A2 - Broken Authentication

globo.com

GTS 33 | PA 05/2019

Agenda - A2 - Broken Authentication

1. Do que se trata?
2. Exemplos
3. Como se Proteger?
4. Saidajaula Monster Fit

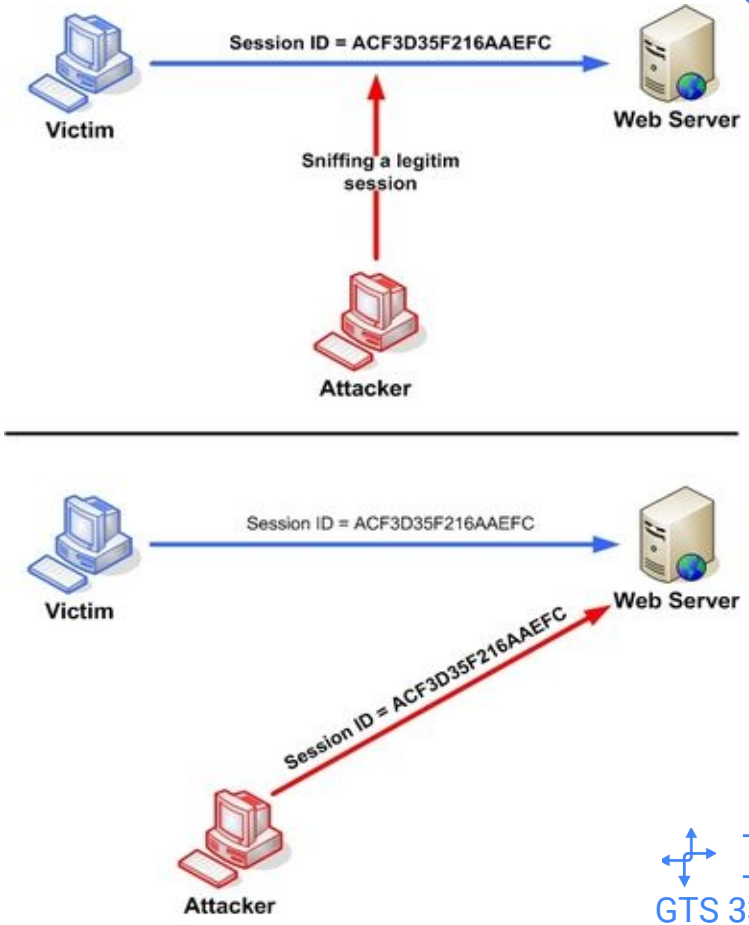
Do que se trata?

Um atacante é capaz de comprometer senhas, chaves ou tokens com a finalidade de assumir outra identidade.

