Aumentando a segurança em aplicações Front End

O que vocês verão nessa apresentação

Com os avanços da tecnologia, as táticas utilizadas por pessoas má intencionadas estão cada vez mais avançadas.

Vamos compartilhar algumas das pesquisas e ações que tomamos em nossas aplicações afim de garantir a segurança dos usuários.

Riscos

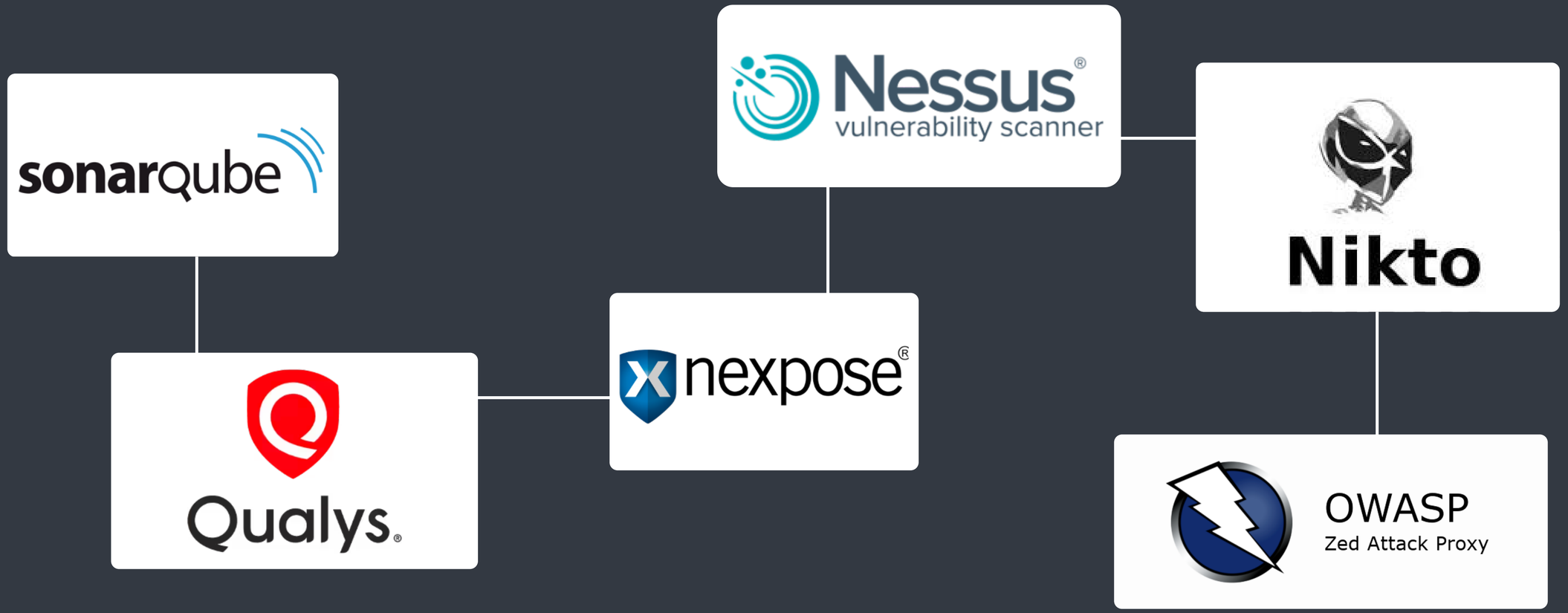
O Front-end normalmente é a primeira camada que o seu usuário entrará em contato. Quando mais seguro, mais difícil se tornará para que uma pessoa má intencionada engane o usuario ou consiga informações confidenciais da sua aplicação.

- Clicar em um link malicioso
- Interagir com um formulario falso
- Obter informações sobre a sessão do seu usuario
- Ser exposto a um protocolo não seguro
- Ser redirecionado para um site falso

E esses são apenas alguns dos muitos riscos que seu usuario corre na camada do frontend ...

