A3 - Sensitive Data Exposure

globo.com

GTS 33 | PA 05/2019

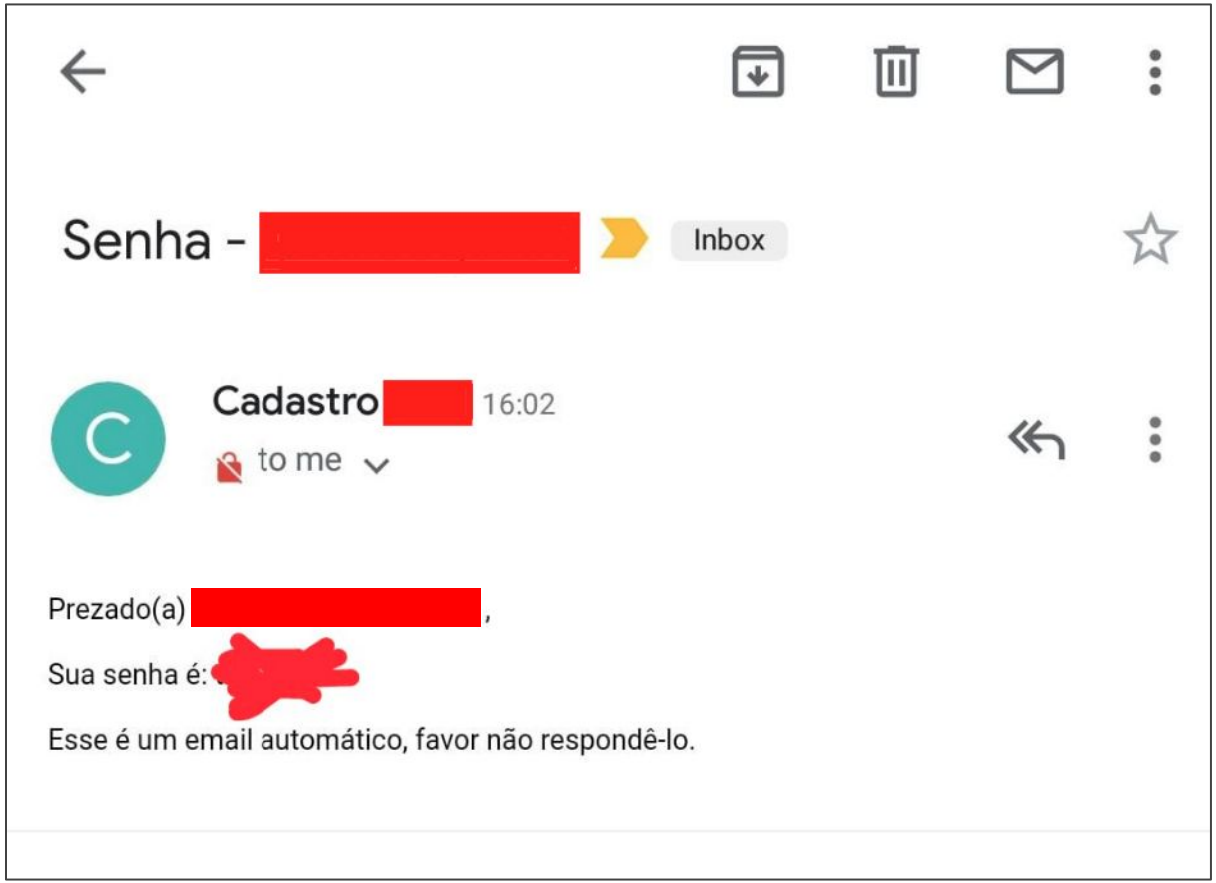
Agenda - A3 - Exposição de Dados Sensíveis

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

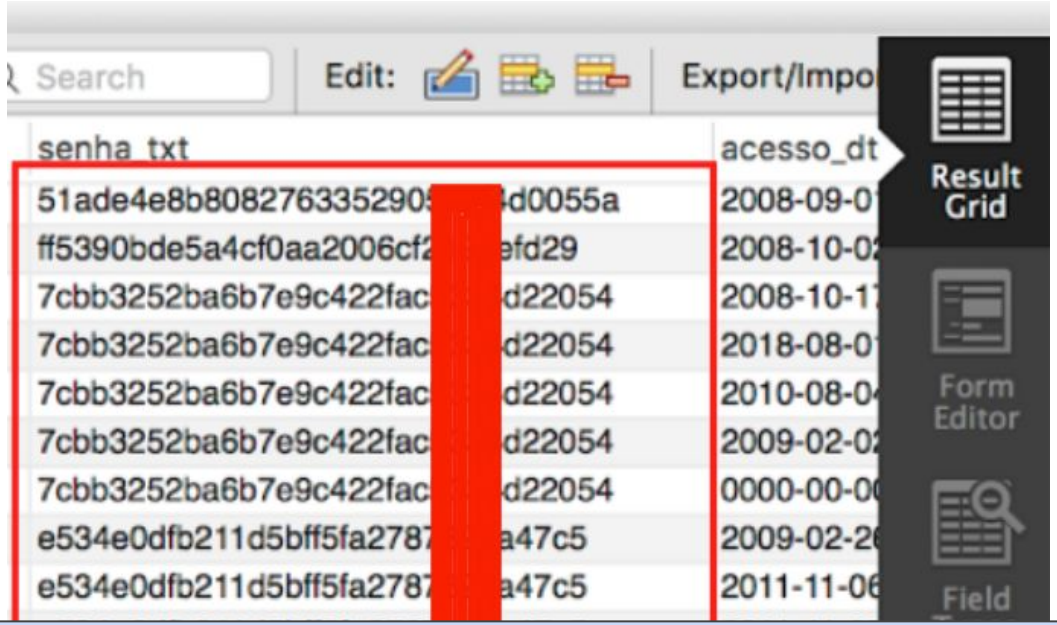
Do que se trata?