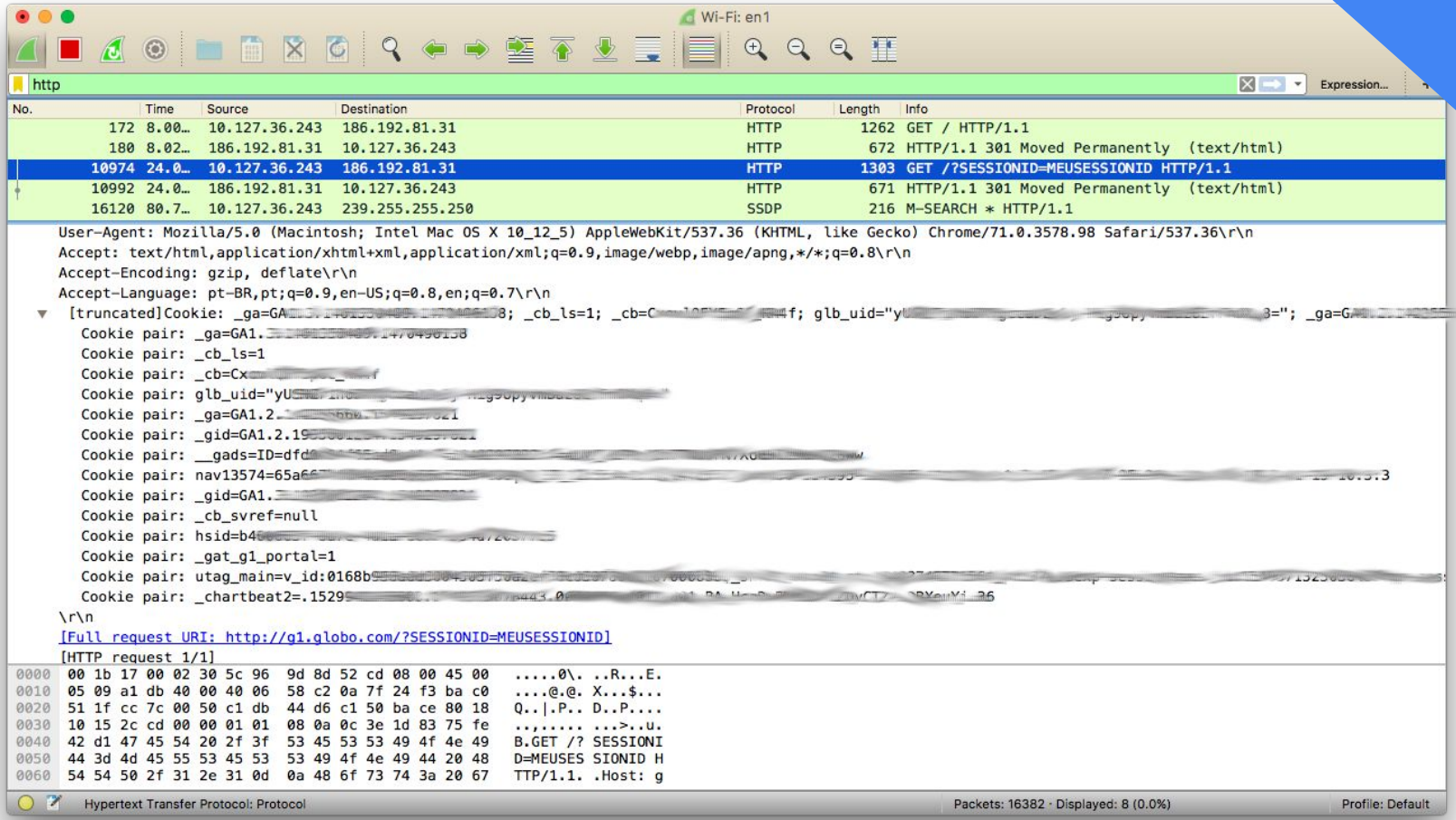
Mensagens de Erro Diferentes

Mensagens de Erro Diferentes

http://site.com/?sessionID=AFC3D35F216AAEFC