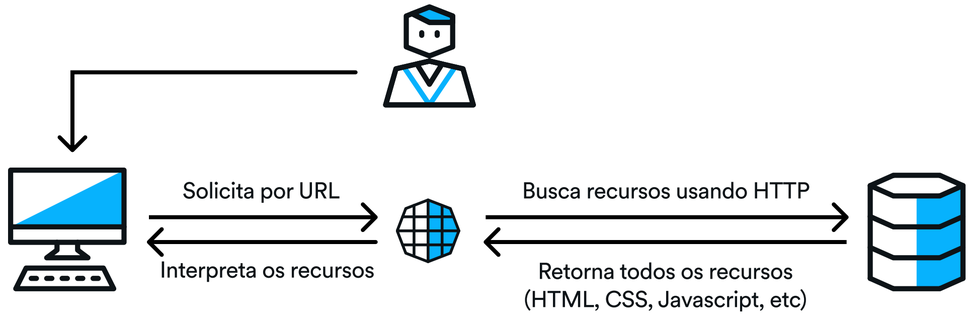
Ferramentas

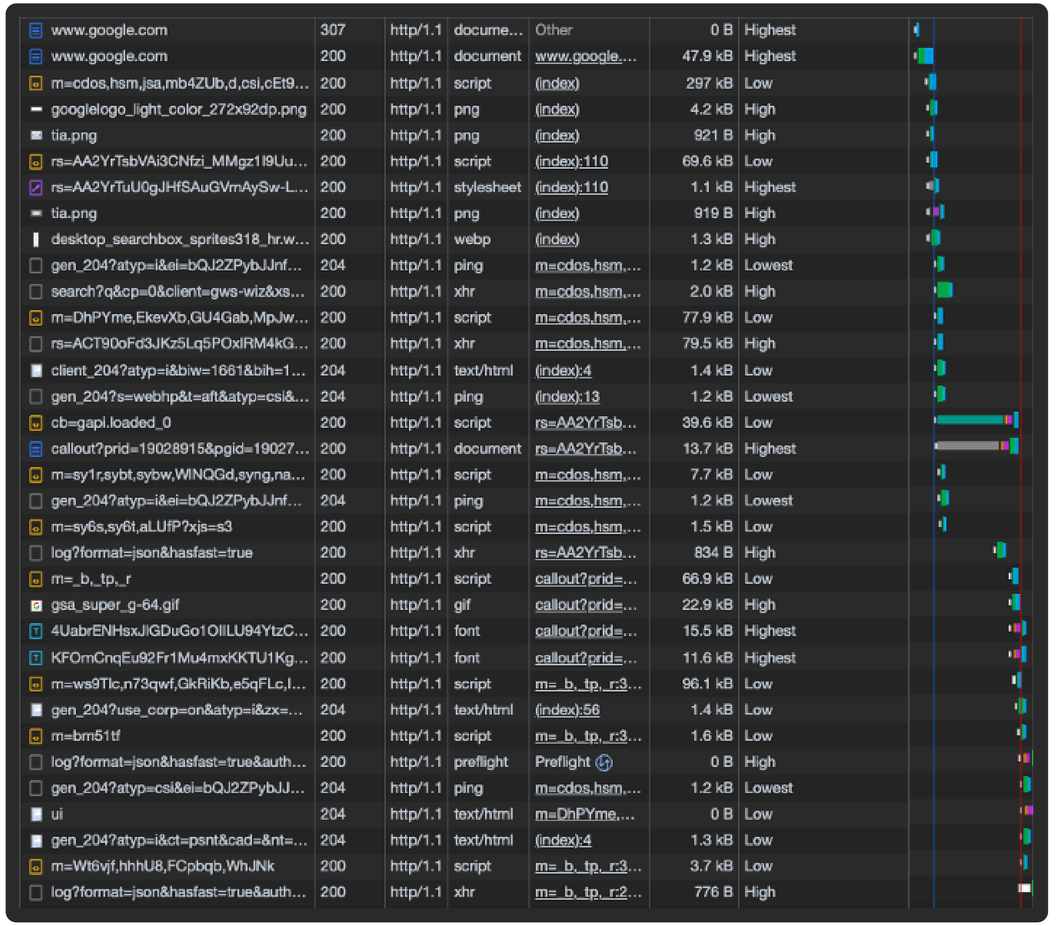
Hoje, contamos com diversas ferramentas no mercado para nos auxiliar a verificar a segurança de nossas aplicações



