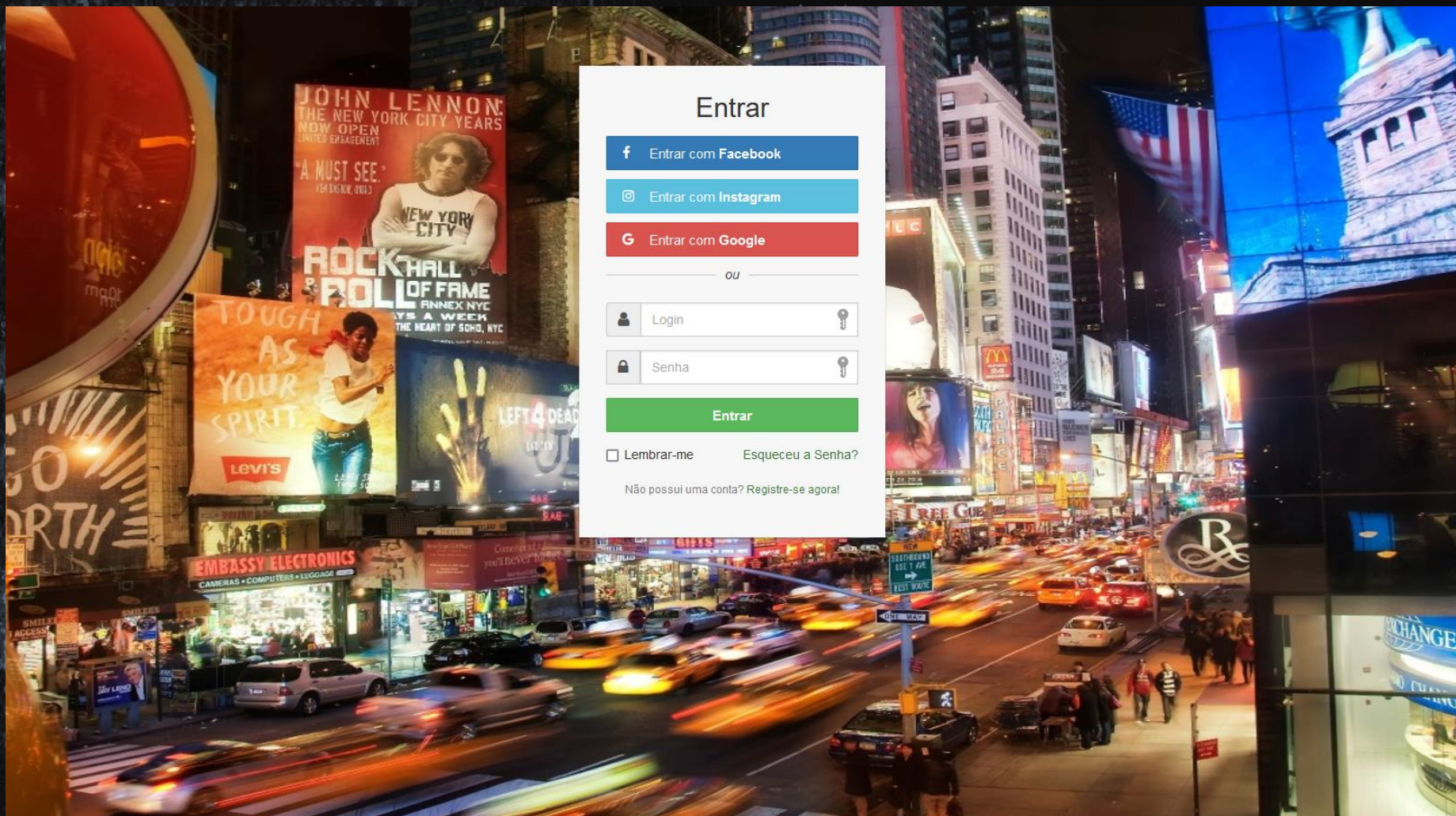


CP2102

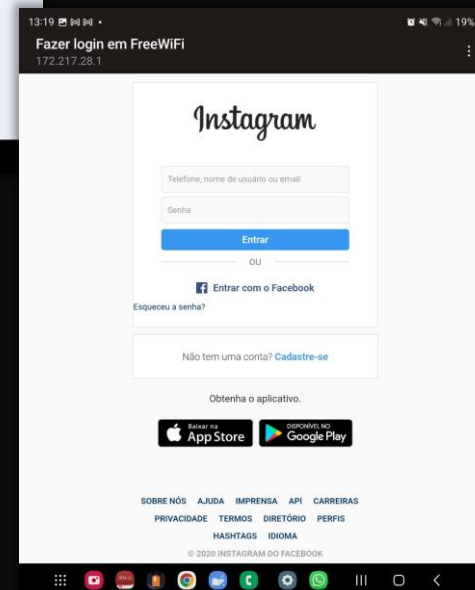
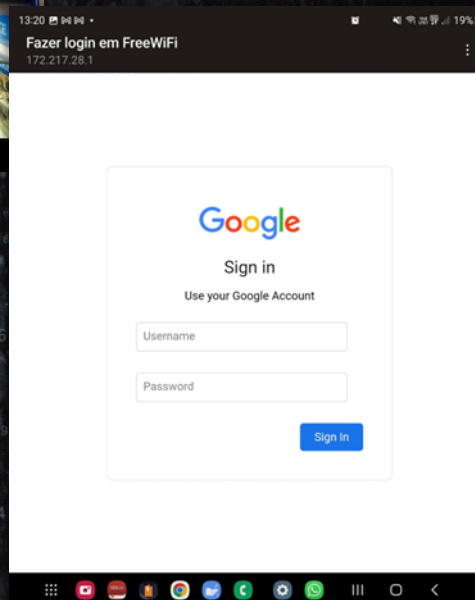
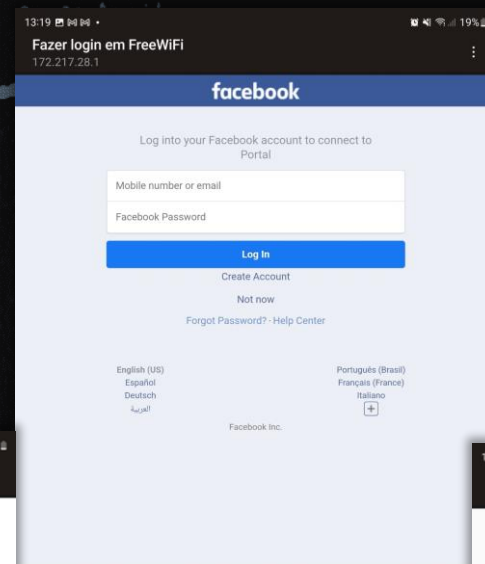
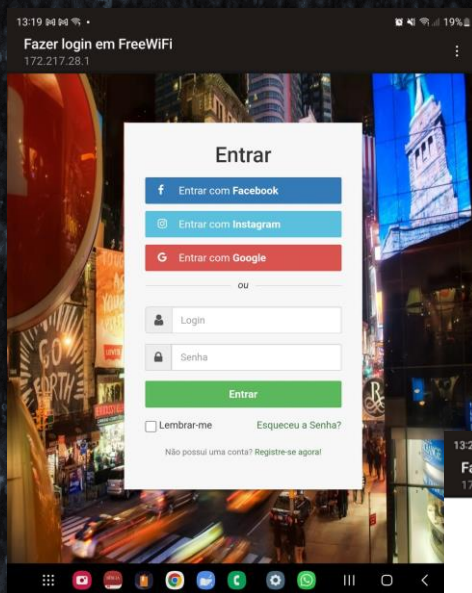


CH34X

E se um atacante tiver explorar este cenário?



Vários templates para uso



Gerenciamento realizado via SERIAL (conexão USB)



COM4

Enviar

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

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

Erro (error.txt): erro1.htm

Tecla ? para ver a lista de comandos

Connected clients: 0

☒ Auto-rolagem ☐ Show timestamp

Nenhum final-de-linha 9600 velocidade Deleta a saída

Conexão Serial (Putty ou App)



COM4

Enviar

Connected clients: 0

***** Lista de Comandos *****

- * T - Para ler os Termos de Uso da ferramenta *
- * MModelo> - Para usar os modelos (Ex: MPortal.htm) *
- * E<Erro> - Para usar os modelos (Ex: EErro.htm) *
- * S<SSID> - (Ex:SInternet ou SFree_WiFi) *
- * L - Mostrar logs dos dados captrados *
- * D - deleta os dados no arquivos de LOGS *
- * C - Mostrar as configuracoes do sistema *
- * A - Listar os arquivos do Cartao de memoria *
- * 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

172.217.28.1/admin.htm

deve se autenticar nessa rede antes de poder acessar a internet. [Abrir página de acesso à rede](#)



WiFi Phishing Admin

SSID

FreeWiFi

MODELO

bhack.htm
portal.htm
modelot1.htm
facebook.htm
insta.htm
...

RETORNO

ebhack.htm
errfb.htm
errgoo.htm
erro1.htm
errn04.htm
...