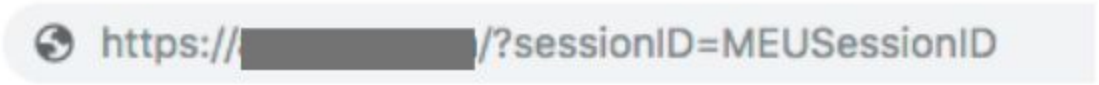


Session Hijacking



globo.com

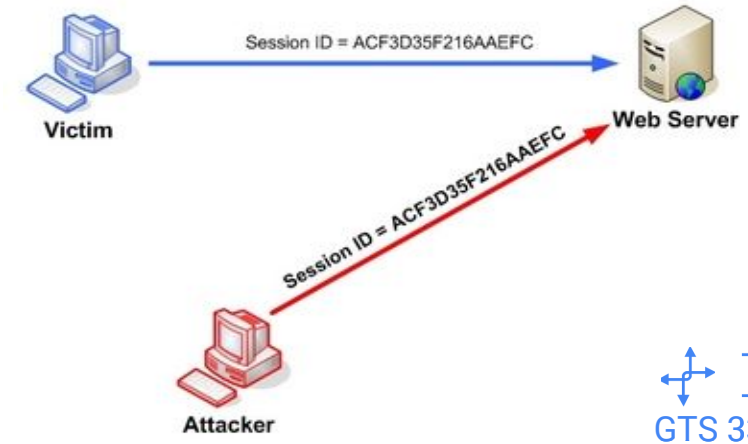
Session Hijacking



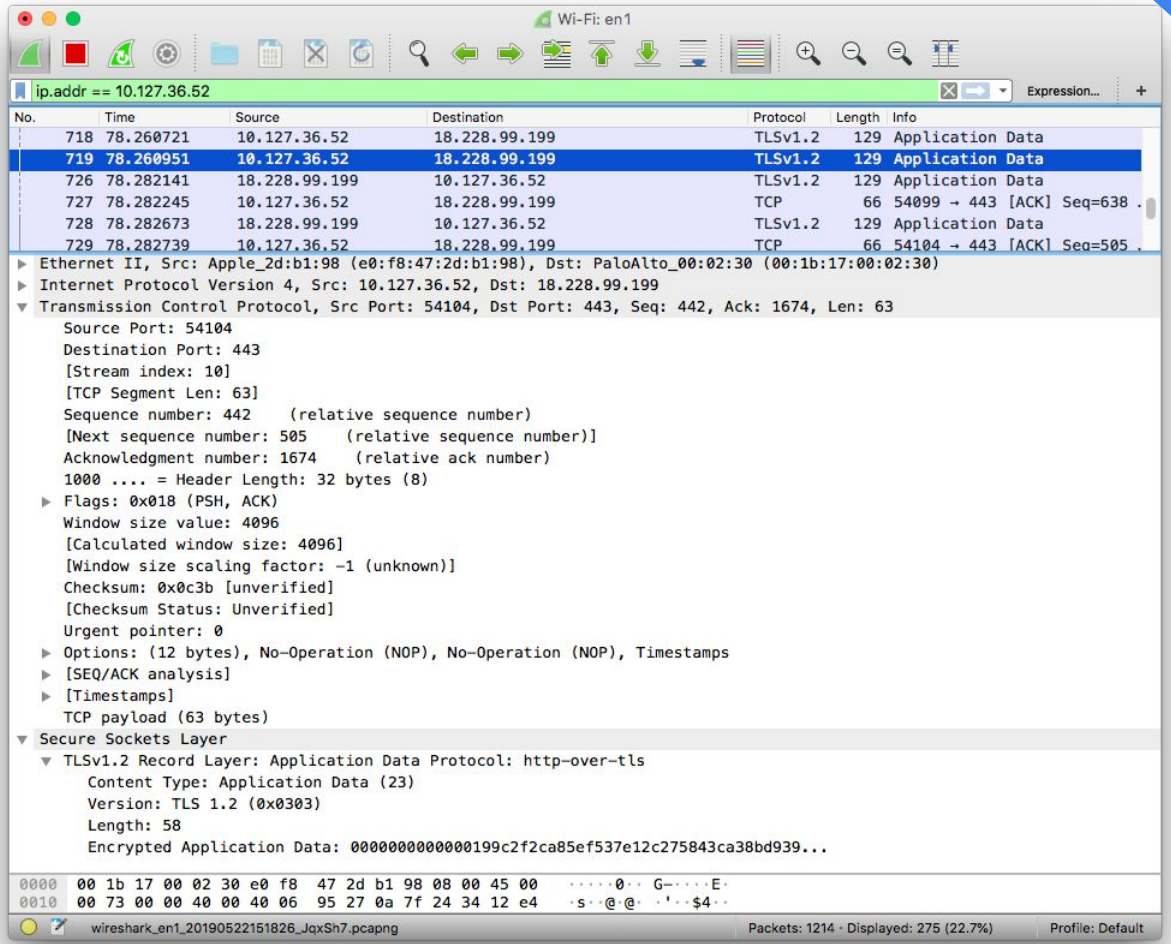