Navegador

Entendendo como o navegador funciona





www.google.com	307	http/1.1	docume…	Other	0 B	Highest
www.google.com	200	http/1.1	document	www.google.…	47.9 kB	Highest
m=cdos,hsm,jsa,mb4ZUb,d,csi,cEt9…	200	http/1.1	script	(index)	297 kB	Low
googlelogo_light_color_272x92dp.png	200	http/1.1	png	(index)	4.2 kB	High
tia.png	200	http/1.1	png	(index)	921 B	High
rs=AA2YrTsbVAi3CNfzi_MMgz1l9Uu…	200	http/1.1	script	(index):110	69.6 kB	Low
rs=AA2YrTuU0gJHfSAuGVmAySw-L…	200	http/1.1	stylesheet	(index):110	1.1 kB	Highest
tia.png	200	http/1.1	png	(index)	919 B	High
desktop_searchbox_sprites318_hr.w…	200	http/1.1	webp	(index)	1.3 kB	High
gen_204?atyp=i&ei=bQJ2ZPybJJnf…	204	http/1.1	ping	m=cdos,hsm,…	1.2 kB	Lowest
search?q&cp=0&client=gws-wiz&xs…	200	http/1.1	xhr	m=cdos,hsm,…	2.0 kB	High
m=DhPYme,EkevXb,GU4Gab,MpJw…	200	http/1.1	script	m=cdos,hsm,…	77.9 kB	Low
rs=ACT90oFd3JKz5Lq5POxIRM4kG…	200	http/1.1	xhr	m=cdos,hsm,…	79.5 kB	High
client_204?atyp=i&biw=1661&bih=1…	204	http/1.1	text/html	(index):4	1.4 kB	Low
gen_204?s=webhp&t=aft&atyp=csi&…	204	http/1.1	ping	(index):13	1.2 kB	Lowest
cb=gapi.loaded_0	200	http/1.1	script	rs=AA2YrTsb…	39.6 kB	Low
callout?prid=19028915&pgid=19027…	200	http/1.1	document	rs=AA2YrTsb…	13.7 kB	Highest
m=sy1r,sybt,sybw,WINQGd,syng,na…	200	http/1.1	script	m=cdos,hsm,…	7.7 kB	Low
gen_204?atyp=i&ei=bQJ2ZPybJJnf…	204	http/1.1	ping	m=cdos,hsm,…	1.2 kB	Lowest
m=sy6s,sy6t,aLUfP?xjs=s3	200	http/1.1	script	m=cdos,hsm,…	1.5 kB	Low
log?format=json&hasfast=true	200	http/1.1	xhr	rs=AA2YrTsb…	834 B	High
m=_b,_tp,_r	200	http/1.1	script	callout?prid=…	66.9 kB	Low
gsa_super_g-64.gif	200	http/1.1	gif	callout?prid=…	22.9 kB	High
4UabrENHsxJlGDuGo1OIlLU94YtzC…	200	http/1.1	font	callout?prid=…	15.5 kB	Highest
KFOmCnqEu92Fr1Mu4mxKKTU1Kg…	200	http/1.1	font	callout?prid=…	11.6 kB	Highest
m=ws9Tlc,n73qwf,GkRiKb,e5qFLc,I…	200	http/1.1	script	m=_b,_tp,_r:3…	96.1 kB	Low
gen_204?use_corp=on&atyp=i&zx=…	204	http/1.1	text/html	(index):56	1.4 kB	Low
m=bm51tf	200	http/1.1	script	m=_b,_tp,_r:3…	1.6 kB	Low
log?format=json&hasfast=true&auth…	200	http/1.1	preflight	Preflight	0 B	High
gen_204?atyp=csi&ei=bQJ2ZPybJJ…	204	http/1.1	ping	m=cdos,hsm,…	1.2 kB	Lowest
ui	204	http/1.1	text/html	m=DhPYme,…	0 B	Low
gen_204?atyp=i&ct=psnt&cad=&nt=…	204	http/1.1	text/html	(index):4	1.3 kB	Low
m=Wt6vjf,hhhU8,FCpbqb,WhJNk	200	http/1.1	script	m=_b,_tp,_r:3…	3.7 kB	Low
log?format=json&hasfast=true&auth…	200	http/1.1	xhr	m=_b,_tp,_r:2…	776 B	High

Entendendo o protocolo de requisição

HTTP

Requisições HTTP

O protocolo HTTP é um dos principais protocolos utilizado hoje para comunicacao entre navegadores e servidores.