DADOS


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

Salvar

http://172.217.28.1/admin.htm

É possível criar um novo rede em segundos

deve se autenticar nessa rede antes de poder acessar a internet. [Abrir página de acesso à rede](#)



WiFi Phishing Admin

SSID

FreeWiFi

MODELO

bhack.htm
portal.htm
modelot1.htm
facebook.htm
insta.htm
...

RETORNO

ebhack.htm
errfb.htm
errgoo.htm
erro1.htm
err404.htm
...

DADOS

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

Salvar

<http://172.217.28.1/admin.htm>

Define o nome do SSID

Define a página do Ataque

Define a página do Erro

Exibe os dados capturados

Entre e marque
seus amigos

 Entrar com Facebook

 Entrar com Instagram

 Entrar com Google

ou

 Login

 Senha


Entrar

☐ Lembrar-me [Esqueceu a Senha?](#)

Não possui uma conta? [Registre-se agora!](#)

  **BHACK**
SEGURANÇA TI - CONHECIMENTO


BHACK EDITION

 **BHACK**
SEGURANÇA TI - CONHECIMENTO

Cuidado, hackers podem estar onde você menos imagina!

WALL OF SHEEP


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



Como criar novos arquivos

Nossas lojas Tenha sua loja Regulamentos Acessibilidade Guia de segurança

Atendimento Compre pelo tel: 0800 773 3838 Meus pedidos



Bem-vindo :)
Entre ou cadastre-se

Ver ofertas para minha região

0

Todos os departamentos

Ofertas do Dia

Celulares

Móveis

Eletrodomésticos

TV e Vídeo

Informática

Saldão

Black das Blacks

Cartão Magalu

Smartphoniza

Identificação

Quero criar uma conta

E-mail

[Dúvidas? fale conosco](#)

Continuar

Já sou cliente

E-mail, CPF ou CNPJ

Senha

[Esqueci minha senha](#)

Continuar

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



SingleFile

★★★★★ 948 ⓘ

Produtividade

100.000+ usuários

Remover do Google Chrome

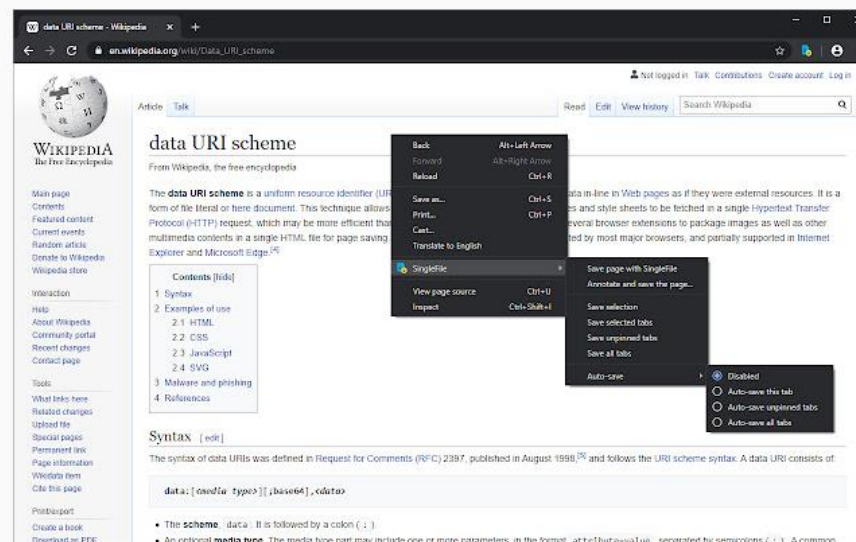
Visão geral

Práticas de privacidade

Comentários

Suporte

Itens relacionados



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>

The screenshot shows the GitHub repository page for **AcadiTi/Bhack2022**. The repository is public and has 0 stars, 1 watching, and 0 forks. The main branch is **main** with 1 branch and 0 tags. The repository contains a commit **f19a918** from 1 minute ago with 2 commits. The commit message is **AcadiTi upload full material**. The commit details show a table of files:

File	Commit Message	Time
Case	upload full material	1 minute ago
SD CARD	upload full material	1 minute ago
Script	upload full material	1 minute ago
.gitattributes	Initial commit	10 minutes ago

Below the table, there is a prompt to **Add a README** to help people understand the project. The right sidebar shows the **About** section with the description **Material apresentado na Bhack 2022**, and the **Releases** and **Packages** sections, both indicating no published items.

Utilizando Hardware Hacking para coleta de credenciais



Obrigado!



/leonardolarosa



/school/acaditi



/academiainovadora



/acaditi_oficial



/@ACADITI