Session Hijacking

https://site.com

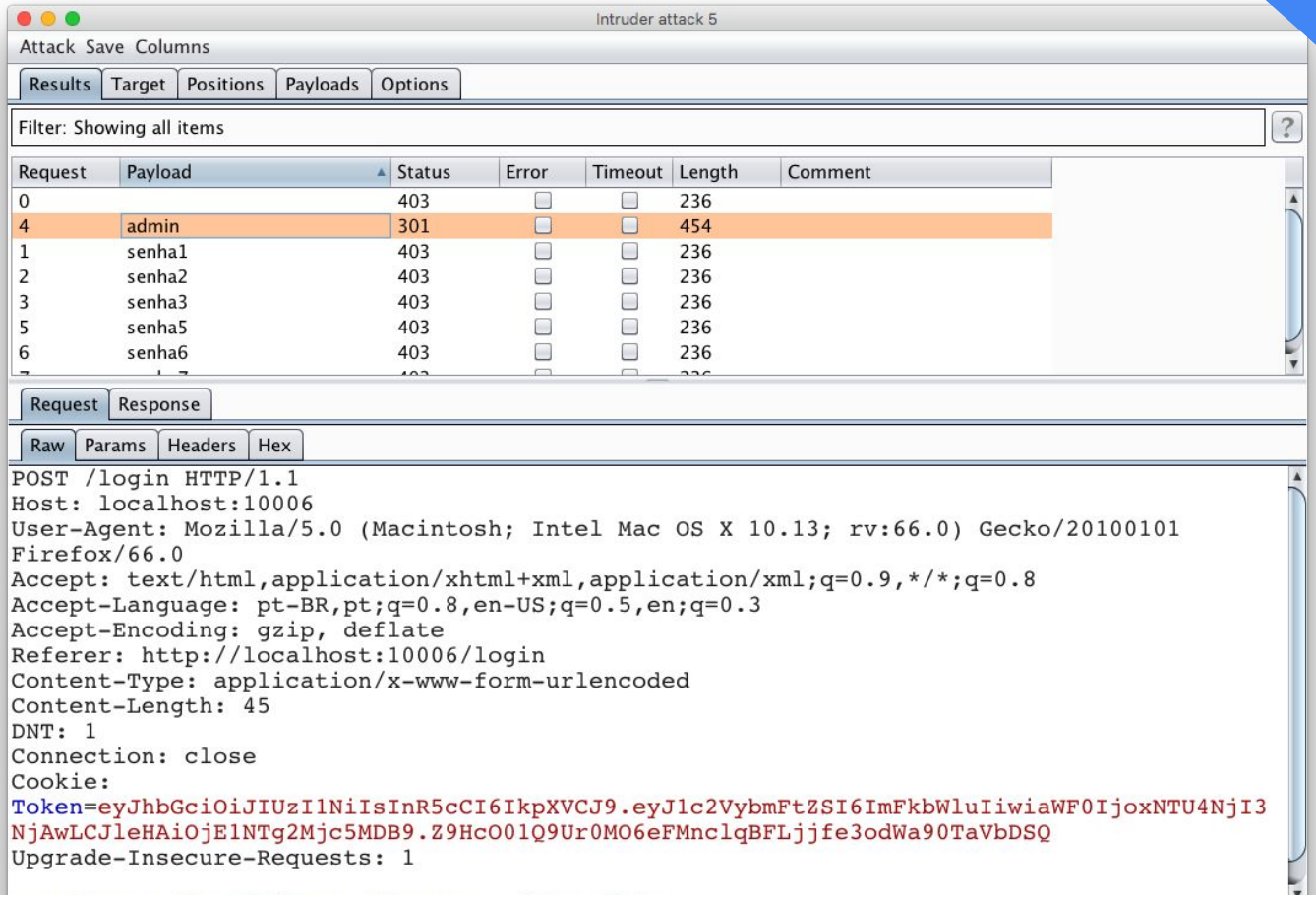
{'user' : 'user1',
'sessionID' : 'ACF3D35F216AAEFC'}