globo.com

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.



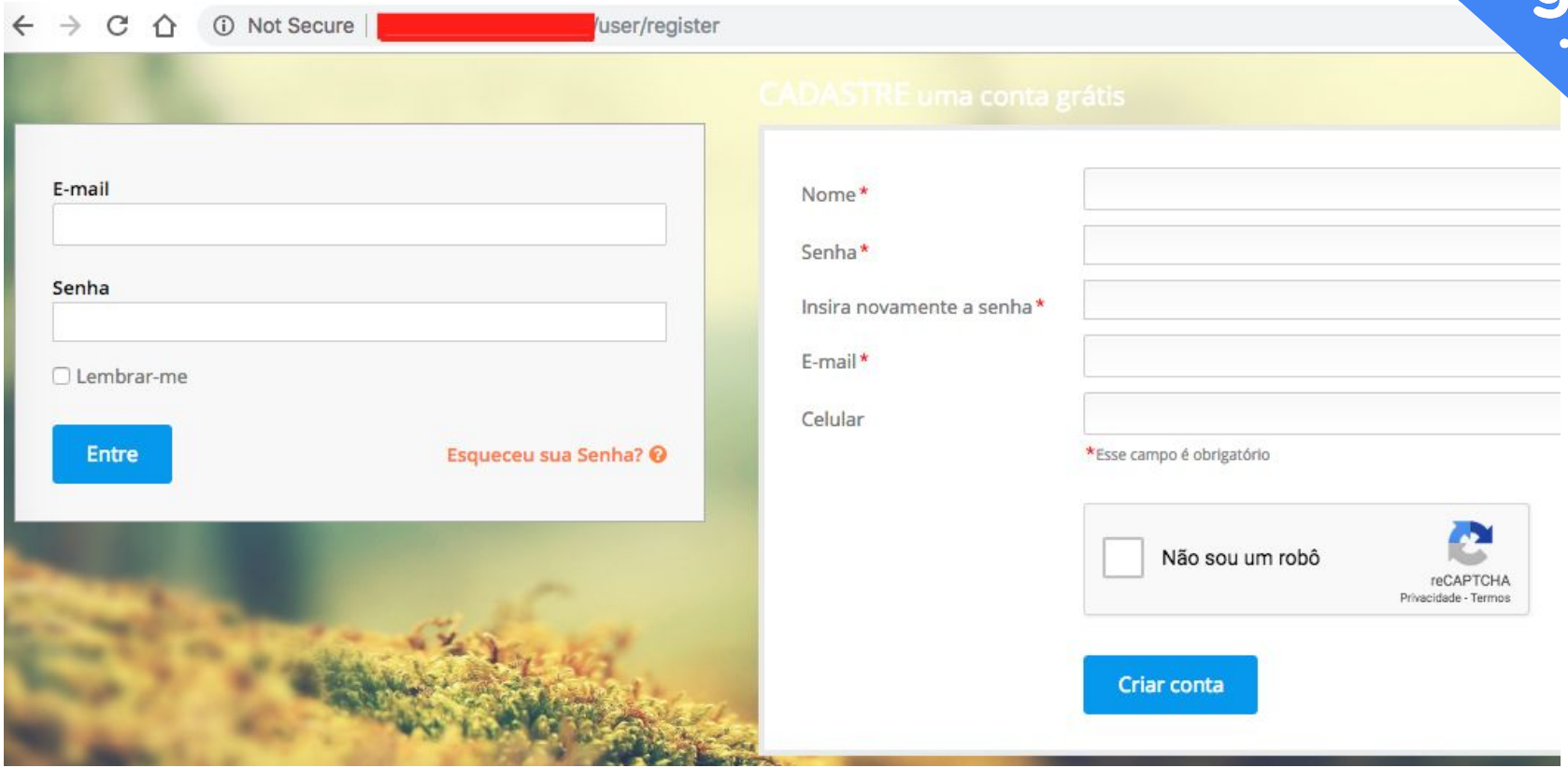
Função "Esqueceu sua senha?"



