

# A3 - Sensitive Data Exposure



# Agenda - A3 - Exposição de Dados Sensíveis

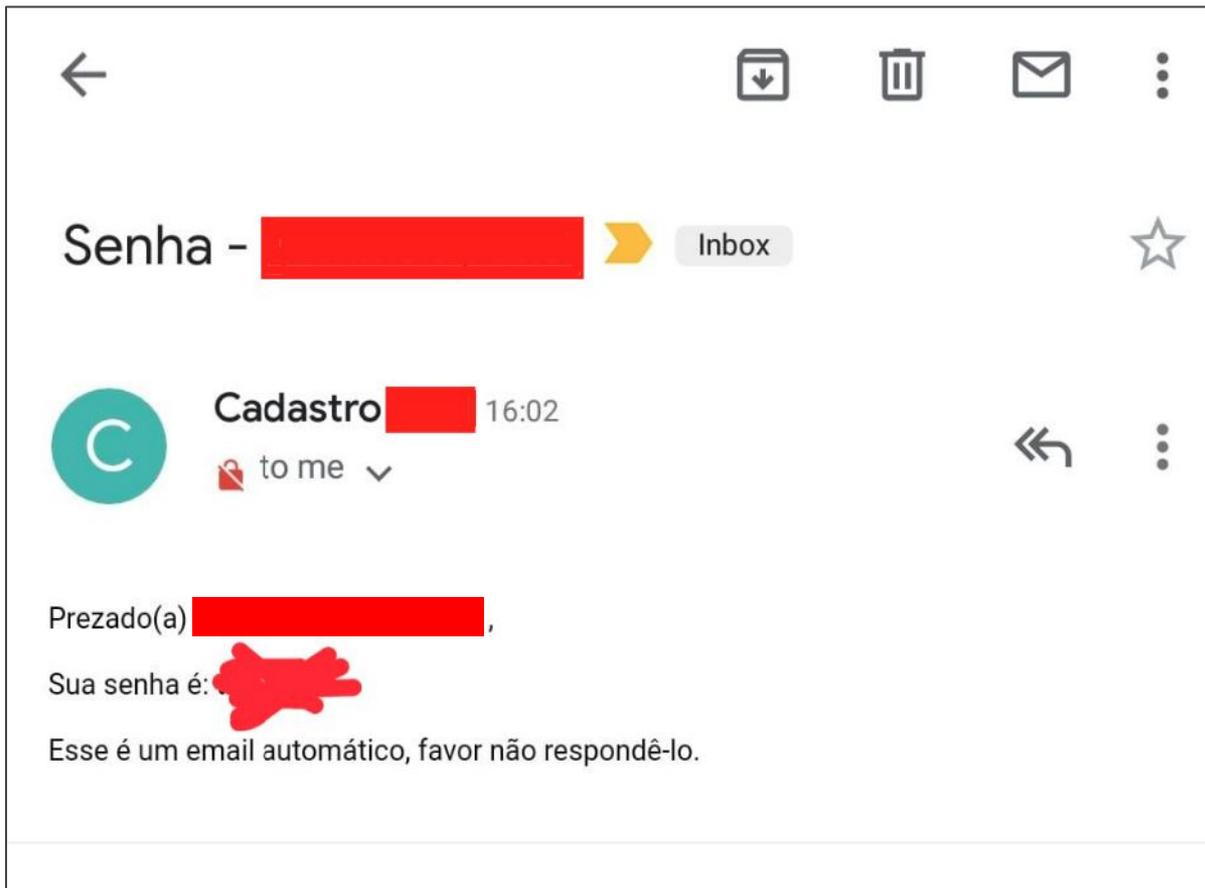


1. Do que se trata?
2. Função "Esqueceu sua senha?"
3. Senha passada como parâmetro na URL
4. HTTP vs HTTPS
5. Como se proteger?
6. Snake Pro

## Do que se trata?



Muitas aplicações web não protegem devidamente os dados sensíveis, tais como **cartões de crédito** e **credenciais de autenticação**. Os atacantes podem **roubar** ou **modificar** esses dados desprotegidos com o propósito de realizar **fraudes** de cartões de crédito, roubo de identidade, ou outros crimes.



Função "Esqueceu sua senha?"



senha txt		acesso_dt
51ade4e8b808276335290	d0055a	2008-09-0
ff5390bde5a4cf0aa2006cf2	efd29	2008-10-0
7cbb3252ba6b7e9c422fac	d22054	2008-10-1
7cbb3252ba6b7e9c422fac	d22054	2018-08-0
7cbb3252ba6b7e9c422fac	d22054	2010-08-0
7cbb3252ba6b7e9c422fac	d22054	2009-02-0
7cbb3252ba6b7e9c422fac	d22054	0000-00-0
e534e0dfb211d5bff5fa2787	a47c5	2009-02-2
e534e0dfb211d5bff5fa2787	a47c5	2011-11-0

**Your Hash:** 7cbb3252ba6b7e9c422fac5334d22054  
**Your String:** q1w2e3

Senha criptografada



https://[REDACTED]/account/password/reset?password=newpassword&confirm-password=newpassword

# Alterar sua senha

Insira um novo senha para usar para fazer login. Faça-o seguro!

A sua definição de senha é inválido.

A senha deve ter mais de 8 caracteres

Senha passada como parâmetro na URL



← → ↻ 🏠 ⓘ Not Secure | ██████████/user/register

### CADASTRE uma conta grátis

**E-mail**

**Senha**

Lembrar-me

**Entre** [Esqueceu sua Senha?](#)

**Nome\***

**Senha\***

**Insira novamente a senha\***

**E-mail\***

**Celular**

Não sou um robô  reCAPTCHA  
Privacidade - Termos



```
x [22:24] rafael.santos@labs:~/go/src/github.com/globocom/secDevLabs/owasp-top10-2013
$ sudo tcpdump -i lo0 -X host localhost | grep -C 2 user= --color
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo0, link-type NULL (BSD loopback), capture size 262144 bytes
0x02f0: 554a 7038 6434 6762 656c 524e 7531 7767  UJp8d4gbelRNU1wg
0x0300: 6f32 3365 7968 4d45 6a4b 5565 7955 3668  o23eyhMEjKUeyU6h
0x0310: 5734 7041 410d 0a0d 0a75 7365 723d 7261  W4pAA....user=ra
0x0320: 6661 656c 2670 6173 733d 7669 6e69 4a72  fael&pass=viniJr
0x0330: 7368 6f77 3230                               show20
```

## HTTP vs HTTPS

# Como se proteger?



1. Tenha a certeza de **criptografar** todos os dados sensíveis em repouso e em trânsito de uma forma que iniba estas ameaças. 
2. Não armazene **dados sensíveis** desnecessariamente. Descarte-os o mais rápido possível. Dados que você não tem não podem ser roubados. 
3. Certifique-se que as **senhas são armazenadas com um algoritmo projetado especialmente para a proteção de senhas**, como o bcrypt, PBKDF2 ou scrypt. 





## Narrativa do ataque



## 1. Entrar na pasta da app

```
$ cd secDevLabs/owasp-top10-2017-apps/a3/snake-pro
```

## 2. Inicializar o container

```
$ make install
```

## 3. Acessar a página

```
localhost:10033
```



## A3 - Sensitive Data Exposure