Session Hijacking



Session Hijacking



Ataque Força Bruta

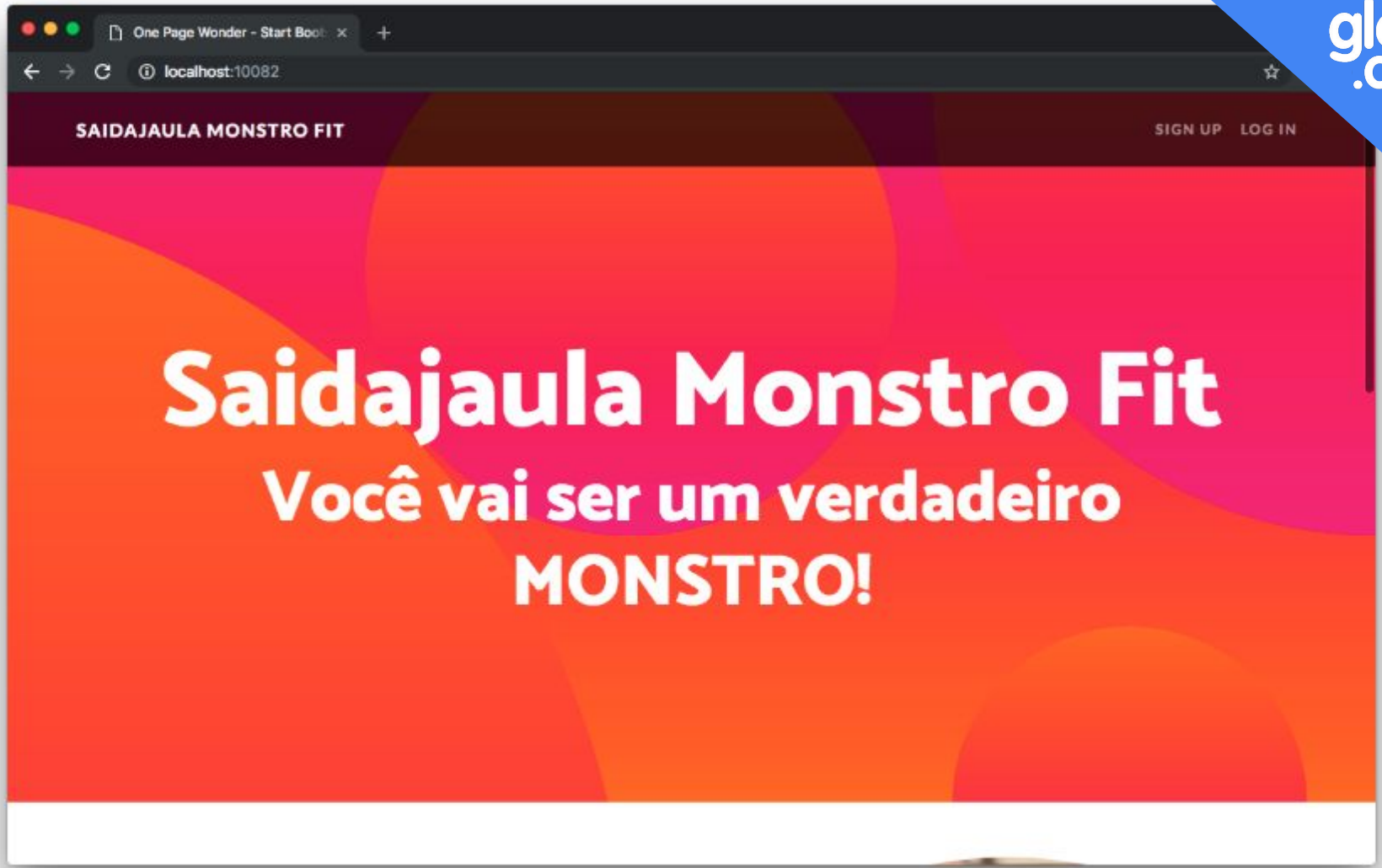
Ataque Força Bruta

Como se proteger?

1. Uso de **sistemas multistage** com barreiras adicionais ao sistema de autenticação. 🚷
2. Uso de **CAPTCHA** para mitigar um ataque de força bruta em rotas específicas da aplicação. 😺
3. **Conscientizar** usuários sobre os benefícios de utilizar senhas fortes e **não reaproveitadas**. 🔎

Como se proteger?

4. Envio de **e-mails** para a conta registrada do usuário informando sobre alterações importantes na conta, como troca de senha, login realizado num dispositivo desconhecido etc. 📩
5. **Padronizar** mensagens de erro para que elas não acusem exatamente que elementos do formulário estão inválidos. 💬
6. Evitar uso de **dados de usuários previsíveis** na geração de cookies e identificadores de sessão, por exemplo. 🕒
7. **Manuseio seguro** de credenciais, transmitindo em um canal seguro como, por exemplo, o HTTPS. 🔐


One Page Wonder - Start Boot
localhost:10082
SAIDAJAULA MONSTRO FIT
SIGN UP
LOG IN
Saidajaula Monstro Fit
Você vai ser um verdadeiro
MONSTRO!

Narrativa do ataque

Hands on!

1. Entrar na pasta da app

```
$ cd owasp-top10-2017-apps/a2/saidajaula-monster
```

2. Inicializar o container

```
$ make install
```

3. Acessar a página

```
localhost:10082
```

globo.com

A2 - Broken Authentication