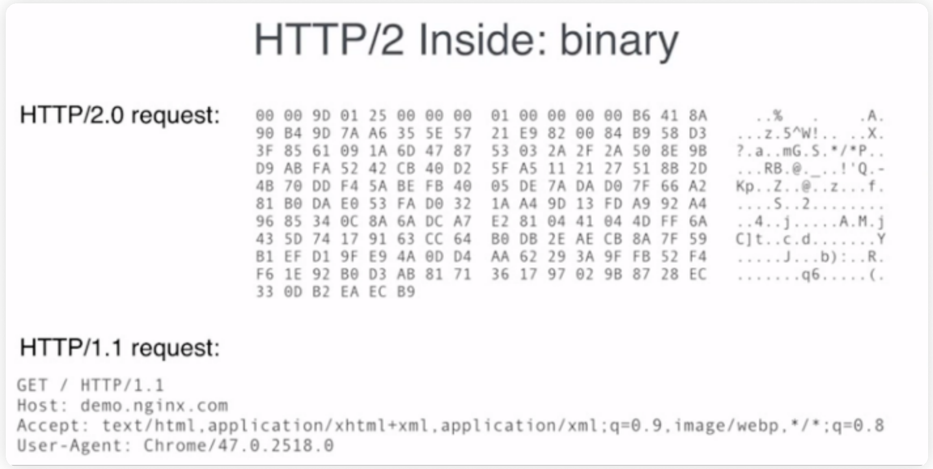
Fonte: Mazer.dev

HTTP/1.1 vs HTTP/2

No HTTP/2 as requisições ocorrem por meio de conexões criptografadas, aumentando a segurança do usuário e da aplicação.

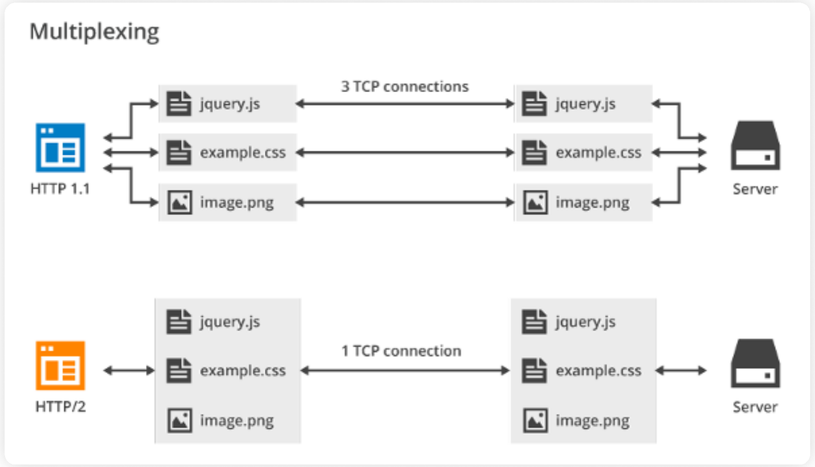
HTTP/1.1

- Textual
- Sequencial



HTTP/2

- Binário
- Multiplexação
- SSL/TLS
- HTTPS



Entendendo os cabeçalhos e respostas

Cabeçalhos

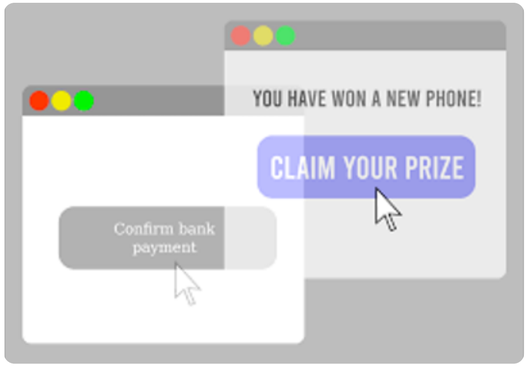
Response Headers

Utilizando os cabeçalhos de forma correta, você pode sinalizar para o navegador do seu cliente como ele deve se comportar, e isso pode protege-los de algumas das práticas mais comum utilizada hoje por invasores

Prevent XFS

- Evite que sua aplicação possa ser usada dentro de um Iframe.

  X-Frame-Options: SAMEORIGIN



Prevent CSRF

- Habilite o envio de cookies em requests de origem diferente do seu domínio, e liste somente os domínios confiavéis.

  Access-Control-Allow-Origin=http://mobile.yoursite.com

  Access-Control-Allow-Credentials=true

Response Headers

Utilizando os cabeçalhos de forma correta, você pode sinalizar para o navegador do seu cliente como ele deve se comportar, e isso pode protege-los de algumas das práticas mais comum utilizada hoje por invasores

Prevent Man-in-the-middle

- Sinalize que sua aplicação só deve ser acessada através do HTTPS (443)

  Strict-Transport-Security: max-age=31536000 ; includeSubDomains

Prevent XSS

- Crie uma "white-list" de todas origens de onde sua aplicação pode coletar os recursos

  Content-Security-Policy: default-src 'none';

Prevent MIME Sniffing

- Sinalize que o MIME type do seu projeto não pode ser alterado

  X-Content-Type-Options: nosniff

Obrigado!

Dúvidas?

Johnny Trentin
Frontend Engineer

Bruno Cabral
Frontend Engineer