Your Hash: `7cbb3252ba6b7e9c422fac5334d22054`
Your String: `q1w2e3`

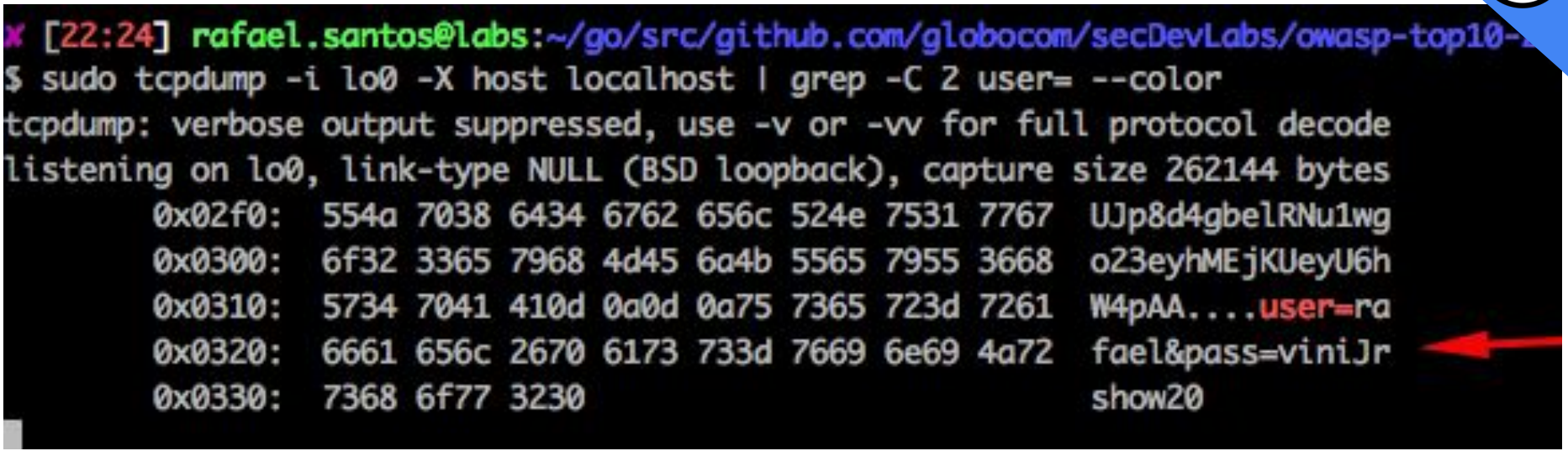
Senha criptografada

Senha passada como parâmetro na URL



globo.com

HTTP vs HTTPS

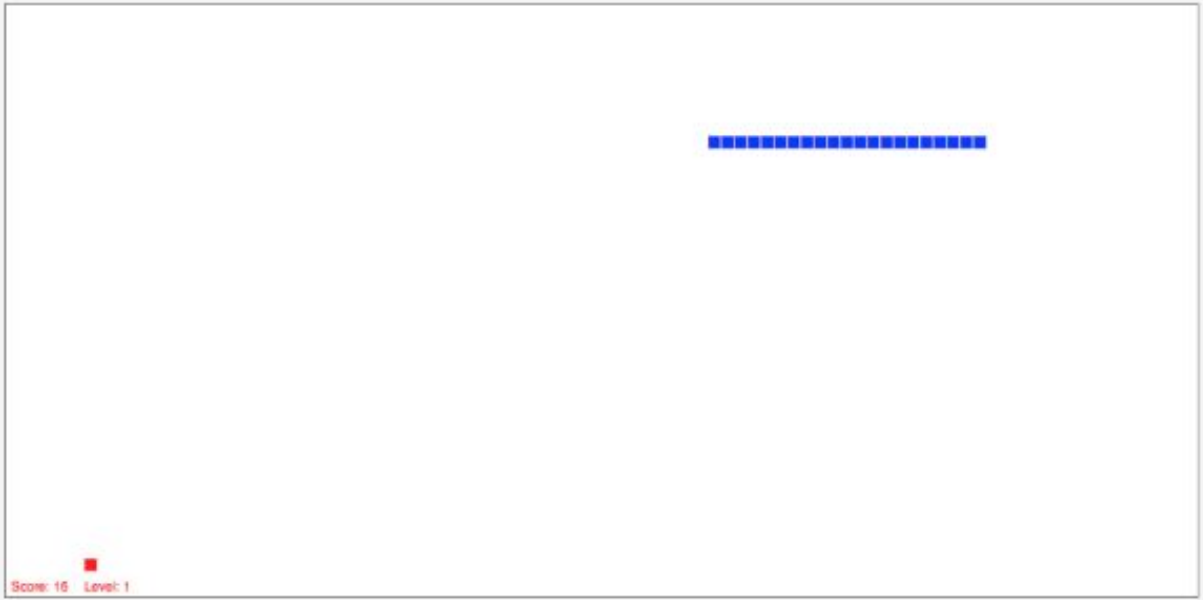


HTTP vs HTTPS

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. 💪

SnakePro



Narrativa do ataque

Hands on!

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
```

globo.com

A3 - Sensitive Data Exposure